DECEMBER 2022

CTA IN FOCUS

CYBER THREAT ALLIANCE

LETTER FROM THE PRESIDENT & CEO

As we close out 2022 and look forward to 2023, only one thing seems certain: next year won't unfold the way many people think it will. The war in Ukraine, on-going tensions between the US and China, and the criminal ecosystem "arms race" could generate a wide variety of different incidents, effects, and trends. In that kind of environment, organizations like CTA play a key role by helping members manage and mitigate uncertainty.

We don't often cast intelligence sharing in those terms, but in fact, it provides a buffer against the unknown. The chances that any individual company will identify the latest threat or figure out the mitigation for a new vulnerability range from small to medium. However, the chances are effectively zero that any given company will identify, analyze, and respond effectively to every event in an uncertain environment on its own. Thus, cybersecurity companies face a tremendous amount of uncertainty.

As with risk management in general, a key tool for handling this kind of uncertainty is distributing it across a broader group. It's the same idea behind insurance. Looked at in this way, CTA membership provides a kind of insurance for cybersecurity providers. It increases the chances that you will become aware of a threat, vulnerability, or mitigation sooner and can address the threat, understand the vulnerability, or adopt a mitigation. It reduces the chance of surprise and increases the likelihood of effective response.

CTA currently provides this uncertainly buffer to 37 members from 12 countries; 18 are based in the US, while 19 are headquartered elsewhere. Among our members, we have network security firms, telecommunication companies, end point protection specialists, and industrial control system experts. Some are large, while others are small. Some focus on enterprise customers, while others target consumers. Taken together, this diversity reduces the uncertainty even more.

Being part of CTA offers many benefits. Among those benefits is an increased ability to manage the inherent uncertainty of cyberspace. We appreciate all those companies and individuals that already contribute to this work. If you are not yet part of the Alliance, we would like to talk to you and find a way for you to participate. We will never entirely eliminate risk or uncertainty from cyberspace, but CTA will continue to work hard to make that uncertainty as small as it can.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CTA WELCOMES MEMBERS AND ADVOCATES IN 2022

CTA is pleased to welcome seven new members to the Alliance this year, including Cloudbric, DataDome, Maltiverse, Nozomi Networks, and Trellix. (Our two latest members will be announced publicly soon.) We also welcomed six new partners and two strong advocates to our CTA Champion program, Craig Newmark and Andrew Grotto.

Welcome all to the CTA! We look forward to working with you to increase the level of cybersecurity across the digital ecosystem.

MEMBERS

cloudbric
DATADOME
maltiverse
NOZOMI NETWORKS
Trellix

PARTNERS

E-ISAC
GASA Global Anti-Scam Alliance
H-ISAC HEALTH · ISAC
KrCERT/CC
quad9
SIGHTLINE SECURITY

CYBER THREAT ALLIANCE
CTA CHAMPION

Craig Newmark
Web pioneer, philanthropist, and leading advocate

Andrew Grotto
Dir., Stanford Program on Geopolitics, Technology and Governance
Stanford University

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>10 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	32%
IP ADDRESS	18%
DOMAIN NAME	5%
URL	3%
NETWORK TRAFFIC	35%
FILE PROPERTIES	6%
HOST	1%

TOTAL EARLY SHARES

3-5
PER WEEK

725+

CTA Member Feature

CHANGING ATTACKER BEHAVIOR HIGHLIGHTS THE IMPORTANCE OF INFORMATION SHARING

BY CAITLIN CONDON
SR. MANAGER, SECURITY RESEARCH

The past few years have witnessed a convergence of major attack trends that shaped the security landscape with blunt force. In 2021, zero-day exploitation hit an all-time high, ransomware business models matured and expanded with devastating effect, and organizations were plagued by widespread attacks on business-critical technologies.

The security landscape in 2022 has been marked by more nuance and only slightly less over-the-top bombardment. As of this writing, only 20% of the vulnerabilities Rapid7 researchers tracked as high-priority risks this year were confirmed to have been used in ransomware attacks, compared with more than 40% in 2021. And while the overall number of confirmed zero-day attacks appears to be smaller this year, attackers are still leveraging flaws quickly; more than half of the vulnerabilities we've analyzed in 2022 were exploited within a week, and "0" is still the most common value in our time to known exploitation dataset.

It's unlikely that ransomware is in decline, or that adversaries have tempered their use of novel attacks. It's more likely that fewer organizations are reporting ransomware incidents, whether out of fear or because evolving tactics have lowered confidence in intrusion and detection timelines. In the wake of Log4Shell, we've also seen collective overhype on "4Shell-like" vulnerabilities that ultimately posed nowhere near the risk of their predecessor — but whose notoriety distracted organizations from more mundane yet more important forms of risk.

As we at Rapid7 like to note, however, there have been some silver linings to the last several years of lightning-fast exploitation and at-scale attacks. One of the brightest is a renewed focus on information sharing, from open platforms for vulnerability research and fresh ways of tracking known-exploited CVEs to broad, collaborative recommendations on shoring up defenses and combating ransomware.

We hear consistently from practitioners that they're too overwhelmed and under-resourced to make cybersecurity a passion pursuit. They want to be able to do their jobs and log off at a reasonable hour, and they need tools and risk-based intelligence that make their work simple. As we look to 2023 and beyond, we need continued information and intelligence sharing, not only so we can understand the trends that make security hard, but so we can continue to build innovative solutions to make it easier.

CTA Member Profile

MEMBER SPOTLIGHT: REVERSINGLABS

ReversingLabs, the software supply chain security platform for Dev and SOC teams, is proud to be a member of CTA — a role we have held since 2016.

The partnership with CTA has allowed for the consistent exchange of high-quality data, in which ReversingLabs uses our Titanium Platform to analyze the files given to us by the CTA. With the most mature engine and the largest file repository of its kind, ReversingLabs values its CTA membership to continue this important work.

CTA serves as an important source of data for ReversingLabs' goal of increasing the coverage and quality of our malware repository. ReversingLabs digests around 30,000 files per day from the CTA, which are processed with our proprietary automatic static and dynamic analysis before being shared with our customers via ReversingLabs' Titanium Platform.

ReversingLabs is honored to contribute its resources back to CTA as a proud member of this organization. On a daily basis, ReversingLabs shares around 8,500 analyzed samples daily with CTA, making us one of the top 10 contributors to CTA. And ReversingLabs is working to expand this sharing to include network indicators of compromise (IoCs), as well.

At a time when the threat landscape continues to change, ReversingLabs is thankful for its CTA membership, and looks forward to continuing this fruitful collaboration.

BY ZORAN ZIZEK
SR. PRODUCT MANAGER

CTA Member Feature

CISCO TALOS: LESSONS LEARNED FROM THE WAR IN UKRAINE

Cisco Talos has had the privilege of working with and supporting our partners in Ukraine this past year during the Russian-Ukraine war. We have seen numerous attempts to take down critical infrastructure within Ukraine as efforts to weaken the state and its people. In light of this, Ukraine has been largely successful in repelling these attacks, or quickly recovering when the attacks were successful, and we have yet to see any major disruption like we did in the 2017 NotPetya cyber-attack. While the world must remain vigilant as this conflict continues into the new year, there are several lessons to be learned.

We cannot underestimate the preparedness of Ukraine when it comes to cyber defense. Ukrainians have had ample training in the disruptive power of cyber-attacks since the initial Russian invasion of the Crimea peninsula in 2014, the Black Energy and Industroyer attacks in 2015, NotPetya in 2017, and other less-well known attacks. They don't hope for the system to hold up, they expect it will be attacked and are trained on what to do when that happens. They have built a layer of resilience into not only their environments, but also into the people who handle those environments. The strong public-sector support from the Cyberpolice Department of the National Police of Ukraine and State Special Communications Service of Ukraine (SSSCIP) is another key factor in extending these lessons into the private sector.

Secondly, tying cyber-attacks to kinetic war outcomes has been more difficult than presumed. While there was certainly a large amount of wiper malware attacks during the initial invasion, and we currently see an increase in successful attacks against critical infrastructure, it has not turned the tide of the war. This could be because the Russian armed forces needed access to the same infrastructure and would not risk taking it out, or because it's much harder and more costly to take out critical infrastructure at a precise and indicated time. It takes time and energy for sophisticated threat actors to get and then maintain a foothold within a system without being noticed by users and security professionals. As the battlefield moves and shifts, it's possible that cyber threat actors can't establish access quickly enough in the systems where needed.

Finally, behind the scenes intelligence sharing with partners and governments across the globe is having a real impact. There remains the possibility of larger collateral damage on the world stage, especially as the conflict drags on. However, it is clear that the combined defense between partners and government agencies to share information on what they are seeing, and to take action against it, can continue to do good.

BY AMY HENDERSON
DIRECTOR OF STRATEGIC PLANNING &
COMMUNICATIONS, CISCO TALOS

CTA Member Feature

2022 YEAR-END MEMBER PERSPECTIVES: WE ARE STRONGER TOGETHER

SONICWALL®

Year 2022 has so far been a year of data breaches, crypto hacking/theft, massive zero-day exploitable RCE vulnerabilities and the usual variations of ransomware, either targeting specific organizations or being deployed in mass volume attempting to compromise large numbers of random victims. Even the war in Ukraine was not limited to just military operations; it included cyber warfare targeting critical civilian and communication infrastructure.

Even though the log4J vulnerability was first exposed at the end of 2021, its exploitation continued in large volumes well into 2022, and even months after the disclosure, a significant number of log4j library instances remained unpatched (ref: Qualys research report), thus making perimeter and server agent-based security products the only components protecting the server infrastructure. Prompt response and information sharing among security vendors is absolutely critical in such instances and could be the key difference between successful and failed exploitation attempts. Knowledge of vulnerability details, exploit permutations, known post-infection activity, and common post-exploitation artifacts is key to stopping such attacks.

The malware threat landscape continued to feature initial delivery vectors of what's commonly perceived as benign files (office, pdf files), as well as script based initial attack vectors (usually sent inside of archives), thus allowing attackers a greater chance to bypass certain security and filtering mechanisms and increase the chances of unsuspecting victims actually opening the files. Timely sharing of newly discovered and variations of existing attack delivery vectors can greatly enhance efficacy of security products and enable development of generic protection techniques that would stop future attack permutations.

Targeted attacks, including network breaches, continued to use social engineering techniques as well as known and zero-day unpatched vulnerabilities to gain access and obtain necessary credentials for lateral propagation inside the network, followed by deployment of ransomware and data exfiltration malware. Knowledge of how various threat actors operate is extremely helpful in identifying any potential breaches early in the process, keeping the compromise to a minimum.

CTA brings security vendors together and not only enables information sharing among them, but also introduces them to valuable third-party information sources, including government sources, which allows critical information necessary to create protection techniques and identify potential breaches to be accessible quickly and easily.

BY ALEX DUBROVSKY
VP SOFTWARE ENGINEERING
& THREAT RESEARCH

cloudbric

Recently, the Hybrid Multi-Cloud has come to be recognized as an ideal IT model and strategic alternative for the contact-free era. Hybrid Multi-Cloud is economically more efficient, and enterprises can quickly expand their resources to process large data while it maintains the security of core business and manages and performs backups for critical data.

However, as more use cases have been reported, more cybercriminals are shifting their attention towards the critical data within the multi-cloud. Because enterprises handle various types of confidential information, they must acknowledge the necessity of "cloud security," and proactively prepare against cyberthreats.

There are many security companies that provide services for enterprises to achieve cloud security, but for these companies to provide their services, they require accurate, massively aggregated threat information. It can be difficult for the security companies to aggregate enough threat information that they can apply effectively. However, the Cyber Threat Alliance can provide a solution.

CTA is a non-profit, international organization founded with the purpose of solving cyber threat issues using the core principle of cooperation and next-generation security governance. CTA aggregates threat information collected from its members every day, enabling members to update and advance their threat intelligence and detection capabilities to reinforce the cyber ecosystem. All CTA members are required to provide a minimum quantity of high-quality threat information which also suggests that even becoming a member of the alliance is impressive and notable.

Cloudbric joined CTA as a member in 2022, providing and sharing threat intelligence since. The threat intelligence shared by CTA is used to upgrade the security level of Cloudbric's own rule set used for web security. Through testing, we were able to see that the detection rate of several rule sets, including the Malicious IP Reputation rule set showed significant improvements with the threat intelligence shared by the CTA.

As a member of CTA, we feel pride in taking part in improving the cybersecurity level worldwide. Like an old African proverb, says, "If you want to go fast, go alone. If you want to go far, go together." Cloudbric is honored to join the never-ending battle against hackers, and we hope to stand together to the end.

BY MINJUNG YUN
CHIEF PRODUCT OFFICER

CTA Update

CTA PROUDLY ENDING THE YEAR ON A SERIES OF WINS

CTA is very proud to be named **Cyber Not For Profit Team of the Year** by the independent, UK-based Cyber Security Awards. The winners are among the best in the information security industry. This award is a direct reflection of the commitment made by all 37 CTA members to come together to protect the digital ecosystem.

We are also excited to share that our president and CEO, Michael Daniel, is a recipient of a Cybersecurity Visionary award in this year's CyberSoop50 awards, as well as a recipient of Homeland Security Today's 2022 Mission Awards for his contributions to keeping America safer from myriad threats.

Congratulations to all for these momentous achievements!