Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Importance of Business Information in Cyber Threat Intelligence (CTI), the information required and how to collect it

Today most threat feeds are comprised of IOCs with each feed providing 1-10M IOCs per year. As the CTI platform adds more feeds , the ability to filter and prioritize threat information becomes a necessity. It is well known that the SOC, Incident Response, Risk and Compliance groups are the primary consumers of CTI. Generating CTI prioritized in order of relevance and importance is useful to help focus the efforts of these high-performance groups. Relevance and importance can be determined using business and technical ...

Copyright SANS Institute

Author Retains Full Rights

AD

Applying Business and Technical Context to prioritize and generate relevant Cyber Threat Intelligence (CTI)

GIAC (GREM) Gold Certification

Author: Deepak Bellani, deepak.bellani@gmail.com
Advisor: Mark Stingley
Accepted: April 19, 2017

Abstract

Today most threat feeds are comprised of IOCs with each feed providing 1-10M IOCs per year. As the CTI platform adds more feeds , the ability to filter and prioritize threat information becomes a necessity. It is well known that the SOC, Incident Response, Risk and Compliance groups are the primary consumers of CTI. Generating CTI prioritized in order of relevance and importance is useful to help focus the efforts of these high-performance groups. Relevance and importance can be determined using business and technical context. Business context is organizational knowledge i.e. its processes, roles and responsibilities, underlying infrastructure and controls. Technical context is the footprint of malicious activity within the organization's networks, such as phishing activity, malware, and internal IOCs. In this paper, we will examine how business and technical information is used to filter and prioritize threat information.

© 2017 The SANS Institute Author retains full rights.

© 2017 The SANS Institute, Author Retains Full Rights

1. Introduction

The Cyber Threat Intelligence (CTI) function in most organizations is heavily reliant on external threat information feeds received from various sources such as law enforcement, Information Sharing and Analysis Centers (ISAC), and paid feeds by commercial providers. Most threat feeds consist of Indicators of Compromise (IOC) with each feed providing 1-10M IOCs per year. Information is gathered from bulletins, alerts and files exchanged via email and DropBox. Very soon the sheer volume, types and formats of threat information becomes overwhelming to standardize, process, analyze and action quickly. According to a recent SANS survey (Shackleford, August 2016), only 28% of surveyed organizations have a dedicated CTI team, which suggests that in most organizations, already stretched security resources have CTI as one of their many duties, forcing them to run on maximum effort. If your organization has the budget to spend on CTI tools, then this becomes somewhat easier with automation, but today most teams manually comb through IOCs and use spreadsheets and scripts to find evil in their environment (Paul Poputa-Clean, January 2015).

Operating at maximum effort on a daily basis for a sustained period-of-time results in burnout (Colin Chisholm, March 2016) making this approach unviable in the long term. According to the same survey (Shackleford, August 2016), only 52% of the respondents indicated that CTI tools are used, with no integrations with other security tools. Why? While threat cataloging, storing and sharing standards exists, they are not widely used, and in most cases threat information is not prepackaged, for example in STIX while sharing, limiting the use of automation as a force multiplier (Shackleford, August 2016). Industry is aware of this problem and is taking steps to standardize (OASIS under the leadership of Dept. of Homeland Security), integrate and automate. For instance, SIEMs collect logs from devices across the enterprise and therefore are the best place to look for IOCs and the chain of events leading to a compromise or an actionable event. Many SIEMs have recently developed threat information related capabilities such as automated feed ingestion and search, which is evidenced by 43% survey respondents using SIEMs for CTI activities (Shackleford, August 2016). Unfortunately, as detection capability catches up, technical IOCs develop shorter life-

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

spans forcing CTI professionals to move up the kill chain to using TTPs, which for the most part is still involves homegrown solutions (Shackleford, August 2016) or manual identification, categorization, analysis, and action. All the while, time remains of the essence.

The confluence of the above factors introduces the need for criteria that help prioritize efforts and accelerate the process to analysis and action. Business context such as critical business processes and infrastructure information, sensitive data, key personnel, mission critical service providers, nature of connectivity and controls will help prioritize threat intelligence efforts for immediate action. Analysis of the enemy's malicious footprint within our environment yields an abundance of information, such as our gaps and critical vulnerabilities, their ability to exploit, traverse and hide, the data they deem valuable and exfiltrate, people they target and how, and most importantly how quickly were they able to infiltrate and action on their objectives. This tells you not only about the enemy, but if the cybersecurity apparatus is appropriately focused (direction and depth), and if the exploitable targets and assets overlap with the organization's high-value targets and assets.

Most CTI Teams today struggle to get to the analysis phase and answering the above questions, as evidenced by less than 15% of the respondents that had achieved aggregation, processing of data into a full picture view that wraps events with IOCs (Shackleford, February 2015). The resources are stretched and turnover is high, and yet the team does not want to miss a single indicator or the potential presence of an enemy. What should the team work on first? How can this prioritization be performed in a repeatable and consistent manner? What are the elements that assist with this decision? This paper will attempt to answer some of these questions.

2. Pre-requisites

The most important pre-requisite for securing the organization is a blueprint that provides information on the organization's infrastructure and assets (Townsend, McAllister, September 2013). An automated, accurate, and current version of blueprint could be a configuration management system, which provides insight into the

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

organization's assets, their location, their relationship to other assets, and potentially the path an enemy might take to get to them. Mature IT organizations have their business services mapped from the top down, starting with the user down to the storage device that holds the data. This information is used to identify the impact of an event or incident on the infrastructure and business operations (Department of Energy, April 2000). Configuration information is the crucial foundation on which the security architecture is overlaid, such as application availability, network, and intrusion monitoring platforms, full packet capture and logging. The ability to search through logs for Indicators of Compromise is required, and if it can be automated using a script or native functionality within a tool, it is a huge help. Most vendors of security products are now automating the ingestion of threat feeds within SIEMs, and functionality if a match is found or specific criteria are met, provide search and alert functionality (Dr. Eric Cole, April 2016). The benefit of correlating configuration information with security events is the ability to lookup the past chain of events, identify upstream and downstream impact, and to gauge the intent of the enemy, for example, disrupting a business service or targeting sensitive data. Various aggregators, such as Splunk, assist in a similar fashion and are much easier to setup and use compared to an SIEM, but as of now, don't provide the detailed drill down capability to the device level.

Another requirement is the access to threat information. This can be accomplished via files, emails, alerts, bulletins and feeds. Threat information used for a variety of security measures, such as, detecting footprints of malicious activity within internal networks, preventing access to destinations that might cause harm, and disseminating signature information to the various detection and prevention appliances (Shackleford, August 2016). This information can be enriched using some additional resources such as VirusTotal to identify related behavior, for example, the name of an injected .dll file and its location. Technical threat information, such as file hashes and IP address are specific and have a short life span, hence better suited to automated ingestion (Paul Poputa-Clean, January 2015). Operational threat intelligence is about a near-term imminent attack or an attack in progress (Chismon, Ruks, MWR Security, 2015). Again, this information is very specific but higher up the kill chain, for example, the attack vector used such as spear phishing, the weapon deployed such as .pdf attachment and the vulnerability

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

exploited. Strategic threat information is generally more verbose, and not easy to automate, for example threat actor dossiers containing their background, patterns in their past activities, and the weapons deployed (Paul Poputa-Clean, January 2015). Across all these threats, there is a modus operandi to be understood, malware to be analyzed, and specific characteristics to be documented, yielding significant insight into the enemy.

Malware is the enemy's weapon of choice, and they have a vast arsenal which includes malicious URLs, keyloggers, bots, information stealing Trojans, rootkits, and file loaders, to name a few. A variety of infection vectors is used, like large-scale spearfishing campaigns, seemingly innocuous monkey videos or factory installed applications on devices, that provide a backdoor to the enemy. After compromising the victim, the approach could be a quick smash and grab, or a persistent settlement and long-term intelligence gathering (F-secure Labs. The Dukes). Malware analysis can reveal significant information about the enemy such as notable texts, which could be campaign identifiers providing both the date and the target of the campaign, or a URL(s) for command and control (Lenny Zeltser, February 2015). The vulnerability exploited to spread, coding languages used to provide functionality and assist with obfuscation, and the modules written to develop persistence, all provide insight into the enemy's capabilities and direction. A malware analysis laboratory is required to access this treasure of information. It's preferable to have it run in a disposable and reversible environment, such as a virtual machine, and the toolkit must consist of a disassembler and debugger such as IDAPro and OllyDbg, which are free to use and easily available. Some automated analysis capability, such as the BinText or PeScanner tools and Windows command line such as Strings2, can be used for a quick extraction of some embedded strings. OfficeMalScanner for MS Office documents and JSDidier tools for PDF are very useful for analyzing documents. A memory analysis tool such as Volatility Framework will complete this toolkit nicely (Lenny Zeltser, March 14 2015).

3. Current Approach

The Intelligence function within the military is mature, and commanders rely on it to win wars. Cyber Threat Intelligence while still in development, uses a variety of non-standardized information sources, borrowed tools from other cybersecurity functions,

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

scripts and spreadsheet magic, and produces remarkable results. Correspondingly, 64% of SANS survey respondents felt CTI improved their overall security and CIRT functions, and 73% felt it led to better and more informed decision making (Shackleford, 2016). Over 48% of the respondents also felt that CTI helped reduce breaches, which saved of tens of millions of dollars and in some cases hundreds of millions in capital market value. As a point of reference, Yahoo stock price dropped 5% in a matter of hours after their major data breach was announced (Reuters, December 2016).

3.1. Sources of threat information

Insight into what the enemy looks like, its activity and behavior, is obtained from peer teams who share the indicators and signatures they find. This sharing is organized via threat feeds. Historically, the intelligence and the military agencies and lately cyber security companies have been sharing their analysis and putting out reports detailing patterns in enemy behavior, also known as tactics, techniques, and procedures (TTP) and technical indicators used to paint a picture find and the enemy. Finally, the enemy does communicate with its creation and task it to perform some activity within our network. Network packet capture and analysis provides some insight into that activity (Sans Institute, July 2016).

3.1.1. External IOCs (threat feeds)

The CTI function in most organizations is heavily reliant on external threat intelligence information received from various sources such as Information Sharing and Analysis Centers (ISAC), US Cyber Awareness System (US CERT), Automated Indicators Sharing (AIS) via the CISCP program developed by DHS, public feeds such as MalwareDomains, Open Threat Exchange (OTX) and paid feeds by commercial providers. Additional intelligence information sources such as Zeus Tracker, CyberCrime-Tracker and SpyEye are used by CTI teams. It’s also a good idea to monitor for connections to known Tor exit nodes and regularly check the various Pastebin sites such as Slexy, Pastie, Github, Frubar Paste and Codepad.

Threat feeds contain observables such as malicious IP addresses, domains, file hashes, phishing emails sent by adversaries, malware information, and vulnerabilities exploited. Paid feeds can provide aggregated threat information, threat scores, reduce

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

false positives and provide some enrichment information. Customized threat feeds can provide additional services, such as compromised credit card information, money mule information, compromised employee email account information, compromised company (internal) servers and IP address information. The next step is to look for and block these observables using SIEM, endpoint detection, intrusion detection, sandboxes, intrusion prevention systems and aggregators (Ricardo Dias, October 2014). Remember to enable the file hashing feature in the logging appliances and software; only then will the logs contain file hashes. If a match is found, the CTI team pivots and looks for additional indicators of compromise, moving up and down the Kill Chain (Hutchens, et al Lockheed Martin). Additionally, procedures are followed in accordance with the organization's cybersecurity policies, such as notifying the CIRT team for further investigation.

3.1.2. Threat Reports

The National Cyber Investigative Joint Task Force (NCIJTF) at the Federal Bureau of Investigation (FBI), produces a 'daily digest' called Cywatch, which is an amalgamation of current cyber threats and cyber incidents identified in the US and abroad. US-Cert regularly puts out reports under its publications section. Recently, the DHS and the FBI, released a Joint Analysis Report (JAR) on the malicious activity called Grizzly Steppe carried out by Russian actors. The enemy's TTPs and indicators of malicious activity were also offered, allowing organizations to search within their network for compromise. Other examples of free threat reports are Verizon's Annual Data Breach Investigations Report, Mandiant's Annual M-Trends, Symantec's Internet Security Threat Report, Microsoft's Security Intelligence Report and Akamai's Quarterly Security Bulletin.

Many threat reports provide comprehensive information on a threat actor, such as their history, evolution in capabilities, tools and techniques, weapons used, preferred infection vectors, decoys, their ability to exploit vulnerabilities, command and control operations, and any affiliation with state or criminal actors. The reports also generally contain tactical information such as observables attributed to the actor, but within hours of publication, these are obsolete (Mandiant APT1 Report). The strategic information in these reports is used to prioritize Cybersecurity spending, allocate resources, develop

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

policy, and often provide arguments to support a closer monitoring of targeted assets or acquisition of a new capability. For example, if malicious attachments and URLs were not shared so easily via email, there would be no need for sandboxes, URL whitelisting or antivirus scanning of files and attachments. IF CEOs and VPs were not frequently and actively targeted, daily backups of employee computers would not receive as much importance as it does now. Ransomware has motivated data dependent organizations to back up mission critical data with regularly and think out-of-the-box (Brian Krebbs, September 2016). The heavy exploitation of Adobe vulnerabilities is enabling organizations to prioritize the vulnerability management process and in some cases, consider restricting the use of certain products, such as Adobe Flash (Brian Krebbs, December 2016).

3.1.3. Using Network Tools to find malicious activity

The basic approach using network tools to find the adversary involves identifying unusual activity. For example, a deviation from ‘normal’ would be network traffic at unusual hours or unknown destinations. Outbound communication using an IRC or http channel at unusual hours that is not scheduled or expected requires closer examination. Packet capture tools like Wireshark are extremely useful in such cases, especially the ‘follow the TCP stream' functionality that lets you analyze the traffic characteristics like destination ip, port number, identify if any files were exchanged, and download the file(s) to compare its MD5 hash to known IOCs.

IDS and IPS systems can also be used to look for connections to malicious domains. The advantage here is the use of automation. For example, hunting for a malicious domain ‘chinacsrmap.org’ in http traffic, is made easy by using a Snort rule property like uricontent:”chinacsrmap.org”. On the downside, this approach does produce a high rate of false positives.

An advanced methodology to improve detection by reducing false positives and develop a more accurate response is the use of indicators moving up the Kill Chain (Hutchens, et al. Lockheed Martin). For example, in the Joint Analysis Report on Grizzly Steppe released by the DHS on December 29, 2016, different types of indicators were provided, such as file hashes, .dll filenames, and ipv4 addresses. Additionally, a Yara rule

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

was provided for the PHP web kit which included certain strings that are artifacts of the code used by the adversary. Network administrators were asked to review their network perimeter netflow or firewall logs using these indicators to assist in determining whether their network had experienced suspicious activity. While there are many drawbacks of that report, it is clear however that viewing the actions of the enemy in their entirety is more useful. Therefore, the road to cybersecurity advancement involves leveraging not only the powerful network tools but other internal IOCs and the analysis of enemy code as well (Brian P Kime, March 2016).

3.2. Current Prioritization

The prioritization process of threats is fragmented across most CTI shops. Many teams prioritize threats based on the order in which they are received in the feed. Some groups prioritize based on security bulletins indicating the hot vulnerabilities of the day. Some assign CVSS scores and action accordingly. To some degree, these approaches have worked as seen in the previously mentioned SANS survey. But with bad actors routinely making headlines, breaching networks, and exfiltrating mission-critical and non-public personally identifiable information, the damage to people's lives is significant and in some cases puts companies out of business. Clearly, a different approach that uses different prioritization criteria to provide better results is needed.

3.3. Analysts versus information

There are many issues that contribute to and exacerbate the problem of inadequate staff and the need for prioritization. We may have touched on them earlier, but below is additional information that will provide context and improve the discussion.

1. Team sizing

Many organizations are adopting a cautious approach to CTI and investment is not easy to come by (Shackleford, February 2015). Many leaders have no exposure to the intelligence agencies, hence have no insight into the compelling value delivered by CTI. Often teams in the industry and civilian agencies are multi-tasking CTI with other responsibilities. With limited insight into the organization, resources, and capabilities of the enemy, CISO and other C-suite leaders have little awareness of the nature and scale of response required from them.

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

2. General nature of the threat feeds

As seen in the industry commentary that followed the recent Grizzly Steppe JAR, the indicators provided needed additional contextual information to be useful, for example, the time the ipv4 were used by the Russian intelligence or their proxies. Consumers of threat feeds would also like the indicators vetted, a risk score, some industry or vertical focus, and the prepackaging in a standardized format (Shackleford, August 2016).

3. Analyst skills and training

Many CTI teams are made up of analysts from other branches of cybersecurity, such as security engineering, SOC and incident response. While these skills are foundational and valuable, what about critical thinking and the ability to analyze terabytes of data? (Shackleford, August 2016). What about tradecraft and structured analytical techniques? Analysts must be trained to spot indicators of change, track events, spot emerging trends and develop hypotheses on outcome and impact. After developing these hypotheses, analysts must evaluate all the evidence systematically to disconfirm the hypotheses (US Government, March 2009). Analysts can lean on the Kill Chain or Diamond Model to provide some structure for organizing the evidence.

4. Lack of Tool Integration

To be successful CTI must leverage all the tools used IT and Cybersecurity, and it needs a platform that integrates most of these tools with the threat feeds, resulting in a seamless cross-pollination of threat information, real-time analysis and automated remediation available at the press of a button for the CTI analyst (Shackleford, August 2016). While this ideal platform is not available today, some level of integration is available, such as firewalls and ePO ingesting signatures. Data Virtualization is another emerging technology that might help CTI analysts mine data, without having to worry about where and how it is stored. This approach does require the analyst to learn how to work with and interpret the data.

5. Coordination with Software Development on Vulnerability Management

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Software development teams rarely perform adequate software security testing and in many cases, do not remediate all the identified coding defects and security vulnerabilities. While in development a record of these 'known' defects and vulnerabilities is maintained. When the code is put in production, the handoff on these known defects and vulnerabilities does not take place. Often defective code is allowed into production to meet deadlines, with little accountability for the risk. In most cases, the solution can be simple, such as access to the code and testing repository for the security team enabling knowledge transfer and a handoff with a roadmap to address defects and vulnerabilities in the next agile scrum. An advanced approach is to adopt secure coding practices and integrate security plugins in developer IDE (Robert Schiela, July 2016). A step in the right direction is thinking of 'infrastructure-as-code' and using DevOps tools with security testing capabilities like 'Docker' (Alyssa Robinson, December 2016).

3.4. Coming up short

It is very difficult for most CTI teams to research, analyze and act on all the indicators provided by the threat feeds they subscribe to. In fact, per a recent SANS survey (Shackleford, 2016) that number is limited to approximately one hundred indicators per week. How does the CTI team determine if the hundred or so indicators will be the most impactful for their organization? What about the other indicators not looked at? Would not addressing those indicators in a timely manner result in the organization being the news headlines tomorrow? The constraints discussed above setup the CTI teams in a race against time and they are looking for approaches to help deliver maximum impact for their effort.

4. Recommended Approach

The current CTI prioritization process might benefit from additional sources of information that could act as filters helping distill what is most impactful. The filters must be reliable and allow the CTI analyst to quickly identify what is relevant and the best use of their time. This will help accelerate the cycle from standardize and process to action.

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

4.1. Additional Sources of Information

Two sources of information internal to the organization and very reliable as filters are the business context and the technical context. Business context consists of the business processes, dependencies and controls, and the technical context is the tools and TTPs of the adversary. The technical context is the result of an organization's experience with the adversary, therefore useful in sifting out IOCs associated with similar behavior. Business context helps sift out IOCs that are associated with processes and assets considered critical to the business.

As part of the Business Impact Analysis (BIA) organizations identify their critical assets and mission critical processes. It's also their fiduciary duty to document the dependencies and the safeguards (controls). This information is vetted at the management level and signed off by its officers, who in turn are held accountable for protecting the assets and the organization by the regulators, shareholders, Office of Inspector General (OIG) or Congress. The information in the BIA can be used to prioritize CTI efforts ensuring cybersecurity protects what is valued most. Technical context is analyzing the methods and the tools used or leveraged by the adversary against the organization itself or other similar organizations. It includes phishing attacks, malware, user behavior analysis, and pattern and anomaly analysis.

4.1.1. Business Context

1. Business processes, roles, and responsibilities

The Cybersecurity and Information Technology organization units exist to support the business or the mission. All the regulators require a detailed Business Impact Analysis (BIA) plan that identifies the business processes grouped per criticality, procedures, roles and responsibilities to ensure the continuity and survivability of the business in case of a mission-impacting incident. The critical processes are the heartbeat of the organization because they support the mission, revenue generation or customer service operations and therefore must have the maximum layers of cyber protection and operational redundancy. Using the BIA plan as a guide, the limited CTI resources can be prioritized to protect the organization. Threats affecting mission critical processes get addressed first, followed by critical, urgent and important processes. If the organization

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

has a good Enterprise Risk Management (ERM) process, then all the supporting policies and risk classification systems will be aligned, for instance, Third Party Risk Management (TPRM), Data Classification, Management and Governance, and Business Continuity (BC). This alignment is critical to ensure there is no subjectivity in communication to the CEO and Board of Directors. The smooth flow of information across the organization is critical to ensure Cybersecurity gets the decisions it needs quickly. For example, if some desktop computers at a branch are infected and the entire branch needs to be firewalled off to prevent the infection from spreading to mission critical information systems, the channels of communication for notifying organization leadership must be smooth, and previously identified protocols must be followed for containment and eventual remediation. If there is any subjectivity involved in evaluating and classifying the type, severity, and impact of the risk, the resulting delay may lead to miscommunication and potentially the wrong decision by leadership, putting the entire organization at risk.

Keeping the mission or business information current requires some level of automation to keep the overhead low during data gathering, and a scalable central repository where the information can be updated as things change directly by the various stakeholders or via automation. Information on the processes, their criticality, the products they support, their revenue impact, supporting applications, dependencies and underlying infrastructure is all valuable information to help prioritize the CTI team's efforts. Additional business information such as asset inventory including data assets, third parties supporting various business processes and the nature of their access to the network, and third party employees with access to sensitive organizational assets is required by the CTI team to identify weak links in the chain and enhance the resilience of critical processes.

2. Infrastructure maps and dependencies

Service dependency maps of IT application and infrastructure are critical for reducing downtime and strategic allocation of IT resources. Without visibility into IT applications and infrastructure dependencies, it is difficult and time-consuming to prioritize, triage, and resolve incidents. This information is also useful for the CTI teams

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

as they analyze the different scenarios involving breaches and the actions an adversary might take to achieve their campaign objectives. Over the last few years malware has been designed with longevity and versatility in mind, for example, OnionDuke toolset includes various modules for credential stealing, information gathering and denial of service. CosmicDuke had keylogging, taking screenshots, credential stealing, privilege escalation, persistence, information exfiltration, and user cryptographic certificate exporting capabilities (F-Secure Labs, The Dukes). The CTI shop cannot focus only on the perimeter defenses. It must follow a disciplined approach using a step by step evaluation of the various layers of infrastructure, dependencies, and existing controls to game out how the adversary will infiltrate, the steps they will take to cover their tracks and the evidence they will leave behind (Brian P Kime, March 2016).

3. Controls

It is critical to document control information for each process, application, and asset. Data shared with a third party must be documented, including the type of data shared and protection mechanisms such as encryption, masking, and tokenization used. A particular challenge is legacy systems, for which little to no documentation is available, and the resources have left the company taking that knowledge with them. IT management is hesitant to make changes to the environment because of the critical services supported and availability expectations. Mainframe operations and SWIFT terminals are perfect examples of such legacy systems.

Technology is rapidly rendering many controls obsolete, for example, the use of 3-DES is only reserved for legacy systems, while AES is the new standard. Adversaries are now using cloud computing to crack passwords making twelve character passwords unsafe. Cloud compute service providers are being used to host temporary domains for phishing campaigns, infection and C&C (Darren Pauli November 2016), overwhelming firewall blacklisting controls. As mentioned previously, with rapid security staff turnover, if control information is documented, it can be tested regularly and enhanced when needed to ensure operational effectiveness. If the control is operationally effective, it is another barrier between the asset and the adversary and one action item less for the CTI team.

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

4.1.2. Technical Context

1. Malware analysis

Malware provides an abundance of information and the malware reverse engineer extracting this information is an underutilized resource in most CTI shops with many organizations not viewing it as a top three area for skilled resources, as evidenced in the most recent SANS survey (Dave Shackleford, March 2017). For a CTI shop to be able to generate its own intelligence and contribute meaningfully to the community, an investment in this capability is highly recommended. To support this recommendation, let's take some notable incidents and highlight how malware analysis provided some valuable threat intelligence.

In mid-2016, a Remote Access Trojan (RAT) NanHaiShu surfaced in Southeast Asia finding victims with some relation to the territorial disputes in the South China Sea. Targets included the Department of Justice of the Philippines, organizers of the APEC summit, and an international law firm representing the involved parties (F-Secure, July 2016). A spear fishing campaign was used to infect the targets prior to key dates, such as March 2015, the deadline for the Philippines to submit a response, June 2015, the deadline for China to submit a response, October 2015, news on US Ship movements, November 2015, the APEC Summit. A VBA base64 decoder function popular amongst Chinese programmers was found in the malware, and all the C&C servers pointed to IP address in China. Coding characteristics such as the use of SCRIPT tag to move the IE window outside the viewable area, resizeTo command to hide the window, and common jscript routines found in the malware samples, connect these incidents and the threat actor orchestrating them. Some adversaries have a preference for tools and C&C, for example, APT1 used Remote Desktop extensively on their infected hosts, and also used HUC Packet Transmit Tool for 100% of their communications between the IP addresses attributed to them (Mandiant APT1 Report). The use of Remote Desktop Protocol (RDP) provided valuable information such as the use of Chinese (Simplified) – US Keyboard, assisting with attribution. The targets of industrial espionage were spread across several key industries, four of which are strategic emerging industries in China's 12th Five Year plan. The attacks coincided with a large deal or negotiation often giving the Chinese access to insider information and intimate knowledge of the other party's position.

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Across these campaigns, much of the code was the same or similar, helping association and attribution, for example, APT1's use of WEBC2 backdoor dates back to 2004. Terrabytes of data has been exfiltrated, almost always as .RAR files and ultimately routed to China.

Reverse Engineering the Tinybanker or Tinba malware will show four hard coded domains, all resolving to only one IP address 77.79.11.71 in Lithuania (Peter Kruse from CSIS and TrendMicro, 2012). This net block has many suspicious and malicious domains, including money mule websites, fake anti-virus, counterfeit goods, drive-by and C&C servers. To initiate the C2, this malware sends encrypted EHLO string as a message, artifacts such as cfg.bin and bin.exe files are created in the directory %ALLUSERSPROFILE%\Application Data\default. The infected hosts were directed to a defined list of websites, which on further research attributes them to a large organized gang operating out of the Eastern Block countries. Another APT FIN6, a gang that focuses on payment fraud, prefers to use commonly available malware instead of building their own tools, for example, Grabnew (a.k.a Neverquest and VawTrack) malware to capture user credentials and then download AbbandonPOS and Trinity, both POS malware (FireEye FIN6). In one campaign, FIN6 used the Metasploit PowerShell module to download and execute shellcode to setup a local listener, that would in turn, execute any code received over a specific port. FIN6 preferred to use utilities native to the host for maintaining stealth, such as Windows Credentials Editor for privilege escalation, and Plink, a command line utility to create SSH tunnels to its C2 servers so it can use RDP. It appears these FIN groups already have access or the credentials to their host which is not surprising as Germany, Russia, and Eastern Europe are the most sophisticated underground markets for trade or exchange of tools, credentials, and access (Nettitude Perception, July 2016), similar to communities dealing in stolen card data.

Lately, a sinister trend has gained traction with nation-state APTs, which is the use of crime-ware to achieve objectives. The BlackEnergy malware dates back to 2007 when it was used to send spam and harvest credentials, but the world took notice of a gang named QueDagh when they used BlackEnergy to target the Ukrainian government (F-secure BlackEnergy). It was the perfect black-ops weapon because it was easily

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

available and used by criminals in the past so attribution would be almost impossible. The malware toolkit came with builder applications used to generate its new victims, server side scripts and an interface to control the bots. The basic toolkit was simple enough for a novice to use effectively. The targets were political in nature and the weaponized attachments used in the spearfishing campaign had Ukrainian names. The attackers had researched their targets well, because these BlackEnergy malware samples referenced proxy servers, a feature prior versions did not have. One proxy server was associated with the Ukrainian Railway, another was an internal proxy under the domain giknpc.com.ua which in turn hosts three domains, one of them was Ukraine's fourth largest city in the southeast. The timing of the campaign coincides with Russia's incursions into Crimea and analysis of the code suggests the use of modular components to accomplish actions such as, such as hiding in legitimate files by hijacking existing drivers, .dll injection, harvesting credentials and exfiltrating information. The level of sophistication further confirms a cross pollination of skills, tactics, and tools.

As discussed Malware can be a very valuable contributor to intelligence gathering efforts and provide rich insights into the adversary, for example, a sophisticated modular code with stealth indicates a highly skilled or well-resourced adversary. If it's a smash and grab of credentials and financial information, then it's most likely a criminal gang, versus a targeting of political organizations, stealth, and persistence indicating a nation state. Malware that has not been seen in the wild before suggests a custom toolset for a fresh campaign, and if it coincides with significant events in the business context then, you know you are probably dealing with a well-prepared adversary and their objective.

2. Phishing activity

Phishing was used in 95% of the incidents attributed to state-sponsored actors and over two-third of cyber espionage incidents have use phishing (Verizon 2015). The goal was not to elicit credentials or information from the user, but to just get them to 'click' on the weaponized attachment or malicious link so a beachhead could be established on the host and access gained to the network (Verizon 2015). There are enough news sources and awareness campaigns that warn users to be wary of emails from suspicious origins or those asking for sensitive information, nevertheless, 23% of recipients open phishing

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

messages and 11% click on attachments (Verizon 2015 DBIR). This trend is becoming unfavorable where 30% opened the phishing email, and 12% clicked on the malicious attachment (Verizon 2016 DBIR). The question is why do people 'click'? The attacker takes advantage of a combination of five factors – 1) Timing 2) Emotional state of the recipient 3) Tone of the language in the email 4) Information of the recipient on social media 5) Mental state of the recipient (Nettitude Perception, July 2016). Simply put, if the timing is right, the victim is emotionally stressed, which affects their mental state and their decision-making ability, and the email is relevant to the target, correctly worded, and convincing enough, the chances the target will 'click' skyrocket. That explains why APT1 requires English language proficiency from its employees (Mandiant APT1 Report).

If the contents of the phishing emails include industry specific terms and topics then it suggests that they were deliberately designed with specific targets in mind (F-Secure, July 2016). This provides clues to the threat's motivation, intent and objectives (FireEye APT28 report). The actor will register domains or use filenames pertinent to the topic that will interest the recipient, use exploits designed to work on target systems, for example, APT28 used emails written in Georgian, targeting the Georgian Ministry of Internal Affairs, and exploited a Windows XP vulnerability (FireEye APT28 report). The business context was significant because US, NATO, and Georgian cooperation was causing significant angst to Russia and some months later the two countries were at war. The targets of phishing also provide clues on the adversary, for example, the targeting of trade secrets and political organizations indicates a nation state, while the targeting of a PII data or POS terminals indicates cybercriminals (Nettitude Perception, July 2016).

3. Internal IOCs

Another area that is under-represented in intelligence gathering is internal sources, which as the data suggests only 54% of the survey respondents did in 2016 and 46% respondents did in 2015 (Dave Shackleton, March 2017). Internal traffic is a rich source of information, for example, minor spelling mistakes, typographical and syntactical error in header content and order provide network administrators the opportunity to detect malware (Tobias Lewis, December 2013). Another example of

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

Internal IOCs is behavioral detection which offers promising results over time and with fine tuning, for example, analyzing the timing of human generated versus automated events, user activity, data upload/download patterns and the variance of domains and URLs (Tobias Lewis, December 2013).

Other top IOCs of internal activity that can be automated and prioritized for action include requests on unusual ports, unusual privileged account activity, ex-employee or off-hour logins, large volumes of data transfers, suspicious registry or file changes and unexpected settings changes (Jason Mack, July 2015). To put this in business context, the company CEO or a database administrator exporting large data files using unauthorized applications such as Drop Box or Twitter outside of authorized hours is due for an immediate investigation by the CIRT team, and is also an action item for the CTI shop. Did the CEO have too much personal information about their hometown, school, pet's name, car, interests, and habits on their social media site? This information is used as answers to security questions and often tend to be included in passwords (Lewis K, 2014). Using their work computer did they access Linked In and click on a weaponized document, such as a candidate's resume or job description, from a bogus profile? Linked In is an example of adversaries creating fraudulent profiles with the intent of undermining the security of organizations (Satnam Narang, Symantec, Dec 2015). Malware is learning to hide in plain sight by using common web-based applications and social media sites that are 'allowed' by employers such as Twitter, GitHub and Cloud Drive (FireEye 2014).

End Users circumvent Acceptable Use policies because they feel that policies restrict them from using the tools and resources they needed to do their jobs (Cisco 2008). These security policies are outdated and need to be updated (Maxwell Chi, March 2011). Perhaps the security policy could be updated to allow a role based access to social media, for example, data owners or administrators should be allowed limited functionality, such as a Database Administrator might be allowed access to Linked In, but the security team could block the uploading or downloading of large files and browser redirection. Any unauthorized changes to the social networking application, its plugins, and other features should be blocked as well (Dr. Eric Cole, December 2010).

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

4.2. Recommended Prioritization

The CTI team should work on adversary targeting activity in decreasing order of importance as outlined in the BIA, for example, mission critical assets and processes should be a priority. If the most valuable asset of the organization is in the data center and phishing is the predominant tactic used, then technology and resources should be focused on blocking those emails and origins, while in parallel customized phishing training should be provided to data center staff mimicking adversary behavior. If a business chooses to grow its operations in a foreign country, and POS malware is very common, then all POS terminals and user laptops used in that country must have limited functionality and put on separate VLANs. Agency officials, CEOs and other officers such as General Counsels are high-value targets and their activity and access should be constantly monitored. If similar organizations report whaling in their threat feed the CTI team should notify their officers or officials, and immediately take appropriate action, such as, temporarily blocking personal email on company property.

5. Conclusion

Using the recommended approach aligns the CTI team directly with the organization's mission and the priorities defined by its officers. This approach does not change how the CTI shop functions but what it works on. It starts with identifying processes, applications, and resources supporting mission critical activities and the threats that seek to disrupt them. For example, if a threat feed identifies a vulnerability in an application that supports a mission critical process, it can be patched immediately by using an emergency change order and the required justification and approvals would not be hard to come by. If the CTI shop at a retail organization showed that by adopting domain and application whitelisting policies for endpoints, a 90% reduction in infections can be achieved forcing threats to change tactics, the company leadership would support it. This impact-driven approach makes strategic cybersecurity conversations with organization leadership easier, such as requesting and justifying budgets, restructuring processes, or requiring additional penetration testing for web based applications. Using business and technical context filters to sift through threat feeds and prioritize pertinent

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

indicators is a deliberate decision by the CTI team to narrow their focus, pick their battles and become more effective.

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

6. References

Dave Shackleford. (August 2016). The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing.

Dave Shackleford. (February 2015). The SANS Survey: Who's Using Cyberthreat Intelligence and How?

Colin Chisholm (March 2016). Boiling the Ocean: Security Operations and Log Analysis

Paul Poputa-Clean (January 2015). Automated Defense Using Threat Intelligence to Augment Security.

Department of Energy (April 2000) Software Configuration Management – A Practical Guide, https://energy.gov/sites/prod/files/cioprod/documents/scmguide.pdf

Dr. Eric Cole (April 2016) Threat Hunting: Open Season on the Adversary

Chismon, Ruks, (2015), Threat Intelligence: Collecting Analysing Evaluating; MWR Security

Eric M. Hutchins⇤, Michael J. Cloppert†, Rohan M. Amin, Ph.D (Lockheed Martin Corporation). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

US Government (March 2009). A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis.

Alyssa Robinson (December 2016). Continuous Security: Implementing the Critical Controls in a DevOps Environment.

Robert Schiela, (July 2016). Secure Coding Best Practices. Software Engineering Institute (SEI)

Townsend, McAllister (September 2013). Implementation Framework – Cyber Threat Prioritization. Software Engineering Institute (SEI)

Brian P Kime (March 2016) Threat Intelligence: Planning and Direction

F-secure Labs. The Dukes – 7 years of Russian Cyberespionage

Lenny Zeltser (March 14, 2015) – Malware Analysis Toolkit (https://zeltser.com/build-malware-analysis-toolkit/)

deepak.bellani@gmail.com

© 2017 The SANS Institute Author retains full rights.

Lenny Zeltser (March 14, 2015) – Mastering four stages of Malware Analysis (https://zeltser.com/mastering-4-stages-of-malware-analysis/)

Reuters (December 2016). http://fortune.com/2016/12/15/yahoo-shares-hack/

Sans Institute (July 2016). Score Security Checklist

Brian P Kime (March 2016). Threat Intelligence: Planning and Direction

Mandiant APT1 (October 2004) APT1 Report: Exposing One of China's Cyberespionage Units

Ricardo Dias (October 2014) Intelligence-Driven Incident Response with Yara

Brian Krebbs (September 2016) Ransomeware Getting More Targeted, Expensive (https://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive/)

Brian Krebbs (December 2016) New Critical Fixes for Flash, MS Windows (https://krebsonsecurity.com/2016/12/new-critical-fixes-for-flash-ms-windows/#more-37246)

Darren Pauli (November 2016). http://www.theregister.co.uk/2016/11/21/hacker_dishes_advanced_phishing_kit_to_hook_clever_staff_in_10_mins/

Dave Shackleford. (August 2016). Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey

F-secure Labs (July, 2016). NanHaiShu – RATing in the south China Sea

F-secure Labs. BlackEnergy and QueDagh, the convergence of crimeware and APT attacks

Peter Kruse from CSIS Security Group and Feike Hacquebord from TrendMicro (2012). W32.Tinba (Tinybanker) The Turkish Incident

FireEye (April 2016) Follow the Money, Dissecting the operations of Cybercrime Group Fin6

Nettitude (July 2016). Perception Financial Services Cyber Threat Briefing Report

Tobias Lewis (December 2013). Http header heuristics for malware detection

Verizon (April 2015) Data Breach Information Report

Verizon (April 2015) Data Breach Information Report

Jason Mack (July 2015). Using Network Based Security Systems to Search for STIX and TAXII Based Indicators of Compromise

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

FireEye (July 2015). HammerToss – Stealthy Tactics Define a Russian Cyber Threat Group

Satnam Narang, Symantec (Dec 2015). https://www.symantec.com/connect/blogs/fake-linkedin-accounts-want-add-you-their-professional-network

Lewis K (2014) Entrepreneur's Organization. https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Dr. Eric Cole (December 20110). Enabling Social Networking Application for Enterprise Usage

Cisco (2008). Data Leakage Worldwide – The Effectiveness of Security Policies

deepak.bellani@gmail.com

© 2017 The SANS Institute, Author Retains Full Rights

Last Updated: May 1st, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Security West 2017	San Diego, CAUS	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, CH	May 15, 2017 - May 20, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VAUS	May 21, 2017 - May 26, 2017	Live Event
SEC545: Cloud Security Architecture and Ops	Atlanta, GAUS	May 22, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, AU	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, GB	May 22, 2017 - May 27, 2017	Live Event
SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Stockholm 2017	Stockholm, SE	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Philippines 2017	Manila, PH	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS Riyadh 2017	OnlineSA	May 06, 2017 - May 11, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced