MARCH 2022

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

As I write this introduction, the Russian-Ukrainian war dominates cybersecurity discussions. Although we have not yet seen a spike in destructive cyber activity, either inside Ukraine or elsewhere, no cybersecurity practitioner believes we should lower our guard. The Russian government could choose to ramp up its activities at any point, and we must be prepared for such an eventuality.

A key part of being prepared is sharing and collaboration, and CTA excels at facilitating multi-company collaboration against threats. This capability did not develop by accident. We have spent the past five years developing and honing it. This 5th birthday milestone provides a good opportunity to reflect on how CTA helps its members prepare.

Our Webex channel is available to members to post questions or findings, as well as to discuss what is going on. The early sharing program provides members a way to give the rest of CTA a heads up about upcoming publications, and the biweekly Intelligence Committee meetings provide a regular forum for information exchange at human speed. By participating in these analytic sharing activities, our members are better prepared to assist their customers and clients.

Preparation also means being able to respond rapidly when an event occurs. CTA facilitates that kind of preparation too. We can rapidly convene our members in response to a crisis or increase our collective situational awareness. We have connections to information sharing organizations and government cybersecurity centers, supporting preparedness beyond the cybersecurity vendor community.

Finally, over the long term, preparedness means becoming more resilient to the malicious cyber activity that has become endemic to cyberspace. CTA works in this area too, through advocating for cybersecurity policies that incentivize investments in cybersecurity and implementation of best practices. We support long-term projects aimed at shifting the balance between intruders and defenders in cyberspace, seeking to reduce the burden on defenders and raise the costs for intruders.

President Dwight D. Eisenhower once said, "The Plan is nothing. Planning is everything." In a highly interconnected, digital world, this aphorism regularly proves true. Cyber plans frequently fail – usually upon first contact with an adversary – but planning and preparation enables organizations to adapt rapidly to the changed circumstances. Thus, without preparation, changing circumstances can overwhelm an organization and render even the best cyber defenses useless. CTA membership can be a force multiplier for preparation and another element of a resilient defense.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

CELEBRATING FIVE YEARS OF CTA

The Cyber Threat Alliance recently celebrated its fifth birthday in January 2022. Hear from our members in this webinar as they discuss sharing over the long run and celebrating five years of enduring collaboration.

"When we share, I see other people's data too. I see what they do, and I get some calibration of my own capabilities. Sometimes that serves as a wakeup call, sometimes it serves as a source of pride."

Dorit Dor
VP of Products, Check Point

"No one vendor can discover everything alone so collecting information together, disseminating and putting it to productive use is the best way to combine our energies to succeed vs adversaries. CTA continues to stand out as a shining example of how sharing can work well."

Joe Levy
CTO, Sophos

"The early share program is really wonderful. Let's say it's a day, or even a few hours — whatever the timing, it does help."

Joe Chen
VP Engineering Symantec Division of Broadcom

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>7 MILLION
MONTHLY AVERAGE

200 MILLION
SINCE FOUNDING

OBSERVABLE DIVERSITY
(AVERAGE)

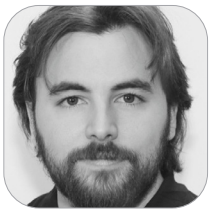
FILE HASH	37%
NETWORK TRAFFIC	29%
IP ADDRESS	15%
URL	7%
FILE PROPERTIES	5%
DOMAIN NAME	4%
HOST	3%

TOTAL EARLY SHARES

3-5
PER WEEK

575+

VICTOR ACIN
LABS MANAGER
BLUELIV



Blueliv.

CTA Member Profile

WELCOME BLUELIV TO CTA

One of the core principles in which Blueliv was founded was the exchange of information. We have always strived to foster relationships with industry peers by sharing knowledge related to cybercrime and providing the community with the means to counter external threats with our products and services. In addition, we believe that cyberthreat intelligence must be actionable, hence, we've built a product that focuses on providing context to threats and helping customers understand specific threats that are targeting their organizations, where quality was as important (if not more) than quantity. As CTA shares the same ethos, we thought it was the perfect place for Blueliv to contribute, and to advance our common goal.

The truth is that no single vendor has all the existing information on cyberthreats, in the same way that threat actors and groups do not have all the expertise required to carry out their campaigns. If they are collaborating to bring forward new threats, it is imperative that we, as defenders, collaborate in the same way they do to stand a chance of protecting ourselves and the customers that we serve. Blueliv believes that collaboration is the future of cybersecurity, and only by sharing will we, as an industry, be able to adapt to this rapidly changing threat landscape.

Blueliv appreciates the importance CTA places on context. Without context an IoC is just something to block on a firewall or an EDR, but with threat context it becomes intelligence, which can be actioned by companies and individuals to better protect themselves and their data.

Most of the exchange partnerships and agreements out there are made for either samples or command and control servers. These exchanges are useful, but it also means we have to digest and sift through all of the information provided to find the intelligence that is of interest to us, and of value to our customers. CTA members provide contextualized information, which we can use directly in our investigations, or selectively process to obtain better results more efficiently.

We're extremely proud to be one of the top contributors by sharing context on malware samples, URLS, threat actors and their relationships since joining the CTA at the end of 2021. We're keen to share more and collaborate with other members to improve context and deliver even better threat intelligence to our customers and the wider industry.

Blueliv would like to see CTA continue to grow into a world-class membership association in cyber threat intelligence and be the glue between the government, technology vendors, and public and private companies in the fight against cybercrime.

DEREK MANKY
CHIEF, SECURITY INSIGHTS
& GLOBAL THREAT ALLIANCES

FORTINET

CTA Member Feature

CTA'S FIVE YEAR JOURNEY

First off, on behalf of Fortinet, let me say Happy Birthday, CTA!

Anyone could easily see there is a lot to celebrate. Over the course of five short years, CTA has grown from an idea about sharing information through corporate walls into a global presence that represents a diverse ecosystem of members, industries, and intelligence.

CTA membership has continued to grow, not just in numbers but also in viewpoints. Visibility into the global threat landscape has been enhanced through the addition of new members in different parts of the world, and in the different viewpoints that comes from members who come from a mix of industries and technologies. Membership now consists of a diverse mix of pure-play security vendors, research organizations, and technology sectors (e.g., telecommunication carriers, OT), along with strong input from our Contributing Allies and Supporting Partners.

I'm pleased at how CTA has continued to grow over these past five years in meeting its original goal of enabling the sharing of information, context and intelligence amongst members to elevate global security posture and disrupt cybercriminal operations. The early share program has been a tremendous success and is a real benefit of membership, and it has been a great trust building exercise. The early share program effectively levels the playing field on intelligence, sharing real time reports, blogs and resources prior to public release. This provides researchers trusted access to threat reports, so customer protections can be put in place early in the attack lifecycle.

Magellan has also been a great achievement and a real benefit to the organization. Magellan was designed to visualize and automate the secure transfer of information and intelligence amongst CTA members. Its success can be seen by the increasing numbers of diverse observables and contextual information being shared, including kill chain and mappings of techniques, tactics and procedures. Magellan is a great example of a true bidirectional platform that has gone to solve the 'last mile' problem enabling actionable threat intelligence.

The Cyber Threat Alliance was founded on the seed of an idea shared by a couple of people and supported by the organizations for whom they worked. Fortinet has been with the CTA since Day 1 and shared the vision of what it could be. We're proud to have been part of this journey and it has been a pleasure working with such strong leadership across the board, committees and membership base.

That vision is only getting stronger, and highlights a road to success. CTA, you'll be 10 before you know it.

CYBER THREAT ALLIANCE

JASON MINNICK
CHIEF TECHNOLOGY OFFICER
CTA

CTA Feature Update

UPDATE ON MAGELLAN

In the wake of our 5-year anniversary, it gave me a great opportunity to reflect on the evolution of CTA's technical sharing capabilities. In 2017, we started out with a basic (but extremely reliable) STIX 1.2 TAXII server. I have always thought of the initial iteration as a prototype. A very important prototype, nonetheless. It ultimately gave us an opportunity to better understand the path forward as sharing data at the volume and frequency that we were striving for is very challenging. Things like a trial environment, scalability, advanced visualizations, search tooling, analysis tools to support custom sharing rules, all had to be taken into consideration to consider the next iteration of the platform a success.

As the CTO and chief architect of the redevelopment effort, I will say, we could not have pulled this task off with the great support of our members. Their feedback as well as in-kind donations of their developer's time was critical in us having enough engineering rigor to pull off all the tasks that we needed to accomplish. After finishing development in 2020, we were able to migrate all our members from the prototype to the service that we now call Magellan with relative ease.

Fast forward to 2022, we now have one of the largest STIX 2 ecosystems on the planet. The challenges we overcame to get to where we are today have been very rewarding. In redeveloping our product, we have successfully deployed a distributed infrastructure that is easy for members to consume, easy for prospective members to demo, easy for CTA staff to analyze while at the same time, providing the same great reliability our members came to know with the prototype. At the start of the planning process, I could not have imagined a more successful outcome. Thanks again to all those who were involved in making the Magellan product a huge success!

HEAR FROM CTA MEMBERS ON THE VALUE OF MEMBERSHIP

CTA features a series of guest blogs to shine a light on the day-to-day role that our members play in shaping and supporting the work of CTA. Read on to hear directly from our members's marking CTA's fifth birthday.

"We started the CTA with just a handful of partners. Today, there are 34 member organizations, who all share the same goal of protecting users everywhere and we continue to recruit additional members. While we all may be competitors at some level, what we have built over the last five years is an amazing amount of trust in the industry. Security isn't an individual effort — it's a team sport, and you must trust the person next to you to be an effective team."

Matt Watchinski, VP Cisco Talos
Talos celebrates the Cyber Threat Alliance's 5th birthday

"All members of the CTA have distinguished backgrounds and strengths to combat cyberwarfare. Utilizing our leading research arm, Check Point Research, Check Point is finding and sharing global cyber attack data to the entire CTA community. We understand that we all need to work together and are committed to the shared goal of protecting the world from nefarious hackers and state-sponsored adversaries."

Jason Min, Head of Business & Corporate Dev, Check Point
Check Point Software Technologies Celebrates CTA's 5th Birthday

"The CTA has shown that together we can do more. We have proven that collaboration can – and does – make us all better equipped to provide protections for all our customers, while still remaining fierce competitors."

Kathy Whitbey, Principal Business Operations Manager, Unit 42 Palo Alto Networks
Happy 5th Birthday, Cyber Threat Alliance!

"At Symantec, we are proud to share our research and intelligence with CTA for the greater good, and we are happy with the intelligence we receive in return. In the next five years, my hope is that CTA continues to grow and other members of the cybersecurity industry join us in realizing these benefits. Happy anniversary, CTA!"

Joe Chen, VP Engineering Symantec a Division of Broadcom
Symantec Broadcom Celebrates CTA's 5th Birthday

"On a handshake, remarkable leaders decided to throw out a lawsuit, against their despised competitor, and do something good for the public good. That never happens, and yet, that's what they did. Remarkable."

Rick Howard, CISO CyberWire and CTA Champion
"Don't let this fail:" The founding of the Cyber Threat Alliance

CYBER THREAT ALLIANCE

NEIL JENKINS
CHIEF ANALYTIC OFFICER
CTA

CTA Feature Update

FIVE YEARS OF SHARING

No celebration of CTA's 5-year anniversary would be complete without a look back at how our sharing has grown over time. We can start by looking at our easiest metric to track, total observables shared. CTA members have quickly grown from sharing about 500,000 per month to almost 7.5 million per month. Much of this growth can be attributed to new members coming on board to grow our ranks. But we also know that our existing members regularly make changes to their data feeds to increase the sharing they provide to their fellow members.

More importantly, we can look at the context that members share with these observables to enrich them and the diversity in the types of observables that are shared over time. Early in CTA's history, observable sharing was heavy in file hashes, regularly accounting for 90% or more of the observables shared. As we began outreach to other potential members, we heard their desire for more network-based observables, such as IP addresses, domain names, and URLs. We asked our members to begin to diversify their sharing, and they quickly stepped up. These days, file sharing makes up between 50-60% of our overall observables with network observables, DDoS-related observables, and others in the mix. This diversity helps our members gain a broader view of the threat environment.

In terms of context, we require our members to share specific contextual information with us in every submission, to include first and last seen and kill chain phase. Over time, and enabled by our Magellan platform, members have begun to increase the sharing of context objects such as file samples, malware names and types, MITRE ATT&CK techniques, victim country and sector, and recommended courses of action. We measure context using our points system and have seen our average points per submission continually increase over time. On average, members now submit at least three different context objects above the required context with each submission.

While automated sharing is the backbone of CTA, we must acknowledge the amazing early sharing of blogs and reports that members provide to each other generally around 24-72 hours before public posting. Members began to provide early shares to each other in May 2018. Through most of 2018, members shared a couple of early shares a month with each other. This helped to build confidence and trust, and now members routinely provide an average of 4 early shares a week with each other. Our members have shared over 575 early shares since the program started. In most cases, members are able to take action on this data early and get ahead of malicious cyber actors before they know that their activity is public.

CTA's sharing shows no signs of slowing down. Thanks to our current members for their hard work and we look forward to seeing what innovations new members can bring!

CTA Member Feature

NFT AND CYBERCRIME

Authored by the TEHTRIS Team

Non-Fungible Tokens or NFTs are "THE" new playground for attacks against various crypto currencies. Defenders must also adapt. TEHTRIS, together with its partner the Cyber Threat Alliance, strives to constantly improve cybersecurity by sharing information on new cyber threats. This collaboration is fruitful, and CTA celebrates its 5th anniversary this year. Let's take a look at NFTs as a potential source of cyberattacks.

NFTs are digital tokens linked to a unique digital or physical asset; they can encompass everything from video clips to artwork. Like cryptocurrencies, NFTs rely on blockchain technology. Since each NFT is linked to a different asset, each NFT is unique, and no single value exists for NFTs in general.

Google reported that as of December 2021 NFT keyword searches surpassed cryptocurrencies. According to a report by DappRadar, last October, NFTs reportedly generated $148 million more compared to September. Digital design is on a roll! How can you not be greedy when you see so many dollars being generated? Thus, it was obvious that cyberattackers were going to take a close interest in the subject and that the abuses related to this new concept would soon become known.

The rise of this new concept brings with it a new playground for hackers to proceed to:

- **Identity theft**, cyber criminals steal a victim's personal information by using sophisticated cyberattack tactics, including social engineering, phishing and malware, and then perform criminal acts using a victims ID.
- **Fake websites**, scammers can also create fake NFT stores and sell NFTs that do not exist. This type of attack based on typo squatting is becoming legion, as cyber criminals use domain names that impersonate popular platforms to make their attacks more credible.
- **Phishing**, cybercriminals pose as companies, and then canvass numerous artists to offer them partnerships. Once the relationship is established, a malicious link was injected and escapes the vigilance of antivirus software.

The purchase of NFT requires basic safety hygiene such as multi-factor authentication, tokenization of tweets, ensuring the legitimacy of links etc.

Although NFTs are new, the malicious actors' techniques are not. The same phishing lure or illegitimate domain name can be used for other kinds of cybercrime. That's one reason why TEHTRIS is a CTA member – the information we receive from CTA can be used to help protect our customers against malicious activity associated with NFTs, among other threats.

For more information on the subject: https://tehtris.com/en/blog/nft-the-new-cybercrime-paradise

<TEHTRIS>
FACE THE UNPREDICTABLE