GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Detecting and Preventing Attacks Earlier in the Kill Chain

GIAC (GSEC) Gold Certification

Author: Chris Velazquez, chrisvelaz.cv@gmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: August 30, 2015

Abstract

Most organizations place a strong focus on intrusion prevention technologies and not enough effort into detective technologies. Prevention of malicious attacks is ideal, but detection is mandatory in combatting cyber threats. Security vendors will only provide blocking signatures when there is a near zero false-positive rate. Because of this, there are signatures that are not implemented resulting in false-negatives from one's security devices. This paper provides a look at tools that can be used to improve the detection of attackers at every phase of their attack. The intelligence learned from these attacks allows one to defend against these known attack vectors. This paper will look at a variety of open-source network IDS capabilities and other analysis tools to look at preventing and detecting attacks earlier in the cyber kill chain.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

With a wide variety of threats that we face in today's world one needs to implement strong preventative controls as well as good detective systems (Hutchins, 2011). Ever since the internet went global, there have been malicious users' intent on exploiting vulnerabilities in these systems (Hutchins, 2014). It's important to learn from these attacks and feed them back into one's tools to see whether other machines have been impacted by the same adversary (Hartley, 2014). This paper will largely focus on the Lockheed Martin Cyber Kill Chain and how to implement controls and technology to protect organizations.

The Cyber Kill Chain is an intrusion-based methodology that allows one to focus on the different stages of an attack (Hutchins, 2011). By implementing tools to foil attacks at the different stages of the attacks and identifying attacks in various stages, there can be detective and preventive measures taken to ensure that similar attacks are detected. A defense in depth strategy is very effective and is critical in stopping and detecting a variety of attacks that organizations face today (Krikken, 2014). It's important to have multiple layers to ensure that if one of the defenses is bypassed there is another line of defense to protect one's organization's assets.

The key is to see that one has the ability to detect and prevent attacks at every phase (Hutchins, 2011). By looking at a brief overview of technology, from host, to network level, one will have an opportunity to look at what tools or solutions may fit in one's organization (Krikken, 2014). Intelligence plays a huge role in today's cybersecurity world and is critical if an organization is going to be successful in defending against the threats (Krikken, 2014). By generating indicators of compromise, IOC's, one will be able to prevent and detect known attacks before an adversary is able to set up residence in one's environment.

2. Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain is an intrusion based attack methodology (Hutchins, 2011). This attack methodology is based on seven phases of a successful

© 2015 The SANS Institute Author retains full rights.

attack. The seven stages are depicted on Figure 1 below by Lockheed Martin (LMCO, 2011).

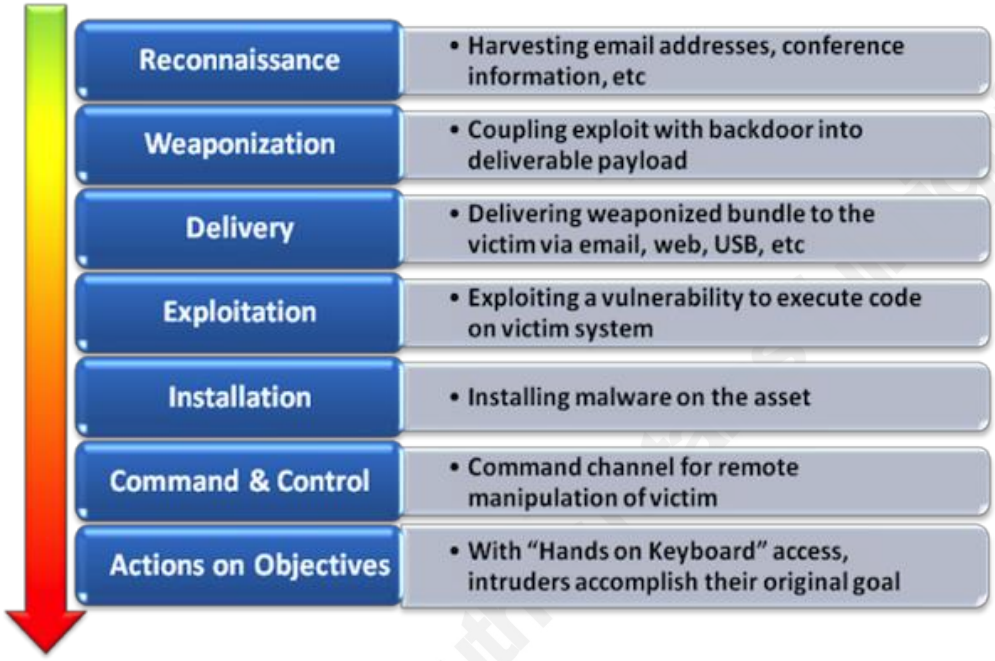


Figure 1- Lockheed Martin Cyber Kill Chain

By attempting to spoil an attack at every level of the kill chain, it will create a strong security posture (Krikken, 2014).

2.1. Reconnaissance

Reconnaissance is the first step of any sophisticated attack on an organization and is one of the stages used by an attacker most heavily (Hutchins, 2011). There are a variety of techniques that an adversary can use to achieve this goal (LMCO, 2014). The paper will look at both active and passive reconnaissance techniques and explain methods of mitigating the exposure of an organization to an attacker.

Active reconnaissance is an attack in which an adversary engages a targeted network to gain information about vulnerabilities (Rouse, 2014). "The simplest way to prevent most port scan attacks or reconnaissance attacks is to use a good firewall with properly implemented access control lists ACL's that will minimize the exposure of ports and services to the internet" (Rouse, 2014). An intrusion prevention system, IPS, is also helpful in blocking attacks that are attempting to potentially exploit a service on your network. IPS technology can detect scanning during an attack and shut them down before

© 2015 The SANS Institute Author retains full rights.

the attacker can gain too much knowledge of one's network. Active reconnaissance is detectable through the use of network perimeter devices, and security information and event monitoring tools, SIEM. Through the correlation of logs over a periods of time one can see who is probing one's network to determine who may be targeting your systems (Rouse, 2014). If an attacker is using an automated scanner then it will most likely set off alerts in IDS/IPS systems as well (Kim, 2014). Performing active reconnaissance on one's own systems from an external location, just as an attacker would, is valuable in determining if there are any vulnerabilities that are exposed to the internet.

Passive reconnaissance is an attempt to gain information about targeted computer systems and networks without actively engaging with the systems (Hutchins, 2011). This could be performed through the collection of information about users from the company website. This can include emails, telephone numbers or through user's personal social media. LinkedIn and other social media networks can hold information about employees and help an attacker identify their potential target. An employee's social media profile may provide information that may indicate particular technologies used by a company that will help an attacker plan and attack against an organization (Czumak, 2014). By understanding information about a potential victim, a social engineering attack's likelihood of success increases once a victim's hobbies or personal information is collected. Cybercriminals can also harvest information about a target by checking websites such as WhoIs to determine what public address space is owned by a target (Clark, 2014). Many information discovery activities are used heavily by advanced adversaries to help increase the likelihood of a successful attack on a target (Czumak, 2014).

Reconnaissance is one of the most difficult stages to detect from a security monitoring perspective. Active reconnaissance is being performed by adversaries all the time and cannot be prevented effectively. It's important to ensure that employees are well educated of the threats and that they protect the specifics of their information to ensure that cybercriminals aren't able to harvest that information to attack an organization.

Chris Velazquez, chrisvelaz.cv@gmail.com

© 2015 The SANS Institute Author retains full rights.

2.2. Weaponization

Depending on how much information an attacker was able to gain through reconnaissance a deliverable payload that will meet the needs of the attack objectives will be selected (Hutchins, 2011). This phase can be conducted at the attacker's convenience as well. The adversary can collect as much information about an organization and wait until they have an accurate weapon based on the amount of reconnaissance and intelligence gained on a target. Because this stage is largely dependent on the accuracy and amount of reconnaissance performed it's important to limit the exposure of an organization's publically available information to eliminate the ease and effectiveness of spear-phishing type attacks (Clark, 2012). Also, ensuring that known security vulnerabilities are patched quickly is very important in preventing exploitation.

2.3. Delivery

The payload of choice is then sent to the target by the most practical and effective means, which can include sending it by email, placing it on a USB stick then dropped near a target employee who is likely to insert it into his or her system, or target employees are lured to a specially prepared malicious website from where the target employee will be infected (Eijndhoven, 2011). The delivery phase is the first phase which an organization can implement technology as a mitigating control. Figure 2 shows the Cyber Kill Chain in action and the importance of its location in the kill chain.

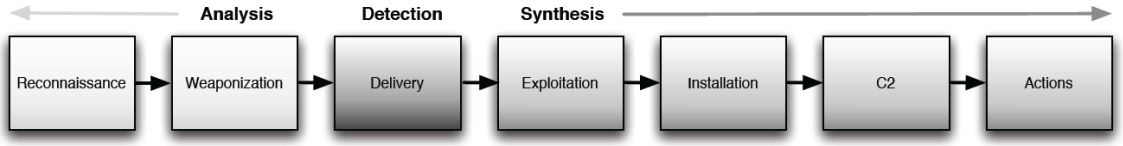


Figure 2- Kill Chain in Action

One of the first technologies that will be looked at is network intrusion detection systems, NIDS. There are many different solutions for NIDS that provide excellent capabilities; but for this paper Suricata will be looked at.

Suricata is a network IDS, IPS, and NSM engine that is supported by the community and is highly scalable (OISF, 2014). Suricata has the ability to do file matching file magic, file size, file name, extension, and file MD5 checksum. One will be able to determine what files have been downloaded on the network. If there is an

© 2015 The SANS Institute Author retains full rights.

indicator for a known bad IP address, one will be able to determine whether or not there were any files downloaded from that IP if the attacker is using clear text protocols. This file detection capability allows one to take an inventory of all files that have been seen on one's network and will allow one to correlate these events if they're are sent to a centralized SIEM.

The features described here are taken from the Suricata website user guide at https://redmine.openinfosecfoundation.org/projects/suricata/ page. The Suricata engine contains repository of potential malware that can be analyzed and all files. Live rule reloads allows one to use new rules without restarting Suricata which is important to ensure that one isn't missing events as a result of a scheduled rule upload. PCAP's of traffic enable you to have a network forensic capability and determine the types of network transactions that are occurring in your environment. Suricata rules contain large amounts of open source intelligence and signatures provided by the community. Suricata also accepts Snort signatures which are often provided from various threat intelligence sources.

The ability to apply higher-level inspection on network traffic, instead of just performing layer 3 and 4 analysis, is critical in detecting network based threats. With Suricata, one will be able to determine if one has files going to foreign countries by leveraging the geo-ip lookup capabilities built into Suricata. With multi-threading capabilities, Suricata is able to fully utilize powerful hardware platforms, from a single thread to dozens of threads. This allows commodity hardware to achieve 10 gigabit speeds in real live traffic without sacrificing ruleset coverage. Suricata also has flow-logging capability to get network statistics of one's environment which will help determine what users may be the top talkers.

This paper will look at demonstrating Suricata's ability to perform file analysis on a network. The Suricata engine uses a YAML, YAML Ain't Markup Language, configuration file that's very easy to read and that all the configurations for Suricata are set. The YAML configuration file makes it easy to determine what settings are configured making the administration of Suricata fairly straightforward. The simplicity of

© 2015 The SANS Institute Author retains full rights.

the YAML configuration file lowers the learning curve for administration and allows Suricata to be administered by administrators with minimal experience.

One of the very useful features of Suricata is file extraction which requires some configuration. The file extraction code works on top of the HTTP parser which itself is largely a wrapper for libhtp. The HTTP parser takes care of de-chunking and unzipping the request and/or response data if necessary. The HTTP parser runs on top of the stream reassembly engine" (OISF, 2014).

The control, `stream.checksum.validation,` controls whether or not the stream engine rejects packets with invalid checksums. This is normally a good idea, but the network interface performs checksum offloading a lot of packets may seem to be broken. This setting is enabled by default, and can be disabled by setting it to "no". The parameter `stream.reassembly.depth` controls how far into a stream reassembly is done. Beyond this value no reassembly will be done. This means that after this value the HTTP session will no longer be tracked. By default a setting of 1 Megabyte is used. 0 sets it to unlimited.

The parameter `libhtp.default-config.request-body-limit / libhtp.server-config.<config>.request-body-limit,` controls how much of the HTTP request body is tracked for inspection by the http_client_body keyword, but is also used to limit file inspection. A value of 0 means unlimited. `libhtp.default-config.response-body-limit / libhtp.server-config.<config>.response-body-limit` is like the request body limit, only it applies to the HTTP response body.

Each file that is stored will have a name "file.<id>". The id will be reset and files will be overwritten unless the waldo option is used.

© 2015 SANS Institute, Author retains full rights.

© 2015 T etains full rights.

Figure 3- Suricata File-Store/ File-log configuration

```
- file-store:
   enabled: yes      # set to yes to enable
   log-dir: /var/log/suricata/files/    # directory to store the files
   force-magic: yes  # force logging magic on all stored files
   force-md5: yes     # force logging of md5 checksums
   waldo: file.waldo # waldo file to store the file_id across runs
```

```
- file-log:
     enabled: yes
     filename: files-json.log      append: yes
     #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
     force-magic: no   # force logging magic on all logged files
     force-md5: no     # force logging of md5 checksums
```

Figure 3- Settings in Suricata

All settings in the stream engine, reassembly engine and the HTTP parser affect the workings of the file extraction. The files that are actually extracted and stored to disk are controlled by the rule language. The sample rule being demonstrated is below. Any files meeting this criteria are extracted and stored in the file.rules file specified.

```
# Store all Windows executables
alert http any any -> any any (msg:"FILE magic -- windows";
flow:established,to_client; filemagic:"executable for MS
```

Figure 4- Snort Rule to collect and store all Windows EXE

Once the configurations have all been set, Suricata is now ready to detect, and extract files that are being delivered to systems on your network. A list of hashes of all files is also available, and can be helpful when one is trying to determine whether specific files are exchanged over the network. For example, intelligence of a potentially malicious IP is received, a determination of whether there has been any files downloaded from that IP address can be made.

The WinSCP executable will be used to show Suricata's capabilities of file detection. For example, if one has intelligence that the website 37.235.108.13 (WinSCP) has been compromised, then a determination of whether users received a version of WINSCP that was laced with malware can be made. By taking a look at a JSON event

© 2015 The SANS Institute Author retains full rights.

that is sent to Splunk, we can see a sample of the log output provided by Suricata. These alerts will generate log events that show the following information.

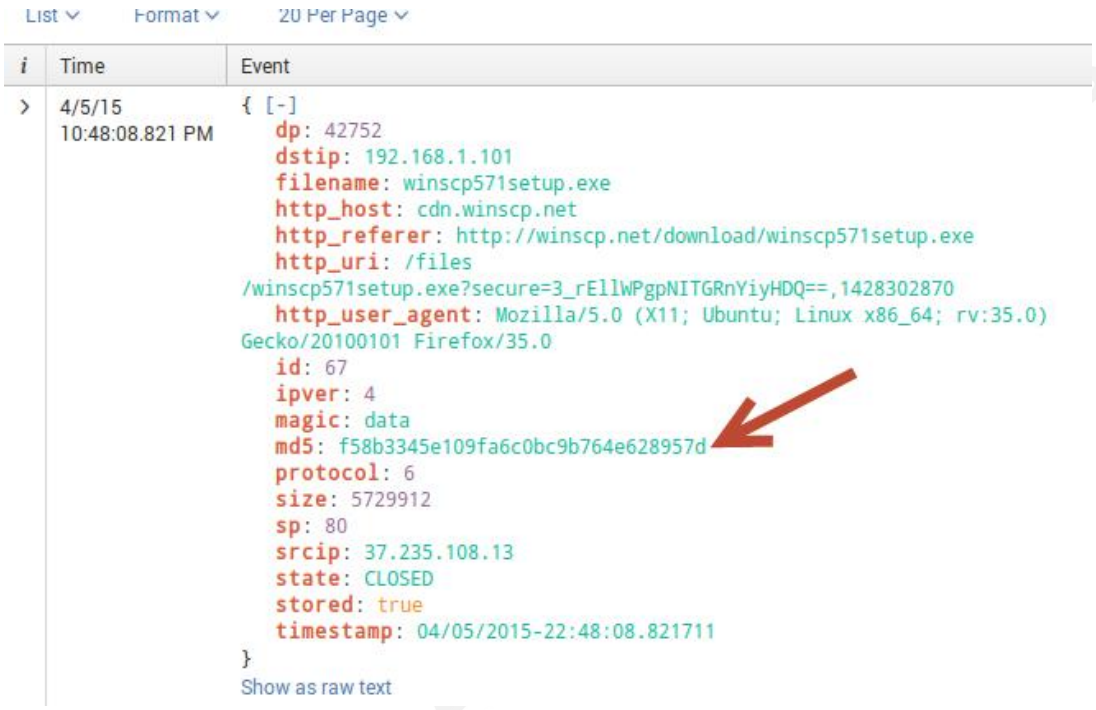


Figure 5-Suricata Rule Fire details in Splunk

Another scenario could be that the determination has been made that there is a machine at 192.168.1.101 that downloaded a file from the compromised site. Intel is received that the MD5 hash value of the file is f58b3345e109fa6c0bc9b764e628957d. A search in Splunk shows that particular file associated with that hash is stored on the Suricata server.

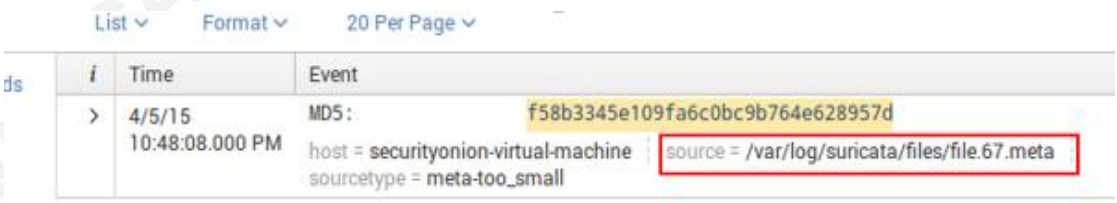


Figure 6-Suricata File Meta Data Log in Splunk

We can then go to the storage location of the file to acquire the file and perform some analyses on the file. Suricata provides the exact unaltered file and a check on the file shows that the file is indeed the same. Now that the file is acquired, additional analysis can be performed on that

Chris Velazquez, chrisvelaz.cv@gmail.com

© 2015 The SANS Institute Author retains full rights.

file.

```
securityonion@securityonion-virtual-machine:~/Downloads$ md5sum winscp571setup.e
xe
f58b3345e109fa6c0bc9b764e628957d  winscp571setup.exe
```

Figure 7 MD5 Hash of Windows EXE captured

If the system has the capacity to store PCAP files then you have the ability to perform some additional network forensic analysis as well. Suricata will break the PCAP files into the configurable size.

```
rw-r--r--  1 root root 10387549 Apr  3 22:11 log.pcap.1428124085
rw-r--r--  1 root root 10374076 Apr  3 22:18 log.pcap.1428124286
rw-r--r--  1 root root 10373032 Apr  3 22:22 log.pcap.1428124696
rw-r--r--  1 root root 10406052 Apr  3 22:22 log.pcap.1428124944
rw-r--r--  1 root root 10406138 Apr  3 22:22 log.pcap.1428124956
rw-r--r--  1 root root 10409740 Apr  3 22:22 log.pcap.1428124967
rw-r--r--  1 root root 10409302 Apr  3 22:23 log.pcap.1428124976
rw-r--r--  1 root root 10409668 Apr  3 22:23 log.pcap.1428124983
rw-r--r--  1 root root 10387287 Apr  3 22:25 log.pcap.1428124990
rw-r--r--  1 root root 10362558 Apr  3 22:35 log.pcap.1428125100
rw-r--r--  1 root root  1934876 Apr  3 23:00 log.pcap.1428125711
rw-r--r--  1 root root      114 Apr  3 23:07 log.pcap.1428127637
rw-r--r--  1 root root  9021997 Apr  3 23:30 log.pcap.1428128140
```

Figure 8-PCAP's of all traffic flowing through Suricata

There are many other features Suricata has to offer that aren't looked at in-depth here but can be valuable in detecting the delivery of malicious payloads. Suricata also has the ability to be an inline NIPS device that can block traffic based on rules as well.

Along with network based intrusion detection technologies, there also many host-based intrusion detection systems that can provide visibility into the endpoint to ensure that attacks are detected. Host-based detection technologies can be used to detect files that arrive on machines and either delete or quarantine a file before execution on a system. Prevention is ideal, but detection is a must in information security (Cole, 2001). These host-based agents can perform file integrity monitoring, analysis of files and registry changes on a system. They can also hash files of a system.

A HIDS can use a variety of detection mechanisms to detect attacks or intrusion attempts. One of the techniques HIDS can use is pattern matching to detect known attacks by their signatures, or the specific actions that they perform. "The IDS looks for

© 2015 The SANS Institute Author retains full rights.

traffic and behavior that matches the patterns of known attacks. The effectiveness is dependent on the signature database, which must be kept up to date. Pattern matching is analogous to identifying a criminal who committed a particular crime by finding his fingerprint at the scene (Shinder, 2005)". Fingerprint analysis is another type of analysis that can be performed to match. While pattern matching will be successful in detecting a variety of known attacks, it will be more successful if paired with anomaly-based detection to look for behavior that is abnormal.

Anomaly-based detection watches for deviations from normal patterns of behavior. This requires first establishing a baseline profile to determine what is normal in the environment. The IDS then begins monitoring for actions that are outside of those normal parameters. This allows you to catch new breach attempts that a signature has not been created for yet (Shinden, 2005). There are several different anomaly detection methods, including metric model, neural network, and machine learning classification. One of the problems with anomaly-based IDS is the higher occurrence of false positives, because behavior that is unusual will be flagged as a possible attack even if it's not.

Email is still one of the most successful methods of delivery into an organization (Clark, 2014). Spam filters are critical in stopping the delivery of malicious software into an environment. Malicious emails can be sent with a variety of methods including URLs, attachments, and in some cases malicious email bodies as well. In 2013, phishing was associated with over 95% of incidents attributed to state sponsored actors, and for two years running, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing (Verizon, 2015). The user interaction is not about eliciting information, but for attackers to establish persistence on user devices, set up camp, and continue their stealthy march inside the network (Verizon, 2015). Malicious phishing user training should be at the center of an organization's effort to secure its data and systems (Lovinus, 2014). Nothing is as effective as a well-trained, vigilant user for snuffing out suspicious network activity, and will prove time and again to be the number one malware tool money can buy (Lovinus, 2014). An HP survey showed that 69 percent of IT professionals experience phishing attempts for their credentials at least once a week and is one of their main security concerns (Wisdom, 2014). Email scanners that scan the

© 2015 The SANS Institute Author retains full rights.

attachments of emails can be a very valuable defense to prevent malicious payloads from entering your environment. Email URL scanners can also provide protection from links that may lead to malicious websites.

Drive-by-downloads are also a very common mechanisms used by attackers to infiltrate an organization. "Most drive-by download attacks use malware distribution networks, rather than being completely self-contained, the exploit code itself is hosted on a different web server and is exposed through the compromised web page using a technique like a URL embedded in malicious script code" (Microsoft, 2014).

(Microsoft, 2014)

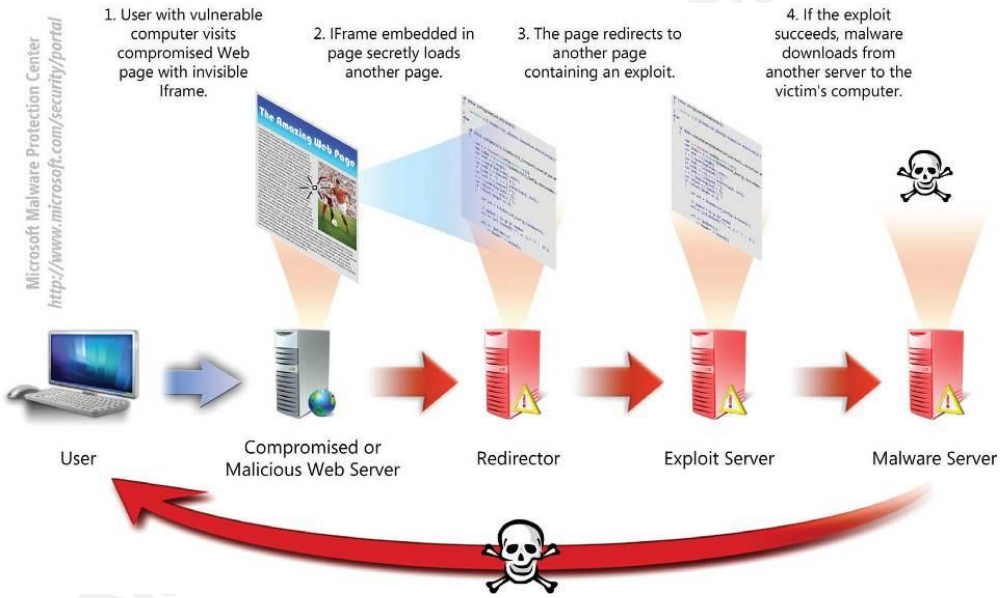


Figure 9- Microsoft Drive-by download

A mitigation technique of this risk can be to deploy web proxies to filter the categories of websites that users are allowed to access on your network. Network security devices that block and inspect files downloaded can help prevent malicious payloads from reaching systems (FireEye, 2014). The delivery of malicious files is not limited to the network, but also local attacks as well.

USB's still present a significant vulnerability in many companies. Because users can become infected just by inserting a USB drive and can take over a machine it is still a very common attack method. Worms are still frequently distributed and spread by USB

© 2015 The SANS Institute Author retains full rights.

drives (Microsoft, 2014). Since Malware scanners cannot scan the Firmware that is present on USB drives it makes very hard to defend against (SRLABS, 2015). These attacks aren't limited to thumb drives, but all types of USB devices from keyboards and mice to smartphones have firmware that can be reprogrammed to do all kinds of evil (Valcarcel, 2014). Stopping and detecting the delivery of malware is an important stage in the kill chain and is possible through a defense-in-depth strategy.

2.4. Exploitation

Exploitation is the next stage of the Cyber Kill chain and is essentially the successful delivery of a malicious payload to a user or system. Once the weapon is delivered to victim host, exploitation triggers the intruder's code.

Patching is one of the best methods to increase the difficulty of the exploitation phase. If the attacker has weaponized a payload that is exploiting a known-vulnerability and the required security patches are installed prior to exploitation then the attack is defeated. The ability to patch quickly is essential to ensuring that known vulnerabilities are not exploited on systems (GFI, 2012).

Application whitelisting is the one of the most powerful mechanisms for prevention of malware delivery onto systems (Fox, 2014). There are many different products available that provide host-based intrusion detection technologies that can perform a variety detection capabilities. The difficulty with application whitelisting is the overhead that it causes and the maintenance of software versions. (Fox, 2014). Whitelisting is a simple list of applications that have been granted permission by the user or an administrator. When an application tries to execute, it is automatically checked against the list and, if found, allowed to run. "An integrity check measure, such as hashing, is generally added to ensure that the application is in fact the authorized program and not a malicious or otherwise inappropriate one with the same name" (Fox, 2014). This type of protection can stop malware dead in its tracks. In large enterprises, where applications are constantly being changed, it becomes very difficult to maintain an accurate list of applications. Because of the difficulty of the maintenance of these lists blacklisting is usually implemented instead (Rouse, 2014).

© 2015 The SANS Institute Author retains full rights.

Blacklisting is not as comprehensive as whitelisting and is becoming obsolete due to the evolving threats in cybersecurity, but it is still a common practice in almost all organizations. Application blacklisting, sometimes just referred to just as blacklisting, is used to prevent the execution of undesirable programs (Rouse, 2014). Programs that have security threats or vulnerabilities should be monitored and protected, as well as those that are not inappropriate within any company. However, if there were not signatures that stopped the malware from being delivered then there is also a likelihood that the attack could contain a new variant of a malware that won't be stopped from a blacklisting mechanism. Blacklisting is the method used by most antivirus programs, intrusion prevention systems and spam filters.

2.5. Installation

Installation of a remote access trojans or backdoors on the victim system allows an adversary to maintain persistence inside the environment. Advanced techniques used by highly motivated attackers as part of an attack include maintaining persistence through by injecting code into windows applications, or even registry (McAfee, 2015). Although there may have not been a signature to detect the malware from being delivered to or exploiting the system, there may be an antivirus, AV, signature that vendors have ready for a particular malware (LMCO, 2014). AV won't catch truly advanced attackers, but may have an opportunity to detect known commodity attacks. Once attackers have achieved installation they may attempt to bury themselves deep in the system by changing many different files on the system so that they can maintain their foothold in the environment.

Once an attacker achieves persistence on a system the integrity of the machine and all of its data can potentially be compromised. Many users try to clean these malware infections using antivirus applications which may not be the best. An adversary may install a rootkit, which is extremely difficult to detect and nearly impossible to remove all remnants of the infection (Hoffman, 2015). Once a system has a known compromise the safest bet is to go with a complete operating system rebuild (Kassner, 2015).

© 2015 The SANS Institute Author retains full rights.

2.6. Command & Control

The attacker has successfully established a control channel from within one's network to an attacker's infrastructure. There are many different approaches that an adversary may use to establish an outbound connection. Attackers may use HTTP, HTTPS, or even DNS to send and receive data to a victim machine (CPNI, 2012). IDS and network devices, such as firewalls can detect these channels by searching across data from your organization. Some malware may call home frequently, however if the attacker is extremely patient then the malware may only reach out once a day or even less frequent (Hutchins, 2011). The detection of files using compressed methods, such as .RAR files, is important since attackers often use compressed formats to perform exfiltration of data (TrendMicro, 2012).

C2 methods can be broken down into 2 categories, either push, or pull. Attackers can use either a hub to send commands through or can communicate directly out to machines (CPNI, 2012).

(CPNI, 2012)

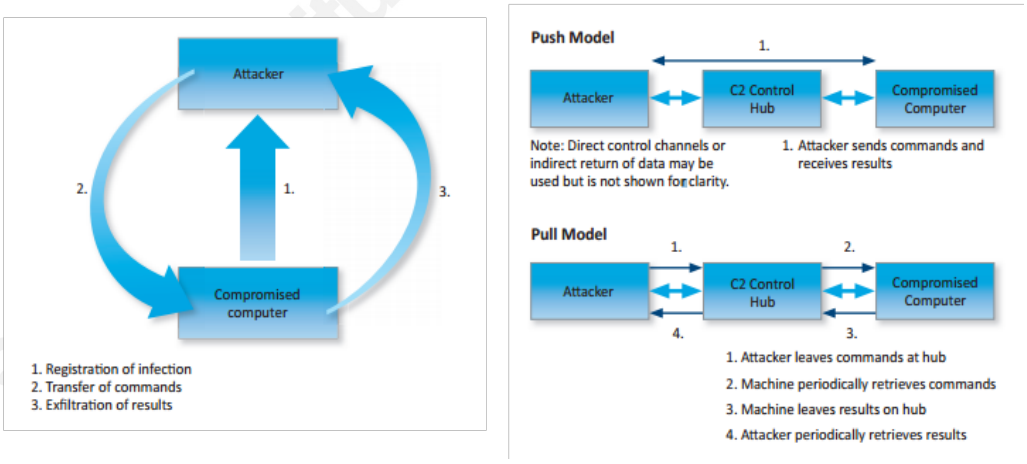


Figure 10-CPNI Push and Pull model of Command and Control Communication

Monitoring and analyzing the network traffic for anomalous traffic is key in detecting these channels. SIEM tools can correlate this data and look for events that may be going to malicious IP addresses (CPNI, 2012). Since malware authors change IP addresses and domain names of the C2 infrastructure, it becomes very difficult to write

© 2015 The SANS Institute Author retains full rights.

signatures for these connections. Threat intelligence sent to SIEM tools can help with detecting known C2 channels to see if that particular attack may have occurred on one's network in the past (Chuvakin, 2014).

2.7. Actions on Objectives

Now the attacker has everything that he or she needs to begin working towards their objective. Intruders may have a variety of goals like identity theft, intellectual property theft, or cyberterrorism. Once an attacker has reached this phase, they have succeeded in their attack. Once an attacker is inside they may need to escalate their privileges in order to reach their target. Mandiant's attack lifecycle shows the repeating nature of an attacker to continuously move through a network to gain access to their target. An APT threat actor may live in an organization for years until detected.

(APT1, 2013)

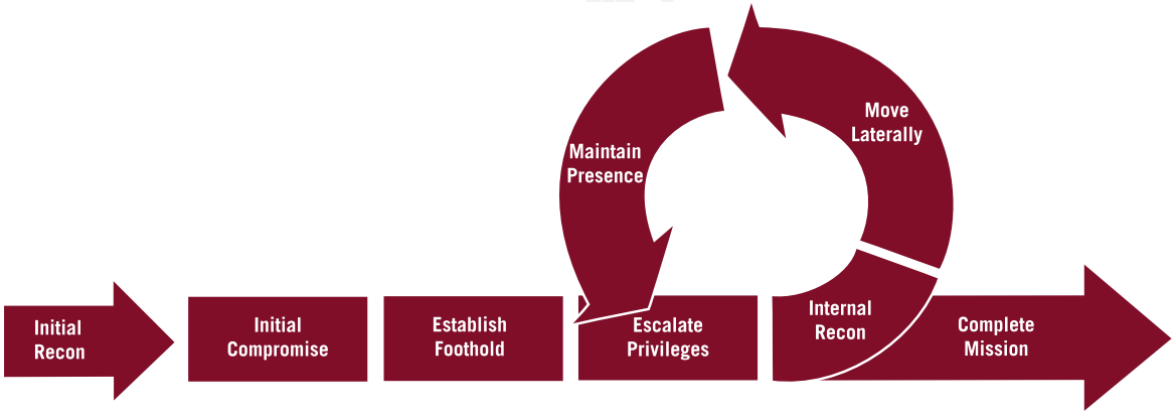


Figure 11-Mandiant Attack Life Cycle

3. Conclusion

Detecting and preventing attacks earlier in the kill chain is critical in defending against cyber threats. By implementing defense layers to detect and block attacks earlier in the kill chain organizations decreases the amount of remediation that needs to be performed by the security team. Delivery is one of the most critical stages in the kill chain and many organizations have good preventative technologies that will block malicious payloads from entering their networks. Prevention is important, but it is also

© 2015 The SANS Institute Author retains full rights.

essential to have intrusion detection technologies so that an organization can leverage to further analyze whether there has been a breach.

By leveraging tools such as Suricata, an organization can detect attacks earlier in the kill chain and prevent an attacker from establishing a foothold in one's network. Once an attacker has established a foothold in the environment, an attacker can be extremely patient in accomplishing their mission. Instead of only detecting attacks that reach the command and control stage of the kill chain, organizations should look at stopping these attacks earlier in the chain and begin to move towards a proactive defense with layered preventative and detective technologies. There is no silver bullet in cybersecurity, but utilizing the defense-in-depth strategy will help secure one's environment from a variety of attackers.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

2015 Data Breach Investigations Report (DBIR). (2015, January 8). Retrieved June 10, 2015, from http://www.verizonenterprise.com/DBIR/2015/

Advanced Evasion Techniques & Advanced Persistent Threats. (n.d.). Retrieved May 9, 2015, from http://www.mcafee.com/us/security-awareness/articles/advanced-persistent-threats-advanced-evasion-techniques.aspx

APT1. (n.d.). Retrieved May 8, 2015, from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Brief, T. (n.d.). Advanced Threat Detection and Response. *Advanced Threat Detection and Response*. Retrieved May 18, 2015, from https://www.splunk.com/content/dam/splunk2/pdfs/technical-briefs/advanced-threat-detection-and-response-tech-brief.pdf

Chuvakin, A. (2014, March 26). How to Use Threat Intelligence with Your SIEM? Retrieved January/February, 2015, from http://blogs.gartner.com/anton-chuvakin/2014/03/26/how-to-use-threat-intelligence-with-your-siem/

Clark, J. (n.d.). 11 tips to stop spear-phishing. Retrieved May 22, 2015, from http://www.csoonline.com/article/2132618/social-engineering/11-tips-to-stop-spear-phishing.html

Cole, E. (2001). Hackers beware. Indianapolis, IN: New Riders.

Constantin, L. (2012, February 29). Malware increasingly uses DNS as command and control channel to avoid detection, experts say. Retrieved May 9, 2015, from http://www.networkworld.com/article/2186385/network-security/malware-increasingly-uses-dns-as-command-and-control-channel-to-avoid-detection--ex.html

Czumak, M. (2014, February 05). Passive Reconnaissance - Security Sift. Retrieved June 10, 2015, from http://www.securitysift.com/passive-reconnaissance/

Davidoff, S., & Ham, J. (2012). Network forensics: Tracking hackers through cyberspace. Upper Saddle River, NJ: Prentice Hall.

Defense in Depth: A Holistic Approach to Cyber Security | Automation World. (2015, May 22). Retrieved June 10, 2015, from http://www.automationworld.com/security/defense-depth-holistic-approach-cyber-security

Detecting APT Activity with Network Traffic Analysis. (n.d.). Retrieved May 9, 2015, from http://www.trendmicro.com/cloud-content/us/pdfs/security-

Chris Velazquez, chrisvelaz.cv@gmail.com

© 2015 The SANS Institute Author retains full rights.

intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

E Network Threat Prevention Platform. (n.d.). *SECURITY REIMAGINED*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/fireeye-network-threat-prevention-platform.pdf

Eijndhoven, D. (2014, December 02). Mapping Defenses Using the Cyber Kill Chain. Retrieved May 6, 2015, from http://darkmatters.norsecorp.com/2014/12/02/mapping-defenses-using-the-cyber-kill-chain/

Fox, J. (2014, February 19). Top 10 Common Misconceptions About Application Whitelisting - InfoSec Institute. Retrieved June 10, 2015, from http://resources.infosecinstitute.com/top-10-common-misconceptions-application-whitelisting/

Gardner, B. (2014). Cost of a Data Breach. *Building an Information Security Awareness Program*, 15-24.

Hartley, M. (2014, September 08). Strengthening Cyber Kill Chain with Cyber Threat Intelligence. Retrieved June 10, 2015, from http://www.isightpartners.com/2014/09/strenghtening-cyber-kill-chain-cyber-threat-intelligence-part-1-of-2/

Higgins, K. J. (2010, January 27). Anatomy of a Targeted, Persistent Attack. Retrieved June 11, 2015, from http://www.darkreading.com/attacks-breaches/anatomy-of-a-targeted-persistent-attack--/d/d-id/1132841

Hoffman, C. (2014, November 22). Stop Trying to Clean Your Infected Computer! Just Nuke it and Reinstall Windows. Retrieved May 10, 2015, from http://www.howtogeek.com/202590/stop-trying-to-clean-your-infected-computer-just-nuke-it-and-reinstall-windows/

Horowitz, M. (2015, April 8). How useful is antivirus software? Retrieved June 10, 2015, from http://www.computerworld.com/article/2472120/security0/how-useful-is-antivirus-software-.html

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (n.d.). Intelligence-Driven Computer Network Defense. Retrieved May 5, 2015, from cyber.lockheedmartin.com%2Fhs-fs%2Fhub%2F444799%2Ffile-2164322071-pdf%2FDocuments%2FTechnical-Papers%2FWhitepaper-_Intelligence_Driven_Defense.pdf%3Ft%3D1432776204858

© 2015 The SANS Institute Author retains full rights.

Infographic: Cyber Kill Chain®. (n.d.). Retrieved June 10, 2015, from http://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html

Kassner, M. (2015, May 22). Rootkits: Is removing them even possible? Retrieved June 10, 2015, from http://www.techrepublic.com/blog/data-center/rootkits-is-removing-them-even-possible/

Kim, P. (n.d.). The hacker playbook: Practical guide to penetration testing.

Krikken, R. (2014, August 08). Introducing Gartner's Cyber Attack Chain Model. Retrieved June 5, 2015, from http://blogs.gartner.com/ramon-krikken/2014/08/08/introducing-gartners-cyber-attack-chain-model/

Lovinus, A. (2014, September 10). Vigilant Users Are the Best Malware Tools; 10 Steps for Effective Anti-Phishing Training - HardBoiled. Retrieved June 10, 2015, from http://blog.neweggbusiness.com/news/vigilant-users-best-malware-tools-10-steps-effective-anti-phishing-training/

O. (2014, May 9). Suricata. Retrieved May 10, 2015, from http://suricata-ids.org/

Paper, G. W. (n.d.). *Patch Management: Fixing Vulnerabilities before They Are Exploited*. Retrieved May 9, 2015, from http://www.gfi.com/whitepapers/fixingvulnerabilitiesbeforetheyareexploited_EN_GEN_wp.pdf

Rice, A. (2014, June). Command-and-control servers: The puppet masters that govern malware. Retrieved June 11, 2015, from http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware

Rouse, M. (2011, June 11). What is application whitelisting? - Definition from WhatIs.com. Retrieved June 10, 2015, from http://searchsecurity.techtarget.com/definition/application-whitelisting

Rouse, M. (n.d.). What is active reconnaissance? Retrieved June 10, 2015, from http://whatis.techtarget.com/definition/active-reconnaissance

Shcherbakova, T., & Vergelis, M. (2015, May 13). Spam and Phishing in the First Quarter of 2015. Retrieved June 10, 2015, from https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/

Shinder, D. (2005, July 13). SolutionBase: Understanding how an intrusion detection system (IDS) works. Retrieved June 10, 2015, from

© 2015 The SANS Institute Author retains full rights.

http://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/

SIR. (n.d.). Retrieved June 10, 2015, from http://www.microsoft.com/security/sir/glossary/drive-by-download-sites.aspx

To Protect What's Important To You. (n.d.). Retrieved May 9, 2015, from http://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-cc_qinetiq_report.pdf

Turning USB peripherals into BadUSB. (n.d.). Retrieved June 10, 2015, from https://srlabs.de/badusb/

Valcarcel, J. (2014, July). Why the Security of USB Is Fundamentally Broken. Retrieved June 10, 2015, from http://www.wired.com/2014/07/usb-security/

Wisdom, S. (2014, August 27). TippingPoint network security survey reveals top network security concerns. Retrieved June 10, 2015, from http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/TippingPoint-network-security-survey-reveals-top-network/ba-p/6587710#.VXS_889VhBc

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.