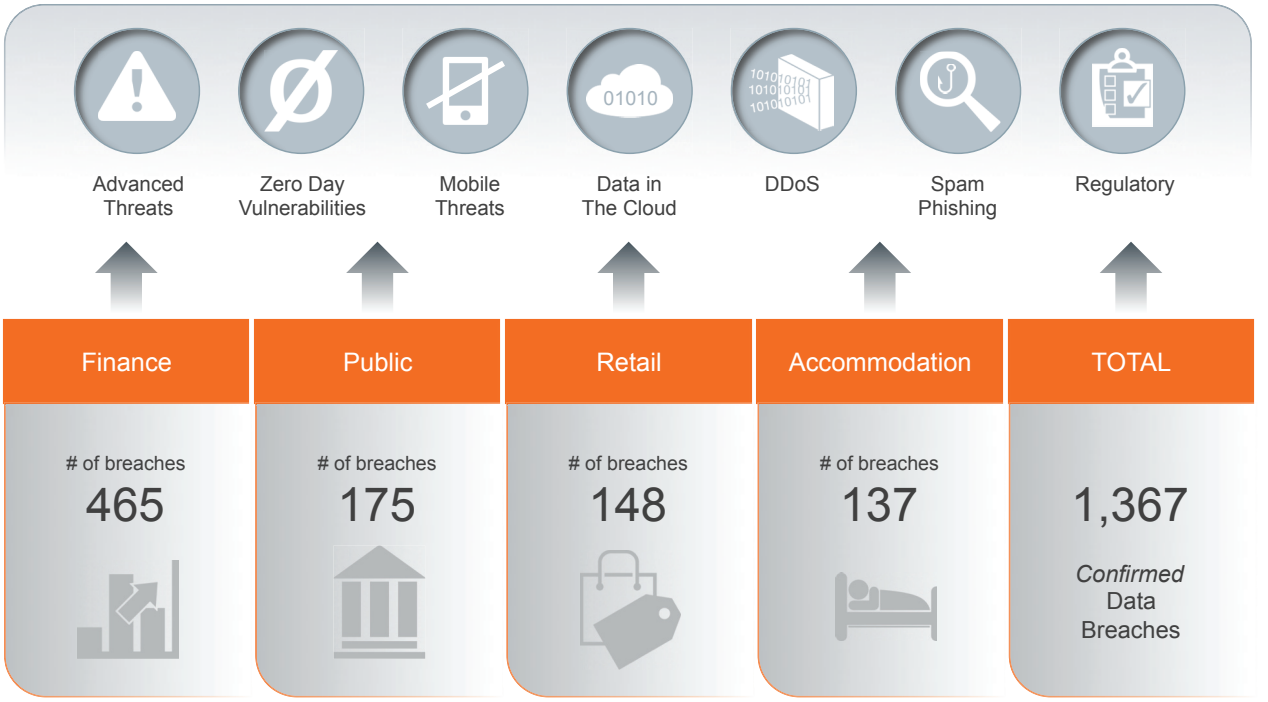
CYBER THREAT ALLIANCE

A New Way To Share Threat Intelligence

You don't have to be entrenched inside the world of network security to see how serious attacks have become in the world of computing. In the past year alone, we've seen breaches on a scale that we would have once considered unthinkable: tens of millions of credit card records, addresses, phone numbers, usernames and passwords, and other kinds of personally identifiable information have been stolen from corporations, organizations and government bodies. This information is quickly bundled up into packages and sold to criminals to facilitate financial fraud.

But the threats don't stop with the theft of customer data. Other attackers focus on building large botnets and illicit infrastructure for different means. Botnets today are often used to launch massive Distributed Denial of Service attacks on targets located around the world. Recruiting a botnet and taking a competitor offline for an extended amount of time is literally as simple as a few mouse clicks and sending a handful of anonymous virtual currency to the bot's master. Other botnets are used to help distribute spam by the billions and infiltrate social media accounts to spam stories and comments that typically link to sites selling counterfeit goods.

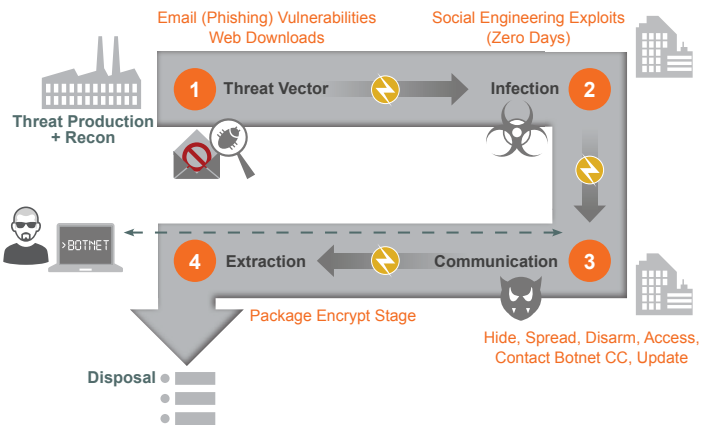
The Verizon 2014 Data Breach Investigations Report states that, in 2013, over 63,000 incidents were reported across 95 countries with 1,367 of these leading to actual breaches. Although financial organizations were the primary target, all verticals were attacked.



Source : 2014 Verizon Data Breach Report, 2013 data

Stopping Advanced Persistent Threats

Advanced persistent threats, also called advanced targeted attacks, take the average threat life cycle shown below and change each part to make the whole process more elusive. Cybercriminals, acting alone or in groups, utilize phishing emails and zero-day vulnerabilities as favorite infection vectors. These criminal operatives use fresh and often highly customized code to get past existing signature-based malware defenses and, once inside the network, command and control botnets to orchestrate the extraction of data.



To stop targeted, advanced threats you need the most relevant threat intelligence in a very timely manner. It's clear that the battle against online criminals is staggering in scope and difficult for any one group to combat effectively and with agility.

What is Being Shared Today?

Since the early days of network security technology, security companies have been sharing threat information. As far back as the 1990s antivirus companies have shared virus samples with each other. However, their methods of sharing have been suboptimal, with no central standards to define format or even the naming of malware. Sometimes antivirus companies would even publish a new virus sample before sharing to claim bragging rights. A more recent and promising initiative – Norman Sample Sharing Framework (NSS) — was born at VB2009 and was introduced at Caro2010. Some companies are already using this framework to exchange virus samples.

The bigger issue is that viruses are only one of many elements of the threat life cycle, and further, while the endpoint is an important place to stop attacks, sensors and prevention systems are also needed in network, storage and management systems. These vendors too should be contributing and sharing.

Unlike the early malware sharing initiatives driven by a few commercial companies, the CVE (Common Vulnerability & Exposure) initiative was driven by an independent organization (MITRE) and supported by the US Department of Homeland Security. Now the vulnerability management community has a standard way to identify vulnerabilities through the National Vulnerability Database. Groups like FIRST and a global network of Computer Emergency Response/Readiness Teams (CERTs) have built their own structures to dispatch information to their members and Internet users as a whole. These groups have done a great job linking together vendors and federal agencies focused on, among many other things, combatting the people responsible for crime on the Internet.

Given their huge installed base of end users, Microsoft also has a big part to play when it comes to threat intelligence sharing. It started the Microsoft Active Protection Program (MAPP) in 2008. The program was extended through MVI (Microsoft Virus Initiative) and VIA (Virus Information Alliance). More recently Interflow was established, a security and threat information platform. and has since established Interflow, a security and threat information exchange platform, currently in a private preview, for professionals working in cyber security.

More recently industry verticals have been starting alliances to try and share information more quickly. The retail industry has been particularly hit in the last 12 months. The Retail Industry Leaders Association (RILA) launched the Cyber Security and Data Privacy initiative, which will work closely with the Department of Homeland Security. Almost simultaneously The National Retail Federation announced it was going to establish a retail- specific Information Sharing and Analysis Center (ISAC). Speaking of ISAC, the National Council of ISACs listed at least 15 different ISAC organizations ranging from Utilities, Emergency Services, Transportation, to Healthcare. One of the most successful is FS-ISAC for the Financial Services.

How companies and organizations utilize threat intelligence can be one of the defining methods to detect, react, respond and deter online attacks. In the past, much of that information required a pair of human eyes to review and interpret the data and act on the intelligence gathered. Today's online criminals typically bounce from place to place and computer to computer as fast as you can snap your fingers, making the intelligence you looked at from a few hours ago ancient history. The only way to be able to respond to threats in a timely manner is through automating actions based on the threat intelligence you collect as quickly as possible - seconds matter during an active attack.

MITRE, with assistance from the US Department of Homeland Security, has created a new framework for sharing information: STIX and TAXII. STIX (Structured Threat Information eXpression) is an open language used to represent threat-specific information in a structured manner. TAXII (Trusted Automated eXchange of Indicator Information) is an open set of services and protocols, which allows groups to securely exchange STIX information. Both are freely available, community-driven and showing very good adoption rates among many groups and communities.

Is it time for a NEW type of partnership in the security world?

If you asked this question to companies that have been breached, the answer would be a definite yes. It is very apparent that security companies are still reluctant to share the best threat intelligence when they could market any new finds to their advantage. At a time when advanced threats seem to lead to breaches every day while Enterprises spend more and more on security products, the industry needs to assess what changes are required.

The Cyber Threat Alliance (CTA)

The Cyber Threat Alliance is a group of cyber security practitioners from organizations that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and/or their customers.

The CTA's founding members are Fortinet, McAfee, Palo Alto Networks and Symantec, with an open invitation to other organizations that share in our goals and objectives and meet the minimum requirements for participation. These four organizations are commercial entities answerable to shareholders, and they will compete in the market based on their product and corporate differentiators – however they have decided to put the customer first and make the very best and latest threat intelligence available to their substantial end point and network security appliance installed bases.

What are the goals of the Cyber Threat Alliance?

The goal is to disperse threat intelligence across all member organizations in a timely manner to raise the overall situational awareness and better protect their organizations and their customers.

Initially the focus will be setting up a simple process whereby members can share the latest threat intelligence. Later more sophisticated standards allowing richer information will be implemented. Longer term, as membership increases, quality controls will become stricter across members again placing an emphasis on quality versus quantity.

What type of threat intelligence will the Cyber Threat Alliance be sharing?

To be effective against advanced threats, the CTA will first focus on important individual elements of the threat life cycle, like vulnerabilities and exploits, new malware samples, and botnet command and control infrastructure. In the future, contextual data about when and where attacks occur will be added, improving the group's ability to identify attack trends.

Commitment to Standards

As with all industry wide initiatives, the key to long-term success will be the development of standards — dedicated commitment to using technologies like STIX and TAXII to build rapid and actionable threat intelligence sharing in order to react quickly to threats. Fortinet, Palo Alto Networks, McAfee and Symantec have a large footprint of security devices and endpoints that reach across small businesses, retailers, large enterprises, as well as carriers and service providers. These companies maintain large and talented threat research groups combing the web for new threats and changes to existing threats and attacks. By combining the information gleaned by these groups, we believe it allows each member company to better protect their customers and the Internet as a whole.

The CTA's initial goals are to build mechanisms to allow rapid sharing of threat intelligence across some specific elements of the threat lifecycle: new malware as it appears online, botnet command and control information, as well as new vulnerabilities and exploits discovered.

It's essential for companies today to be able to go beyond basic information sharing – context is key. The CTA will allow member companies to put the intelligence shared into context, and will make that intelligence actionable by members who can use that specific information. It will also allow members to take effective and prompt action on that intelligence, based on each member's unique needs, technologies and processes. We believe this is one of the biggest pieces of the puzzle today.

Who can join the CTA?

The CTA's long-term goals include sharing other types of information based on member needs as well as encouraging and recruiting membership among other network, end point, security groups, organizations, and vendors. However there are specific criteria for membership. Potential members really need to contribute advanced threat intelligence in timely manner. Volume is not the objective – high quality threat intelligence is. All members will be measured on their contribution to the alliance.

If you are interested in learning more about the CTA, or would like to discuss how you can help contribute to the group, please visit us on the web at

www.cyberthreatalliance.org

CYBER THREAT ALLIANCE

FORTINET, MCAFEE, PALO ALTO NETWORKS AND SYMANTEC CO-FOUND THE INDUSTRY'S FIRST CYBER THREAT ALLIANCE

What is the Cyber Threat Alliance?

The Cyber Threat Alliance is a group of cyber security practitioners from organizations that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and/or their customers.

What is the goal of the Cyber Threat Alliance?

The goal is to disperse threat intelligence on advanced adversaries across all member organizations to raise the overall situational awareness in order to better protect their organizations and their customers.

Who is in the Cyber Threat Alliance?

Founding members are Fortinet, McAfee, Palo Alto Networks and Symantec. There is an open invitation to other organizations that share in our goals and objectives and meet the minimum requirements for participation.