DECEMBER 2021

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

Long-term, effective alliances are rare in many industries. They are tough to build and difficult to maintain. They require a large up-front investment to get off the ground, but they also need sustained engagement to keep going. Alliances must maintain a common mission, even if the way individual members might go about achieving that mission is different. The return on investment can be difficult to quantify and is often not immediate. Once the "latest shiny object" aspect has worn off, getting attention for an alliance's work can prove challenging. They also have to carefully navigate legal boundaries and ensure equity among members. Finally, the trust that makes an alliance viable takes time to build but is easily lost.

CTA was built to meet these challenges head-on. This quarter's newsletter showcases various ways that CTA works as an alliance. For example, we profile several Board members who have personally invested in CTA over an extended period of time – and why they have chosen to make that commitment. We have articles from TEHTRIS and K7 that illustrate the return their companies receive from participating in CTA. Similarly, Patrick Donegan, a CTA champion, argues that increased telecommunication company participation in CTA would mutually benefit those companies and the alliance. Scott Algeier with the Information Technology ISAC describes how our common mission and philosophy enables our organizations' mutually beneficial partnership. SecurityScorecard explains how CTA's policy advocacy work fits with its approach to improving our digital ecosystem's security. Lastly, the newsletter's summary statistics show that CTA continues to attract new members, improve its offerings, and command attention long after our launch nearly five years ago.

Of course, we have no intention of resting on our laurels, because an alliance's value can easily erode. Looking forward to 2022, we will deploy new features on our automated sharing platform, enabling us to gain more insight into the data members share with us. We will continue to seek improvements to the quality of our shared information. We will maintain the regular interaction among our member companies that promotes trust. We will invest in projects that will demonstrate the potential insights combined information can generate, even if the individual information bits are already publicly known. And we will continue to participate in industry-wide endeavors to improve our resilience against malicious cyberactivity.

Many alliances and partnerships fade quickly after they are announced. CTA is a different type of alliance, one built for performance and endurance. To those of you who are already part of the alliance, I thank you for your on-going support. For those considering membership, come join us in our efforts to improve the security of our digital ecosystem. This alliance is here for the long run.

J. Michael Daniel

President & CEO, Cyber Threat Alliance

CTA BOARD DIRECTORS SPOTLIGHTS

The Cyber Threat Alliance Board of Directors are cyber industry leaders who have made tremendous impact across the industry. In an effort to learn more about these impressive cybersecurity visionaries, we are spotlighting these luminaries. Read HERE for the first three director profiles.

Corey Thomas
Chairman & CEO, Rapid7

"I am incredibly impressed, not only with the information and threat sharing, but especially the collaboration on threat analysis. By sharing and working together, organizations and companies around the world can better protect the digital ecosystem."

John Petrie
Counselor to the NTT CISO, NTT Ltd.

"We, as corporations, cannot defend against all the attacks from around the world alone. We must work together. Participation in the CTA allows us to do just that."

Dr. Dorit Dor
Chief Product Officer, Check Point

"The growing cyber threat landscape cannot be solved by one individual or company, and we need to work together to battle the rising cyber threats across the world."

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>6 MILLION
MONTHLY AVERAGE

KILL CHAIN DIVERSITY
(3 MOS AVERAGE)

RECONNAISSANCE	1%
WEAPONIZATION	>0%
DELIVERY	6%
EXPLOITATION	16%
INSTALLATION	53%
COMMAND + CONTROL	22%
ACTIONS ON OBJECTIVES	2%

NOTE: Every IoC submitted to CTA must be associated with a kill chain phase.

TOTAL EARLY SHARES

3-5
PER WEEK

525+
IN THREE YEARS

DEVIN LYNCH
SENIOR DIRECTOR, POLICY &
GOVERNMENT AFFAIRS

SecurityScorecard

CTA Member Feature

CYBERSECURITY IS A TEAM EFFORT

At SecurityScorecard, our mission is to make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risks to their boards, employees, and vendors. This is a lofty goal, but it is foundational to our work, resonates deeply, and guides everything we do.

It is a key reason we joined the Cyber Threat Alliance (CTA)- to improve the cybersecurity of the global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing across not only the cybersecurity practitioner community, but among corporate and government executives as well. Working with the CTA aligns with our mission by allowing us to build connections with like-minded organizations, leverage our technology, data, and analytic capabilities to support CTA's own important mission, and work together to solve problems.

Cybersecurity is a team effort that involves different levels of risk management. As each of us protects against risks and malicious threat actors, in a manner commensurate with our risk appetite, we can only defend against what we know. Partnering with CTA allows us to collaborate in an information-sharing environment that makes its members smarter and more informed, strengthens our platform and therefore supports our customers' cyber health and the health of their entire cyber ecosystem. CTA working groups, such as the Public Policy committee, allow us to learn, share, and discuss the dynamic cybersecurity policy issues affecting our industry, and position us to adapt and pivot to meet all new mandates and regulations in this dynamic policy space.

It is in this area of policy leadership where we believe CTA is strongest, and where we are most excited to see CTA's future success evolve. As administrations change, and the breadth and speed of cybersecurity threats and proposed solutions emerge from all corners of Washington, we believe coalitions like CTA support policymakers and industry by helping them first identify and better understand the problems we face and then guide them toward data-driven solutions based upon industry-led best practices. CTA's collaborative and non-partisan approach enables candor and builds trust among alliance members.

CTA also creates a space for public-private collaboration and communication of threat information that will contribute meaningfully to future policy solutions. The dynamic nature of cybersecurity, which includes the persistent advancement of technology and evolution of threat vectors, demands a rapid, transparent, and collaborative effort to mitigate against malicious outcomes.

We believe the CTA is best positioned to be this collaborative entity, and we are proud to share our threat information and to partner with this august group.

CTA Member Feature

COLLECTIVE INTELLIGENCE FOR A SAFER INTERNET

The increase in the number and complexity of cyber attacks, along with the maturity and impressive organization of hackers today, imposes new challenges on companies. They have no choice but to innovate continuously, in order to extend their capacities of anticipation and detection of cyber threats.

Tomorrow's cybersecurity will have to be collaborative and cooperative: creating a consortium of experts working towards the same goal, while bringing together some of those experts, is key to serve the interests of everyone.

Threat landscape

The professionalism of groups operating ransomware, the maturity of hackers and their new organizational capacity (e.g., cartel formation, RaaS, etc.) justify the necessity of joining forces to better anticipate, prevent, and neutralize threats.

If we were to summarize the current panorama of the most feared threats, it could be presented as follows: ransomware attacks, supply chain attacks, and denial-of-service attacks. Even if the most important threat in volume is still the denial-of-service attack, which is the easiest to implement for novice attackers or unscrupulous competitors, it is obvious that ransomware attacks are of particular concern.

However, one of the emerging threats of the last 12 months is undoubtedly the one targeting software supply chains. Everyone remembers the attacks against SolarWinds and Kaseya, which impacted more than 20,000 large companies and administrations worldwide, including very sensitive entities, such as certain critical government services.

Collective defense: the solution is the CTA

TEHTRIS actively contributes by participating in the Cyber Threat Alliance. The primary objective of the CTA is to give each member access to quality cyber intelligence via a shared platform maintained by the consortium. This platform automates the collection and the contextualization of information on threats.

Thus, cyber intelligence, which was previously abstract or unknown to some, becomes concrete, contextualized and immediately exploitable: it can be activated to improve analysis, detection, and deployment of response strategies to better protect the ecosystem. More generally, this initiative allows harmonizing the quality of exploitable cyber intelligence, extending its use to as many people as possible, and thus strengthening our ability to fight cybercrime.

This project is completely in line with TEHTRIS' sharing values. On the one hand, it allows us to improve the quality of our cyber defense arsenal, for better service and protection of end users, and on the other hand, to have a better knowledge and understanding of the cyber threat environment by strengthening our knowledge of exploitable intelligence as well as continuing our work to improve our tools and services, particularly through automation and reduction of detection & response time. The security, availability and integrity is ensured. Sharing information in real-time between partners, with the same background or not, will enable us to provide a high-quality service.

The latest attacks show the need to have ever more robust solutions, like what TEHTRIS provides for its customers. TEHTRIS' position is based on the implementation of resilient solutions for the protection of systems.

Conclusion

With an increasingly hostile environment and a growing attack surface, there is no choice but to innovate. Collaboration will be the key to success. TEHTRIS understands this and has integrated Open Innovation into its global corporate strategy.

Authored by the TEHTRIS Team

<TEHTRIS>
FACE THE UNPREDICTABLE

SAMIR MODY
VICE PRESIDENT THREAT RESEARCH

K7 COMPUTING

CTA Member Feature

WE NEED MULTI-DIMENSIONAL VISION

It might be a cliché but today's cyberthreat landscape is a complex and dangerous place, with the range, depth and scope of attacks increasing in sophistication and impact, seemingly on a minute-by-minute basis.

The Internet is the global arena for millions of these cyber assaults involving all manner of digital infrastructure from Industrial Control Systems (ICS), to cloud and enterprise servers, to IoT devices and personal PCs and smartphones, etc. The adversaries are state-sponsored groups, organized cybercriminals, terrorists, and hacktivists, all with highly diversified motives, and their targets are governments, institutions, enterprises, and ordinary netizens world-wide.

In this milieu we, the defenders, the good guys, have our work cut out to protect the global netizenry 24/7/365. No single cybersecurity provider can possibly have visibility of all attacks across all technologies and platforms, geographies, and, of course, time, regardless of the adversary and target victim. If we can't see it, we can't smite it.

Enter CTA! CTA provides its members with Multi-Dimensional Vision. CTA's membership encompasses great diversity including providers of Endpoint Protection, Network and Cloud security, and even ICS and IoT security, across continents and time zones, each of whom shares automated Cyber Threat Intelligence (CTI) data, i.e. its current "visibility", in real-time on CTA's Magellan platform to be distributed to all other members. Human sharing of CTI takes place both via "Early Shares" of research content and IoCs well before they go public, as well as via people-to-people discussions within confidential Algorithm and Intelligence Committee meetings Further to this CTA has forged lasting relationships with governmental and institutional partners who share valuable information, thus adding yet another dimension to our multi-dimensional visibility of cyber attacks. All of this allows CTA members to provide more robust and comprehensive cyber protection for their respective users, in a united and combined effort to fight cyber adversaries to fulfill our bounden duty, to execute our mission, of safeguarding the digital, and even physical, lives and rights of global netizens.

CTA Champion Feature

EXTENDING TELCO CTI SHARING

By Patrick Donegan, Founder & Principal Analyst at HardenStance

I spend quite a lot of my time working within the telecom sector- the unwitting conduit for most of the cyber attacks that are delivered into our environments. One of the challenges telcos face is to take a broader view of cyber security risk to their business and their customers beyond just the telecom network infrastructure itself.

This is something that has become even harder in recent years due the disproportionate attention paid by politicians and the media – hence by telcos themselves – to the risk from deploying Chinese products in their telecom infrastructure. Every politician has an opinion on Huawei. But hardly any are familiar with real world attacks like 'Operation Soft Cell', disclosed in 2019, which saw Chinese hackers exfiltrate Call Detail Records (CDRs) from ten telco operating companies, via an initial foothold gained in an externally- facing web server.

Telco security professionals do a pretty good job of sharing threat intelligence amongst themselves. For example, they collaborate really well at a peering level to protect against DDoS attacks. The fact that MIRAI hasn't been used to generate anything on the scale of the 2016 attacks is in no small part due to collaboration among telcos- domestically and at the international level.

There are nevertheless two areas where the telecom sector needs to make a lot more progress in threat intelligence sharing. The first is with other sectors of industry. A telco's office IT is potentially just as vulnerable as a bank's or an automotive manufacturer's. And as 'Operation Soft Cell' showed, lateral movement by threat actors from IT into OT is every bit as much of a risk to a telco as it is to any other organization. The second area where progress is needed is internally. Most threat intelligence teams in telcos are not engaging effectively enough with business leaders within either the office IT or telecom infrastructure domains today- let alone across those two equally important domains.

The Cyber Threat Alliance already has members that are either telcos, telco affiliates or organizations with ownership links to telco groups such as AT&T Alien Labs, ElevenPaths, NTT and Verizon. Telcos looking to extend best practice cyber security from their telecom infrastructure to their office IT should take a look at how CTA and its members can potentially help.

CTA Partner Feature

COLLABORATION IS ESSENTIAL IN CYBER DEFENSE

By Scott C. Algeier, IT-ISAC Executive Director

Active participation in organizations that share cyber threat intelligence, including threat actors' tactics, techniques, and procedures, can reduce a company's cyber risk. Collaborating with analysts from peer companies serves as a force-multiplier to your security team. It lowers the cost of defense by providing access to intelligence and mitigations from trusted peers, without having to invest in a host of additional expensive tools. Quite simply, companies are stronger together than separately. This is why active participation in established information sharing forums is increasingly considered by policymakers to be an essential component of a sound cybersecurity program.

In the same way, collaborating across industries and information sharing communities is essential in order to mitigate today's unrelenting cyberattacks. This is why the IT-ISAC actively partners with like-minded organizations. Effective operational partnerships provide a scaling capability that enables us to share information with the larger cybersecurity community, to engage analysts across the globe, and to receive active threat intelligence. Partnerships with organizations such as the National Council of ISACs, the Cyber Threat Alliance and The CompTIA ISAO, among others, are core to our mission. These partnerships improve the security of individual corporate networks and the critical infrastructure community collectively.

In addition to partnering across information sharing organizations, the IT-ISAC itself supports three critical infrastructure sectors--IT, Elections, and Food and Agriculture. "Information Technology" has evolved since our founding over 20 years ago. So has our membership, which includes hardware manufacturers, software companies, threat intelligence providers, cloud and SaaS providers, operational technology, smart manufacturing and other technology companies. In addition, our Elections Industry Special Interest Group provides a trusted forum for election technology companies to collaborate on a range of security issues impacting the industry--from finding and mitigating vulnerabilities to identifying and stopping attacks on corporate networks. Companies in the Food and Agriculture industry share intelligence on unique threat actors targeting the industry, as well as specific mitigations to ward off attacks.

Collaboration is essential in cyber defense. Not only does it make it easier for an organization to protect itself, but it is also a relatively low-cost way to fulfill gaps in security operations. As one of CTA's guiding principles states, intelligence sharing is for the greater good. The stakes are high--the future of cyberspace depends on the good guys to work together. If your organization is not already active in an information sharing community, it is not doing all it can to defend itself.