JUNE 2022

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

This quarter's newsletter highlights one important aspect of CTA's value to the digital community – sharing during a crisis. When a crisis hits, sharing intelligence becomes even more important than normal. However, you don't want to be exchanging business cards during a major cyber event and you don't have time to review, cross-check, and get comfortable with new people and organizations during such stressful times. That's where organizations like CTA come in. We build the trust community and establish the communication links before a crisis occurs. We create the structures and policies that make sharing during incidents easier, and we enable intelligence to reach more organizations faster than what occurs through ad hoc, informal networks.

Of course, such informal networks will always exist and they play an important role in crisis response. Being able to work with such groups is critical in responding effectively to malicious activity. But they cannot replace formal sharing organizations like CTA. That's why cybersecurity providers need to make sure they have access to both kinds of networks for when that inevitable bad day happens.

While crises are unpredictable, other events occur on a regular timeline. Every year, we elect two representatives from among our affiliate member companies to serve a two-year term on CTA's Board of Directors. This year, two board members are stepping down and two new members are joining the board. Our outgoing members are Corey Thomas and Joe Levy. Corey, CEO of Rapid7, has been a strong supporter of CTA from the beginning and has served on CTA's Board of Directors for over four years. Joe, CTO for Sophos, has contributed significantly to CTA's success as an organization and he has been on the Board since 2019. Corey and Joe have consistently provided wise counsel and thoughtful input, helping guide CTA in its first years as a formal organization. I want to thank them personally for their advice and guidance.

It is also my pleasure to welcome two new members to the CTA Board, although they are hardly new to CTA. Jaya Baloo, Chief Information Security Officer at Avast, and Joe Chen, Vice President of Engineering at Broadcom Symantec, will join the Board at this quarter's meeting. I have worked with both Jaya and Joe for some time now, and Joe was instrumental in getting CTA started as a formal organization back in 2016-2017. I am looking forward to working with both of them in their new CTA capacity.

As this newsletter highlights, unplanned crises and gradual evolution will always co-exist among cyber threats. CTA exists to combat both kinds of threats. While we may not be able to predict exactly when the next crisis will occur, we can be confident that one will happen. When it does, CTA will be ready to do what it does best – enable network defenders of all kinds to share the information they need to combat the threat and mitigate the crisis.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

INCIDENT RESPONSE BLOG: CYBER INCIDENTS IN UKRAINE

It's hard to imagine a better example of the importance of sharing threat intelligence during a crisis than the current Ukraine Russia conflict. Cybersecurity companies are reporting various cyber-attacks targeting organizations in Ukraine, including government agencies and critical infrastructure companies.

Cyber Threat Alliance members stand ready to respond and collaborate on all cyber incidents related to this activity. CTA has put together a compilation blog of our members' blogs posts and links to articles concerning cyber activity associated with the Ukraine conflict. CTA members also share pre-release blogs through CTA's Early Sharing program. Such sharing helps ensure that industry response efforts coincide with the most up-to-date understanding of these threats. CTA will continue to update our incident response blog while we monitor any new events that may occur regarding Ukraine.

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>11 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	35%
NETWORK TRAFFIC	32%
IP ADDRESS	16%
URL	6%
FILE PROPERTIES	5%
DOMAIN NAME	4%
HOST	3%

TOTAL EARLY SHARES

3-5
PER WEEK

630+

Symantec
A Division of Broadcom

JOE CHEN
VP ENGINEERING
BROADCOM

CTA Member Feature

CTA – MAKING THREAT INTELLIGENCE SHARING WORK

Symantec, now a part of Broadcom Software Group, helped found the Cyber Threat Alliance with the mission to share threat intelligence to protect the mutual customers of our members. When we think about the value we get, one benchmark we use is: Are our customers receiving faster protections?

A special part of CTA is the robust early sharing program that offers members early access to research from other members. This allows members to check and add protections before the rest of the industry even sees the research. When customers ask us about newly published research, we can easily tell them we have already seen it and have protections in place. At Symantec we have a goal to share all of our research with other members before publication because we see the value it provides us on the other side.

The relationships we've built through the CTA and the mutual trust between members allows early research sharing to be successful. And beyond that, it puts members in a position to work together in a time of crisis. Since we regularly collaborate in a steady state, it makes us comfortable to jump into action together to respond to a cyber incident. A recent example of sharing during an incident was the 2021 Log4j vulnerability. One of our researchers recalled when the news of the vulnerability first broke. The influx of research from fellow members allowed us to more quickly add and improve detections on top of the research our teams did independently.

During global events like the Log4j vulnerability, the recent Ukraine and Russia conflict or the Covid pandemic, CTA enables collaboration, and that allows all members to have a quicker response to cyber threats than we would on our own. Symantec is proud to be a part of this program that protects our mutual customers and creates good will.

CTA WELCOMES NEW BOARD MEMBERS

We are pleased to announce that Jaya Baloo, Chief Information Security Officer, Avast, and Joe Chen, Vice President of Engineering at Symantec, a Division of Broadcom, have been elected as Affiliate Directors to the CTA's Board of Directors for a two-year term. "Both of them have extensive experience in the cybersecurity industry and they will bring a great perspective to the CTA Board of Directors. We are looking forward to having Jaya and Joe help govern CTA alongside our other board directors.

We would like to extend a huge thank you to our out-going board directors, Corey Thomas, President & CEO, Rapid7, and Joe Levy, CTO, Sophos. Both Corey and Joe provided key strategic direction to CTA and their contributions to CTA have been invaluable.

THANK YOU, COREY AND JOE!

RAPID7
COREY THOMAS
President & CEO

SOPHOS
JOE LEVY
CTO

WELCOME, JAYA AND JOE!

Avast
JAYA BALOO
CISO

Symantec
A Division of Broadcom
JOE CHEN
VP Engineering

CTA Member Feature

PREPARING FOR THE NEXT ZERO-DAY: CYBER THREAT INFORMATION SHARING

When a new malware or cyber attack creates a cyber crisis–the next zero-day, log4j, SolarWinds breach–what can we do to mitigate its effects?

SecurityScorecard believes the answer to that question sits left-of-boom: before a cyber event. To respond to the threat of a cyber crisis, we need to understand the cyber risk environment in real-time and take everyone's responsibility in cyber defense seriously. Principally, that means we need to share more cyber threat information in a cyber crisis.

More shared data, with an understanding of one's cyber attack surface and a quantitative understanding of one's cyber risk, can empower companies, owners, and operators of critical infrastructure, as well as the federal Sector Risk Management Agencies, to act promptly to mitigate and defend their systems in a cyber crisis. This approach also relies on key public-private partnerships, novel cyber defense collaborations, and strong information-sharing practices.

This is one of the reasons why SecurityScorecard shares information with the Cyber Threat Alliance. As a nonprofit organization focused on cybersecurity, CTA extends the information-sharing ecosystem by "working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field." The power of these partnerships and others like them help all who contribute to them and are as critical today as ever.

CTA members collaborate and disseminate threat information and technical guidance (e.g., TTPs, IOCs, etc.) to their members quickly and in actionable ways. We believe critical infrastructure owners and operators across every sector (e.g., water, financial services, information technology, etc.) should lean on and utilize the tools, services, and community built by the CTA, especially in a high cyber threat environment.

SecurityScorecard's mission is simple: to make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risks to their Boards, employees, and vendors. We do that, in part, through information sharing with CTA and its members.

Partnerships like these build trust and strengthen the information-sharing ecosystem that is necessary to protect against malicious threat actors. SecurityScorecard will continue to support CTA and its members and provide our 360 cyber risk intelligence and share information to support CTA members' core cybersecurity missions.

The more data these partnerships have, the more information we share, and the more effective they will be in our defense during the next cyber crisis.

Authored by the SecurityScorecard Team

SecurityScorecard

CTA Member Profile

MEMBER SPOTLIGHT: SANDS Lab

KIHONG KIM
CEO
SANDS LAB INC.

SANDS Lab provides information on cyber threat intelligence, and we have always tried to find ways to effectively share the information we collected and analyzed with Korean and international companies. CTA members are highly competitive companies with the business model suitable to solve the threat intelligence sharing problem, and therefore we decided to join CTA.

CTA provides great value through its emphasis on mutual information sharing. For instance, other intelligence services are more like one-way platforms, which means users pay them and then get the information they are sharing only – not mutual sharing. For open-source and free services, the quality of their information is not great enough to use, nor always well-maintained, and therefore we cannot use their information as intelligence. However, in CTA, we clearly see the fact that the members – which disclose their company name or brand name – are helping each other by sharing the information they have onto the CTA platform. Also, the point system that must be maintained is an important element of CTA.

Since today's cyber threats are more sophisticated and advanced, the speed and pattern of attacks are fast and diversifying. Global companies with multiple customers will inevitably encounter various and uncountable security threats. As we all know, it is physically impossible to analyze all the security threats and protect their customers based on them. To counter that, we can identify various threats early by sharing the information collected and analyzed in real-time through a global alliance like CTA.

By analyzing the various intelligence information collected from CTA on our platform and providing it to our customers, we can build a massive system that can actively respond to various threats coming from around the world. We love that the collected and analyzed information can be shared back on the CTA platform, and then other CTA members can cite it in various intelligence reports.

With CTA, information that has already been verified is exchanged through a standardized interface, so the situation, points, and quality of information sharing are checked in real-time, which has a significant advantage for members.

We are excited about the work we have been able to do through CTA. When we found out the websites which spread malicious codes of various ransomware in Korea, we tracked them down. In the process, we were able to identify different types of malicious codes that the group distributed and several malware variants by profiling using our analysis system platform. We were also able to analyze information on money laundering using the information of cryptocurrency wallets by detecting the flow of C&C servers. We even found out how they spread malicious codes and how ransomware infection works in detail using a technique ID. It was such a meaningful milestone for us because we were able to provide a detailed report on these issues to our customers in the end.

CTA can help mitigate concerns around some of the most significant emerging threats of our times. For example, In Korea, there are several cases of supply chain attacks disguised as legitimate software for political and economic purposes. Since these attacks were conducted based on trust therefore it wasn't easy to recognize and respond to them in advance. To get around this problem, it is necessary to be able to recognize information on unknown vulnerabilities and attack techniques used in these new attacks. Through the CTA platform, we want to get the information on zero-day vulnerabilities of numerous global software being used in Korea, collect the information on attack codes that attack these zero-day vulnerabilities, and provide them together to generate response information for our customers. For example, If the information on attack groups (or attackers) that develop the attack codes and conducted the attacks is also profiled and provided, we can identify the reason or purpose of each attack conducted on a specific company or institution. This may allow us to set up a response strategy from the long-term perspective and then build cyber resilience.

Today's cyber threats target countries all over the world. We are excited to be a part of CTA and appreciate the support and collaboration other CTA members show us.

K7 COMPUTING

CTA Member Feature

THREAT INTELLIGENCE SHARING DURING A CRISIS

Cometh the hour, cometh the solution. It takes a crisis to bring out the best or worst of a planned system. A crisis contextually involves an individual, an organisation, a nation and/or the world at large, and the complexity of the response increases exponentially, in that order.

Cybersecurity planning is typically done with worst scenarios, i.e. crises, in mind. Threat intel is indisputably required for a mature cybersecurity posture, encompassing a comprehensive and robust plan, relating directly to heightened readiness/proactive action, swift response and quick recovery.

The parameters of threat-intel-sharing, the what, why, when and whom, differs according to the magnitude and complexity of the crisis, especially when cyberspace encroaches upon the physical. A case in point is the ongoing war between Russia and Ukraine. Due to the sensitive and confrontational nature of crises such as this, wherein cyberattacks precede or complement boots on the ground, judicious intel sharing is likely, directly influencing collaboration between national and international security agencies, and private sector organisations. Trust is of critical importance, and may be sparse or absent within mass intel-sharing groups.

Clearly, the parameters of intelligence-sharing are subject to stringent guidelines and rules. Different countries, agencies and companies have different regulatory data-sharing policies. However, the consequences matter too. For example, in a crisis that affects an entire nation, and could literally put lives at risk, should critical data that is otherwise protected by, say, an NDA, be shared, perhaps with caveats? As it may not be possible to predict the course of events, amendments and exceptions to sharing intel may need to be made as a crisis unfolds so as to facilitate the action that the situation warrants.

Another important point to consider, one that is especially relevant during a crisis, pertains to how much intel can be shared without compromising on competitive advantage. Is it possible to provide intel that is not so diluted as to render it almost useless? Is there a mechanism of due compensation, of recognition, for the quality, quantity and timeliness of shared information that will, over time, encourage such important intel sharing?

CTA provides a trusted, elegant and elaborate platform and framework for its membership, comprising high-caliber cybersecurity organisations, and partners, inclusive of government agencies, to share intel with confidence, thus helping to manage a crisis. K7 is pleased to contribute to this effort as a member. Cometh the hour, cometh the CTA?

RATHNA KALIDAS
SENIOR PRODUCT MANAGER
K7 COMPUTING