SEPTEMBER 2022

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

Putting threat intelligence to use is no easy task. On the surface, using threat intelligence seems like it should be easy, but even sophisticated organizations struggle with producing, sharing, and consuming it. In fact, the difficulties associated with using threat intelligence in a meaningful way leads many people to wonder whether the effort is worthwhile.

CTA is designed to help cybersecurity providers and other related organizations address this problem and make using threat intelligence easier. For technical threat intelligence, we have developed an automated sharing system that operates at speed at scale and uses industry-accepted formats, such as STIX 2.0 and MITRE ATT&CK. For other kinds of threat intelligence, we have created a diverse, global trust community that enables connections across a variety of organizations.

In this newsletter, we highlight some of our members and partners who put threat intelligence to use. Check Point discusses its views on threat intelligence sharing, while Chief Analytic Officer Neil Jenkins explains how CTA's shared technical data has changed over time. We profile Telmex-Scitum, a Mexican-based cybersecurity company and our first Latin American member, and the Retail & Hospitality Information Sharing and Analysis Center lays out why it is a CTA partner. Finally, we highlight the Virus Bulletin Threat Intelligence Practitioners' Summit track, which will have multiple presentations focused on how to use cyber threat intelligence in practical situations.

Putting threat intelligence to use may not be easy, but it is important. Thanks to all our members and partners who put in the work hard to use threat intelligence daily. As a result of these members and partners' efforts, CTA has evolved into an important hub for threat intelligence sharing and use. We look forward to continuing this work.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CTA ON THE ROAD: VIRUS BULLETIN AND AVAR 2022

Join the CTA-sponsored **Virus Bulletin Threat Intelligence Practitioners' Summit (TIPS), Thursday, September 29th in Prague**, and learn more about how to put threat intelligence to use in your organization.

In today's dynamic and complicated threat landscape, traditional security tools alone aren't enough to protect your organization. In the talks on the VB TIPS track we will explore how threat intelligence, a method for collecting information on various forms of malicious cyber activity, is used in practice to bolster your in-house cybersecurity measures. While easy to talk about in concept, making threat intelligence practical for your organization requires some thought and investment.

vb 2022 PRAGUE 28-30 Sept 2022

Coming in December, join us as we once again sponsor the **Association of Anti-Virus Asia Researchers (AVAR) conference being held December 1st and 2nd in Singapore**.

This year's theme will be "Cybersecurity Counter Punch," as the world eases out of the pandemic, with all entities, organizations, corporates, individuals, etc., trying to balance between the new and old "normals", how have the cybersecurity industry's responses to cyber threats evolved? How have technology and technical expertise evolved strategies to fight back, be it tactics (Red Team/Blue Team, takedowns), tools (AI/ML, Binary Instrumentation), products (XDR, IoT Security), or intelligence to take on and challenge the threat actors?

AVAR 2022

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>11 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	36%
NETWORK TRAFFIC	32%
IP ADDRESS	17%
DOMAIN NAME	5%
FILE PROPERTIES	5%
URL	3%
HOST	2%

TOTAL EARLY SHARES

3-5
PER WEEK

675+

CTA Member Profile

MEMBER SPOTLIGHT: TELMEX-SCITUM

WHY DID TELMEX-SCITUM JOIN CTA?

When we first learned of CTA, we noticed that it was different from other alliances because its members included prominent names in the industry, and they were committed to sharing intelligence not only in an automated fashion but also person to person through the members' research and intelligence teams. For those key reasons we were very excited to be part of CTA.

WHAT ARE YOU MOST EXCITED ABOUT IN TERMS OF THE WORK YOU HAVE BEEN ABLE TO DO THROUGH CTA?

Thanks to what we have learned as a member of the CTA, we make our customers safer. We treasure the ability to exchange ideas and have productive discussions with like-minded people that are part of the CTA committees.

HOW DOES MEMBERSHIP IN CTA HELP TELMEX-SCITUM PROVIDE GREATER SECURITY FOR CUSTOMERS?

Telmex-Scitum has one of the most prominent incident response teams in Latin America. We respond to multiple cases at the same time, and many times the expert judgment from one of the CTA members concerning a recently observed TTP or a second opinion over some code found during the investigation gives us the evidence to arrive to conclusions faster.

At the same time, all CTA members have access to, and share, IOCs and observables that enrich our own telemetry, giving us the possibility of detecting malicious activity quickly in our customers' networks.

HOW DO YOU SEE CTA FITTING INTO THE BROADER CYBERSECURITY LANDSCAPE IN LATIN AMERICA?

CTA members share intelligence related to Latin America, which plays a significant role in protecting the cybersecurity landscape across the region, allowing all member companies to create detections and stop malicious activity for their customers that reside in LATAM.

WHY IS INFORMATION SHARING IMPORTANT IN TODAY'S TURBULENT CYBERSECURITY ENVIRONMENT?

It is a fact that across the cybersecurity industry, nobody knows everything. Every vendor has telemetry based on where their security solutions are deployed, the incident response engagement that they manage, and the campaigns their threat intelligence teams investigate. When we all share our 'partial visibility' as a community, we get the bigger picture of the problem; this allows us to allocate resources towards what matters the most.

WHAT VALUE DOES TELMEX-SCITUM GAIN FROM PARTICIPATING IN THE VARIOUS WORKING GROUPS THAT FOCUS ON SPECIFIC THREAT CAMPAIGNS OR SPECIFIC EVENTS, LIKE THE OLYMPICS OR ELECTIONS?

The working groups have evolved how we collaborate because it is in those working groups that new ideas appear regarding the platform, how we consume the intelligence, and what courses of action we can take as members to translate what we share into detections and disruption of malicious activity. It only makes us stronger.

WHAT DOES TELMEX-SCITUM VALUE MOST ABOUT CTA MEMBERSHIP?

- We appreciate that the CTA is diligent in ensuring that each new member has the necessary capabilities to contribute to the alliance and ensure reciprocity among all members.
- The CTA always acts as a facilitator among members to promote discussions and join forces to tackle cybersecurity challenges.
- The diversity of the members enriches the visibility globally and brings new intelligence that otherwise would be lost among the noise.
- The members' caliber and willingness to share intelligence makes the alliance unique.

WHAT DO YOU SEE AS THE MOST SIGNIFICANT EMERGING CYBERSECURITY CHALLENGES AND HOW CAN CTA HELP TO MITIGATE THESE CONCERNS?

The threat landscape changes constantly. We are in an industry where in less than 24-hours we can face a global crisis. CTA brings structure to the ambiguity in those cases, acting rapidly to get information and proposing possible courses of action to members.

DO YOU HAVE ANY LAST WORDS IN CLOSING?

CTA's collaborative channels are full of smart, amazing people; being able to go to people and ask about an early share before it's published generates a lot of value, as does being able to verify analytic conclusions with other members. It can also be difficult for others to see what we see in Mexico and Latin America, so when we spot something that we can then share through CTA, everyone benefits.

CTA Data Sharing Update

CTA HITS A MILESTONE: 250M OBSERVABLES

Recently, CTA members passed another important milestone, sharing over 250 million observables through our automated platform since our incorporation in 2017. There are lots of people to thank for reaching this milestone, but none are more important than our members who have done the hard work to translate their data feeds and generously share observables and the associated context. This shared data is available to all of our members to improve the protections for their customers.

Our shared data has changed greatly over time. Early in our sharing, members were sharing fewer than one million observables a month and more than 90% of them were file hashes. As our membership has grown, our sharing has naturally increased. Not only do we now get more data – often more than 400,000 observables per day – we also get more diverse data. We now categorize our shared observables in three buckets of roughly equal size: file hashes, network observables (IPs, URLs, and Domains), and network traffic observables (ports, source and destination information, etc.). A significant number of observables related to hosts and emails are also routinely shared. This diversity provides opportunities for our members to identify and stop malicious behavior.

We routinely work with our members to understand what data and context they need and incentivize our members to share that data. One-on-one discussions, surveys, and working groups allow us to hear from our members and prioritize their needs. We then focus on that priority information by adjusting our requirements, incentivizing members through our points system, or sometimes by just asking nicely. Members routinely share much more information than they have to, one of the amazing things about our community. As a result of our data quality engagements, our shared data now includes more file samples, more diversity, more information on MITRE ATT&CK phase, and more information on victim country and industry than ever before.

Data quality isn't an objective measure, so we are constantly working to listen to the feedback from our members and make adjustments. Thankfully, our membership is willing to listen and help out their fellow partners in cybersecurity.

NEIL JENKINS
CHIEF ANALYTIC OFFICER
CYBER THREAT ALLIANCE

DR. DORIT DOR
CHIEF PRODUCT OFFICER
CHECK POINT

CTA Member Feature

‘CROWD PROTECTION’- THE NEED FOR COMMUNITY DEFENSE

By Dr. Dorit Dor, Chief Product Officer, Check Point

Five years ago, on May 12, 2017, the world fell victim to a major ransomware attack known as the infamous ‘WannaCry’. The attack had an unprecedented scale, spreading around the world like wildfire.

The attack resulted in an outbreak affecting more than 200,000 Windows computers across 150 countries in only a few days. In the cyber-security community, the attack was referred to as a global “wake up call.” But did the world really wake up to the disturbing alarm?

What if an alternative scenario had happened? In this alternative scenario, cybersecurity companies quickly blocked the attack, identified the source and important indicators of compromise, and distributed this information to cybersecurity companies and other significant organizations within the global security community. If such sharing had occurred, those organizations would have then been able to update security systems, alert CISOs around the world, and trace the leads that would bring the discovery of the attackers. Hard to imagine? Impossible?

In fact, since WannaCry, the world has witnessed a series of large-scale mega attacks, from the SolarWinds attack to the exploitation of the Log4J vulnerability – and each time found organizations all amazed and almost disoriented looking for remediation and aid.

Is this unavoidable? Global phenomena require global collaboration through actionable mechanisms.

> “There is no competition in the effort for a safer digital ecosystem.

Coalitions such as the Cyber Threat Alliance allow for a safe platform to exchange valuable threat intel among organizations that might be bitter rivals on a business level, but firm fighters for a safer global digital ecosystem. Leveraging and aggregating big data telemetry from millions of endpoint devices and external feeds (such as ones coming from CTA), and millions of indicators of compromise (IOCs) everyday points to an overwhelming comprehensive threat landscape. Sharing helps to disclose new threats and techniques, and at the same time allows you to produce new protection capabilities, thereby enriching your security architectures and prevent new attacks.

When a malicious link is detected and blocked in a zero-day attack in the US, the threat data should then immediately be shared across all attack vectors allowing protections for this attack to be updated in real time. This same zero-day malicious link should then be blocked quickly if a similar attack is happening in another region. Sharing information about the cybercriminals and their tactics between members in a trusted global community can mean prevention before the next mega attack.

The power of such a community is a solution for cyberattacks, seemingly one of the most disrupting forces threatening the human society worldwide.

SUZIE SQUIER
PRESIDENT
RH-ISAC

CTA Partner Feature

HOW TO PUT THREAT INTELLIGENCE INTO ACTION

By Suzie Squier, President of the Retail & Hospitality ISAC

Putting threat intelligence into practice has to be about two core principles: focus and actionability.

For the Retail & Hospitality ISAC (RH-ISAC), we have a laser focus on our membership’s priorities. Our Core Members are consumer-facing businesses ranging from retailers, hotels, restaurants, and casinos to consumer-packaged goods manufacturers and other retail platforms. We know their intel needs, their environments, and their sore spots. We focus our collection and production capabilities on addressing those priorities directly and exclusively. Because of this focus, our members know that any intelligence and recommendations they receive from us are vetted and valuable. We sort through the overwhelming volume of existing intelligence in open- and closed-sources and determine what best meets the needs of our membership as they themselves have defined through requests for information (RFIs), regular benchmarks, and surveys. Through this focus, RH-ISAC ensures our intelligence output is specific to our audience’s organizations, industry, and regional intelligence needs.

This brings us to actionability. RH-ISAC serves as a force multiplier for our membership by providing them with enriched, contextualized intelligence, allowing our members to focus on their cyber defense operations. This means that what we provide them not only has to be focused on their needs, but they also need to be able to use it and integrate it into their operations as easily as possible. To ensure the maximum value for intelligence, RH-ISAC focuses on three areas.

First, we provide technical intelligence, like IOCs and tactics, techniques, and procedures (TTPs), that can be used by defenders to block malicious activity through security controls and configurations.

Second, we provide tactical intelligence, including open-source events and research findings, that can be used to develop trend analysis and form defense and response plans.

Third, we provide strategic intelligence and analytics, such as mid- and long-term patterns, to inform organizational and structural posture and policies.

One of the core ways RH-ISAC enhances the intelligence and services we provide for membership is through our partnerships, such as the one we have with CTA. Through these partnerships, we are privy to conversations and briefings from leaders in the cybersecurity community that we can bring back as additional information and insights to help members continue to strengthen their security operations. The partnership with CTA broadens our awareness of the threat landscape, which, in turn, broadens the awareness of our member companies.

In addition, Michael Daniel has always been of invaluable support and help with any questions we may bring his way.

We have found great benefit in our CTA partnership already and look forward to continuing to work with Michael and his great team.

Interested in CTA membership or a partnership?

Send us an email at **newmember@cyberthreatalliance.org**

Learn more at **https://www.cyberthreatalliance.org/**