AVAR 2023

SECURE ECOSYSTEM: STRATEGIC, PRAGMATIC, FUTURISTIC

28th - 30th NOV 2023

GRAND HYATT DUBAI

26th ANNUAL CYBERSECURITY CONFERENCE

PARTNERS

SILVER SPONSORS

AV comparatives

cisco | TALOS

CYBER THREAT ALLIANCE

NETWORKING KIT SPONSOR

K7 SECURITY

INTERNET SPONSOR

ReasonLabs

T-SHIRT SPONSOR

SE Labs
INTELLIGENCE-LED TESTING

ASSOCIATE SPONSORS

aramco

kaspersky

NAME BADGE SPONSOR

ThreatBook

SUPPORTING SPONSORS

AppEsteem®

CSA
CLEAN SOFTWARE ALLIANCE

eset Digital Security
Progress. Protected.

赛可达实验室
skd labs

MEDIA PARTNERS

ACNNEWSWIRE

CIO TECH OUTLOOK

CYBER DEFENSE MAGAZINE

INTERNATIONAL BUSINESS MAGAZINE

SECURITY MIDDLE EAST
THE MAGAZINE FOR SECURITY

WORLD BUSINESS OUTLOOK

mid east information

CONTENTS

CONTENTS

CEO MESSAGE

I warmly welcome the international cyber security community to AVAR 2023! This conference is the 26th edition of AVAR's annual conferences and has been designed based on what we have learned from organizing these conferences for a quarter of a century. The latest cyber threats, the gravest cyber security challenges, and the most advanced counter measures will be discussed at AVAR 2023. The topics may vary from year to year but the quality of expertise, hospitality, and depth of relationships that are the hallmarks of AVAR's events will remain the same.

AVAR 2023 is the first AVAR conference to be hosted in the Middle East. The United Arab Emirates is not only a significant hub of economic activity but is also at the forefront of the region's digital transformation, which have made the nation an attractive target for threat actors with 71 million cyber attacks blocked this year. With an expected Information and Communications Technology (ICT) expenditure of $23 billion in 2024 and a cyber security market of AED 1.8 billion, the UAE has emerged as a focal point for the cyber security industry in the region.

AVAR has chosen 'Secure Ecosystem: Strategic, Pragmatic, Futuristic' as the theme for this year's conference. This theme reflects the importance of viewing cyber security as an ecosystem with strategic focus areas, the need for pragmatic solutions, and the emphasis that must be placed on anticipating the evolution of both technology and cyber threats.

AVAR's conferences are known for extensive knowledge sharing from experts. AVAR 2023 includes 42 presentations and panel discussions with 60 speakers from 38 organizations and 23 countries. In addition to the knowledge sessions, we will again be honoring regional cyber security leaders by presenting awards to CISOs who have achieved significant cyber security transformation in their organizations.

Cyber security will never stand still. Every step forward in technology brings new challenges for cyber defenders, as we are now witnessing with the rise of generative AI. The only way for us to ensure the safety of the digital world is to share what we know and to seek out those who have expertise that we lack. AVAR 2023 enables both, and its success entirely depends on the enthusiastic participation of all cyber security stakeholders. I thank all the speakers, partners, sponsors, and delegates who participate in the event. When we work together, the whole world sleeps peacefully and that is something to be celebrated.

I again welcome you to AVAR 2023, and thank you for your contributions to cyber security.

Kesavardhanan J
CEO of AVAR

BEERS WITH TALOS

Podcast

THREATS, BEERS & NO SILVER BULLETS

Join Lurene, Matt, and Mitch from Talos
(and their guests) to talk about emerging threats,
hacking all the things, and vital security topics.

Caution: *You can accidentally learn things while enjoying this podcast.*

Listen at **cs.co/bwt**

AGENDA

DAY 1 Tuesday, 28th November, 2023

Time	Activity
16:30 – 18:00	Registration
19:00 Onwards	Welcome drinks reception and dinner

DAY 2 Wednesday, 29th November, 2023

Time	Track 1
9:00 – 9:30	Registration
9:30 - 10:40	Conference opening Welcome Address: Kesavardhanan J, CEO, ***AVAR*** Special Address: His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security, ***United Arab Emirates Government*** Keynote Address: Lt. Colonel. Dr. Hamad Khalifa Al Nuaimi, Head of Telecommunication, ***Abu Dhabi Police***
10:40 – 11:00	Refreshment Break

Time	Track 1	Time	Track 2
11:00 – 11:30	**Zero-day exploits of ransomware operators (Windows OS)** Boris Larin ***Kaspersky***	11:00 – 11:30	**Abusing Electron-based applications in targeted attacks** Jaromir Horejsi ***Trend Micro***
11:30 – 12:00	**Don't flatten yourself: restoring malware with Control-Flow Flattening obfuscation** Geri Revay ***Fortinet***	11:30 – 12:00	**The Good, the Bad and the Ugly of Advanced EDR Bypass Tool Frameworks** Andrew Shelton L ***K7 Computing***
12:00 – 12:30	**Multi-hopping in reversed SOCKS – the usage of open source proxies by Chinese threat actors** Vanja Svajcer ***Cisco Talos***	12:00 – 12:30	**Turn the tables: How we use GPT to detect phishing websites** Eduard Alles, Marius Benthin ***G DATA***

DAY 2 Wednesday, 29th November, 2023

Time	Track 1	Time	Track 2
12:30 – 12:50	**Machine learning or behaviour heuristics? The synergy of approaches to defeat advanced ransomware threats** Vladimir Strogov, ***Acronis*** Sergey Ulasen, ***Constructor Technology***	12:30 – 12:50	**APT-C-60 : Observing the hunter** Romain Dumont, ***ESET***
12:50 – 14:00	Lunch Break		
14:00 – 14:30	**Unmasking the Dark Art of Vectored Exception Handling_ Bypassing XDR and EDR in the Evolving Cyber Threat Landscape** Donato Onofri, Sarang Popat Sonawane, ***CrowdStrike***	14:00 – 14:40	**Panel discussion – Positioning cyber security as a contributor to stakeholder value** Aloysius Cheang, ***Huawei*** Anil Pais, ***Al Danube*** Illyas Kooliyankal, ***CyberShelter*** Javed Alam, ***DAMAC Properties*** Dr. Mohammad Khaled Smith Gonsalves, ***CyberSmithSECURE***
14:30 – 15:00	**Reversing Nim binaries** Holger Unterbrink ***Cisco Talos***	14:40 – 15:00	**Evolution of the crypto-mining botnet targeting Russian users for years** Ivan Korolev, Igor Zdobnov ***Doctor Web***
15:00 – 15:30	**CloudWizard: an APT hiding in the dark for 7 years** Georgy Kucherin, Leonid Bezvershenko ***Kaspersky***	15:00 – 15:30	**IoT Malware Riding Pegasus – How to Hunt and Analyze GobRAT** Yuma Masubuchi ***JPCERT***
15:30 – 15:50	Refreshment Break		
15:50 – 16:20	**Panel discussion – Mitigating cyber risk from geopolitical tensions** Anoop Kumar, ***GN Media – Gulfnews*** David Brown, ***CyberGate*** Dr. Hamad Khalifa Al Nuami, ***Abu Dhabi Police General Head Quarter*** Dr. Hossam Elshenraki, ***Dubai Police Academy*** Waqas Haider, ***HBL Microfinance Bank LTD*** Holger Unterbrink, ***Cisco Talos*** Michael Daniel, ***CTA***	15:50 – 16:20	**Linux Hypervisor-level behavior analysis** Alexey Kolesnikov ***Positive Technologies***
		16:20 – 16:50	**Is Lazarus Preparing for War?** JunSeok Kim, MyeongSu Lee, MyungUk Han, TaeHyeon Song, ***AhnLab***
16:20 – 16:50	**The Art of Cyber Espionage: Unleashing the Power of SCADA and ICS Hacking** Muhammad Shahmeer ***Younite***	16:50 – 17:10	**Plenty of Smish in the Sea – Time to Cast the PhishNet** Dr. Khalid Alnajjar, ***F-Secure***

DAY 2 Wednesday, 29th November, 2023

19:00 – 19:30	Pre-dinner Drinks
19:30 – 22:00	Gala Dinner

DAY 3 Thursday, 30th November, 2023

Time	Activity
10:00 – 10:20	Keynote Address: Ravi Baldev, CTO Cyber Resilience, ***Dell Technologies EMEA***

Time	Track 1	Time	Track 2
10:20 – 10:50	**UEFI Secure Boot Bypasses and The Dawn of Bootkits** Martin Smolár ***ESET***	10:20 – 10:50	**Amplifying Threat Intelligence via Generative AI-Driven Aggregation and Enrichment** Dr. Jason Zhang, Kyle Campbell ***Anomali***
10:50 – 11:20	**Understanding ransomware rebranding** Dr. Vlad Constantin Craciun **Bitdefender**	10:50 – 11:20	**MEGALO-(AN)-DON: Uncovering data espionage, blackmailing and shell companies in mobile lending apps targeting Asia** Jagadeesh Chandraiah **Sophos**
11:20 – 11:40	**GoldenJackal Chronicles: Delving into Enigmas and Unanswered Questions** Giampaolo Dedola ***Kaspersky***	11:20 – 11:40	**Rebrand to X?: SteelClover Cornucopia** Rintaro Koike, Shogo Hayashi ***NTT Security Holdings***
11:40 – 12:00	Refreshment Break		
12:00 – 12:30	**SmoothOperator – 3CX Supply Chain Attack** Dinesh Devadoss, Niranjan Jayanand ***SentinelOne***	12:00 – 12:30	**Panel discussion – Improving data security in the digital-first enterprise** Anton Shipulin, ***Nozomi Networks*** Bassil Mohammed, ***PwC Middle East*** Kiran Kumar, ***Help AG*** Kumar Prasoon, ***Y100.ai*** Siham Benhamidouche, ***Schneider Electric*** Simon Edwards, ***SE Labs***
12:30 – 12:50	**Next Generation Firewall Deployment for Predictive Analysis of Network Anomalies Using Artificial Intelligence (Sponsor Presentation)** Almuhaisen, Salman N ***Saudi Aramco***	12:30 – 12:50	**Very Real Assault on Virtual ESXi: The Evolving Linux Ransomware Threat** Vigneshwaran P ***K7 Computing***

DAY 3 Thursday, 30th November, 2023

Time	Track 1	Time	Track 2
12:50 – 13:10	**Adaptive File Analyzer: NLP combined with Heuristic analysis to detect malicious email attachments** Kalpesh Mantri, Abhishek Singh ***Cisco Talos***	12:50 – 13:10	**ValleyFall Spyware – Tales of malware discovery and hunting in the wild** Marian Gusatu ***Gen Digital***
13:10 – 14:20	Lunch Break		
14:20 – 14:50	**Space Pirates: hack, steal, repeat!** Denis Kuvshinov, Stanislav Rakovsky ***Positive Technologies***	14:20 – 14:50	**An Efficient Approach for Automating Threat Intelligence Analysis through Similarity Detection** Hyunjong Lee, ***SANDS Lab*** Chang-Gyun Kim, ***KSign***
14:50 – 15:20	**Unveiling the DarkGate Malware: A Comprehensive Analysis of Its APT Group, Development Timeline, and Capabilities** Aravind Raj, Nihar Deshpande ***Quick Heal***	14:50 – 15:10	**Once Gifted is always Gifted** Chetan Raghuprasad ***Cisco Talos***
15:20 – 15:40	**Cybercrime Atlas: Using Maps to Create a More Secure Ecosystem (Sponsor Presentation)** Michael Daniel ***CTA***	15:10 – 15:40	**Let's Chat about Gross Public Text generation** Righard Zwienenberg, ***ESET*** Eddy Willems, ***G DATA***
15:40 – 16:00	Refreshment Break		
16:00 – 16:40	**Panel discussion: Efficacy of Realworld Testing for EDR and XDR Solutions** Dr. Jason Zhang, ***Anomali*** Michael Daniel, ***CTA*** Simon Edwards, ***SE Labs*** Righard Zwienenberg, ***ESET*** Samir Mody, ***K7 Computing***	16:00 – 16:20	**Unraveling the MOVEit Vulnerability: A Journey from Exploitation to Clop Ransomware Infestation** Prashant Tilekar, ***Forescout Technologies***
16:40 – 17:00	**Lazarus and Bluenoroff: New and "Rusty" Tricks for macOS** Mellvin S ***K7 Computing***	16:20 – 16:40	**This Picasso is a con artist – an update on the latest Ghostwriter activities (Sponsor Presentation)** Vanja Svajcer, ***Cisco Talos***
		16:40 – 17:00	**Rising to Prominence: A Deep Dive into TargetCompany's Evolutionary Path with Mallox** Earle Maui Earnshaw, Nathaniel Morales ***Trend Micro***
17:00 – 17:10	Closing ceremony		
17:00 – 17:55	AGM and Members' Meeting		

WE ARE CTA

WE ARE STRONGER TOGETHER

CTA's mission is to improve the overall cybersecurity of the global digital ecosystem. We seek to:

PROTECT END-USERS

DISRUPT MALICIOUS ACTORS

ELEVATE OVERALL SECURITY

https://www.cyberthreatalliance.org

CYBER THREAT ALLIANCE

AVAR 2023

SPEAKERS/AUTHORS AND ABSTRACTS

ZERO-DAY EXPLOITS OF RANSOMWARE OPERATORS (WINDOWS OS)

Abstract:

In February 2023, I discovered a number of attempts to execute a 0-day elevation of privilege exploit on Microsoft Windows servers owned by various companies around the world. This exploit used a previously unknown vulnerability in the Common Log File System (CLFS) driver and supported the latest versions/builds of Windows OS (including Windows 11). The vulnerability was assigned CVE-2023-28252 and fixed after my prompt report to Microsoft. Further analysis showed that this exploit was used by a sophisticated group of cybercriminals who are conducting ransomware attacks and have used at least five different Common Log File System (CLFS) vulnerabilities since June 2022. Some of them were confirmed to be 0-days.

In this presentation, I will share an in-depth analysis of:

- The internals of the Common Log File System (CLFS) driver and the main reasons why it is being exploited that often lately
- The root cause of the five vulnerabilities used by attackers and their exploitation
- Techniques used by attackers and new exploit mitigations from Microsoft

I will also share the tactics, techniques, and procedures (TTPs) of the attackers and how the usage of these and similar exploits can be detected.

Boris Larin
Kaspersky

Bio:

Boris Larin, Principal Security Researcher, Kaspersky,
Twitter: @oct0xor

Boris is a Principal Security Researcher in the Global Research & Analysis Team (GReAT) at Kaspersky. In his current role, Boris is responsible for finding zero-days exploited in the wild. He has discovered a number of large APT attacks and reported 15 zero-day exploits used in the wild in different malware campaigns. Besides work, Boris is very passionate about reverse engineering, vulnerability research and video games. Previously, Boris was the first researcher recognized in Sony PlayStation's bug bounty program on HackerOne after discovering critical vulnerabilities in the firmware of PlayStation 3 & 4. He also makes "impossible" modifications for video games - he reverse engineered and rewrote Metal Gear Solid 2 to add a full-fledged third-person camera to the game. He has presented his research at many conferences such as: CanSecWest, Security Analyst Summit (SAS), BlueHat, TyphoonCon, CodeBlue, Chaos Communication Congress, OffensiveCon, etc.

ABUSING ELECTRON-BASED APPLICATIONS IN TARGETED ATTACKS

Abstract:

Electron is a popular framework for creating pseudo-native applications with web technologies like JavaScript, HTML, and CSS. By packaging the application source codes with a particular version of Chromium (front-end part) and Node.js (back-end part), Electron allows to have just one codebase which can be run on different platforms (Windows, MacOS, and Linux).

This versatility and popularity brought attention of threat actors, as we observed several attacks against Electron-based applications, particularly supply chain ones.

In this presentation, we will look at the Electron framework (what it really is from developer's, end-user's, and defender's point of view) and discuss possible infection vectors – exploiting Chromium vulnerabilities, or trojanizing the Electron applications by replacing/patching the app.asar archive (containing application sources) to embed malicious code.

Then we will follow with analyses of several real-life cases, which we recently researched, and which involved Electron-based applications.

These include

a) a secure chat application (MiMi chat) trojanized by Iron Tiger threat actor, targeting Windows, Linux and MacOS secure chat users. Trojanized chat application becomes downloader of additional native backdoors (HyperBro for Windows, rshell for Linux and MacOS).

b) chat-based customer engagement platforms (Comm100 & LiveHelp100) trojanized by a currently unclassified threat actor. Trojanized applications download multi-stage JavaScript payload, which later downloads native multi-stage backdoor & stealer.

c) a live chat application (MeiQia) vulnerable to CVE-2021-21220, then trojanized and exploited by threat actor Water Labbu. Trojanized live chat application becomes downloader of additional malware (custom batch scripts, Cobalt Strike, or system monitoring tool).

We will analyze not only the trojanized JavaScripts, but we will also briefly discuss the interesting native malwares too (custom backdoors, stealers, ...).

At the end, we will talk about targets of these campaigns, as well as the connections to previous campaigns operated by the mentioned threat actors.

Jaromir Horejsi
Trend Micro

Bio:

Jaromir Horejsi is a Senior Threat Researcher for Trend Micro Research. He specializes in tracking and reverse-engineering threats such as APTs, DDoS botnets, banking Trojans, click fraud, and ransomware that target both Windows and Linux. His work has been presented at RSAC, SAS, Virus Bulletin, HITB, FIRST, AVAR, Botconf, and CARO.

DON'T FLATTEN YOURSELF: RESTORING MALWARE WITH CONTROL-FLOW FLATTENING OBFUSCATION

Abstract:

Control-Flow Flattening (CFF) is an obfuscation/anti-analysis technique used by malware authors. Its goal is to alter the control flow of a function to hinder reverse engineering. Using CFF makes static analysis complex and increases the time investment for the analyst significantly. Malware authors have already discovered this, and a steady increase can be seen in malware samples that use CFF. Soon every analyst will have to face it daily, which calls for know-how and tooling to help them.

This presentation intends to provide the needed know-how and tooling. First, we will discuss the general approach to fighting CFF. We will discuss identifying CFF and which components are essential to restore the control flow.

We will compare three different approaches to fight CFF: basic pattern matching, emulation, and symbolic execution. Their implementation will be demonstrated as IDAPython scripts.

Geri Revay
Fortinet

Bio:

Geri has more than 13 years of experience in cybersecurity. He started on this path as he specialized in network and information security in his M.Sc. in computer engineering. Since then, he has worked as a QA engineer for a security vendor, then changed to penetration testing first as an external consultant and then as an internal consultant at Siemens. He is a hacker at heart and a consultant by trade. He worked on both IT and OT systems. In the past years, he focused on security research in binary analyses and reverse engineering, which led him to Fortinet. At FortiGuard Labs, he currently does malware analysis and reverse engineering related research.

THE GOOD, THE BAD AND THE UGLY OF ADVANCED EDR BYPASS TOOL FRAMEWORKS

Abstract:

The rapid evolution in the ability of malware to circumvent advanced defence capabilities can partly be attributed to the extensive availability of openly-shared EDR-bypass techniques and PoCs, and red teaming tool frameworks. Threat actors conveniently employ these bleeding-edge approaches and tools as part of their TTPs at different stages of the attack chain to deliver their payloads either directly or as stagers to make it more subtle, thereby gaining remote, prolonged, undetected access to various parts of the target environment. It is far from trivial for our EDR solutions to keep pace with all these new-fangled delivery mechanisms and nefarious activities, but we can only attempt to do so if we are keenly aware of these capabilities via diligent, hands-on research.

Let us begin with the abuse of Bruteratel, an advanced red team and adversary simulation software and post-exploitation tool which has vast capabilities such as a built-in debugger to detect EDR hooks, support for exfiltration over multiple protocols, patching against AMSI, and Module Stomping. Bruteratel consists of a server component that is dubbed as the tool's interface, and a client component known as "badger" which is the final payload for backdoor access.

Next, we have the infamous CobaltStrike that has been exploited by threat actors for years. This tool boasts extensive capabilities, including features like Indirect syscalls, sleep obfuscation, and spoofing call stacks with timers.

Finally, another red teaming tool gaining popularity is Silver C2, which offers features like Compile-time obfuscation and In-memory .NET assembly execution.

While all these post-exploitation tools share some common functionalities, they are implemented uniquely.

In this presentation we will reveal the panoply of EDR-bypass techniques implemented in the above-mentioned post-exploitation tools based on our analysis of available versions. We will also rely on our investigations into real-world scenarios in which we have observed groups such as APT 29 utilise DLL sideloading techniques to inject post-exploitation payloads into Lolbins. Additionally, we'll discuss the utilisation of Bumblebee, a loader known for deploying Silver C2 in compromised victim machines. We will also highlight how many ransomware groups have employed similar post-exploitation frameworks to ensure discreet access to compromised systems. Last, but not least, we will divulge which of the 3 tool frameworks is the Good, which the Bad, and which the downright Ugly.

Andrew Shelton L
K7 Computing

Bio:

Andrew Shelton Lotus Edison completed his Bachelor's degree in Computer Science Engineering from Anna University, Chennai. In 2021, he began his professional journey as a Threat Researcher at K7 Computing's Threat Control Lab. His primary job responsibilities involve reversing and writing detections for various malware, handling enterprise escalations as well as keeping up with the latest trends. Andrew is passionate about programming, malware analysis and reverse engineering, and his research findings are published on the K7 Threat Control Lab's technical blog page. During his leisure time, he enjoys playing combat flight simulation games and traveling with his friends.

MULTI-HOPPING IN REVERSED SOCKS – THE USAGE OF OPEN SOURCE PROXIES BY CHINESE THREAT ACTORS

Abstract:

Our organization has recently discovered a targeted espionage campaign that has likely persisted since at least March of 2021. The activity specifically targets a Saudi non-profit organization and evades detection by injecting custom malicious backdoors, named 'zar32.dll' and 'zor32.dll' into the process 'rundll32.exe' for maintaining persistence. Although some observed TTPs were similar to the TTPs previously discovered by Symantec and attributed to a new threat actor Lancefly, we decided to attribute the discovered activities to a new actor we named Zazor, based on the specific file names used for their implants.

Although the initial access vector was unknown, we observed Zazor establishing command and control (C2) infrastructure using various customized reverse proxy tools such as Fast Reverse Proxy (frp), sSocks and Venom as well as the set of custom implants. The usage of open source reverse proxies by Chinese actors has been noted previously in research by Ahnlab, Symantec and Cisco Talos. We specifically mentioned the usage of Fast Reverse Proxy together while documenting the discovery of the Alchimist post-exploitation framework in October 2022.

This presentation will introduce the attendees into the world of proxy tools commonly used by Chinese threat actors. We will document their history, their basic and more advanced functionality as well as their significance for threat actors. We will discuss in depth the most notable recent campaigns with the emphasis on comparing the tools and techniques exhibited in the attacks. Here, the focus will be on Zazor, as it is a previously unknown threat actor using a specific set of implants. We will discuss the functionality of the newly discovered implants in detail as well as the infection chain we discovered. We will compare Zazor's TTPs with the activities of Dalbit, Lancefly and other actors commonly using open source proxy tools.

The attendees should leave the session armed with the knowledge that will help them to recognize malicious usage of reverse proxies as well as the known Chinese threat actors employing them.

Vanja Svajcer
Cisco Talos

Bio:

Vanja Svajcer works as a Technical Leader at Cisco Talos. He is a security researcher with more than 20 years of experience in malware research, cyber threat intelligence and detection development.

Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks all the time spent hunting in telemetry data to find new attacks is well worth the effort. He presented his work at conferences such as Virus Bulletin, RSA, CARO, AVAR, BalCCon and others.

TURN THE TABLES: HOW WE USE GPT TO DETECT PHISHING WEBSITES

Abstract:

During the last year, discussions have been ongoing about the threat that large language models like the recently published GPT from OpenAI pose with regards to cyber security. Attackers could use "AI" to create malware or new attack vectors like social engineering with greater proficiency. As such, the cyber security community at large expects a rise of Phishing attacks that would benefit from such services. Phishing websites are easy to create and thus a vast amount come online on a daily basis. This prompts for an acceleration of the analysis and classification process for potential phishing sites. In our research we try to turn the tables with regards to using machine learning and large language models to detect and successfully block phishing sites.

Large language models are suitable to identify common structures within text-based datasets. Since the concept of phishing sites stayed the same over the recent years a pre-trained model could be of long-term use without the necessity of re-training. We show that large language models can also learn the variations of phishing sites without the need to visually classify the sites, as well known applications in the past have done. This helps with identifying phishing sites even when the attackers change their modus operandi or target market, shifting from i.e. specific local banking sites to grabbing online service tokens.

We utilized OpenAI's API to finetune several models based on GPT-3. The evaluation of our classification system shows an F1 Score of 0.92 with a phishing certainty threshold of 90%. In particular, the system is able to identify phishing with a high precision. The classification is modular and based on nine methods to extract relevant features from DOMs. After an initial evaluation of these DOM features we combined them into a robust ensemble classifier to efficiently distinguish phishing from clean sites. We based this on 4020 training and 1980 testing URLs gathered from internal sources which were labelled manually before. The cost saving in this approach is remarkable, we spend less than 20$ to train all our models and each classification costs on average 0.001$. In our research we show that this approach can be scaled easily to track a large number of sites and classify them in a short time.

For testing purposes we conducted a real world case-study with 1900 real world URLs from a phishing feed. Thereby we could evaluate the quality of this feed for our production systems. This shows how our system can be useful in relation to real world automation opportunities that reduce time and cost for human analysts and enable systems with mass analysis capabilities of phishing URLs.

In this paper we present our procedure to work with the OpenAI API, describe common limitations when working with data from phishing sites, compare our different representation methods and finally evaluate our results. We also show that using LLMs is an effective way to combat cyber criminals around the world while saving costs on manual analysis and classification.

TURN THE TABLES: HOW WE USE GPT TO DETECT PHISHING WEBSITES

Eduard Alles
G DATA

Bio:

Eduard Alles studied in Bochum at the Ruhr-University. He wrote his masters thesis about "Automatic Decryption After a Ransomware Attack by an AV-Solution" and work since 2022 as a Virus Analyst at G DATA CyberDefense AG. During his work he focuses mainly on Threat Hunting and detection of browser-based attacks.

Marius Benthin
G DATA

Bio:

Since November 2022 Marius Benthin is working as a Junior Virus Analyst at G DATA CyberDefense AG. He finished his master studies in IT Security at the Ruhr University Bochum with his master thesis about malware attribution to APT actors. In March 2020 he completed his dual studies at the University of Applied Sciences Darmstadt in cooperation with G DATA.

MACHINE LEARNING OR BEHAVIOUR HEURISTICS? THE SYNERGY OF APPROACHES TO DEFEAT ADVANCED RANSOMWARE THREATS

Abstract:

The paper focuses on a successful and fruitful combination of the ML-based approach and the heuristics-based approach in the case of Advanced Ransomware Defense, where the advanced ransomware is the ransomware that maliciously exploits the trusted context of execution, so it is the case of ransomware injection into well-known trusted processes, system services, that are used for the disguise of the malicious encryption.

The Machine Learning is used for malicious or benign classification of call stacks that match injections into trusted processes. The heuristics-based technique is based in our case on just one of the examples of injections, using such API as CreateRemoteThread[1] and WriteProcessMemory[2]. This approach is applied with good results to the case of Ruyk ransomware[3], one of the deadliest malware weapons.

We show how the Machine Learning helps to find those call stacks which with high probability match malicious injections. Then we augment the results of the ML classifier with the special detection of threads, created in the trusted process, using other sensors, including kernel drivers. This combination provides the maximum accuracy and the ability to remediate the attack.

The paper also presents the architectural materials as well as the links and references to the hands-on demonstration of collecting suspicious stacks. We also show how to use ML decisions and pair these decisions with the thread creation events as the sensor examples. The links with demonstrations use the execution of the real-world Ryuk malware strain (other malwares can be considered for the presentation). The analysis of the events flow is also shown in the kernel debugger coupled with the case analysis with the help of other tools like Process monitor.

MACHINE LEARNING OR BEHAVIOUR HEURISTICS? THE SYNERGY OF APPROACHES TO DEFEAT ADVANCED RANSOMWARE THREATS

Vladimir Strogov
Acronis

Bio:

Vladimir Strogov has 30+ years of experience in kernel level development in both storage and security areas (file systems, virtualization, data protection, reverse engineering, anti-malware solutions). He has worked on multiple Veritas and Symantec projects for nearly a decade. Additionally, he has worked at Kaspersky Lab in Core Drivers Group in roles of technical expert and team leads. Strogov is currently the Director of Development, Kernel Team at Acronis, having joined the team in 2016.

Sergey Ulasen
Constructor Technology

Bio:

Sergey Ulasen, PhD is Senior Director of AI Development at Constructor Technology, leading AI/ML/NLP research and development areas. He is the developer of the "Eugene Goostman" bot, the first ever bot to pass the Turing test. Ulasen is an expert in artificial intelligence computer systems with emphasis in natural language processing, speech recognition, image processing, and complex system modelling and research. He has 20+ years of experience in developing robust, scalable, and configurable commercial software for scientific and business applications. Ulasen developed the award-winning Natural Language Processing software.

APT-C-60: OBSERVING THE HUNTER

Abstract:

APT-C-60, also known as 伪猎者 (translation: False hunter) or APT-Q-12, is an East Asian cyberespionage group active since at least 2018, and initially reported by Qihoo 360 in 2021. It mainly focuses on high-profile targets such as governments, trade industries, and think tanks in Asian countries such as China and South Korea. We've been monitoring APT-C-60 for over a year and the group keeps adapting its toolset to deliver its fully featured backdoor, which we have dubbed SpyGlace.

In this presentation, we describe how the various components of their attack chain evolved and the combination of techniques used to stay under the radar while achieving code execution and persistence on compromised systems. We detail the various features of the SpyGlace backdoor and, more importantly, present undocumented modules such as a keylogger and a credential stealer. During our investigation we noticed a handful of metadata the operators left behind, which allowed us to obtain further information on the operators' profile and their modus operandi. We also show how we decrypted logs found on their C&C server, unveiling useful details on their environment.

Finally, we demonstrate how forensic analysis with file carving on VHD (Virtual Hard Disk) files helped us recover deleted files and gain yet further insights into the threat actor's testing processes. The presentation builds on that collection of artifacts to create strong links between APT-C-60 and the group's evolving malicious components.

Romain Dumont
ESET

Bio:

Romain DUMONT is a malware researcher working for ESET. His work involves malware analysis and threat hunting.

He likes a good reversing engineering challenge and has previously worked on vulnerability assessment with a focus on Windows components.

UNMASKING THE DARK ART OF VECTORED EXCEPTION HANDLING: BYPASSING XDR AND EDR IN THE EVOLVING CYBER THREAT LANDSCAPE

Abstract:

Cyber attackers and malware authors constantly adapt their tactics to bypass XDR (Extended Detection and Response) and EDR (Endpoint Detection and Response) solutions, aiming to achieve their malicious objectives. This dynamic landscape of cyber threats extends beyond commodity malware and ransomware, with targeted attacks focusing on specific individuals, organizations, or industries.

This discussion centers on techniques that exploit "Vectored Exception Handling" mechanisms, which have become prevalent among malicious actors and Red teaming and Post Exploitation tools. These techniques allow forceful jumps to inject malicious code, discreetly bypass security products functions, like circumventing hooks and Windows' AMSI security feature.

By selectively evading EDR monitoring capabilities, this approach not only evades traditional security measures but also poses challenges for cybersecurity researcher and professionals conducting in-depth analysis. When exceptions occur in a program, they are typically handled by catch blocks, managed internally by the Structured Exception Handler (SEH). Starting with Windows XP, Microsoft introduced Vectored Exception Handlers (VEH): an unframed exception handler mechanism enabling developers to override SEH at a higher level in their code. Due to the priority in exception handling, researchers and malicious actors have found ways to exploit VEH to alter command flow, bypass monitoring, and execute malicious code.

In this presentation, we will explore Exception Handling internals and the functions executed to handle User Space Exceptions. We will also delve into Vectored Exception Handling Abuse and its effectiveness in bypassing EDR. We will Demo a bypass for AMSI mechanism, by crafting multiple VEH, in a technique we call VEH2. Additionally, we will discuss other potential uses of VEH code and provide insights into the detection of this bypass technique.

UNMASKING THE DARK ART OF VECTORED EXCEPTION HANDLING: BYPASSING XDR AND EDR IN THE EVOLVING CYBER THREAT LANDSCAPE

Donato Onofri
CrowdStrike

Bio:

Donato Onofri is a seasoned Red Team Engineer. With over a decade of experience, his activities include Reverse Engineering, Red Team, Threat Research and Penetration Testing.

Passionate about both the Offensive and Defensive sides of Cyber Security, Donato has worked with industry leaders like CrowdStrike and Hewlett-Packard Enterprise and as an advisor and engineer for Governments and Financial institutions. His research delves into state-of-the-art security techniques, malware analysis, and internals. Holder of GREM, GXPN, OSCP, OSCE, and OSWE certifications, his expertise is underscored by multiple recognitions for vulnerability discovery.

He is also the co-author of the book **"Attacking and Exploiting Modern Web Applications"**.

Sarang Popat Sonawane
CrowdStrike

Bio:

Sarang Sonawane currently holds the role of Security Researcher within CrowdStrike's Malware Research Team, he boasts an 7+ years of experience with a primary focus on reverse engineering. His significant contributions to the field can be observed through his few published blogs, available on CrowdStrike's official website, where he shares insights and findings related to emerging malware threats. In recognition of his expertise, he has also presented poster at the AVAR 2022 Conference held in Singapore. Beyond his dedication to cybersecurity, he thrives on intellectual challenges and is an accomplished participant in Capture The Flag (CTF) competitions, including his successful completion of the Flare-On 9 challenge in the previous year. Outside of his malware analysis pursuits, Sarang passionately engages in cricket matches and eagerly ventures out on explorations to uncover new destinations.

REVERSING NIM BINARIES

Abstract:

For a reverse engineer one of the first steps is to differentiate between library code and code the author wrote. This can be especially hard depending on how the compiler has optimized the code or which programming language was used. This research's objective is to make life easier for analysts and reverser engineers while analysing Nim based binaries. We started this research a while ago, because we saw more and more interest in Nim in the offensive security community and more malware authors using Nim executables to make the life of an reverse engineer harder.

The evolution of programming languages has created more portable languages that can be compiled for different platforms with little or no changes, without the recourse to virtual machines. This comes at the cost of a lot of boilerplate code which is added by the compiler or the Intermediate code translator. These languages often have their own definition of strings, calling convention and in some cases the intermediate code translator can implement different optimizations which in the end results in very complex executables.

The NIM compiler has several optimization options, it can be optimized for speed or size for example, which will result in dramatically different binaries. This presentation starts to demonstrate these differences and their impact on the final binary. Then it moves to show how an analyst can identify the non-library code, so that she can focus her efforts on analysing the logic of the executable, instead of getting lost in library code. To help out in this task we will present IDAPro scripts that will do part of the binary analysis and identify imported library or boilerplate code and create well known structures for language specific objects like strings. We will demonstrate how to write a COFF parser to automatically generate IDA FLIRT Signature files from Nims source code files. The latter can easily be applied to other programming languages or certain libraries built with uncommon compiler switches.

Holger Unterbrink
Cisco Talos

Bio:

Holger is a longtime security enthusiast, with more than 25 years of experience in the information security industry. He started his career as a penetration tester and is now working for Cisco Talos as technical leader in the malware and threat hunting sector. He finds new, cutting-edge security threats and analyzes their components. Holger is a frequent speaker at international security conferences such as BlackHat, Recon, HackInTheBox, Internet Security Conference, NorthSec, CiscoLive and others. He is also the author of several offensive and defensive security tools and won the IDA plugin contest with his Dynamic Data Resolver (DDR) IDA plugin in 2020.

EVOLUTION OF THE CRYPTO-MINING BOTNET TARGETING RUSSIAN USERS FOR YEARS

Abstract:

The boom in the cryptocurrency market naturally attracted the attention of many cybercriminals wanting to get their piece of the pie. To make money, they first created relatively simple trojans. These launched mining tools on infected computers and tried to conceal their presence in the system. Over time, the number of such threats grew, and they evolved. For instance, they began substituting the cryptocurrency wallet addresses copied into a clipboard.

However, far from all crypto-mining trojans, and, therefore, the cybercriminals who used them, were able to make a go of it. One of the most successful such malicious apps is a multi-functional miner, written in the AutoIt scripting language, that targets Russian users. By making constant improvements to the trojan and tinkering with how it was distributed, its author was able to build a botnet made of thousands of infected computers, which ultimately netted him a profit of several million dollars. In our presentation, we will trace the evolution of this botnet and its infrastructure, study its distribution channels, and learn which countermeasures it uses to prevent infections from being treated; we will also take a closer look at its ever-expanding functionality.

Ivan Korolev
Doctor Web

Igor Zdobnov
Doctor Web

Bio:

Ivan Korolev joined Doctor Web in 2014 as a malware analyst and since 2019 has been working as a team leader for botnet research team. He is focused on analyzing targeted attacks, botnets and emerging threats. He likes to find vulnerabilities and participate in bug bounties in spare time.

Bio:

Igor Zdobnov joined Doctor Web in 2002 as a malware analyst and since 2009 has been working as a chief malware analyst. He is leading different security projects inside the company, threat intelligence, threat detection and prevention. He is passionate in malware analysis, reverse engineering and building machine learning malware detection systems.

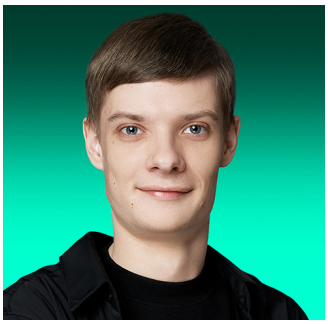
CLOUDWIZARD: AN APT HIDING IN THE DARK FOR 7 YEARS

Abstract:

In this talk, we will present the story of CloudWizard, an APT that has been targeting organizations in the Russo-Ukrainian conflict area. We first unveiled this APT in early 2023, while analyzing a campaign that we dubbed CommonMagic. While the nature of this campaign was highly targeted, it was unclear which threat actor was carrying out the discovered attacks. So, we decided to dig deeper, and our research led us to many interesting findings.

While searching for more clues, we found an even more sophisticated campaign with targets in Central and Western Ukraine. During our investigation, we discovered a previously unknown modular spyware. It has numerous features such as keylogging, screenshot taking and even stealing emails from webmail clients – we identified a total of 13 malicious modules.

Analysis of this sophisticated spyware helped us identify the threat actor behind the discovered campaigns. During our talk, we will tell how we managed to attribute the investigated implants to an APT that was last seen 7 years ago, back in 2016.



Georgy Kucherin
Kaspersky

Bio:

Georgy Kucherin is a junior researcher at Kaspersky's Global Research and Analysis Team and a fourth-year student at Moscow State University. He is passionate about analysis of complex malware and reverse engineering. His previous research includes attribution of the SolarWinds attack, as well as thorough investigations into APTs such as Operation Triangulation, Turla, FinFisher, APT41 and Lazarus.

Leonid Bezvershenko
Kaspersky

Bio:

Leonid joined Kaspersky in 2020 as an intern in the Global Research and Analysis Team (GReAT). In 2021, he was invited to the GReAT as a Junior Security Researcher. In 2023, he was promoted to Security Researcher. In this role, Leonid focuses on open source security, reverse engineering, and malware analysis. His research includes the analysis of APT campaigns, such as Operation Triangulation and CloudWizard. Additionally, he is actively involved in the development of internal tools and infrastructure. Leonid is currently a student at Moscow State University's Faculty of Computational Mathematics and Cybernetics. He is also a member of the Drovosec CTF team.

IOT MALWARE RIDING PEGASUS – HOW TO HUNT AND ANALYZE GOBRAT

Abstract:

GobRAT is a Golang malware targeting routers and other Linux devices discovered in February 2023, and there are samples for various architectures (x86, x86-64, MIPS, ARM). This presentation will describe the details of GobRAT and introduce an analysis tools for the malware, as well as demonstrating the C2 server hunting method.

First, the attack flow using this malware will be described, based on cases in which we have handled. After that, GobRAT's internal structure, mode of execution and custom communication protocols, which are obtained by reverse-engineering the malware, are presented. The malware can control communications of the infected router and perform further attacks into the internal network. Attackers have been continuously developing GobRAT, and now it has become a sophisticated RAT containing 32 commands. In this presentation, the commands added and those updated in the new version will be explained with demonstrations.

Next, a GobRAT hunting method is introduced. Most types of GobRAT cannot be hunted by VirusTotal. However, since this type of malware uses the custom protocol for communication with C2 servers, its C2 servers can be discovered by scanning, and then new versions of GobRAT can be obtained from the download server. In this presentation, a method for hunting GobRAT's C2 servers and a list of C2 servers obtained by the scan will be presented. Finally, a GobRAT string decrypter and a command emulation tool, which the speaker has created to support the analysis of GobRAT, will be presented with a demonstration. After that, the speaker will propose ways to address GobRAT. From this presentation, you will understand how to analyze IoT malware and how to hunt C2 servers to respond to similar malware.

Yuma Masubuchi
JPCERT

Bio:

Yuma Masubuchi has been engaged in malware analysis in JPCERT/CC Incident Response Group since 2020. He has delivered training on malware analysis techniques and also shared technical findings on JPCERT/CC's blog (https://blogs.jpcert.or.jp/en/). He received the M.S. degree in Informatics from Institute of Information and Security in 2021. He has presented at CODE BLUE.

LINUX HYPERVISOR-LEVEL BEHAVIOR ANALYSIS

Abstract:

Behavioral analysis in Linux operating systems is challenging due to a wide variety of distributions, lack of convenient tools, and incompleteness of data that the tools provide. Even well-known tools have their flaws. All this makes it easy for attackers to remain invisible to protection tools, including sandboxes. Attackers use various techniques:

- Make direct system calls that bypass intercepts on user functions.

- Use non-standard techniques to inject themselves into a legitimate process that doesn't trigger alerts.

- Run malicious code in the OS kernel to interfere with the standard user activity monitoring system.

This is just a small sample of practices employed by attackers.

In our report, we will introduce the audience to the DRAKVUF open source solution and its advantages. We will discuss the flaws of the existing Linux security auditing tools and talk about the challenges we encountered when developing a hypervisor-level solution.

Alexey Kolesnikov
Positive Technologies

Bio:

Alexey Kolesnikov, Malware Detection Team, PT ESC (Positive Technologies Expert Security Center)

I analyze and parse malware designed for Windows and Linux, create signature- and behavior-based rules for PT Sandbox and PT EDR, and develop solutions for agentless malware analysis in isolated environments.

THE ART OF CYBER ESPIONAGE: UNLEASHING THE POWER OF SCADA AND ICS HACKING

Abstract:

In today's world, cyber espionage is becoming increasingly prevalent, especially in the critical infrastructure sector. This is why it is essential to understand the art of cyber espionage through the exploitation of Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS). In this presentation, we will take a deep dive into the techniques used by attackers to compromise SCADA and ICS systems, and gain access to sensitive information. The session will be interactive, with live demonstrations showcasing how these systems can be manipulated to cause physical damage, disrupt operations, and steal data. Attendees will learn how to identify vulnerabilities and harden their SCADA and ICS systems to prevent attacks. We will explore attack scenarios and their impact on critical infrastructure. This will enable attendees to develop a comprehensive understanding of the threats that their organizations face and the techniques used by attackers to exploit vulnerabilities. The presentation will be conducted by a seasoned cybersecurity professional with extensive experience in SCADA and ICS hacking. Attendees will learn from real-world examples and leave with practical knowledge that can be immediately applied to their organization's security posture. This presentation will provide a practical understanding of SCADA and ICS hacking techniques and the steps that organizations can take to protect themselves from attacks. The session will begin with an overview of SCADA and ICS systems, their components, and their importance in critical infrastructure.

Muhammad Shahmeer
Younite

Bio:

Shahmeer Amir is a world-renowned Ethical Hacker and the 3rd most accomplished bug hunter who has helped over 400 Fortune companies, including Facebook, Microsoft, Yahoo, and Twitter, resolve critical security issues in their systems. He has founded multiple entrepreneurial ventures in the field of Cyber Security, and currently leads three startups in four countries.

As the CEO of Younite, Shahmeer's premier company is working on next-generation audio-video communication technologies. He is also the CEO of Veiliux, Asia's first mainstream Cyber Security startup present in the Asia Pacific, UAE, and the UK. Authiun, another startup, is a complete passwordless authentication solution for the 21st century.

Shahmeer is the Cyber Security Advisor to the Ministry of Finance Government of Pakistan, involved in multiple projects regarding Deep Sea Tracking, Digital Transformation of Legislation, and Digitization of Pakistani Cultural Content. He is also a member of Forbes Technology Council.

As an Engineer and a Cyber Security professional with relevant certifications from renowned organizations like EC-Council, Mile2, SANS, etc., Shahmeer is currently looking at the Blockchain technology for his doctorate. He has authored three books, including Bug Bounty Hunting Essentials, and a dozen research papers.

Shahmeer is a highly sought-after keynote speaker on Cyber Security, Blockchain, and other technologies, having been invited to over 80 conferences globally. including Blackhat, GiSec, FIC, AEC Alberta, Hackfest and many more. He has also been accepted at multiple prestigious academic institutions in their entrepreneurship programs, including Stanford. As a CTO of companies, Shahmeer has learned to code in 25 languages and read code in 35, making him an expert in multiple technologies.

IS LAZARUS PREPARING FOR WAR?

Abstract:

North Korea has been engaged in constant demonstrations of physical force against South Korea since the division of Korea. And recently, South Korea and North Korea have been engaged in a war without gunfire in cyberspace.

On March 20, 2013, the hacking of Lazarus Group, known to be supported by North Korea, paralyzed the computer network of media and banks in South Korea. Ten years later, in 2023, the National Intelligence Service (NIS) of South Korea publicly revealed that Lazarus Group had hacked into the country's defense and bio industries, exploiting vulnerabilities in well-known security programs.

The Lazarus group is identified to have targeted key industries in South Korea, including chemical, energy, finance, defense, construction, and pharmaceuticals, using vulnerabilities in not only the software disclosed in NIS's recent release, but also in two other programs. According to our internal logs, there have been over 90 attempted attacks in the first half of 2023 alone. Consequently, we have reported the discovery of three 0-day vulnerabilities present in the software utilized by Lazarus group for these attacks to relevant institutions in South Korea as of March this year.

The vulnerable programs that have been exploited are essential security programs that must be installed when using electronic financial services in South Korea. The number of systems with these programs installed is estimated to be greater than the country's population of 50 million. The damage to South Korea is unimaginable if such software is exploited. In January of this year, Wladimir Palant, the developer of AdblockPlus (ad blocking browser extension), even published an article titled "South Korea's online security dead end" criticizing the South Korea's internet banking security.

We've been tracking Lazarus Group's hacking cases since 2021, and we've also done forensic analysis on some cases. This presentation introduces Lazarus Group's latest TTPs (Tactics, Techniques and Procedures), including the process of several Korean companies being compromised by Lazarus Group, software vulnerabilities used at this time, disable security software using BYOVD, and anti-forensics techniques.

The Lazarus group is a highly malicious attack group that operates not only in South Korea but also around the world, it is necessary to jointly respond through information exchange and cooperate among security experts around the world.

JunSeok Kim
AhnLab

Bio:

Junseok Kim works in the malware analysis team in the AhnLab Security Emergency response Center (ASEC), where he specializes in incident response, malware analysis, and cyber threat intelligence. His passion lies in researching advanced persistent threats (APTs) that target South Korea, and he is committed to becoming an expert in this area. Recently, he has become interested in vulnerability analysis.

IS LAZARUS PREPARING FOR WAR?

TaeHyeon Song
AhnLab

Bio:

Taehyeon Song is a member of the analytics team at AhnLab ASEC. He works on incident response and malware analysis, and is particularly interested in analyzing APTs related to South Korea and finding various zero-day vulnerabilities.

MyeongSu Lee
AhnLab

Bio:

Myeongsu Lee started his IT career while working in the military in 1999, and he conducted security-related lectures and security projects such as reverse engineering, exploit development/patch analysis, web hacking, network hacking, digital forensics in 2006. He joined AhnLab in 2011 and has been working as an incident response analyst at A-FIRST (AhnLab Forensics & Incident Response Service Team).

MyungUk Han
AhnLab

Bio:

Myunguk Han is a malware researcher at AhnLab.

Having spent many times deep in malware and vulnerabilities, He loves reverse-engineering and passionate in computer itself. When he has free time, he reads some of the cyber attacks reports for self-improvement.

PLENTY OF SMISH IN THE SEA - TIME TO CAST THE PHISHNET

Abstract:

Social engineering attacks aim to get unauthorized access or sensitive information by exploiting human vulnerabilities and trust, and with recent advances in natural language processing (NLP), threat actors are now able to produce sophisticated phishing attacks that are convincing, persuasive, and coherent using generative language models such as GPT-based ones (e.g., WormGPT and FraudGPT). One particularly concerning trend in phishing attacks is the rise of smishing (SMS phishing). This attack vector has become more prevalent due to the widespread use of mobile devices and the trust associated with text communication, especially when received from a known sender (via spoofing attacks). For instance, in April 2023, Traficom (the Finnish National Cyber Security Centre) reported aggressive smishing campaigns aimed at collecting payment and card information by posing as tax returns, bank messages, and delivery service (OmaPosti) notifications; similar incidents have been observed globally. In order to effectively counter smishing attacks and protect users from falling to them, we propose a novel anti-smishing solution (PhishNet) that employs NLP and open knowledge bases to identify popular persuasion techniques, well-known brands and organizations, and provide contextual analysis to determine the SMS content and intent.

Our anti-smishing solution consists of 5 steps, which are: input preparation, data and feature extraction, URL analysis, content analysis, and decision-making. Briefly, the first step validates the input and ensures the presence of the relevant information while the following step extracts the desired information and features. Next, if the URL is fresh and unknown to our security cloud, this anti-smishing solution conducts a comprehensive analysis of the content of the message using various NLP and machine learning (ML) techniques. We also leverage WikiData to enrich found named entities. Based on all the analyses and present facts, a final decision is reached through an ensemble model, alongside logical conditions. If needed, the content of the phishing page is assessed using ML models.

We rigorously evaluated the solution against a private dataset of real-world benign and smishing messages, where it achieved high accuracy while maintaining a low false positive rate. These results indicate that it is a robust and reliable defense mechanism against the escalating threat of smishing attacks, and utilizing it will greatly protect individuals and organizations against such attacks while preserving user privacy and ensuring minimal disruption to legitimate SMS communications. In this sharing, I will talk about the details of each step of the process, how we evaluated our solution and its effectiveness along with how we continuously improve it.

Dr. Khalid Alnajjar
F-Secure

Bio:

Khalid Alnajjar meticulously analyzes threat data and develops AI models at F-Secure to enhance security against emerging threats, particularly in threat detection and mitigation. Holding a doctorate and postdoctoral tenure in NLP and AI, along with a robust cybersecurity background, he demonstrates significant prowess in both academic and professional realms. With over a decade of experience in AI and software development, Khalid has a proven track record highlighted by notable publications in prestigious conferences and journals, and leadership in innovative AI projects from inception to completion. His expertise also extends to MBA principles, leadership, and management, showcasing a well-rounded mastery crucial for advancing AI solutions and fostering a secure digital environment.

UEFI SECURE BOOT BYPASSES AND THE DAWN OF BOOTKITS

Abstract:

In March 2023, ESET Research confirmed the rumors about BlackLotus, a UEFI bootkit reputedly being sold on underground forums since at least October 2022. This is the first publicly known UEFI bootkit bypassing UEFI Secure Boot. It exploited a one-plus-year-old vulnerability (CVE-2022-21894) to bypass UEFI Secure Boot on fully updated Windows systems, confirming that bootkits are not just for legacy systems anymore, but a potential threat for a majority of UEFI firmware systems nowadays.

In this session, we answer the questions many people have about the state of UEFI security: How is it that the one-plus-year-old known vulnerability can be used to deploy such dangerous threats? Is it the only such vulnerability? And what can we do to protect against such bootkits?

We start with the basics of UEFI bootkits to explain how they persist and what they can do once deployed. Next, we discuss how UEFI Secure Boot works, and most importantly, how it can be bypassed, by looking at several selected cases of known UEFI vulnerabilities – all very easily allowing bypassing or disabling of UEFI Secure Boot. All this to explain why we think it is only a matter of time until another bootkit like BlackLotus appears, and why we think BlackLotus perfectly foreshadows the future of UEFI threats.

Finally, we look into what you can do to protect against UEFI bootkits, what can be done to detect a bootkit once you get compromised, and how to remove it.

Martin Smolár
ESET

Bio:

Martin Smolár is a Malware Researcher at ESET. His main responsibilities include malware analysis with a special focus on UEFI bootkits and firmware implants. Besides malware, he is particularly interested in UEFI security and reverse-engineering of UEFI firmware secrets. In his research, he tries to point out to the problems UEFI systems face, and actively works to make them safer by uncovering various UEFI vulnerabilities and reporting them to the affected parties. To date, Martin has discovered more than ten UEFI vulnerabilities, many of them allowing easy bypasses of the essential UEFI security mechanism – UEFI Secure Boot.

AMPLIFYING THREAT INTELLIGENCE VIA GENERATIVE AI-DRIVEN AGGREGATION AND ENRICHMENT

Abstract:

In the ever-evolving landscape of cybersecurity threats, the rapid and accurate aggregation and enrichment of threat intelligence is of fundamental importance for organizations seeking to safeguard their digital assets. This presentation provides a novel approach leveraging Generative AI, specifically the GPT model, to revolutionize the process of threat intelligence aggregation and enrichment.

Traditional methods of sifting through an overwhelming volume of threat bulletins, articles, and reports can be time-consuming and error-prone. Our proposed system harnesses the power of Generative AI to automate and enhance this process. By utilizing GPT's natural language understanding capabilities, our system can intelligently summarize complex threat narratives, extracting key elements like malware names and threat actor identities, while concurrently enriching associated Indicators of Compromise (IOCs) with these critical components.

The core of our approach lies in the ability of GPT to comprehend contextual information and extract relevant insights from disparate textual sources. Through a combination of supervised and fine-tuned learning, our model has been trained to identify and categorize crucial threat intelligence elements accurately. This not only accelerates the analysis process but also reduces the chances of overlooking critical information.

In this presentation, we will discuss the architecture of our AI-driven threat intelligence system, highlighting the pivotal factors that culminate in achieving optimal performance. We will also present real-world case studies to demonstrate the efficacy of our generative AI-driven approach.

Dr. Jason Zhang
Anomali

Bio:

Jason Zhang is the Director of Cyber Intelligence at Anomali. As a highly motivated cyber threat researcher and a proven product and technology pioneer, Jason has a wealth of experience in technology and product R&D. Prior to joining Anomali, Jason worked at VMware, Lastline, Sophos, Symantec and MessageLabs, specialising in cutting-edge research and automation in threat detection and intelligence analysis. Jason is a regular speaker at leading technical conferences including Black Hat, Virus Bulletin and InfoSec. Jason earned his Ph.D. in signal processing from King's College London & Cardiff University in the UK.

Kyle Campbell
Anomali

Bio:

Kyle Campbell is an Intelligence Engineer at Anomali, where he has been employed for the past year. Kyle is responsible for feed creation and ingestion of OSINT and premium data, ensuring quality across the entire intelligence lifecycle in addition to utilizing analytics to understand and improve upon trends and gaps in intelligence coverage. Kyle holds a bachelor's degree in Digital Security and Forensics and is Mitre Att&ck Defender (MAD) certified.

UNDERSTANDING RANSOMWARE REBRANDING

Abstract:

During the life-time of a ransomware, the owners and operators usually get together to get the most out of it. While at a first glance we would like to believe that a ransomware family is a standalone piece of code, by analyzing hundreds of binaries we have seen that some of them share more than we expected. In this paper we bring some light to a few ransomware rebrandings that we assisted to, based on some recent concrete examples. While some of them may also be confirmed by public articles, there are also cases requiring a lot of attention to spot the actual bonds. In this paper we use generic unpacking techniques as well as Control Flow Graph analysis to understand the sharing of code pieces.

Dr. Vlad Constantin Craciun
Bitdefender

Bio:

Vlad Craciun is an Assistant Professor at the "Alexandru Ioan Cuza" University of Iasi, Faculty of Computer Science (Romania), studying the field of automated binary analysis. He joined Bitdefender Laboratories in early 2009, being involved in projects like file-infector disinfection, post-incident forensics, building of ransomware decryption tools. His current research interests include automated binary analysis, cryptography, symbolic execution, and Control Flow Graph analysis.

MEGALO-(AN)-DON: UNCOVERING DATA ESPIONAGE, BLACKMAILING AND SHELL COMPANIES IN MOBILE LENDING APPS TARGETING ASIA

Abstract:

Years of pandemic, lockdowns, the cost-of-living crisis, and rising inflation have taken money out of people's pockets, especially in developing nations, pushing an increasing number of people to rely on taking out personal loans. Traditional banks have been tightening their lending policies – borrowers need good credit scores, and in some countries, they even ask for collateral to lend money in this tough economic climate. Spotting a gap in the market, several malevolent mobile lending applications have arisen to lend to individuals when they are in a vulnerable situation.

Mobile lending applications have been a problem on app platforms for years, with few legitimate apps and several fraudulent ones. Researchers have been finding lending applications that have been violating policies for years. App platforms have brought in several policy updates to curb illegal applications, but they circumvent these policies with fake information and have been thriving more than ever, particularly in the Google Play Store, due to Android having a higher market share in developing nations. These lending apps claim to charge low interest and have longer repayment schedules, but in reality, have shorter repayment schedules ranging from seven days to a few weeks. Besides that, they collect vast amounts of personal data, identity details, device information, contacts, locations, SMS, and call logs, and store these details in unknown third-party locations, violating various data regulations. Some countries even classify these as hostile. When victims fail to repay within a short duration, they start charging high interest and abuse their personal data by threatening to send sensitive data to friends/relatives on the contact list, post on social media and make threatening calls. Several people have lost lives through suicide, unable to bear the torture of the agents. Technology-wise, there is a sophisticated infrastructure behind these apps, with professional-looking websites, the use of app frameworks, the use of packers to evade app platform policies, fake banking regulation certificates being created on websites to fool users, and user traffic being driven through social media and Telegram groups.

Jagadeesh Chandraiah
Sophos

Bio:

Jagadeesh Chandraiah is a senior malware researcher at SophosLabs, specializing in mobile malware analysis. Jagadeesh has been working at SophosLabs for over 10 years. Jagadeesh started working on Windows malware analysis and is currently focusing on mobile malware analysis. Jagadeesh has a Master's degree in computer systems security from the University of South Wales.

Jagadeesh likes to track malware, research and find novel ways to detect and remediate them. Jagadeesh is a frequent contributor to the SophosLabs Uncut blog and has written blog posts about several mobile malware topics. Jagadeesh also regularly presents his research at international security conferences and in the past has presented his research at DeepSec, AVAR, CARO, and Virus Bulletin.

Outside of work, Jagadeesh enjoys playing badminton.

@jag_chandra

GOLDENJACKAL CHRONICLES: DELVING INTO ENIGMAS AND UNANSWERED QUESTIONS

Abstract:

"GoldenJackal" is a relatively new APT group that we discovered in mid-2020 and publicly documented in 2023. Since 2019, this group has conducted several APT attacks targeting governmental and diplomatic entities in the Middle East and South Asia.

Over the past years, we have closely monitored the group and collected information about their Tactics, Techniques, and Procedures (TTPs). We've observed a consistent level of activity, which characterizes the group as a proficient and stealthy actor gradually expanding its operations. The hallmark of this group lies in its distinct set of .NET malware tools: JackalControl, JackalWorm, JackalSteal, JackalPerInfo, and JackalScreenWatcher. These tools serve various purposes, including:

- Controlling victim machines
- Propagating across systems via removable drives
- Exfiltrating specific files from infected systems
- Stealing credentials
- Gathering information about local systems
- Collecting data on users' web activities
- Capturing desktop screenshots

Based on their toolset and behavioral patterns, we believe the primary motivation of the actor is espionage. In the upcoming speech, I will cover the group's most relevant facets, provide an overview of their toolset, explore their targeting strategies, and how they move laterally inside the targeted network. Additionally, I will highlight the unresolved aspects to inspire fellow researchers to shed light on these areas and aid in enhancing the community's understanding of this cyber threat.

Giampaolo Dedola
Kaspersky

Bio:

Giampaolo Dedola is a Lead Security Researcher at Kaspersky`s GReAT (Global Research & Analysis Team), based in Italy. He focuses his research in the realm of APT attacks, hunting for new threats, analyzing malware, digging up incidents, and profiling the actors behind them.

Over the years, he investigated hundreds of APT campaigns, trying to extend his knowledge on different groups regardless of their origin or targets.

Before joining Kaspersky in 2017 he held the position of L3 SOC analyst, principal malware analyst, and forensic analyst.

REBRAND TO X?: STEELCLOVER CORNUCOPIA

Abstract:

Since 2019, SteelClover have been cunningly attacking under the radar. Their main concern has been money from the beginning and they keep on changing attacking tools and techniques. While there are reports of their activities, they are only snapshots. This session will first review their attack campaigns to identify their motivation to attack, tools, techniques, and their trend.

Next, we will introduce attack cases of MSIX file abuse which SteelClover has been actively using from 2023. While they had been abusing MSI file to conduct attack campaign since 2020, they started to take advantage of MSIX file from 2023. However, many are unaware of MSIX file existence and ignorant of its abuse cases. Needless to say, how to detect and defend oneself from MSIX files exploitation is almost unknown to the public. In this section, we will share defensive knowledge helpful for Blue Team.

Finally, we will present research methods that we have developed and believe still effective even in today to pursue SteelClover including queries available on various tools such as VirusTotal, URLScan, Censys, and Shodan. We have been tracking their activities for more than three years. Despite frequent changes of attacking tools and techniques, there are always some characteristics in every moment. In addition, we will show their mistakes from our continuous research, and some implications of them.

The campaign details, toolset, TTPs, infrastructure, and threat actor information introduced in this session will enable SOC analysts, IR team members, CSIRT personnel, and others to gain a deep understanding of SteelClover's activities. This information will help them to defend their organizations from attacks conducted by SteelClover.

Rintaro Koike
NTT Security Holdings

Bio:

Rintaro Koike is a security analyst at NTT Security Holdings. He is engaged in threat research and malware analysis. In addition, he is the founder of "nao_sec" and is in charge of threat research. He focuses on APT attacks targeting East Asia and web-based attacks. He has been a speaker at VB, SAS, AVAR and others.

Shogo Hayashi
NTT Security Holdings

Bio:

Shogo Hayashi is a security analyst at NTT Security Holdings. His main specialization is responding to EDR detections, creating IoCs, analyzing malware and research cyber threat. He is a cofounder of SOCYETI, an organization for sharing threat information and analysis technique to SOC analysts in Japan. He has spoken at JSAC, VB, SAS, CODE BLUE and has written several white papers and blogs.

SMOOTHOPERATOR – 3CX SUPPLY CHAIN ATTACK

Abstract:

Supply chain attacks have become a major concern for organizations worldwide due to their potential to cause significant damage. The SolarWinds attack affected thousands of organizations, and now, a similar attack has occurred with the 3CX supply chain. 3CX is a VoIP Communication company with 12 million daily users, and in March 2023, SentinelOne uncovered a devastating attack where threat actors trojanized 3CXDesktopApp in a supply chain attack to infect thousands of users worldwide.

The attack compromised the supply chain of 3CXDesktopApp, including both Windows and MacOS installers. During installation of the application, a trojanized library was sideloaded and connected to a Command and Control Server. After fingerprinting the machine, it was observed downloading the next stage payload, which is an infostealer. It has functionality, including gathering system information and browser information from Chrome, Edge, Brave, and Firefox browsers, and in some cases, we observed backdoor malware to carry out their cyber espionage.

This research will provide insights into the complexities of the 3CX supply chain attack and serve as a guide to organizations to implement measures that can enhance their cybersecurity posture against such attacks.

Dinesh Devadoss
SentinelOne

Bio:

Dinesh Devadoss, a Staff Threat Hunter at SentinelOne WatchTower, considers himself to be a wanderer in the binary world. He graduated with a Bachelor of Science degree in Computer Science Engineering. He has extensive experience in threat hunting, malware research, threat intelligence, forensics, and studying about threat evolution. In the past, he has presented his research at the AVAR and Virus Bulletin conferences. His passion (bordering on addiction) is to extensively research malware targeting macOS.

Niranjan Jayanand
SentinelOne

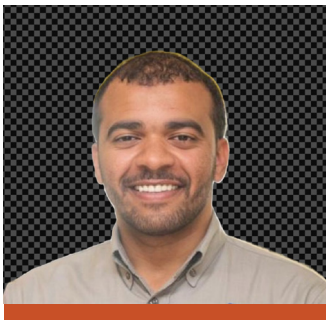
Bio:

I am Senior Manager with SentinelOne taking care of WatchTower Threat hunting program from APJ region and also work as Principal Threat Intel Analyst with a demonstrated history of Threat group hunting, malware reversing, blogging, presenting in conferences, webinars and podcasts etc. Our team partners with MDR and DFIR analysts to stay ahead of attackers and provide actionable intelligence for our customers proactively. My latest work involves discovery and reporting of CISCO ASA vulnerability abused by Akira ransomware group.

NEXT GENERATION FIREWALL DEPLOYMENT FOR PREDICTIVE ANALYSIS OF NETWORK ANOMALIES USING ARTIFICIAL INTELLIGENCE

Abstract:

The rapid evolution of cybersecurity threats necessitates the adoption of advanced defense mechanisms, such as Next-Generation Firewalls (NGFWs), to protect modern networks. This presentation provides a comprehensive overview of NGFW deployment for predictive analysis of network anomalies using artificial intelligence (AI) models. We explore the synergistic integration of NGFWs with AI, enabling proactive threat detection and mitigation. Through the analysis of real-world data, this research demonstrates the efficacy of AI-driven anomaly detection, reducing response times to emerging threats. The study highlights the potential of NGFWs as a critical component of proactive network defense strategies, ultimately enhancing the security posture of organizations in the digital age.



Almuhaisen, Salman N
Saudi Aramco

Bio:

Salman is a recognized subject matter expert in the field of Information Security and data protection with more than 10 years of experience working on different roles. Currently, leading Information Security Analysts group within Saudi Aramco in KSA

VERY REAL ASSAULT ON VIRTUAL ESXI: THE EVOLVING LINUX RANSOMWARE THREAT

Abstract:

Ransomware encryption of corporate ESXi deployments is not new; Babuk ransomware has targeted ESXi infrastructure on Windows. However, the most popular host OS for ESXi is actually Linux, and since Babuk's source code leak, other ransomware offspring have recently come to the fore, particularly targeting Linux.

Akira ransomware is believed to have initiated its campaign in late March 2023. Akira is based on Conti, and Conti was inspired by Babuk. The code most commonly reused between Babuk, Conti and Akira ransomware is the ChaCha encryption implementation. LockBit, the latest ransomware group to target Linux, has focused its attention on encrypting VMware ESXi virtual machines using AES. Another group called Royal Ransomware had also entered the Linux scene, switching in September 2022 to a new and innovative encryption module called "Zeon".

ESXi on Linux provides a few golden infiltration opportunities for ransomware actors such as poorly-configured SSH and other services, high-impact RCE CVEs with respect to VMware itself like CVE-2021-21985 and CVE-2021-21986, and exploitation of the OpenSLP service running on port 427 (CVE-2021-21974). After the initial access, most of the ransomware use command line arguments to encrypt specific ESXi files. As described above, the LockBit, Royal and Akira ransomware have now been identified as prominent threats to ESXi systems hosted on Linux, having already made their mark in the Windows domain.

In this presentation we shall delve deep into the inner workings of the trio of Linux ransomware that target ESXi, exploring code/functionality similarities and disparities between their Windows and Linux flavours. We will also explore the methods for effectively mitigating these debilitating threats within a Linux-based ESXi environment.

Vigneshwaran P
K7 Computing

Bio:

Vigneshwaran Parthiban has graduated from Anna University Chennai with a bachelor's degree in Information Technology. He started his career in 2021 as a Threat Researcher at K7 Computing's K7 Labs. Vigneshwaran's primary responsibilities involve reversing and detecting various types of malware at multiple layers, as well as staying up-to-date with the latest trends in Linux malwares and ELF analysis. His analysis of various malware are detailed on K7 Labs' technical blog page. He likes to hang out with friends and play cricket in his free time.

ADAPTIVE FILE ANALYZER: NLP COMBINED WITH HEURISTIC ANALYSIS TO DETECT MALICIOUS EMAIL ATTACHMENTS.

Abstract:

The key finding of the 2023 Verizon Data Breach Investigations Report (DBIR) was that email attachment is a top malware delivery vector. Email Malware attachment is usually convicted using static or dynamic analysis. Instead of keeping the payload in one file, which is attached to an email, most of the malware employs the technique of spreading the payload and making the attack a multi-stage attack. The first stage, which is attached to the email, is the downloader or dropper. The second or the subsequent stage of malware carries a malicious payload.

Let's take an example of HTML smuggling SHA256 [1], a multi-stage payload. The initial payload has obfuscated script, which uses methods like setTimeout() and debugger identification making dynamic analysis harder. The HTML file has an embedded ZIP file which is encoded in base64. The ZIP file is password protected, making it challenging for dynamic analysis to extract its contents. The ZIP file contains an ISO image. When an ISO image is mounted, it shows an LNK file that executes the JS file, which in turn drops DLL. The DLL initiates a ping command to check the internet's availability and injects itself into the Windows Error Manager.

Detecting multistage malware challenges static and dynamic analysis since not only it requires capturing every stage of downloader and dropper, but also malware employs evasion techniques, such as extended sleep calls, checking for the debugger, lack of proper environment, etc., [2], which are commonly used to avoid capturing malware behavior and evading dynamic analysis.

We designed an adaptive file analyzer to solve the problem of detecting multi-stage malware without capturing every stage of malware for non-PE file formats usually seen in email traffic, such as HTML, OLE, Archives, PDF, etc. In the first part of the presentation, we share the details of the document modeling used by the adaptive file analyzer to understand the contexts under which emails with attachments are sent by threat actors. Once the context under which the email has been sent is computed, lightweight scanning of the file attached to the email, or the first stage of malware is done. In the second part of the presentation, we dive into the details of the correlation engine, which takes as inputs the context of emails from document modeling and correlates with the results of lightweight scanning of files to determine if the attachment is malicious or benign.

In the last part of the presentation, we share the results of the Adaptive file analyzer on the actual customer traffic. An adaptive file analyzer provides an inherent advantage of using the context under which the email was sent, combined with the lightweight scanning of the first stage to determine if the attachment is malicious or benign without analyzing the second and subsequent stages of malware.

ADAPTIVE FILE ANALYZER: NLP COMBINED WITH HEURISTIC ANALYSIS TO DETECT MALICIOUS EMAIL ATTACHMENTS.

Kalpesh Mantri
Cisco Talos

Bio:

Kalpesh Mantri joined Cisco in 2022 as a Security Research Engineer for Talos. He has accumulated over a decade of experience in the field of Cyber Security. In his current research, he leads the way in conducting forward-thinking research projects and creating innovative prototypes on the investigation of email threats with a particular focus on malspams landscape.

Prior to joining Cisco, Kalpesh worked as a Senior Malware Analyst and Security Software Developer focusing on malware reversing, threat hunting and detection techniques as well as APT attack investigations. Kalpesh aided authorities by uncovering many critical APT operations including notable 'Operation SideCopy' and 'Operation HoneyTrap' that target defence sectors. Kalpesh is very active in the cybersecurity community and he regularly presents at various security conferences. Some of his previous conference presentations include Virus Bulletin, AVAR and CARO Workshop events.

https://www.linkedin.com/in/kalpeshmantri/

Abhishek Singh
Cisco Talos

Bio:

Abhishek Singh is a security R&D leader with 15+ years of experience, passion, and a proven track record of driving research and threat detection engineering, which solves complex problems and results in a winning technology leading to revenue gains at Cisco, FireEye and Microsoft. He holds 36 (approved/pending) patents, has authored 17 research papers, seven technical white papers, and contributed to three books. Patents and papers detail work in algorithms, analytics, machine learning-based approaches to detect advanced threats, and architecture of technologies such as the virtual machine-based approach for threat analysis, EDR, RASP, DAST, Active Defense (Deception), email, web and IPS.

Many algorithms and preventive features which Abhishek has designed are key concepts used in technologies like RASP and Active Defense (Deception). His notable recognitions include the following:

- 2019 Reboot Leadership Award (Innovators Category): SC Media
- Shortlisted for Virus Bulletin's 2018 Péter Ször Award
- Cyber Security Professional of the Year – North America (Silver Winner) Cyber Security Excellence Awards 2020

https://www.linkedin.com/in/abhisheksingh1/

VALLEYFALL SPYWARE – TALES OF MALWARE DISCOVERY AND HUNTING IN THE WILD

Abstract:

The "ValleyFall" malware is a new cyber threat we have identified in the wild in late April 2023. The process of uncovering new malware, hunting for related samples, and constructing their network, can prove to be a challenge due to the constantly evolving and stealthy nature of cyber threats. This proactive effort is essential to comprehend the latest tactics and techniques and provide effective defense. This talk covers malware discovery procedures, and we delve into an in-depth analysis of ValleyFall, highlighting the crucial role of hunting in malware research. A brief introduction of this malware family is going to be presented first, followed by the infection chain, the tactics and techniques that we had identified while analyzing its code structure, and pinpoint the malicious functionalities. Subsequently we present the importance of hunting procedures and how to define a hunting methodology. We conclude the presentation with our findings regarding the malware server hive and the impact in the wild based on our telemetry.

Marian Gusatu
Gen Digital

Bio:

Marian Gusatu works as a Specialist Threat Researcher at Gen Digital Inc. His expertise lies in reverse engineering, malware analysis and hunting, as well as vulnerability research from both offensive and defensive perspectives.

SPACE PIRATES: HACK, STEAL, REPEAT!

Abstract:

At the end of 2019, the team at the Positive Technologies Expert Security Center (PT ESC) discovered a new cybercrime group, which they dubbed Space Pirates. It had been active since at least 2017. The first-ever comprehensive research paper describing the group saw light in early 2022. The Space Pirates group have since stepped up attacks on Russian companies: we have come across the group frequently while investigating cyberattacks in the past year. They have hardly changed their tactics, but they have developed new tools and improved their old ones.

The cybercriminals' main goals are still espionage and theft of confidential information, but the group has expanded its interests and the geography of its attacks. Over the year, at least 16 organizations have been attacked in Russia and one in Serbia. Some of the new victims that we identified are Russian and Serbian government and educational institutions, private security companies, aerospace manufacturers, agricultural producers, defense, energy, and infosec companies.

Virtually every investigation we conducted found that the group was using Deed RAT. As far as we can tell, the Space Pirates group is moving away from other backdoors. According to code similarities between Deed RAT and ShadowPad, we suggest that the backdoor is an evolution of ShadowPad. ShadowPad is in turn believed to be an evolution of PlugX. Unlike ShadowPad and PlugX, though, Deed RAT has been known to be exclusive to the Space Pirates group to date. The backdoor is still under active development. We found a 64-bit version of Deed RAT on an infected device while investigating the incident. The structure of the main module and plugin headers is all but identical to the 32-bit version.

During an investigation, we obtained a sample of unknown, functionally different malware. Our timeline of the sample appearing on the infected computer suggested that the malware is delivered via Deed RAT already installed on the machine and belongs to the Space Pirates group. We were later shown to be right. We named the malware Voidoor, after the C&C server and the backdoor malware type. Voidoor used legitimate resources Github and Voidtools.com as C&C server. While we investigated logs from Github and voidtools we found more than 3,500 login events associated with 73 unique IP addresses, and we were able to attribute voidoor to the Space Pirates group after discovering a series of logins from Space Pirates IP addresses that occurred within days of registering the account.

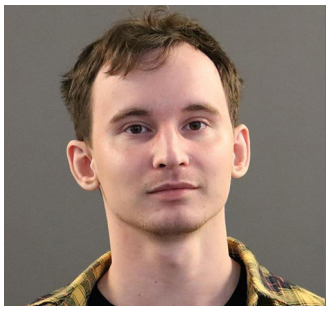
SPACE PIRATES: HACK, STEAL, REPEAT!

Denis Kuvshinov
Positive Technologies

Bio:

Head of Threat Intelligence department, Positive Technologies Expert Security Center. Graduated from the Bauman Moscow State Technical University in 2017 with a degree in Digital and Technical Intelligence Prevention.

Previously worked for Informzashchita. Joined Positive Technologies in 2017. Started out as Information Security Monitoring Specialist, is currently Head of Threat Analysis, Positive Technologies Expert Security Center. In charge of searching for new APT groups (participated in discovering TaskMasters, SongXY, Calypso, Chamelgang, and Space Pirates) and tracking activities of known groups. Responsible for malware analysis and supplying expertise in the form of data on indicators of compromise for Positive Technologies products. Regular speaker at industry-specific conferences: spoke at PHDays and Standoff 10 in 2022.



Stanislav Rakovsky
Positive Technologies

Bio:

Senior analyst of Threat Intelligence department, Positive Technologies Expert Security Center. Stanislav Rakovsky is a seasoned malware researcher at Positive Technologies with a specialized focus on tracking APTs and investigating open-source malicious activities. Stanislav has master's degree in Information Security & Information Security Management, MPEI. Regular speaker at industry-specific conferences: The STANDOFF, PHDays, OFFZONE, Moscow Python Conf, IT Picknick

AN EFFICIENT APPROACH FOR AUTOMATING THREAT INTELLIGENCE ANALYSIS THROUGH SIMILARITY DETECTION

Abstract:

Manually analyzing large-scale threats requires considerable resources. However, this task often becomes repetitive and tedious for cybersecurity experts since many threats are variations of past ones. Furthermore, given that the analysis of threat intelligence — including factors such as threat type, threat actor, and technique IDs — demands time and expertise, processing a large volume of threats is practically challenging.

To alleviate these challenges, we propose the Deep Binary Profiler (DBP). The DBP segments assembly code into multiple functions and then transforms these functions into vectors using an embedding model. By calculating the similarity between each pair of functions, it is possible to trace how newly emerging threats have evolved from past threats and how certain functionalities have been reused in these evolutions. As a result, new threats can inherit threat intelligence from past threats, enabling the automatic analysis of these new threats.

The large volume of threat intelligence stored in the database results in a proportional increase in time complexity during similarity searches. This data volume continues to grow as experts analyze new threats. To mitigate this, we quantized the stored function vectors to produce representative code vectors. These vectors are then converted into strings, termed Function Hash (FHash). Given that similar functions yield similar vector representations, they generate identical FHash strings. By filtering functions with matching FHash values, we efficiently reduced the search space for similarity searches.

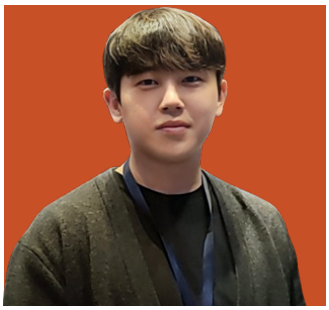
In our experiments, we validated the proposed method using 2,803,509 assembly functions derived from 11,613 malware samples. Among the entire set of functions, 531,892 unique FHashes were extracted, representing approximately 18.9% of the total. This approach enabled a reduction of the overall search space by nearly 99.7%, thus enhancing the performance of similarity searches. Consequently, the DBP technique identifies threat variants in real-time, allowing experts to concentrate their resources on analyzing novel threats.

AN EFFICIENT APPROACH FOR AUTOMATING THREAT INTELLIGENCE ANALYSIS THROUGH SIMILARITY DETECTION

Hyunjong Lee
SANDS Lab

Bio:

Hyunjong Lee is an AI researcher at SANDSLab in South Korea, with a primary focus on applying AI/ML techniques to the field of cybersecurity. He earned his M.S. degree from Dankook University, South Korea, and has four years of experience working as an AI researcher. His research interests center around Representation Learning.



Chang-Gyun Kim
KSign

Bio:

Chang-Gyun Kim is an assistant research engineer at KSign's Security Technical Research Institute.

He has a Master's degree in computing, specializing in artificial intelligence and machine learning, from Imperial College London.

His current research and interests are using artificial intelligence for malware classification and threat intelligence analysis.

UNVEILING THE DARKGATE MALWARE: A COMPREHENSIVE ANALYSIS OF ITS APT GROUP, DEVELOPMENT TIMELINE, AND CAPABILITIES

Abstract:

Evolution of DarkGate and its capabilities:

This paper extensively examines DarkGate malware, revealing its APT group, developmental timeline, and broad capabilities. The evolution of DarkGate is traced from its origin to its present form. The core focus is on scrutinizing its capabilities, encompassing evasion techniques against antivirus (AV) software, along with separate analyses of its code regarding cryptomining, crypto theft, RAT behavior, and ransomware features.

Obfuscation and Shellcode Techniques:

The complexity of DarkGate is explored through its AutoIT script structure, ingenious obfuscation methods, and execution of shellcode techniques. The paper delves into decrypting strings, identifying Command and Control (C2) strings, and unravels its core functional mechanisms, including intricate network traffic decryption.

Evasion Strategies:

DarkGate's strategies for evading network protections are disclosed, with emphasis on bypassing EDR, intrusion detection, and prevention systems, alongside User Account Control (UAC) circumvention for elevated destructive activities.

Impact and Future:

The study encompasses DarkGate's impact on nations, strategic targeting, and spreading tactics. It concludes by spotlighting the global Command and Control network, composed of individuals worldwide who manage infections and execute attack plans.

Speculation and Contribution:

The paper also speculates on DarkGate's future moves based on behavioral analysis that we have conducted. In summary, this investigation offers valuable insights into DarkGate's origin, growth, capabilities, and global impact, contributing to a comprehensive understanding of this complex malware's ramifications.

UNVEILING THE DARKGATE MALWARE: A COMPREHENSIVE ANALYSIS OF ITS APT GROUP, DEVELOPMENT TIMELINE, AND CAPABILITIES

Aravind Raj
Quick Heal

Bio:

Aravind Raj is a Senior Security Researcher at Quick Heal. He specializes in Malware Research and Reverse engineering techniques. He currently works on behavioral methods to detect and prevent cyber threats. He has devised various strategies to counter Ransomware attacks in particular. He has experience in analyzing Windows-based threats, such as APTs, spyware, and banking Trojans. He also specializes in Threat Intelligence and MITRE ATT&CK Patterns.

Nihar Deshpande
Quick Heal

Bio:

Nihar Deshpande is a Principal Security Researcher at Seqrite, specializing in virus and ransomware analysis. With a strong academic background in Computer Science, he excels in developing malware detection algorithms. Nihar has published insights on malware trends and technologies. His expertise includes behavioral analysis, MITRE ATT&CK framework proficiency, and Proof of Concept projects in cybersecurity.

ONCE GIFTED IS ALWAYS GIFTED

Abstract:

Ransomware threats continued to be prevalent in 2023, Talos is seeing a significant surge in the evolution of the new players in the ransomware threat landscape. In our Year in Review 2022 report, we highlighted that the ransomware operators are moving away from operating as silos, and more diverse groups were started appearing. The shift in the trend has continued that not only operating from a diverse group but many new threat actors or cyber criminals whose skill sets range from less – more sophisticated have evolved in the ransomware threat landscape.

Talos believes that one of the important reasons behind the increase of new players in the ransomware threat landscape is the leaking of the ransomware source code or builders. The threat actors are heavily leveraging on modifying the leaked ransomware source code or utilizing the leaked ransomware builders, creating newer versions of ransomware with minor modifications.

Conclusion:

With more cybercriminals gaining access to the ransomware source code or builders, the overall frequency of ransomware attacks would increase. Defenders and Incident responders should be vigilant about the new ransomware families and the threat actors attempt to disguise as known ransomware families. Organizations should be meticulous about enhancing their proactive security measures, implementation of proven backup and recovery strategies, incident response capabilities, and promptly patching and updating their digital infrastructure, along with employee education in creating awareness of the implications of security breaches on the organization.

Chetan Raghuprasad
Cisco Talos

Bio:

Chetan Raghuprasad is a Security researcher with the Cisco Talos, focusing on hunting and researching the latest threats in the cyber threat landscape generating actionable intelligence. He seeks to uncover threat actors' tactics, techniques, and procedures by reversing and analysing the threats to identify the actors' TTPs, motives, and origins. Chetan also publicly represents Cisco Talos by writing the Talos blogs and talking at cybersecurity conferences worldwide.

Chetan Raghuprasad has 15 years of experience in the Information Security sector, having worked within Threat Intelligence, Cyber incident response, and digital forensic analysis teams in technology companies, consulting and financial institutions. Chetan has assisted legal cyber security and Insider threat investigation cases as digital forensic expert.

CYBERCRIME ATLAS: USING MAPS TO CREATE A MORE SECURE ECOSYSTEM

Abstract:

How do you find a location in the real world? You use a map. How do you understand a business process? You make a diagram. The same logic applies in cyberspace. If we want to truly understand how cybercriminals operate and where they are located, then we need to create "maps" or diagrams of their activities. That's what the Cybercrime Atlas is designed to do. Officially launched by the World Economic Forum's Center for Cybersecurity in January 2023, the Cybercrime Atlas project will collect intelligence about cybercriminal activity from many different sources, collate and normalize it, and then generate different views or maps of the associated malicious actions. When fully operational, the Atlas will help defenders protect their networks and governments disrupt the criminal activity. However, to become fully operational, the Atlas project needs support from cybersecurity providers all over the world. This talk will cover the current status of the Atlas project, highlight some initial successes, and identify how companies can get involved in the effort.

Michael Daniel
CTA

Bio:

Michael serves as the President & CEO of the Cyber Threat Alliance (CTA), a non-profit organization that improves the cybersecurity of the global digital ecosystem by enabling high-quality cyber threat information sharing among cybersecurity providers. CTA's mission is to better protect end-users, enable the disruption of cyber adversaries, and elevate overall cybersecurity. CTA's members include more than 36 cybersecurity firms headquartered in twelve countries around the world.

Prior to CTA, Michael served as Special Assistant to the President and Cybersecurity Coordinator on the National Security Council Staff. In this role, he led the development and implementation of national cybersecurity strategy and policy, focusing on improving cyber defenses in the public and private sectors; deterring and disrupting malicious cyber activity aimed at the U.S. or its allies; and, improving the US's ability to respond to and recover from cyber incidents. Michael also helped craft the government's response to significant cyber incidents, such the attack on Sony Pictures Entertainment, the intrusion into the Office of Personnel Management, and the Russian efforts to meddle in our electoral process.

Before joining the National Security Council Staff, Michael served for 17 years in the Office of Management and Budget (OMB), including 11 years as the Chief of the Intelligence Branch in the National Security Division, overseeing the Intelligence Community and other classified Department of Defense programs.

Originally from Atlanta, Michael holds a Bachelor's in Public Policy from Princeton University, a Master's in Public Policy from Harvard, and a Master of Science in National Resource Strategy from the National Defense University's Industrial College of the Armed Forces. In his free time, he enjoys running and martial arts.

LET'S CHAT ABOUT GROSS PUBLIC TEXT GENERATION

Abstract:

ChatGPT is the buzzword of the year. Suddenly everyone mentions and everything uses ChatGPT (or so they say). But many people do not know what ChatGPT really stands for, or what it really is! Many people do not even know ChatGPT is just an example of a Large Language Model (LLM) bundled with some Machine Learning (ML) module and that there are many others in existence. To get a good overview of the progress in LLM technology, we will dig into the short history of LLMs.

There is no doubt about that LLMs can be a great asset for your company's workflow. But at the same time, you should wonder: can an LLM expose your company secrets? The answer is plain and simple: YES! (And it already happened.)

Leaving aside the good things an LLM can be for your company, we will focus on the dangers lurking around the use of an LLM and/or AI and your company depending on it, and showing real-life examples where it went or can go wrong, e.g., with Identity Management, Marketing, PII, (False) Information gathering, creation of (unethical) content, etc.

Of course, LLM and ML failures can lead to some humorous moments too; several of these will be showcased during the presentation.

We will conclude with what you can do to safeguard your company and yourself against all the nasty elements that may occur when using LLMs.

LET'S CHAT ABOUT GROSS PUBLIC TEXT GENERATION

Righard Zwienenberg
ESET

Bio:

Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the Technical University of Delft. His interest thus kindled and studied virus behavior and presented solutions and detection schemes ever since. Initially starting as an independent consultant, in 1991 he co-founded CSE Ltd. In November 1995 Zwienenberg joined the Research and Development department of ThunderBYTE. In 1998 he joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer. After AMTSO – Anti Malware Testing Standards Organization – was formed, Zwienenberg was elected as president. He is serving on the board of AVAR and on the Technical Overview Board of the WildList. In 2011 Zwienenberg was looking for new opportunities and started as a Senior Research Fellow at ESET. In April 2012 Zwienenberg stepped down as President of AMTSO to take the role as CTO and later as CEO. In 2016 he rejoined the AMTSO board for another two-year run. He also is the Vice Chair of the Executive Committee of IEEE ICSG. In 2018, Zwienenberg joined the Europol European Cyber Crime Center (EC3) Advisory Group as an ESET representative.

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences – among these Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, Government Symposia, SCADA seminars, etc. – and general security seminars. His interests are not limited to malicious code but have broadened to include general cybersecurity issues and encryption technologies over the past years.

Eddy Willems
G DATA

Bio:

Eddy Willems is a worldwide known cyber security expert from Belgium. He is a board member of 3 security industry organizations, EICAR, AVAR and LSEC, and is the resident Security Evangelist at G DATA Cyberdefense.

He became a founding member of EICAR in 1991, one of the world's first security IT organizations. Over the years he has served in many extra roles in different security industry organizations. Several CERTs, press agencies, print and online publications and broadcasting media, for example CNN, use his advice regularly. In October of 2013, he published his first book in Belgium and the Netherlands, entitled 'Cybergevaar' (Lannoo). A German translation followed afterwards and an English translation and update, Cyberdanger (Springer), was published in 2019. He is also co-author of the Dutch SF cyberthriller 'Het Virus' published in 2020. Eddy is a known inspiring speaker and is giving lectures and presentations (including TEDx) worldwide for a very diverse audience from children to experts.

UNRAVELING THE MOVEIT VULNERABILITY: A JOURNEY FROM EXPLOITATION TO CLOP RANSOMWARE INFESTATION

Abstract:

This paper offers an extensive analysis of the MOVEit vulnerability, tracing the entire trajectory of the cyber incident from the initial attack to the eventual infestation of Clop ransomware. Through in-depth research, data analysis, and examination of real-world case studies, this study aims to provide a comprehensive understanding of the vulnerability's exploitation, its repercussions on affected organizations, and the emergence of Clop ransomware as the ultimate tool for data extortion.

The paper begins by introducing MOVEit, a widely adopted secure file transfer software, and the critical role it plays in facilitating secure data exchange for various industries. It then presents an overview of the vulnerability that was later exploited by threat actors to compromise the system's security.

Next, the study investigates the initial attack vector employed by cybercriminals to gain unauthorized access to MOVEit systems. It explores the exploitation techniques, such as zero-day exploits, phishing campaigns, or social engineering, that enabled attackers to bypass authentication mechanisms and infiltrate target networks.

With a focus on the anatomy of the attack, the paper dissects the tactics, techniques, and procedures (TTPs) employed by the threat actors to navigate through the compromised network. This analysis aims to shed light on the level of sophistication and persistence demonstrated by the attackers in their pursuit of sensitive data.

As the attackers penetrate deeper into the network, the paper examines their motivations, which primarily revolve around exfiltrating valuable data for future extortion purposes. The study investigates the types of data stolen, ranging from personally identifiable information (PII) to financial records and intellectual property, and the potential impact of their exposure on both organizations and individuals.

Continuing the timeline, the paper delves into the ransomware deployment phase, where the attackers introduce Clop ransomware as a means to monetize their illicit activities. This section analyzes the characteristics and behavior of Clop ransomware, revealing its encryption capabilities and evasion techniques to evade detection by security solutions. The study proceeds to evaluate the extortion aspect of the incident, examining the communication channels used by attackers to demand ransom payments from the targeted organizations. It scrutinizes the ransom negotiation process, the ransom demands, and the consequences of non-compliance, such as the public release of sensitive data.

To conclude, the paper proposes a set of proactive mitigation strategies that organizations can adopt to defend against similar incidents. These strategies encompass vulnerability management, employee cybersecurity training, network segmentation, and the implementation of advanced threat detection and response mechanisms.

In essence, this paper serves as a comprehensive resource for understanding the MOVEit vulnerability and the chain of events leading to the insidious infestation of Clop ransomware. By exploring the attack lifecycle, analyzing its implications, and suggesting practical defense measures, this research aims to empower organizations to strengthen their cybersecurity posture and protect against emerging threats.

UNRAVELING THE MOVEIT VULNERABILITY: A JOURNEY FROM EXPLOITATION TO CLOP RANSOMWARE INFESTATION

Prashant Tilekar
Forescout Technologies

Bio:

My name is Prashant Tilekar. I have done my Bachelor of Engineering degree in Computer from Pune university (India). I have around 8 years of experience in cybersecurity. My previous company was Quick Heal Technologies, I worked there for around 6.2 years Then I joined Forescout in 2022 as Threat detection engineer. Throughout my career, I've noticed that I've always been good at learning new things. I like to write technical blogs and White papers on my research about new things in the conference as well. There are various achievements that happened in my life though as personally and professionally. I am comfortable working with the team and even completing the targets single-handedly.

THIS PICASSO IS A CON ARTIST – AN UPDATE ON THE LATEST GHOSTWRITER ACTIVITIES

Abstract:

Ghostwriter is a name used for a set of activities clustered around misinformation campaigns conducted by at least two threat actor groups, UNC2589 and UNC1151 (based on the Mandiant naming). Based on the previous research, the main goal of conducting the Ghostwriter malicious activities is to harvest journalist credentials in countries neighboring Belarus and using the credentials to publish news articles with false information about the events influencing relationships between the targeted countries. Since the beginning of the war in Ukraine, Ghostwriter activities have shifted their attention to the government, military and business users in Ukraine in Poland. These activities have been attributed by the Computer Emergency Response Team of Ukraine (CERT-UA) mostly to UNC1151. In the second half of the year, we discovered several new campaigns attributed to UNC1151, which allowed us to discover earlier campaigns, reaching back to April 2022. The campaigns were using official documents as lures with a multistage infection process that uses different techniques to drop and run a sample of previously undocumented .NET downloader, Picasso Loader. The loader is used to download, decrypt and reflectively load the final payload, which is appended to an image file and hosted by the infrastructure controlled by the attackers. The latest campaign (end of August, 2023), makes use of the vulnerability in parsing ZIP archives by the WinRAR archiver (CVE-2023-38831), allowing the actors to launch a Javascript equivalent of the Picasso loader in the background when a malicious ZIP file is opened by the victim. This last minute presentation will document the latest activities attributed to UNC1151. In addition to that we will provide attendees with the background information required to understand the wider context and the origin of Ghostwriter activities, which can be traced all the way back to 2016.

Vanja Svajcer
Cisco Talos

Bio:

Vanja Svajcer works as a Technical Leader at Cisco Talos. He is a security researcher with more than 20 years of experience in malware research, cyber threat intelligence and detection development.

Vanja enjoys tinkering with automated analysis systems, reversing binaries and analysing mobile malware. He thinks all the time spent hunting in telemetry data to find new attacks is well worth the effort. He presented his work at conferences such as Virus Bulletin, RSA, CARO, AVAR, BalCCon and others.

LAZARUS AND BLUENOROFF: NEW AND "RUSTY" TRICKS FOR MACOS

Abstract:

The notoriously flamboyant Lazarus threat actor group linked to DPRK has been targeting macOS users for some years now, employing various innovative techniques which successfully circumvent macOS' relatively robust in-built security. There is much to be learned by the researcher community by keeping a keen eye on the technical evolution of the group's TTPs.

The recent 3CX supply chain attack uncovered in March 2023 involved the use of infected dynamic libraries (dylib) packed within a signed-and-notarized application. Further back to last year, we saw the use of bona fide developer-signed Mach-O binaries in Operation Interception and the distribution of fake cross-platform electron-based cryptocurrency pricing applications in their Trader Traitor/Manuscrypt campaign.

Interestingly, a supposed sub-faction or splinter group of Lazarus, named Bluenoroff, has been held responsible for the April 2023 Rustbucket campaign making use of rust-based malware, a specially crafted PDF and a fake PDF reader to launch it.

All these campaigns have multi-stage payloads with forced C2 communications at each stage to retrieve the payload for the subsequent stage. The resultant longer kill chains imply that Lazarus/Bluenoroff do not want their precious weapons to be lying around just anywhere. The precision in terms of time and place for payload deployment complicates the analysis process and makes it harder to figure out their specific agenda. They are becoming more selective in terms of their targets, thus further reducing visibility.

This presentation will reveal the diverse range of recent macOS campaign TTPs of Lazarus and its offspring. We shall also explore potential counter tactics to head them off based on our analysis of the various levels of the attack chain.

Mellvin S
K7 Computing

Bio:

Mellvin earned his Bachelor's degree in Electrical and Electronics Engineering from Anna University in Chennai. Since 2020, he has been working as a Threat Researcher at K7 Computing's Threat Control Lab. In this role, his main responsibilities include reverse engineering and creating detection methods for various types of malware targeting both Windows and macOS platforms. His research findings are regularly featured on the technical blog page of K7 Threat Control Lab. Outside of work, Mellvin has a deep passion for playing cricket, where he excels as a fast bowler, and he also enjoys indulging in smartphone photography.

RISING TO PROMINENCE: A DEEP DIVE INTO TARGETCOMPANY'S EVOLUTIONARY PATH WITH MALLOX

Abstract:

TargetCompany, also recognized by the moniker Mallox, has been operating as a ransomware group for a significant period, positioning it among the most seasoned and unyielding factions to persist. Despite its discovery back in June 2021, TargetCompany has maintained its operational status and undergone transformation throughout, consistently assimilating novel methodologies to sustain relevance within the ever-shifting realm of cybersecurity. This presentation embarks on an exploration of TargetCompany's history, delving into the successive waves of its attacks and its adeptness in adapting to emerging challenges. Furthermore, an investigation will unfold into the sophisticated tactics that TargetCompany has embraced to elude discovery and heighten its effectiveness. Particularly notable is its implementation of Reflective Loading, alongside the deployment of multiple sets of tools for Defense Evasion and Reconnaissance, thereby amplifying its attack capabilities.

Earle Maui Earnshaw
Trend Micro

Bio:

Earle Maui Earnshaw is a member of the Threat Story Experts Team in Trend Micro. She has been serving the company for more than 5 years. Her area of focus includes File analysis and Threat Research, to understand and document how threat works and provide information for solution creation and blog articles. Other focus areas are Ransomware Decryption Analysis and Ransomware Campaign Investigation.

Nathaniel Morales
Trend Micro

Bio:

Nathan is an Electronics Engineering graduate and joined Trend Micro in April 2021. He is currently part of the Threat Hunting Team and contributes to the investigation and monitoring of new emerging cyber threats through the use of various sources such as OSINT, SOCMINT and Internal telemetry. Nathan is committed and dedicated to everything he does, especially in cybersecurity so he'll be able to help in making the cyberworld safe from threats.


K7 SECURITY
360°
360° Enterprise Cybersecurity from the Global Cybersecurity Pioneer
K7 Endpoint Security
Endpoint protection for
Windows | Mac | Linux
deployed On-premises or through the Cloud
K7 Cybersecurity Services
Vulnerability Assessment and
Penetration Testing | Governance,
Risk, and Compliance Consulting
www.k7enterprisesecurity.com

AVAR 2023

PANEL MEMBERS

PANEL DISCUSSION – POSITIONING CYBER SECURITY AS A CONTRIBUTOR TO STAKEHOLDER VALUE

Aloysius Cheang
Huawei

Anil Pais
Al Danube

Bio:

Aloysius is currently the Chief Security Officer for Huawei Middle East & Central Asia based in Dubai, the UAE covering 24 countries geographically and 57 countries functionally. Additionally, he is a Board member with a UK-based cyber leadership focused think tank, Centre for Strategic Cyberspace and International Studies (CSCIS), an ex-Board member of ISC2 Global and currently an advisor to the ISC2 UAE, Singapore and Taipei Chapters. In his career spanning over 22 years, Aloysius had delivering direct business values in strategic, complex, multi-year and multi-million-dollar technology and cyber program for Global 500 organizations worldwide, while managing large multi-cultural, multi-disciplinary team spread across 5 continents and 4 major time zones. He was a Co-Founder and Managing Director of Cloud Security Alliance APAC and was the Chief Standard Officer globally. Prior to the CSA, Aloysius was Worldwide Head for Security for Vodafone Global Enterprise and a Security Practice Leader with PricewaterhouseCoopers Singapore, having started his career with DSO National Laboratories in Singapore focusing on Defence R&D. As a globally recognized cybersecurity expert, Aloysius defined the term "Cybersecurity" having authored the first edition of ISO/IEC 27032 "Guidelines for Cybersecurity" and his professional perspectives are highly valued by major international media such as the BBC, Times, Wall Street Journal, ZDNet, ISMG, MSN News, CXO Insights, Teletimes International, Xinhua News, SCMP, Phoenix Media, The Hindu, The Nation, Bangkok Post, Economic Times Daily, China Times, The Straits Times, ChannelNewsAsia, Zawya, The National, Gulf Business, ITP, Telecom Review, Teletimes and Al Bawaba.

PANEL DISCUSSION – POSITIONING CYBER SECURITY AS A CONTRIBUTOR TO STAKEHOLDER VALUE

Illyas Kooliyankal
CyberShelter

Bio:

Illyas Kooliyankal is a Cyber Security leader with multi decade of experience in pioneering & leading multi-million-dollar transformation programs across institutions, including banking and ISPs. He has laid the foundation of digital secure landscape for prioritizing continuous business growth. Currently he is the Group CEO of CyberShelter Infosec Solutions. His core ideology is to transform & institutionalize a cyber-secure culture for defending the organizations against dynamic threat vectors. With his innovative approaches & proven experience with brilliant community services in the field of cybersecurity, earned him many awards, including CNME Middle East CISO 2021 and IDC Middle East CISO of the Year-2020. Illyas Kooliyankal is also a well-known speaker & writer. He has delivered keynote speeches at many international conferences and has penned down his unconventional & challenging prospective on cybersecurity through various blogs and magazines.

Awards

- CNME Middle East CISO of the Year Award Winner 2021
- IDC Middle East CISO of the Year Award Winner 2020
- CISO 100 Information Security Executive for year 2019 - MESA Awards
- CISO 100 Information Security Executive for year 2018 - MESA Awards
- CISO 100 Information Security Executive for year 2017 - MESA Awards
- EC Council Global CISO Award Runner up (USA)
- Computer News Middle East (CNME) – CISO Award 2018
- CISO 50 Awards for Year 2019
- CISO 30 Awards for the Year 2018
- CISO of the Year 2014 – ISACA

SOCIAL MEDIA

Facebook Account: https://m.facebook.com/cyber2050/

PANEL DISCUSSION – POSITIONING CYBER SECURITY AS A CONTRIBUTOR TO STAKEHOLDER VALUE

Javed Alam
DAMAC Properties

Dr. Mohammad Khaled

Bio:

Javed is a senior executive with 20 years of industry experience leading Cyber Security transformations enabled by digitalization, building effective, diverse teams, secure and compliant cloud migrations, zero trusts, fraud detection, end to end Payment System Security and innovations around threat detection & risk reporting automation. He leads from strategy definition to implementation and delivering value.

He held different roles in the field of Information Security and has spearhead Cyber security transformation or largest Fintech & Ecommerce in India.

As non-executive member he is supervising and advising bodies on their Cyber Security Strategy, IT governance for Startups, (IT) risk and compliance.

Currently, he is Director & Head of IT Governance & Security at Damac Group, Dubai.

PANEL DISCUSSION – POSITIONING CYBER SECURITY AS A CONTRIBUTOR TO STAKEHOLDER VALUE

Smith Gonsalves
CyberSmithSECURE

Bio:

Smith Gonsalves's fascination with computers began at only three years old, quickly evolving into a passion for mastering cybersecurity by his mid-teens. Over the past decade, Gonsalves has been instrumental in shaping security strategies for some of the world's top companies, ranging from hundred million dollar MNCs to billion dollar unicorn firms.

As a Virtual Chief Information Security Officer and Security Advisor, he has provided valuable insights to board members across diverse industries, including SAAS-based product companies, logistics, automobile, EdTech, pharma, BPOs, metal & steel, and oil & gas sectors.

Gonsalves established CyberSmithSECURE with the mission of helping corporates and MNCs protect their assets, manage compliances, and neutralize threats to their growth. Over the past three years, his company has successfully served over 200 companies.

His accomplishments in the field are notable. He is a CERT-IN empaneled auditor and has been honored with the CIO1000 Award 2021 by Enterprise IT World and named Cyber Soldier 2021 by CyberFrat. Gonsalves has trained over 25,000 individuals, including CIOs, CISOs, CEOs, and corporate professionals, in the realm of Cyber Security & Emerging Threat Landscape. He has also contributed as a reviewing author for various publications in the cybersecurity industry, including the book "Mastering Defensive Security" published by Packt.

Gonsalves holds prestigious certifications such as OSCP (achieved at 19), CISA, CCSK, TOGAF, CHFI, CEH, and CEH Practical v10. He is a respected figure in his field, often quoted in prominent newspapers like The Times of India and Mid-Day, and actively participates in research and CxO Conferences as a speaker or moderator. His expertise extends to managing organization-wide security, encompassing cloud, applications, APIs, and containers.

In essence, Smith Gonsalves has devoted his life to information security, leveraging his extensive experience and expertise to develop and implement cybersecurity strategies for his clients.

He encourages fellow cybersecurity professionals to connect for mutual learning and offers his expertise to organizations seeking to ensure compliance and complete security for their most valuable assets.

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

Anoop Kumar
GN Media – Gulfnews

Bio:

Anoop brought in his information security Governance, Risk and Compliance (GRC) Management experience to help GN Media to ensure Project Management and Operational Risk Management, cost reduction and improve People, Process and Technology performances. Over 20 years Information Technology (IT) GRC management experience enabling business-based decisions regarding Project Management, Defining Information Security Governance Risk and Compliance Strategies including Cyber Security Framework, curbing technology vulnerabilities & risk through effective risk & vulnerability management programs, vendor management & organizational leadership. Passionate, persuasive, articulated and communicated effectively with Technology & Business stakeholders to protect against reputational and/or financial implications. Anoop's experience derived from System Security Design, Administration and Integration in Manufacturing, Printing, Media Production, and Digital Media development and publishing with strong project management background:

- Developed IT Security Governance structure to reduce risks in business processes, enhance information security, and comply with regulatory requirements
- Defined GRC Strategy, framework and educated all involved parties followed by an internal certification program
- Defined cyber security strategy, policies, procedures and guidelines which includes identity access management, single sign-on, secure coding practices and continuous security integration in software and system development lifecycle
- Defined social media security and change management procedures, guidelines
- Defined Dev Ops environment security for better agile software development for faster release management
- Created and deployment of Security Awareness Program, Computer Incident Response Team, and Disaster Recovery / Business Continuity Plans to safeguard the organization

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

- Information security policy framework, Information security governance and policy creation Information Security Technology solution design, procurement and integration including contract negotiations and the development and management of strategic relationships

- Risk assessment and management, methodologies, quality assurance and cost reduction:

    - o Reduced weekly average incidents from 600 to 40

    - o Higher quality information—Integrated GRC process and controls allowed management to make more intelligent decisions more rapidly and reduced internal audit overhead

    - o Process optimization—Non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation

    - o Better capital allocation—Invest Business Cases are reviewed for identification of areas of redundancy and inefficiency allows financial and human capital to be allocated more effectively, saved over 4 million in 6 years which includes Microsoft licensing cost reduction, several other Hardware and Software infrastructure operational cost by consolidating system architecture

    - o Improved effectiveness and system sustainability—by practicing SIX SIGMA Failure Mode Effect Analysis (FMEA) activities means GRC activities are directed to the appropriate people and departments with right ownership and accountabilities

    - o Protected reputation—When risks are managed more effectively by proactive security testing and assessments both internal and external facing web technologies, company reputation is enhanced

    - o Reduced costs—Lower costs by security infrastructure consolidation and stringent Software license Management contributed to the overall ROI gains represented by effective GRC activities

- Practiced compliance guidelines for PCI DSS, NESA, DISA, SOX, GDPR, ISO standards and protected customer data and the business

- Project management of significant business projects balancing the cost, quality and on-time delivery

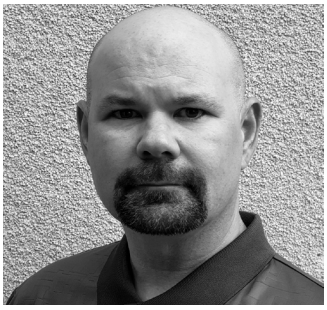
- Devised and managed change management program to ensure successful implementation

- Conducted several Threat and Risk Assessments and IT Security reviews to assess business and technology risks within the current operating model working major consultants like KPMG, Gartner, PWC, McAfee-Intel

- Mandiant and Verizon

- Worked with business units to identify their perceived threats to the integrity, availability, and confidentiality of their information assets

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS



David Brown
CyberGate

Bio:

David Brown is a visionary for a safer digital future, with a proven track record for reducing risk and improving security in information systems as a leading subject matter expert in cybersecurity, incident response, and threat intelligence. With over 25 years of experience in cybersecurity and intelligence-driven secure system design, Security and IT infrastructure architecture, and computer and network defense. He has created and operated defense-in-depth initiatives in the IT and OT space within government sectors of the US Department of Defense and the UAE to highly targeted global oil and gas enterprises.

Dr. Hamad Khalifa Al Nuami
Abu Dhabi Police General Head Quarter

Bio:

Head of Telecommunications Section Information Technology Center, Abu Dhabi Police General Head Quarter, UAE

In 2002 I Joined AD Police and started working as Network technician, at the same time, my passion for educational qualifications was under my target. Thus, I worked hard in parallel and earned my HD (Higher Diploma) degree at CNET from the HCT AlAin, as well as my Bachelor degree in computer Networking. In 2009, I moved to New York and applied for SU (Syracuse University) where I completed my Master Degree in Telecommunication Network Management. In 2018 I earned my higher degree in PHD Project Management from the British University in Dubai.

I attended more than 100+ events, workshops and conferences internally and externally and most of them were about Network Security and telecommunication as well as cyber security. However, my responsibility at AD police GHQ as telecom section manager make me always busy, I do have other role as a telecom committee manager for most of the events around AD city such as , Grand Prix Formula One event.

Founder of "Digital Barza" which has more than 100+ members to accelerate the process of sharing and exchanging the knowledge.

"The train doesn't stop at one station; it keeps on going, so work hard to achieve your targets one after another"

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

Dr. Hossam Elshenraki
Dubai Police Academy

Bio:

Current Position:

Associate Professor in Criminal investigation –Head of policing management &Social Sciences section – Dubai Police Academy

Career history:

- Criminal investigation: officer – Head of Unit – Head of Department from (1992:2004)

- Cybercrimes investigation officer (2004:2012)

- Police Sector Commander in united Nations Mission in Darfur (2012:2015)

- Head of Cybercrimes Criminal investigation Department in Ministry of interior in Egypt (2015:2018)

- Assistant Professor in Criminal investigation – Dubai police academy

Research Experiences:

- Published (7) researches in Cybercrimes field in law and police academies magazines (Sharjah police academy – Egypt police academy- Egypt school of law)

Academic Experiences:

- Lecturer in Egypt police academy in (raising awareness in the field of using internet)

- Lecturer in Police College (Cybercrimes investigation)for second grade with a book

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

- Lecturer in police training institutions in the field of (Cybercrimes investigation)

- Assistant professor in criminal investigation – Dubai police academy

Social Activities:

- Lecturer in "The program of protecting children on line"(for teachers – students- staff of schools)

- Member of the Arab League of cyber security in Lebanon related to The Arab committee for Arab Ministries of justice

- International trainer in the field of Cybercrimes investigation & criminal methods on the internet

- A book by (IGI GLOBAL)on Cyber Children exploitation

- Member in the official technical committee for preparing the cybercrimes law in Egypt

- Member in the official technical committee for preparing the Personal Data Protection law in Egypt

- Awareness lectures for school students & university students about cybercrimes and how to avoid to be a victim in Egypt & Dubai

Conferences:

- Contribute with work papers in more than (15) conferences in Egypt , Lebanon and Dubai in the field of cybercrimes investigation & Data protection by official institutions such(ITU-ARAB LEAGUE – EGYPT MINISTRY OF COMMUNICATIONS – UNIVERSITIES IN EGYPT)

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

Waqas Haider
HBL Microfinance Bank

Holger Unterbrink
Cisco Talos

Bio:

Holger is a longtime security enthusiast, with more than 25 years of experience in the information security industry. He started his career as a penetration tester and is now working for Cisco Talos as technical leader in the malware and threat hunting sector. He finds new, cutting-edge security threats and analyzes their components. Holger is a frequent speaker at international security conferences such as BlackHat, Recon, HackInTheBox, Internet Security Conference, NorthSec, CiscoLive and others. He is also the author of several offensive and defensive security tools and won the IDA plugin contest with his Dynamic Data Resolver (DDR) IDA plugin in 2020.

PANEL DISCUSSION – MITIGATING CYBER RISK FROM GEOPOLITICAL TENSIONS

Michael Daniel
CTA

Bio:

Michael serves as the President & CEO of the Cyber Threat Alliance (CTA), a non-profit organization that improves the cybersecurity of the global digital ecosystem by enabling high-quality cyber threat information sharing among cybersecurity providers. CTA's mission is to better protect end-users, enable the disruption of cyber adversaries, and elevate overall cybersecurity. CTA's members include more than 36 cybersecurity firms headquartered in twelve countries around the world.

Prior to CTA, Michael served as Special Assistant to the President and Cybersecurity Coordinator on the National Security Council Staff. In this role, he led the development and implementation of national cybersecurity strategy and policy, focusing on improving cyber defenses in the public and private sectors; deterring and disrupting malicious cyber activity aimed at the U.S. or its allies; and, improving the US's ability to respond to and recover from cyber incidents. Michael also helped craft the government's response to significant cyber incidents, such the attack on Sony Pictures Entertainment, the intrusion into the Office of Personnel Management, and the Russian efforts to meddle in our electoral process.

Before joining the National Security Council Staff, Michael served for 17 years in the Office of Management and Budget (OMB), including 11 years as the Chief of the Intelligence Branch in the National Security Division, overseeing the Intelligence Community and other classified Department of Defense programs.

Originally from Atlanta, Michael holds a Bachelor's in Public Policy from Princeton University, a Master's in Public Policy from Harvard, and a Master of Science in National Resource Strategy from the National Defense University's Industrial College of the Armed Forces. In his free time, he enjoys running and martial arts.

PANEL DISCUSSION – IMPROVING DATA SECURITY IN THE DIGITAL-FIRST ENTERPRISE

Anton Shipulin
Nozomi Networks

Bio:

Anton Shipulin is an industrial cybersecurity evangelist at Nozomi Networks, as well as the coordinator for the Middle East at the non-profit International Industrial Cybersecurity Center (CCI). He has been a cybersecurity specialist since 2005, working in the architecture, integration, and maintenance of cybersecurity systems, cybersecurity auditing, consulting and project management, the global industrial cybersecurity market and technology intelligence, analysis, and business development. He is passionate about industrial cybersecurity and critical infrastructure protection, knowledge, and information exchange, contributing to multiple industrial cybersecurity community projects. Anton holds professional certifications such as Certified SCADA Security Architect (CSSA), Certified Information Systems Security Professional (CISSP), and Nozomi Networks Certified Engineer (NNCE).

Bassil Mohammed
PwC Middle East

Bio:

A seasoned cybersecurity IT/OT GRC expert bringing 23+ years of hands-on consulting experience in cybersecurity strategy, transformation, risk and resilience. Worked across multiple strategic accounts in the Middle East, North Africa. Has deep understanding of market and clients' needs, emerging technologies, and increasing compliance mandates - introduced value add cyber security services; scalable assets across multiple industries.

Graduated with a BSc in Computer Engineering, followed by a master's degree (with a GPA of 4.0) in Information Security. PhD candidate holding several certifications in the areas of Artificial Intelligence (AI), Cyber Security Governance, Risk, Resilience, Compliance and Fraud management. This includes AI for Business Leaders, SABSA SCF, GICSP, CFE, CGEIT, CRISC, CISM, CISA, CDPSE, COBIT, TOGAF, CISSP, CHPCP, MS AZURE (900), MS AI (900) CBCI, & CCSP. In addition, Bassil is an active researcher with several publications in elite accredited journals on various cyber security.

PANEL DISCUSSION – IMPROVING DATA SECURITY IN THE DIGITAL-FIRST ENTERPRISE

Kiran Kumar
Help AG

Bio:

Kiran is a visionary security leader with a thought of building strong security work culture in the organization

Provide Threat Detection Assurance to more than 50+ customers

He manage security posture across the organization by implementing various cyber technologies

He is the speaker in multiple international cybersecurity conferences like HITB (Hack In The Box), COCOON, GRC Summit. SCADA summit, Financial cyber security summits, IQPC, e-crime, and ISACA ISAFE conference

He has multiple awards like MESA (Middle East Security Award) twice for implementing best security program in the region

He has Industry Experience: Technology, Retail & Supply Chain, Financial, Consulting, Manufacturing, Oil & gas, Federal, Telecom

He has certifications like CISSP, CISA, CISM, CEH, Integrated ISO Lead Auditor, SANS, PMP, C-CISO

Kumar Prasoon
Y100.ai

Bio:

Enterprise Digital Leader 2017 and Digital Retail Leader 2018 by MIT Sloan Review and the Khaleej Times plus CIO of the Year 2018 /2019/2020/2021, Kumar Prasoon is recognised as one of the Global Topmost CIOs in the Middle East and Africa (MEA), Asia and also at the international level. In this prominent role, he makes technology recommendations for the group's executive management on the aspects of Fuzzy Analytics, Business Intelligence; BigData, IoT /IIoT, BlockChain, cloud computing, enterprise 2.0, integrated systems architecture and virtualization. Being the founder of Fuzzy Analytics Framework and Modern Industrial Complex Mathematical Calculus for Emerging Technologies, Kumar is also the global leading Industry Researcher, Scientist and Technology Evangelist for Smart Systems, Smart Retailing, Smart Cities, Smart Parking, Smart Engineering, Smart Instrumentation, Smart Metering and Industry Quantum Mechanics employing the Modern Emerging Technologies. He chairs as an advisory board member with numerous national and international consortiums in the capacity of consulting, research and bringing supreme Industry Innovations. Another strong facet is his contribution to the Academia Sector for the Global Universities from Far East to West where he has mentored , coached and executed successful projects with hundreds of incumbents in Bachelors , Masters and Doctorates in Engineering , IT , Business and Management in the areas of Emerging Technologies, Emerging Markets and Emerging Systems.

PANEL DISCUSSION – IMPROVING DATA SECURITY IN THE DIGITAL-FIRST ENTERPRISE

Siham Benhamidouche
Schneider Electric

Bio:

Siham Benhamidouche has been working for more than 15 years in IT and Cybersecurity.

She started her career in Security at Areva T&D as Network Supervisor and then she became Telecommunication, Security and Messaging Manager to deliver all the security solutions (peripheric and end points) for a secure and performant network to more than 200 sites over the world. In 2012, she moved to Schneider Electric where she has taken over the role of Web Infrastructure Director, maintaining and leveraging Amazon cloud or hybrid model to deliver relevant and secure infrastructures to critical applications.

Since 2017, Siham is working as Digital Risk Leader, protecting all Schneider Electric's public facing footprint to secure interactions with Partners, distributors and Customers, and ensuring compliance with regulations as well as providing web security guidelines, standards and driving Cybersecurity awareness within the Global marketing practice. In 2019, she has also taken the role of Cybersecurity Officer for Middle East and Africa, where she is responsible for leading and implementing the Cybersecurity strategy across the zone, contributing to improve Schneider Electric's cybersecurity maturity and posture.

Simon Edwards
SE Labs

Bio:

Simon Edwards is the founder and CEO of SE Labs, a London-based company that specialises in advanced security testing. He provides tailored security advice to large businesses (CISOs) and more general technical advice to small businesses and individuals.

Simon focuses on cyber security and develops ways to test computer security products and services. He built and ran the world's first real-world anti-virus test and continues to innovate in testing that involves computer hacking.

A founder member of the Anti-Malware Testing Standards Organization (AMTSO), Simon has held a Chair position on its Board of Directors since 2012.

Simon features on the Cyber Security DE:CODED podcast (https://www.decodedcyber.com/), which provides security advice for businesses and individuals, recognising that people need security in both their work and personal lives.

PANEL DISCUSSION – EFFICACY OF REALWORLD TESTING FOR EDR AND XDR SOLUTIONS

Dr. Jason Zhang
Anomali

Bio:

Jason Zhang is the Director of Cyber Intelligence at Anomali. As a highly motivated cyber threat researcher and a proven product and technology pioneer, Jason has a wealth of experience in technology and product R&D. Prior to joining Anomali, Jason worked at VMware, Lastline, Sophos, Symantec and MessageLabs, specialising in cutting-edge research and automation in threat detection and intelligence analysis. Jason is a regular speaker at leading technical conferences including Black Hat, Virus Bulletin and InfoSec. Jason earned his Ph.D. in signal processing from King's College London & Cardiff University in the UK.

Michael Daniel
CTA

Bio:

Michael serves as the President & CEO of the Cyber Threat Alliance (CTA), a non-profit organization that improves the cybersecurity of the global digital ecosystem by enabling high-quality cyber threat information sharing among cybersecurity providers. CTA's mission is to better protect end-users, enable the disruption of cyber adversaries, and elevate overall cybersecurity. CTA's members include more than 36 cybersecurity firms headquartered in twelve countries around the world.

Prior to CTA, Michael served as Special Assistant to the President and Cybersecurity Coordinator on the National Security Council Staff. In this role, he led the development and implementation of national cybersecurity strategy and policy, focusing on improving cyber defenses in the public and private sectors; deterring and disrupting malicious cyber activity aimed at the U.S. or its allies; and, improving the US's ability to respond to and recover from cyber incidents. Michael also helped craft the government's response to significant cyber incidents, such the attack on Sony Pictures Entertainment, the intrusion into the Office of Personnel Management, and the Russian efforts to meddle in our electoral process.

Before joining the National Security Council Staff, Michael served for 17 years in the Office of Management and Budget (OMB), including 11 years as the Chief of the Intelligence Branch in the National Security Division, overseeing the Intelligence Community and other classified Department of Defense programs.

Originally from Atlanta, Michael holds a Bachelor's in Public Policy from Princeton University, a Master's in Public Policy from Harvard, and a Master of Science in National Resource Strategy from the National Defense University's Industrial College of the Armed Forces. In his free time, he enjoys running and martial arts.

PANEL DISCUSSION – EFFICACY OF REALWORLD TESTING FOR EDR AND XDR SOLUTIONS

Simon Edwards
SE Labs

Bio:

Simon Edwards is the founder and CEO of SE Labs, a London-based company that specialises in advanced security testing. He provides tailored security advice to large businesses (CISOs) and more general technical advice to small businesses and individuals.

Simon focuses on cyber security and develops ways to test computer security products and services. He built and ran the world's first real-world anti-virus test and continues to innovate in testing that involves computer hacking.

A founder member of the Anti-Malware Testing Standards Organization (AMTSO), Simon has held a Chair position on its Board of Directors since 2012.

Simon features on the Cyber Security DE:CODED podcast (https://www.decodedcyber.com/), which provides security advice for businesses and individuals, recognising that people need security in both their work and personal lives.

Righard Zwienenberg
ESET

Bio:

Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the Technical University of Delft. His interest thus kindled and studied virus behavior and presented solutions and detection schemes ever since. Initially starting as an independent consultant, in 1991 he co-founded CSE Ltd. In November 1995 Zwienenberg joined the Research and Development department of ThunderBYTE. In 1998 he joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer. After AMTSO – Anti Malware Testing Standards Organization - was formed, Zwienenberg was elected as president. He is serving on the board of AVAR and on the Technical Overview Board of the WildList. In 2011 Zwienenberg was looking for new opportunities and started as a Senior Research Fellow at ESET. In April 2012 Zwienenberg stepped down as President of AMTSO to take the role as CTO and later as CEO. In 2016 he rejoined the AMTSO board for another two-year run. He also is the Vice Chair of the Executive Committee of IEEE ICSG. In 2018, Zwienenberg joined the Europol European Cyber Crime Center (EC3) Advisory Group as an ESET representative.

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences – among these Virus Bulletin, EICAR, AVAR, FIRST, APWG, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, Government Symposia, SCADA seminars, etc. - and general security seminars. His interests are not limited to malicious code but have broadened to include general cybersecurity issues and encryption technologies over the past years.

PANEL DISCUSSION – EFFICACY OF REALWORLD TESTING FOR EDR AND XDR SOLUTIONS

Samir Mody
K7 Computing

Bio:

Samir Mody graduated from the University of Oxford in 2000 with a First-Class Master's degree in Chemical Engineering, Economics and Management. He spent over 9 years at Sophos UK, the final 3 as Threat Operations Manager of SophosLabs. Since August 2010 he has been running K7 Labs in Chennai, India. Samir has actively contributed to the IEEE Taggant System project and other industry collaborations such as AMTSO and CTA. He has co-authored and/or presented papers and participated in panel discussions at various international security conferences (VB, AVAR, EICAR). Samir's interests include reading (philosophy, politics, history, literature, and economics), sport and classical music.

AVAR

Association of anti Virus Asia Researchers

AVAR exists to prevent the spread of cyber threats by fostering international cybersecurity collaboration

The AVAR Platform

Knowledge Center

Professional Development

Networking & Partnering

Conferences & Presentations

Product Launches

Join AVAR Today!

Individual & Corporate Memberships Are Available

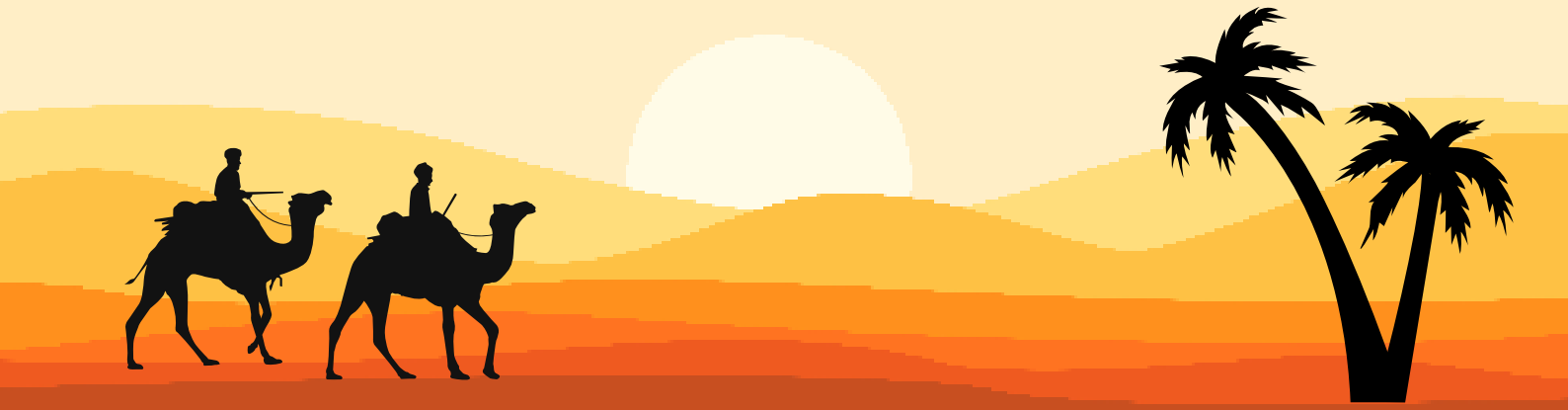
www.aavar.org

AVAR 2023

SECURE ECOSYSTEM: STRATEGIC, PRAGMATIC, FUTURISTIC

/avar-asia/ /avar_asia /aavar.org

www.aavar.org



26th ANNUAL CYBERSECURITY CONFERENCE