MARCH 2023

CTA IN FOCUS

LETTER FROM THE PRESIDENT & CEO

Cyber threat intelligence sharing requires hard work. Six years into running CTA, I have concluded that the situation won't change any time soon, either. No magic easy button, no "click here to share with all the right machines and people" box on a website, appears to be on the horizon despite all the frenzy about artificial intelligence. Threat sharing will continue to require an investment of time and money among people to work well. The question is, why make this effort?

Companies make the effort to join CTA in large part because of the community it provides. Since our formal start in 2017, we have built a robust community of threat researchers and analysts from among our members, who collaborate in many ways, from automated sharing of technical indicators to ad hoc messages in Slack to bi-weekly zoom calls to embargoed sharing of upcoming publications. This community effort has proven that intelligence sharing works, even among competitors. Further, the value of the CTA community grows over time as we add new, diverse members.

This experience with growing CTA points directly to this newsletter's theme: the community effect. This effect occurs in many areas, but it is particularly strong in the networked world of cyberspace. Malicious actors have certainly figured out the power of operating as a community; they share tactics, tools, techniques, exploits, and target lists all the time. As defenders, we need to harness the power that derives from working together across organizational lines to better deny and degrade our adversaries' capabilities.

In this newsletter, we will explore the community effect as it relates to CTA. Our Chief Analytic Officer, Neil Jenkins, discusses his observations about the CTA community we have built. CTA members AT&T Alien Labs, Juniper Networks, Panda Security, and Scitum provide some different perspectives on this theme, and we profile one of our founding members, Cisco Talos. One of our contributing allies, the Information Technology Information Sharing and Analysis Center, describes how the community effect works in its industry. Taken together, these contributions showcase the community effect and the leverage it has.

Overall, CTA makes an excellent case study for the community effect. A sustained investment is required to create a community and keep it going, but the benefits are worth it. We are always excited to add members to the Alliance and have new companies experience the CTA community effect firsthand. If you are interested in joining us in this journey, please reach out and we will get the conversation started.

J. Michael Daniel

J. Michael Daniel
President & CEO, Cyber Threat Alliance

THANK YOU, NEIL!

CTA bids farewell this month to our Chief Analytic Officer, Neil Jenkins, as he is moving on to pursue an analyst position with a cybersecurity industry vendor. Throughout Neil's five years at CTA, he has been instrumental in driving improvements to our data sharing. He pioneered CTA's monthly analytic reports and maintained the weekly sharing reports, providing a clear view of membership sharing stats. Our early share program has grown leaps and bounds with his stewardship over the years. In addition, his leadership of CTA's bi-weekly Algorithm & Intelligence committee helped drive our members' collaborative efforts and ensured that our members were educated and aware of the latest threats and hot topics.

We will miss Neil and wish him the best in his new role.

CALL FOR PAPERS

CTA is once again sponsoring the Virus Bulletin conference Threat Intelligence Practitioners Summit (TIPS). Our theme for the TIPS track is **The Community Effect**.

We welcome abstract submissions for a panel or a standalone talk; submissions are due May 4th to events@cyberthreatalliance.org.

vb 2023 LONDON 4-6 Oct 2023

CYBER THREAT ALLIANCE

MEMBER SHARING SNAPSHOT

OBSERVABLES SUBMITTED

>9 MILLION
MONTHLY AVERAGE

OBSERVABLE DIVERSITY
(AVERAGE)

FILE HASH	35%
IP ADDRESS	18%
DOMAIN NAME	5%
URL	3%
NETWORK TRAFFIC	31%
FILE PROPERTIES	6%
HOST	1%

TOTAL EARLY SHARES

3-5
PER WEEK

780+

CTA MEMBERS AND PARTNERS PROVIDE THEIR PERSPECTIVES ON THE

COMMUNITY EFFECT

CTA Member Feature

THE COMMUNITY EFFECT: AT&T ALIEN LABS

A year ago, the war in Ukraine began, and military actions were complemented by cyber warfare, leaving a trail of wipers along the way. The number of new wipers discovered during 2022 has been unprecedented, and it has required a great effort by the cybersecurity community to stay on top of the latest TTPs and IOCs that were emerging.

During this same period, cybercrime actors continued with campaigns aimed at making fast money. For example, ransomware-as-a-services (RaaS) programs have expanded, with operators, affiliates, and access brokers working together to create a powerful network of threat actors with the ability to quickly increase their level of sophistication and success rate.

With the arrival of 2023, we are seeing once anomalous techniques start to trend in a matter of days. These include the likes of SEO poisoning, a phishing technique whereby cybercriminals will manipulate SEO rankings and promote sites hosting their malicious payloads. Who would have thought that attackers would pay money to advertise their phishing links and lure distracted victims?

Additionally, attackers are catching up with popular technology. For example, they are now using Microsoft OneNote attachments in their arsenal to deliver phishing. These updates are not surprising or unexpected. However, they do remind us as defenders of the need to stay abreast of new adversary tactics, especially as it relates to the various technologies we are tasked to protect.

Luckily, security researchers have help, and are not required to personally observe these trends in attacks and TTPs to be aware of all of them. They are shared in articles, blogs, tweets, podcasts, and more, between colleagues and within communities like the Alien Labs Open Threat Exchange, OTX, who might find them useful to protect their environment against threat actors. OTX is among the world's largest open threat intelligence platforms, with more than 200,000 users in 140+ countries sharing threat data daily.

Over decades, the cybersecurity community has tried many different ways of sharing intelligence and IOCs. This started with email lists, which threat researchers and security analyst had to know about and typically be invited to. The challenge of these groups is apparent in that they were not open and difficult to gain access to. The need for greater collaboration within the defender community soon led to more open, public intelligence and IOC-sharing platforms, such as OTX, and groups like CTA.

The CTA, a group of cyber practitioners who have chosen to work together in good faith to share threat intelligence, in fact stands out in the list of collaborators within cybersecurity. They are doggedly focused on maintaining a strong community by only sharing intelligence among trustworthy parties and preventing malicious actors from getting access to the threat artifacts that could help them adjust their tactics.

As groups like OTX and CTA show, operating as a community enables us to counter the bad guys more effectively. Alien Labs is committed to these efforts because they produce better results, especially for our customers. We look forward to continuing this work in 2023.

BY FERNANDO MARTINEZ SIDERA
CYBER SECURITY PRINCIPAL

CTA Partner Feature

HOW INFORMATION SHARING COMMUNITIES MAXIMIZE YOUR SECURITY SPEND

IT ISAC
FOUNDED 2000

In the climactic scene of the iconic baseball movie Field of Dreams, Terrence Mann, played by James Earl Jones, asserts baseball is "the one constant through all the years" of American history. For cybersecurity policy, "the one constant through all the years" is information sharing. From Presidential Decision Directive - 63 issued in 1998 (which marks the beginning of time for CIP and cybersecurity policy) through today, no matter what other recommendations thought leaders or policymakers advocate, almost everyone always notes the importance of information sharing.

In 1998, there was only a hypothetical case for information sharing. Today there are three core truths of cybersecurity that makes collaboration essential:

- It is more expensive to defend than it is to attack.
- The attackers are actively sharing with each other.
- The threat landscape and attack surface are too complex for companies to defend on their own.

Information sharing communities help companies maximize their limited resources. They provide access to analysts from peer companies defending against common threats, vendor neutral analysis of current and emerging cyber threats, early warnings and indicators and the ability to learn from others.

Building effective information sharing communities is not easy. There is no "out of the box" model that organizations can deploy. The Health ISAC, the Communications ISAC, and the Cyber Threat Alliance, for example, are all successful communities, but they each have different operating models and missions. Each industry is unique, and each company has different capabilities and needs. As communities grow, trust decreases, which is a real challenge for a model whose success depends on trust.

The IT-ISAC is a community of communities. We support specialized sharing communities for the food and agriculture industry, the elections industry, Critical SaaS providers, and the Semiconductor industry. Building smaller communities within a larger membership, enables us to maintain our trust model, increase the sharing of cyber threat intelligence, and identify trends across specific industry segments.

Participation in information sharing communities is increasingly viewed as an effective security practice. These communities are a cost-effective investment of your security dollar. Companies who are not engaged in them are potentially increasing their risk of liability if they were to suffer a breach.

Attackers are sharing with and learning from each other. They are maximizing their skills to attack more effectively. The power of information sharing communities is that they give defenders a fighting chance.

BY SCOTT ALGEIER
EXECUTIVE DIRECTOR

CTA Member Feature

THE POWER OF WORKING TOGETHER ON CYBERSECURITY

At this point, we all know that Cybersecurity can no longer be the sole responsibility of an individual or an organization. Instead, it requires the entire community's collective knowledge, effort, and resources. The CTA has been at the forefront of this movement, harnessing the collective power of its members to drive greater security across the internet.

The power of working together can be seen in how the CTA has tackled global cybersecurity problems. By pooling their resources and insights, CTA members have created a better understanding of emerging threats and how to respond to them in a coordinated way. For instance, members can get the specifics about a threat firsthand, understand whether an attack vector is on the rise or decline, and find out what Tactics, Techniques, and Procedures are the most used by the threat actors.

For those members like us, this is pure gold because, as an MSSP focused on Latin America, we observed threats that were not detected by any security solution, however thanks to the collaboration with the CTA, we share our investigations, and the members can put in place detections in their products that protect not only our customers but the rest of the world. And as part of the same effort, we ensure that the organizations under our watch improve their security posture based on the threat intelligence the other CTA members provide, amplifying the impact of each member's fantastic job.

Moreover, the CTA has provided a platform for in-depth discussions among the most prominent subject matter experts in the community that are part of the CTA's committees, which has enabled members like us to gain insights into the latest trends, better understand the risks associated with specific threats, and develop strategies to mitigate those risks among our customers in the Latin American region.

By creating a safe space for members to share ideas, the CTA has helped to create a vibrant ecosystem of cooperation in the field of cyber security, which enables the members to develop a more secure internet that better protects us all.

BY IMELDA FLORES
HEAD OF SCILABS

CTA Member Feature

THE COMMUNITY EFFECT: JUNIPER NETWORKS

Being part of a community is almost always associated with a net-positive impact to everyone who is part of that community. This is especially true when it comes to the net-positive impact of sharing threat research and threat intelligence indicators within the cybersecurity community. Security vendors who continuously share threat intelligence increase the overall number of threats they can effectively protect consumers of their technology against, and that protection is delivered with greater rapidity when new threats emerge. This is the power of the Community Effect.

There are massive amounts of malware and malware variants created every day. However, there are only so many malware samples and IoCs that a single vendor with their limited resources can uncover. If every vendor is dedicating resources to uncovering the same malware, this drastically reduces the percentage of the growing total out there in the wild that are known and can be protected against.

The Community Effect incentivizes members of this community to share findings, samples, and IoCs. This is obviously a benefit to end customers – they get more widespread protection against cyber threats — but this is also a big benefit to vendors who would otherwise keep research and development advances to themselves to better compete in the market. The Community Effect is what makes it possible for vendors to truly focus on technological innovation. Because vendors are distributing their resources so that a bigger percentage of the total malware in the wild is uncovered, they are using fewer resources uncovering malware individually and reallocating those resources to things like threat analysis and engineering. It's a win for all involved.

Like others in our community, this is what Juniper's membership in the Cyber Threat Alliance has allowed us to do. Since we first became a member in 2018, we've been able to take part in sharing threat intelligence, which in turn has accelerated the research and development work that the Juniper Threat Labs team does. The result is that Juniper customers are better protected, customers of every Cyber Threat Alliance member organization are better protected, and the competitive spirit that drives cybersecurity innovation is very much alive and well.

BY MOUNIR HAHAD
HEAD OF JUNIPER THREAT LABS

CTA Member Feature

THE COMMUNITY EFFECT: PANDA SECURITY

It's been almost four and a half years since Panda Security joined CTA. Despite exchanging threat data for a long time with many industry organizations, we were always looking for new and richer sources of data that would strengthen our capabilities and set up better and more systematic processes. We also knew that quantity didn't mean quality. Once we met the team and understood the capabilities of the platform, the decision to work with CTA was easy. Since then, we have been proudly and consistently receiving and contributing to the alliance with fresh indicators directly sourced from our installed base of endpoint security products.

Many things have changed since then, among them, the acquisition of the company by WatchGuard Technologies in mid-2020, which brought together highly complementary technologies, products and teams, helping to bridge network security, Wi-Fi security, multi-factor authentication, and advanced endpoint security. As a result, customers and partners enjoy the benefits of the WatchGuard Unified Security® framework, which delivers better security, in a more integrated, simplified, and efficient manner. Getting together was better for our companies and for all our combined customers.

Similarly, the community of members of CTA, their reach and the diversity of the combined market areas covered represent enhanced access to intelligence for us, and we are looking forward to doing more with CTA in the future. Getting together has surely been better for everyone.

Lastly, aside from helping to improve our detections, enable faster responses and add data to our view of the threat landscape, there is another important value derived from our CTA membership, which is trust. As security vendors in a market with myriad choices, what we sell and what buyers seek, really, is trust. The CTA brand has certainly helped to increase that trust from partners and customers.

BY JOSU FRANCO
STRATEGY & TECHNOLOGY ADVISOR

CTA Member Profile

MEMBER SPOTLIGHT: CISCO TALOS

WHY DID CISCO JOIN CTA?

We set out to co-create the CTA originally so that cybersecurity companies around the world could coordinate and share vital information that can protect users across the globe. The CTA allows member companies to share our intelligence ahead of publishing time — through automated means and early copies of security research — so that we can all craft detection and prevention for our customers. This allows all of us to create a safer cyberspace for all.

WHAT DOES CISCO VALUE MOST ABOUT CTA MEMBERSHIP?

Community. In many of our relationships, it's a one-way or very technical two-way relationship. There's not a lot of back-and-forth and it's very machine-to-machine. With the CTA, we do a lot of human-to-human, where member companies' analysts talk about problems they're encountering. It's not just a URL or a hash around why one thing is specifically bad. It's talking about deeper things about what kind of policy can we implement to affect change.

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

When it comes to matters of cybersecurity, we are past the point of having governments supply protection for individuals, businesses and nation-states. We as the cybersecurity community are on the frontlines. It takes the Cisco's, Palo Alto's, Symantec's and other security practitioners in the private and public sectors all working together.

HOW DOES BEING PART OF CTA HELP CISCO PROVIDE GREATER SECURITY FOR CUSTOMERS?

CTA helps to expand our cybersecurity community beyond what is reachable through our own company. If we are serious about protecting our customers, that means everything. We can't stand on our own. Through the CTA we have an even larger community of information, threat researchers, and hunters. Without this collaboration, we would see less than we could otherwise.

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

Cisco is often on the front lines of large security events, not only for our cybersecurity professionals but for our networking portfolio as well. As we protect these events, we can learn more about what is happening in the world and how it may affect these areas if we did not participate. Threat hunting is often finding needles in a haystack of needles, and we need one anomaly, one detection to build off. For us, it all comes back to the community we're building, and CTA is a central part of that.

HOW DO YOU SEE CTA FITTING INTO THE BROADER CYBERSECURITY LANDSCAPE MOVING FORWARD?

The threat landscape is constantly shifting and changing, we have our own views of what that looks like, but with a broader group like CTA you can get exposed to what other companies are seeing and using, and how they're approaching a problem. The cybersecurity issues our customers see today, and those coming at us in the future, will take an industry approach to solve them. Working together on these problems gives us a better chance of finding scalable and replicable solutions to protect our customers and the internet at large.

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

Sophisticated threat actors and commodity malware operators are utilizing the same toolsets now. There are many open-source and publicly available tools online that allow threat actors to steal credentials or exploit a vulnerability without developing the skills or building a custom tool themselves. Tools, processes and utilities built into the operating system are also being abused more frequently, so it's getting harder to spot the anomalies. All of this may point to the fact that defenders are getting much better at their job, but it also means threat actors are innovating more, finding new tactics and techniques, and getting better at hiding within our networks. The challenges we faced the past 30 years will inform how we think about the next 30 years, but they are going to be different challenges that require new ways of thinking and new solutions. With a broader community, the CTA can facilitate that discussion.

CTA Feature Update

CTA AND THE COMMUNITY EFFECT

When I think of a community, I think of people with common interests brought together to achieve common goals. Over the years, CTA has worked to provide a place where our members can find a community focused on our shared goal of improving the cybersecurity of the global ecosystem. We come together to share information and collaborate, making the internet safer for the public while disrupting the malicious actors that seek to take advantage of the vulnerabilities in systems and society.

CTA's sharing continues to include diverse observables and samples with the relevant context needed to protect customers and better understand the threat landscape. CTA members provide up to 30 different types of observables and share upwards of 400,000 observables per day through our automated platform. Members have increased their sharing of MITRE ATT&CK techniques and routinely identify the sector and country where malicious activity was observed. In 2022, we leveraged our community to build a working group and review the quality of our data and identify additional sharing that would best help our members. The working group then developed recommendations to drive sharing of new context and observable types that members want.

In 2023, we aim to increase the volume of malicious file samples that are shared via our automated platform. We will also prioritize identifying which CVE is being exploited in a security incident. This CVE context can be used by our members to better understand which CVEs are exploited most often, giving our members the ability to engage directly with their customers to educate and prioritize which vulnerabilities to patch. We are also developing a methodology that will allow members to share confidence levels associated with the observables they are sharing, helping members improve their ability to action shared observables and compare assessments of confidence.

Our community also continues to build trust through our early sharing program and regular collaboration. CTA members shared nearly 200 blogs and reports before their public release in 2022, ending the year on a high note with 22 in December alone. Members can often action the information in these reports as soon as they receive them, ensuring their customers are protected as soon as possible. CTA continues to bring researchers together to discuss recent research and collaborate on the issues of the day.

Communities require trust to engender collaboration and achieve our common goals. At CTA, we continually strive to provide opportunities for our members to build trust and engage in a strong community of cybersecurity providers. We look forward to seeing what our members can do together in 2023!

BY NEIL JENKINS
CHIEF ANALYTIC OFFICER