

INDICATIONS OF COMPROMISE

A Guide to Spotting and Preventing Malware Infection



CONTENTS

INTRODUCTION	4
PART 1 - UNDERSTANDING CYBER ATTACK DELIVERY	6
PART 2 - THE ROLE OF ANTIVIRUS AND PATCH MANAGEMENT	16
PART 3 - ATTACK SURFACE REDUCTION AND BEHAVIOR-BASED ANTIVIRUS	22
PART 4 - SECURING THE LAN TO WAN COMMUNICATIONS	28
PART 5 - LAST-DITCH ACTIONS AND CLEAN UP	34
CONCLUSION	44
REFERENCES.....	45

Defending networks from attack is no easy task for IT professionals. Attacks range in capability and threat; and over-reacting or implementing the wrong technology can be costly and make it easier for the bad guys.

This eBook describes the types of attacks facing a typical network and offers some successful mitigation strategies IT professionals have implemented to protect their networks.

Ultimately, treat this guide as a first step in designing your defense-in-depth strategy. IT professionals must truly understand the risk to the business and that IT security does not have "magic" solutions. There isn't a single technology that can prevent all the bad scenarios, despite what vendors say.

Cyber attacks, malware, and system vulnerabilities have been mystified and media-hyped beyond any sort of reasonable analysis. In fact, the most effective IT strategies against all unknown and known threats are generally the same. Patch and update the operating system, patch and update third-

party applications, restrict administrative access, and use malware defenses. These recommendations come from years of analysis by government and security organizations around the world.

Lastly, offense informs defense. This means IT service providers need to learn how to view their customers' networks as targets. I'm certainly not advocating unleashing your own destructive cyber attacks on unwitting customers, but setting up a virtual cyberdefense lab and downloading free tools to explore vulnerabilities will help you get better at defending and detecting attacks on your own networks.

Remember, as an IT professional you are partially or completely responsible for the confidentiality, integrity, and availability of the IT systems in your care. Don't make it easy for the bad guys; make it frustrating and difficult by putting in detective, preventive, and forensic defensive layers.



Ian Trump, Security Lead at SolarWinds MSP

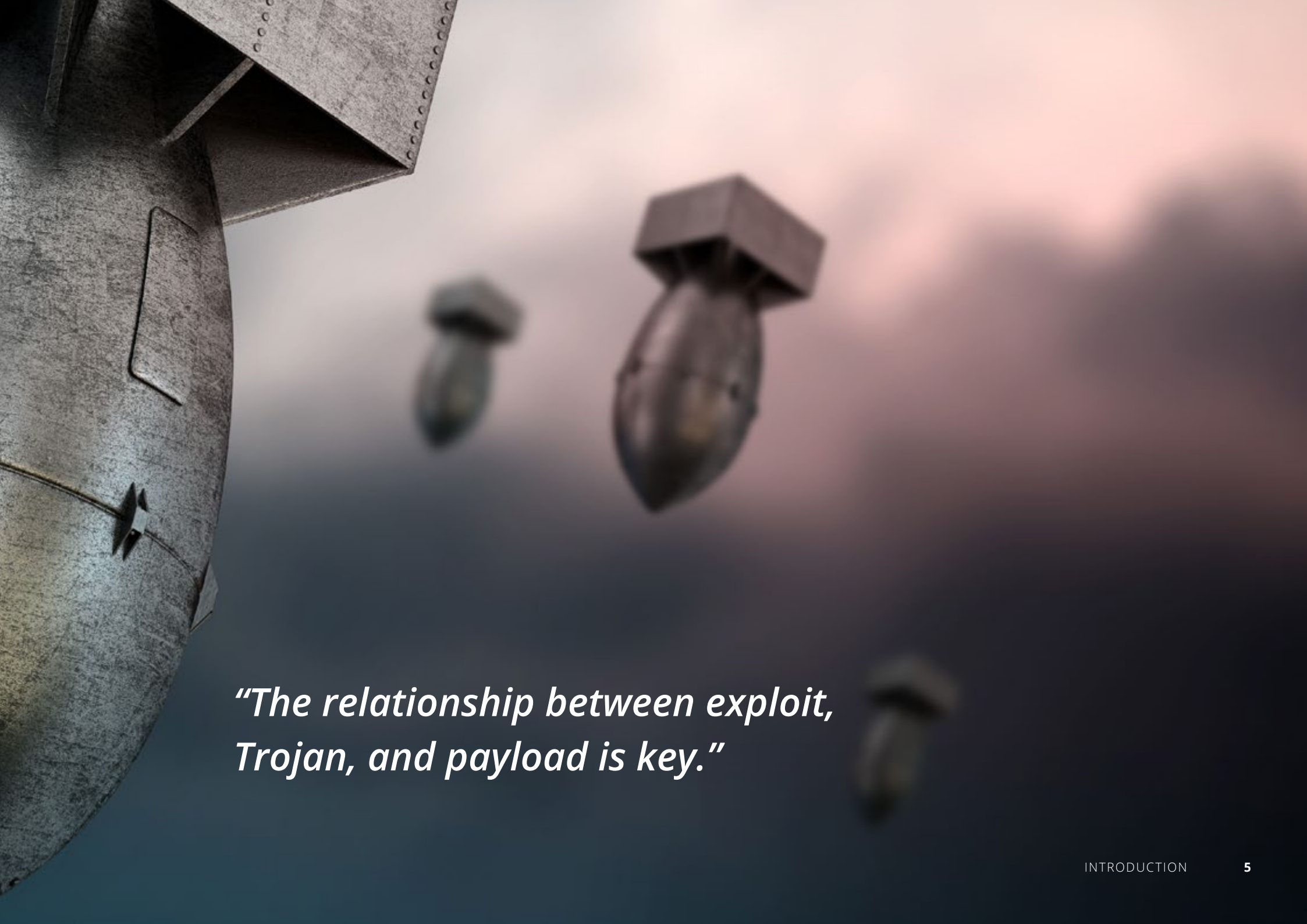
INTRODUCTION



Security discussions with IT providers and MSPs inevitably turn to the effectiveness of anti-malware defenses—to the question of antivirus software’s effectiveness against ransomware in particular. To answer that question, it helps to understand the relationship between exploit, Trojan, and payload.

The diagram on the next page is an adaptation of the Lockheed Martin Cyber Kill Chain®, which describes the various phases of a malware infection from initial exploit to the execution of a payload on an endpoint target.¹ The Cyber Kill Chain is a great way to explain how malware completes its journey from attack delivery to the endpoint and ultimately (in the vast majority of cases) the execution of a ransomware payload on the targeted endpoint.

This eBook is designed to help MSPs and IT service providers understand the diagram and the various technologies and events that lead to an infection being successfully landed by cybercriminals. By doing this, it’ll help you spot a compromise as early as possible and know how best to respond.



*“The relationship between exploit,
Trojan, and payload is key.”*

PART 1—UNDERSTANDING CYBER ATTACK DELIVERY



“Most MSPs and IT service providers fall into the category of threat intelligence services”.

THE LOCKHEED MARTIN CYBER KILL CHAIN



The diagram above shows the complete Cyber Kill Chain with two gray arrows under reconnaissance and weaponization. These two areas are generally out of scope for all but the largest organizations; most MSPs and IT service providers fall into the categories of threat intelligence services.

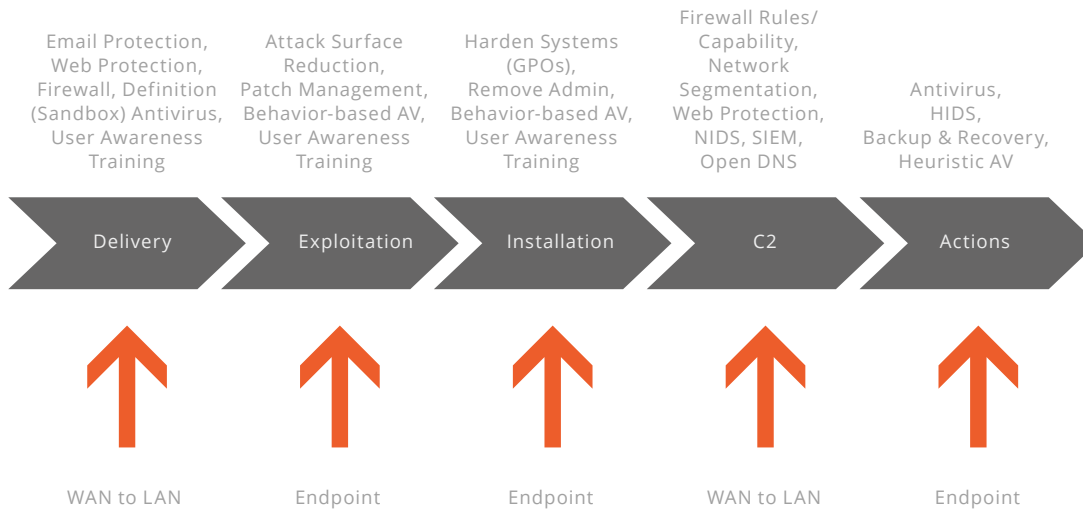
Over time, as the industry learns more about the complete life cycle of a malware attack, machine learning and artificial intelligence

may help provide warning of an imminent attack in the first two stages of the Kill Chain. But as of now, little can be done to degrade the capabilities of cybercriminals in the first two stages.

In fact, criminal psychology/ sociology, geopolitics, economics, and regional disparity will motivate individuals and groups to troll social networks and build exploit kits, sophisticated Trojan programs, and malware/ ransomware payloads.

UNDERSTANDING CYBER ATTACK DELIVERY

ADAPTED FROM THE LOCKHEED MARTIN CYBER KILL CHAIN



Across the top of our adapted “Kill Chain” diagram is a non-exclusive list of mitigation solutions (including user awareness training and a range of technology solutions) mapped to the various stages of infection. The middle section displays the various Lockheed Martin Cyber Kill Chain phases. The bottom section displays the stages of the infection and where the opportunity is to detect, prevent, and recover from the cybercriminal attack.



UNDERSTANDING THREAT INTELLIGENCE

“Many countries use dynamically allocated IPs, so an IP address designated hostile today may change tomorrow.”

Threat intelligence services should be approached with a note of caution. Simply receiving a list of IP addresses and updating firewall solutions is not a practical approach. Many countries use dynamically allocated IPs, so an IP address designated hostile today may change tomorrow; also, administrators occasionally clean malware off machines. Without some context to the threat intelligence, it may not be relevant to block an IP address that's not in the midst of attacking you.

Organizations seeking to extend their defenses into the first two phases of the Cyber Kill Chain are

advised to create and maintain a "Honeypot" environment, which is a trap set up to detect or deflect cybercriminal activity from a network. Current threat intelligence service offerings present a plethora of data without context. Knowing that a South Korean IP address is attacking a Russian IP address may be interesting, but if your business is not located in either country, it's not helpful information. Setting up your own "Honeypot" to collect intelligence from actual attacks on your infrastructure helps mitigate these challenges.

UNDERSTANDING THREAT INTELLIGENCE

“Simply knowing that a South Korean IP address is attacking a Russian IP address may be interesting, but if your business is not located in either country, it’s not helpful information.”

Unless MSPs, IT providers, and organizations are prepared to invest technological effort and implement specific hardware, their limited budgets and IT resources will force them to focus endpoint defenses on the last five opportunities of the Cyber Kill Chain to prevent, detect, and react to a cybercriminal attack.

The first practical step where technology can help prevent the full Cyber Kill Chain from occurring comes in the delivery stage of a cyber attack. In the vast majority of cases, the threat vector is very obvious. The graphic on page 13 is taken from the 2016 Verizon Data Breach Investigations Report, and shows the most frequent methods of malware delivery.²

The success rate of phishing emails, with an astounding 30% open rate,³ makes malicious email attachments and links embedded in emails the epicenter of the fight against cybercriminal attacks. The data also shows we should not neglect the dangers of unprotected web surfing. It's hard to argue against the fact that email filtering, web filtering, and user security awareness training are the keys to successfully interrupting cyber attacks at the delivery stage of the Cyber Kill Chain.

TOP FIVE MALWARE VECTORS



THE ROLE OF CLOUD-BASED SERVICES

With a plethora of cloud-based services, including Gmail and Office 365, the delivery stage is perhaps the most inexpensive phase for businesses to implement malware interception today. It is also relatively easy to implement, with little if any impact on business operations. Email scanning and web surfing proxy services located on-premises or in the cloud provide the majority of cyber attack defenses at this stage.

Cloud-based services push defenses outside the organizational perimeter and provide cyber defense value by preventing the attack from even arriving at the endpoint. Even though many of these services have multiple virus definition engines and heuristic analysis capabilities, cybercriminals do occasionally sneak malware past these defenses using old fashion cunning and guile, enticing an employee to click on a link and/or execute a payload.

The malware-less attack of business email compromise or CEO fraud is an example of a cyber attack that bypasses even the most robust email filtering defenses. Thus, employee awareness training that teaches people to verify any request or unsolicited/

suspicious attachment via verbal confirmation can help guard against these increasingly sophisticated social engineering attacks. The so-called “CEO fraud” attacks frequently result in larger payoffs for cybercriminals than ransomware as they appear to be an executive-authorized money transfer to a business partner.

“Cloud-based services push defenses outside the organizational perimeter and provide cyber defense value by not even allowing the attack to arrive at the endpoint.”

Also, CEO fraud attacks may have other designs than facilitating illicit money transfers. Cybercriminals may also want to steal employee data. According to a SIEM vendor, "Over a third of the respondents to a recent survey reported their executives have fallen victim to a CEO fraud email, and over 80% believed their executives could fall for targeted phishing scams in the future. Those concerns are well-founded. More than 50 organizations, including Snapchat and Care.com, were successfully targeted by CEO fraud emails asking for W-2 information this past tax season alone."⁴

It's fair to say, the first layer of cyber defense should be designed to defeat the attack before it even makes it onto the endpoint. However, when the attack arrives in the form of a fraudulent, yet legitimate-looking email, employee awareness training is the best investment companies can make to prevent large-scale loss.

PART 2—THE ROLE OF ANTIVIRUS AND PATCH MANAGEMENT

In the section, we will concentrate on the initial endpoint attack vector “exploitation” assuming the delivery phase of the exploit has successfully executed against the target endpoint.

From the exploit kit perspective, the targeted endpoint will exist in one of four states, which are covered in the next few pages.

“The Windows Authentication mode is less vulnerable to brute force attacks, as the attacker is likely to run into a login lockout after a finite number of attack attempts.”

STATE 1: MACHINE IS FULLY PATCHED, ANTIVIRUS IS INSTALLED AND UP TO DATE

The only vulnerabilities that exist here are either “human” (end users tricked into installing malware) or zero-day attacks/exploits that would go undetected by the antivirus.

Clearly, user awareness training is the only effective defense against “trickery” or social engineering-based attacks. Only if warnings are dismissed can the exploit successfully deliver its payload. This is the case with Visual Basic

Macro exploits found in phishing emails. Robust antivirus featuring definitions of malware signatures, heuristic detection of exploit activity, and behavior-based analysis of exploit activity may protect the endpoint, but this is frequently not the case.

CONDITION: **GREEN**

THE ROLE OF ANTIVIRUS AND PATCH MANAGEMENT

STATE 2: MACHINE IS NOT PATCHED, ANTIVIRUS IS INSTALLED AND UP TO DATE

The vulnerabilities here are related to exploits that have been developed for the lack of a specific patch. Although antivirus may be up to date, it's questionable whether the exploit will actually be detected. In this scenario, the machine could be easily infected by an exploit designed to bypass antivirus. Research from Recorded

Future indicates that Adobe Flash, Java, and Internet Explorer are the most frequent targets of exploit kits.⁵ Not having the exploitable software installed in the first place is the only effective defense.

CONDITION: **YELLOW**

“The machine could be easily infected by an exploit designed to bypass antivirus.”

STATE 3: MACHINE IS NOT PATCHED, ANTIVIRUS IS INSTALLED, BUT NOT UP TO DATE

The vulnerabilities here are greatly enhanced over the first two states, as the machine is open to a wide range of exploits, not just the latest versions of exploits kits. Similar to state 2, a machine in this state can be easily infected, however it is also likely to be infected over and over again. IT providers and MSPs find themselves in this scenario in all too frequently. The emphasis has to be placed on patching due to the exploit package's ability to execute and deliver a Trojan, which in turn delivers a payload

against an unpatched machine. Antivirus definitions do include the actual malware signatures, but more sophisticated behavioral and heuristic engine updates provide antivirus software with "indications to look for" (such as network traffic to a certain set of IPs) or "suspicious events" such as invoking JavaScript from a document in email. These are all telltale signs of an endpoint about to receive a Trojan.

CONDITION: **RED**

***"These are all
telltale signs of an
endpoint about to
receive a Trojan."***

THE ROLE OF ANTIVIRUS AND PATCH MANAGEMENT

STATE 4: MACHINE IS PATCHED, ANTIVIRUS IS INSTALLED, BUT NOT UP TO DATE

This state is similar to state 1, but cybercriminals have better success as the majority of the cyberdefense is provided by patch installations. The attack surface is the same as State 1, however the machine is more susceptible to a “human” vulnerability, as an entire range of Trojans (installed via phishing email) can infect the machine. This is probably the second most common scenario shortly after patches have been delivered to endpoints. With the

patches in place, the IT provider or MSP has reduced the likelihood of exploitation considerably, however the danger remains from Trojans delivered in the form of email. The combination of phishing emails and social engineering attacks can be conducted using families of older Trojans if the target’s antivirus is not up to date.

CONDITION: **YELLOW**

“The machine is more susceptible to a ‘human’ vulnerability.”

In states 3 and 4 where the antivirus is out of date, the best course of action is to update to the latest definitions and run a complete scan on the endpoints. There is a good chance malware may have been installed while the machine's antivirus defenses were "down." Many users will not admit they may have accidentally clicked on something they shouldn't have, so a Trojan may be lurking on the endpoint waiting to download a payload, held at bay by your other network defenses.

For special purpose systems, such as payroll, accounting, and point of sale, removal of the frequently exploited software, weekly patching, and updating of exploit-friendly software like the aforementioned Adobe Flash is essential. If the software cannot

be removed, then robust antivirus with frequent malware signature updates, behavioral, and heuristic-based analysis offers the best route to protecting these systems.

Assuming there is user awareness training in place, the above scenarios should entail the priority of work for MSPs and IT service providers. This work should be focused on testing and deploying patches quickly and efficiently into the network—obsessing on the definitions or capabilities of antivirus of choice is certainly not a priority activity.

After robust data backups, patching and updating should be the priority to keep systems out of the hands of cybercriminals.

PART 3—ATTACK SURFACE REDUCTION AND BEHAVIORAL BASED ANTIVIRUS

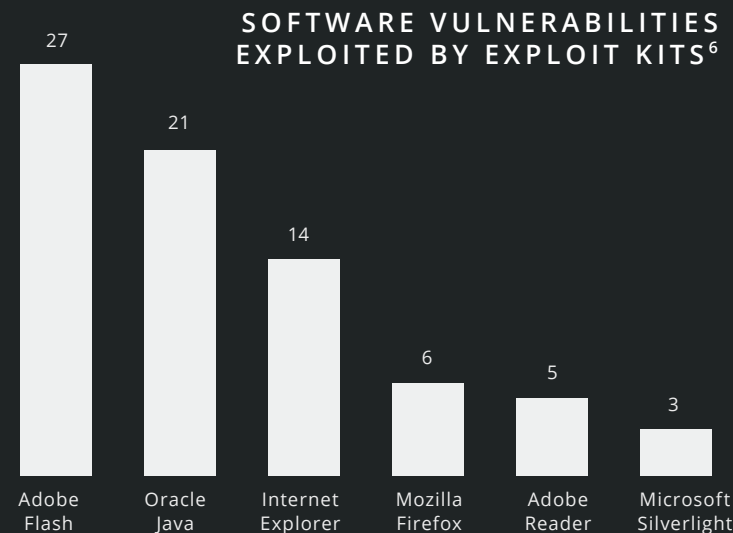
According to the table in the lower right, if you can't commit to a rapid patching of endpoints, then you can often improve security by simply removing the most targeted software. There are a number of reasons businesses may not feel able to commit to a quick-fire patching program, including the lack of an automated process or tool, institutional anxiety over self-inflicted downtime, or the lack of IT attention or cycles to this task.

An approach to organizational security that requires management authorization for the installation and use of the “dangerous 5” (Adobe Flash, Java, Internet Explorer, Firefox, and Silverlight) may be the key to implementing robust security without having to resort to the significant expense of more technological safeguards. In a business environment, removal of Adobe Flash, Java, or Internet Explorer (IE)—or a commitment to keeping them up to date with the latest versions—significantly reduces the potential for endpoint exploitation.

A business workstation without Flash, Java, IE, Firefox, Adobe Reader, or Silverlight that encounters a modern exploit may emerge completely unscathed, as the exploit kit would be unable to find an avenue of attack. This is a very significant finding for regulated industries or

organizations concerned about the confidentiality and integrity of their data systems.

In Part 1 we discussed how definition-based anti-malware technologies, such as endpoint antivirus, web filtering/protection, and mail scanning—combined with user awareness training—can be helpful for stopping the delivery of Trojans and payloads. There is a significant role for endpoint antivirus with behavior-based capabilities and user awareness training at the point of exploitation as well.





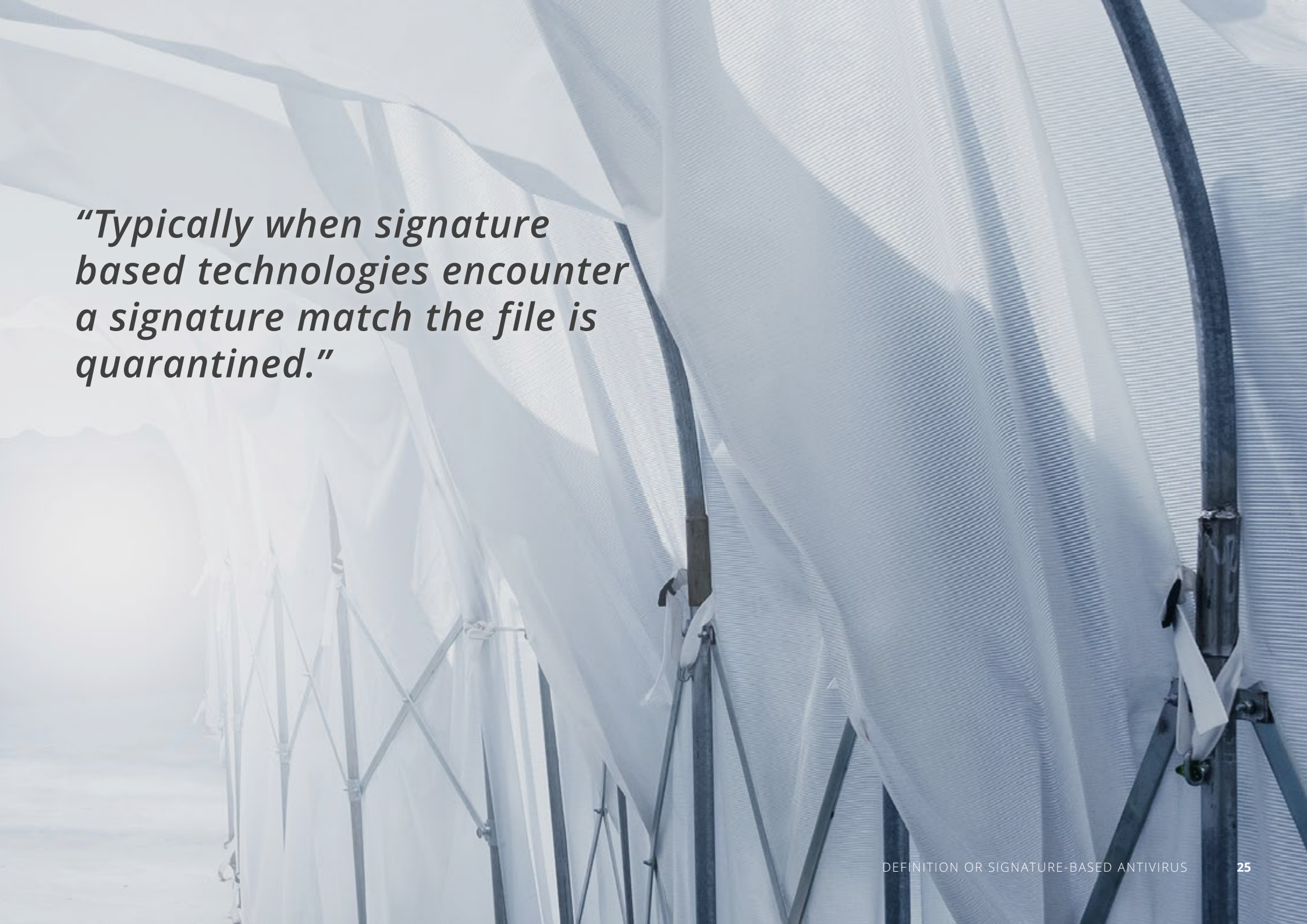
“This is a very significant finding for regulated industries or organizations concerned about the confidentiality and integrity of their data systems.”

DEFINITION-BASED ANTIVIRUS

Definition-based (or signature-based) antivirus compares the signatures (MD5 or SHA-1 hashes) of the files encountered to see if they match a list of known malware. Depending on the capabilities of the software, it may look inside the file for telltale signs of malware. Typically, when signature-based technologies encounter a signature match the file is quarantined.

Cybercriminals writing exploits and Trojans know their malware may encounter endpoint antivirus, so they

frequently include malicious code that disables antivirus and prevents updates or network communication. In highly specialized attacks, the presence of the antivirus software can be used to actually install malicious code. In May 2016, a security researcher, Tavis Ormandy, identified an exploitable overflow in, "the core Symantec Antivirus Engine used in most Symantec and Norton branded Antivirus products."⁶



“Typically when signature based technologies encounter a signature match the file is quarantined.”

BEHAVIOR-BASED ANTIVIRUS

DANGER
INFECTION HAZARD
QUARANTINE AREA

AVOID CONTACT

BE ORGANIZED
BE PREPARED
BE SAFE

WHAT NOW?

CLASS B ZONE





Behavior-based antivirus watches processes for characteristic signs of malware, then compares these signs against a list of known malicious behaviors. For example, given the list of vulnerable software packages above, a document being opened in an email that invokes JavaScript or Adobe Flash could be viewed as “highly suspicious or malware-like behavior.”

Behavior-based detection is required because many malware creators have started using obscuration techniques such as polymorphic or encrypted code segments, which are very difficult to create a hashed signature for. So, an easier way to detect these is to watch for a particular pattern of behavior.

Of course, it’s highly desirable to have layers of defense in place to intercept the delivery of exploits, Trojans, and payloads before they arrive at the endpoint.

But, if those defenses are breached, the combination of removing the targeted software (attack surface reduction), antivirus with a behavior-based engine, aggressive patch management, and end user awareness training can help ward off the most persistent attacks (as well as those accidental visits to dangerous websites).

PART 4—SECURING THE LAN TO WAN COMMUNICATIONS

A low-angle, upward-looking photograph of a biplane in flight. The aircraft's wings, landing gear, and fuselage are visible on the left side of the frame. The sky is filled with several large, colorful parachutes (yellow, orange, and green) and the silhouettes of jumpers descending. The lighting is bright, suggesting a sunny day, with some clouds visible in the background.

“Once malware has landed ... it must reach out to a command-and-control (C2) bot network to receive instructions.”

Once malware has landed, or more specifically once a Trojan has been installed on an endpoint, it must reach out to a command-and-control (C2) bot network to receive instructions. This is perhaps one of the easiest areas to implement firewall architecture, logging, and network controls to detect or prevent endpoint compromise.

C2 infrastructure is provided by previously infected or compromised servers and workstations. These networks can either be rented from Crime as a Service (CaaS) sources or purposely built by cybercriminals to support a Trojan attack. Virtually all modern malware has to “reach” back to a C2 source to download

a payload attack. In some cases, detailed metrics on infection success, geographic distribution, and detailed system information are captured for CaaS marketing purposes. Yes, cybercriminals attempt to collect as much success data about infection as modern companies collect about website visits and customer interactions.

Take, for instance, the “typical” network communication example of a Trojan that has a hard-coded C2 domain of *twinpeakshockey.com* (see below). The Trojan reaches back out to this domain, using a standard DNS query and then attempts to “GET” the ransomware payload *GORSjo.exe* from the C2 server.

In this case, the communication was not conducted stealthily; nor was it encrypted (https). Most web filtering products would quickly identify the IP address (69.89.31.222) or domain as being a dangerous place for an endpoint to visit. Keep in mind DNS protection such as Open DNS and other products provide a valuable layer that can work even against malware using https for communication. Furthermore, downloading an executable (.exe) onto an endpoint would be something that either the firewall or web protection product should hopefully block.

EXAMPLE OF A TROJAN COMMUNICATING WITH A C2 NETWORK

11	4.177967	8.8.8.8	172.16.25.137	ICMP	Echo (ping) reply (id=0x0200, seq(be/le)=7168/28, ttl=128)
12	25.196459	172.16.25.137	172.16.25.2	DNS	Standard query A twinpeakshockey.com
13	25.674355	172.16.25.2	172.16.25.137	DNS	Standard query response A 69.89.31.222
14	25.676099	172.16.25.137	69.89.31.222	TCP	iascontrol-oms > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
15	25.676823	69.89.31.222	172.16.25.137	TCP	http > iascontrol-oms [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
16	25.676879	172.16.25.137	69.89.31.222	TCP	iascontrol-oms > http [ACK] Seq=1 Ack=1 win=64240 Len=0
17	25.677229	172.16.25.137	69.89.31.222	HTTP	GET /GORSjo.exe HTTP/1.1
18	25.677524	69.89.31.222	172.16.25.137	TCP	http > iascontrol-oms [ACK] Seq=1 Ack=188 win=64240 Len=0

ESSENTIAL LAYERS IN YOUR DEFENSE

“The lateral movement technique is designed to create cyber snares to make it difficult for the Trojan to reach back out of the network or infect other endpoints.”

Must-have capabilities at this point include network segmentation, egress (outbound) firewall rules, and a security information and incident management system (SIEM)/log management solution with alerting capabilities. Firewall rules, especially the need for external open ports, have to be mapped to business services.

The basic conceptual firewall rules below help detect and prevent C2 communications as well as further network exploitation by using a technique called lateral movement. These rules are designed to create cyber snares to make it difficult for

the Trojan to reach back out of the network or infect other endpoints.

- Deny rules for workstation subnet: No external DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP
- Deny rules for admins (open as required): No external DNS, IRC, NTP, FTP, ICMP, SMTP, SNMP, RDP
- Deny rules for printer subnets: Deny everything. No printers on the Internet!
- Deny rules for servers. Only DNS, NTP to specific IPs, HTTPS.

As you can see, limiting the ports, protocols, and communications internally and externally in the network at the architecture level can prevent and detect the presence of suspicious or unauthorized network activity.

If these firewall rules are implemented, and a stealthy Trojan tries to use Internet Relay Chat (IRC) protocol to reach C2 infrastructure, this activity would be blocked, and if a SIEM has been implemented, an alert would be triggered.

AN EXAMPLE OF LATERAL MOVEMENT



SERVERS
192.168.2 X
SAN/NSA
File Sharing,
Over https,
Event Logging,
HIDS/HIPS.



FIREWALL
192.168.1 X
Communication
Rules, Detective
Rules, WAP in
DMZ.



USERS
192.168.4 X
GPO: No Coms.
192.168.4 X
Local Admin for
MAX & Mgt.



PRINTERS
192.168.5 X



ADMINS
192.168.3 X
No Admin
Email, Event
Logging,
HIDS/HIPS.

ESSENTIAL LAYERS IN YOUR DEFENSE

As another example, “deny” rules against Simple Mail Transport Protocol (SMTP) on workstations make it more difficult for cybercriminals to use a compromised endpoint as a SPAM bot to blast out more email phishing attacks with Trojan attachments.

By using a combination of outbound firewall rules, network segmentation, and a SIEM to capture log information and alert suspicious activity, the Trojan’s attempts to infect and communicate internally and externally will either be discovered or prevented.

For MSPs and IT providers, developing a standard segmented network architecture and egress firewall rule package for your customers is worth the time and effort. In many cases, the ability to segment the network and write egress firewall rules can be done with the existing infrastructure. When combined with a SIEM to monitor and alert against an endpoint trying to break a firewall rule, the MSP or IT provider can quickly identify the culprit and respond accordingly.

“For MSPs and IT providers, developing a standard segmented network architecture and egress firewall rule package for your customers is worth the time and effort.”



PART 5—LAST-DITCH ACTIONS AND CLEANUP



If the exploit has been received, the workstation is compromised by a Trojan, outbound communications are established, and the payload has landed, then bad things are about to happen.

In the perfect world of the Cyber Kill Chain analysis, the defenses at each stage would have given several opportunities for the endpoint to evade the final stage of compromise—when the payload executes. For the vast majority of SMB/SMEs, this is now a ransomware attack.

Malware varies in quality and capability, from barely functional with very obvious system effects, to stealthy with subtle system effects. In the case of ransomware, not only are the effects on a system noticeable (e.g. encrypted files), but the activity is also highly detectable by heuristics.

Hopefully, a ransomware attack execution is not “normal” activity. In general, workstations in a business environment act in a predictable manner. When CPU cycles suddenly rise due to a process and stay pinned up, and files locally or on a network share start being sequentially accessed and written to, a good heuristic antivirus may interrupt or kill the process that caused this sudden activity—especially if that activity appears to be sustained.

It’s these telltale signs that heuristic malware detection attempts to look for. Ransomware as a category of attack is pretty blatant from a system perspective. Even at the network layer there will be a huge surge in data traffic and server read/write requests from the infected endpoint.



“In the perfect world of the Cyber Kill Chain analysis, the defenses at each stage would have given several opportunities for the endpoint to evade the final stage of compromise.”

YOUR LAST-DITCH LINES OF DEFENSE

Even at this stage, all is not lost. There are still measures that can be taken to limit the ransomware execution's impact. Using Group Policy Objects (GPO) or a third-party application to lock down the %App/Data and %App/User directories to prevent execution of files located in these directories is a great approach. Check out the Ransomware Prevention Kit from Third Tier for more information.⁸

For newer Windows Active Directory environments, implementing application whitelisting using AppLocker or a third-party application may also provide a defense against ransomware payload execution. For further reading, see endnote 9 in the references section—it discusses the use of AppLocker against ransomware. For it to work, your users must not have domain administrator or local administrator privileges.

If a user suspects a ransomware attack is executing—after they have opened an infected email attachment or visited a compromised website—training should include pulling the plug on the system, or pressing and holding down the power button until the computer turns off. If the infection has not spread to the actual server, and the ransomware is executing from the workstation, this action may save many files from being encrypted. IT needs to disconnect the machine, without forgetting to disable wireless, from the office network before it's safe to turn on again.

When dealing with a ransomware attack, there are two components to consider: first, the infected endpoint, which if turned on will begin infecting files almost immediately on startup (if still connected to the network); and, second, the encrypted files themselves.





“Even at this very late stage in the process. All is not lost.”

“You may want to preserve the machine for professional examination by a Digital Forensic Incident Response (DFIR) team or a law enforcement agency.”





The infected endpoint needs to have the exploit mitigated (by patching or removal of the exploited software), the Trojan removed, and the payload or ransomware removed. If any of these components remain, there is a chance the machine will connect to the Internet, reinfect itself, redownload the payload, and the attack may start all over again. A complete reinstall from a scripted .iso “gold image” or known good image from secure media (not a local recovery) may be the only way to remove a more advanced infection.

An infected endpoint may have valuable forensic information about how your layered security was bypassed and may include information about the cybercriminals. If the attack

had a significant impact on your organization, you may want to preserve the machine for professional examination by a Digital Forensic Incident Response (DFIR) team or a law enforcement agency.

If you’re going to try the route of using anti-malware on an isolated or offline system, it may be wise to check for any suspicious network traffic using Wireshark (especially http or https) from a recently cleaned machine before it goes back into service. Sadly, more advanced ransomware payloads deliver credential-stealing capabilities, so all the passwords, including the ones stored in the browser cookies, may be compromised. Therefore, all passwords should be changed.

CALL FOR BACKUP

*“Use caution
when uploading any
encrypted files as
the sample data.”*

TO PAY OR NOT TO PAY

"It's clear that paying a ransom is not in anyone's best interests except the cybercriminals'."



Despite early controversial statements from the FBI, it's clear that paying a ransom is not in anyone's best interests except the cybercriminals'. The only circumstances under which you might consider paying the ransom would be if the data is incredibly valuable to the business and its operations, or if years of research are at stake. Either way you would need to take a long hard look at why that data was not protected from a ransomware attack in the first place.

Keep in mind that the folks who sent, exploited, and installed a Trojan on your system, and then downloaded and executed ransomware, are criminals. If there is an opportunity to extort more money, the cybercriminals will not

give up the opportunity—so don't explain how precious the data is, or the price of recovery will go way up. The last thing you want to do is provide the seed money for a better, more effective version of ransomware.

All ransomware incidents are cybercrime and should be reported. To report cybercrime, please contact your local FBI Field Office¹¹ or file a complaint through the Internet Crime Complaint Center.¹² In the UK contact Action Fraud,¹³ in the EU contact Europol,¹⁴ and in Australia contact Acorn.¹⁵ These bodies will allow you to fight back against cybercriminals.

CONCLUSION

The Indications of Compromise content presented by SolarWinds® MSP will help educate businesses, MSPs, and IT providers about the mechanics of a modern malware attack and the steps and technologies that can mitigate the damage.

An attack can take place in seconds or minutes depending on many factors, but by implementing defenses to intercept malicious activity through the stages of the Cyber Kill Chain and augmenting those defenses with user awareness training, ransomware attacks and endpoint compromises can be prevented.

REFERENCES

- 1 **Lockheed Martin Cyber Kill Chain®**
<http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>
- 2 **Verizon Data Breach Investigation Report 2016**
<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>
- 3 <https://blog.barkly.com/phishing-statistics-2016>
- 4 <https://www.alienvault.com/blogs/security-essentials/clicking-with-the-enemy>
- 5 **Recorded Future**
<https://www.recordedfuture.com/>
- 6 **Digital Shadows**
<https://www.digitalsadows.com>
- 7 **Tavis Ormandy report**
<https://bugs.chromium.org/p/project-zero/issues/detail?id=820>
- 8 **Third Tier Ransomware Kit**
<http://www.thirdtier.net/ransomware-prevention-kit/>
- 9 **Technet Blog**
<https://blogs.technet.microsoft.com/askpfplat/2016/06/27/applocker-another-layer-in-the-defense-in-depth-against-malware/>
- 10 **Heimdal Security**
<https://heimdalsecurity.com/blog/ransomware-decryption-tools/>
- 11 **FBI**
<https://www.fbi.gov/contact-us/field-offices>
- 12 **IC3**
<https://www.IC3.gov>
- 13 **Action Fraud**
http://www.actionfraud.police.uk/report_fraud
- 14 **Europol**
<https://www.europol.europa.eu/report-a-crime/report-cybercrime-online>
- 15 **Acorn**
<https://report.acorn.gov.au/>

SolarWinds MSP empowers MSPs of every size and scale worldwide to create highly efficient and profitable businesses that drive a measurable competitive advantage. Integrated solutions including automation, security, and network and service management—both on-premises and in the cloud, backed by actionable data insights, help MSPs get the job done easier and faster. SolarWinds MSP helps MSPs focus on what matters most—meeting their SLAs and creating a profitable business.

For more information, visit www.solarwindsmsp.com

© 2017 SolarWinds MSP UK Ltd. All Rights Reserved.

RMEB00067EN0117



www.solarwindsmsp.com