TechTarget | SearchSecurity

E-guide

PRO+ Content

Antimalware Protection in the Enterprise

Removing malware: What are the best methods?

In this e-guide

In this e-guide:

Ever since the first viruses were detected, there has been a constant battle of deciding on the most appropriate responses to detected malware.

Should security teams clean up the malware and move on or format the hard drives to start over with a clean system?

This is just one of the important questions this guide sets out to answer. Go in-depth on malware protection best practices in the enterprise. Uncover:

- How vulnerabilities in antivirus tools affects enterprises
- Recent ransomware attack trends
- Characteristic features of endpoint antimalware protection
- The cleanup process for removing malware from client devices

In this e-guide

Vulnerabilities in antivirus tools: What does it mean for enterprises?

Nick Lewis, Program Manager for Trust and Identity - Internet2

Software developers are typically trained in similar ways and, like any other group of people, make similar mistakes over time. Developers at computer security companies are no different. Customers might have expectations that software provided by security companies is secure, but they will be disappointed to know the dismal state of software security. Some companies have devoted significant resources to improving the state of software security, but this is not the norm yet. Recent discoveries of antivirus vulnerabilities in the Symantec AV scanning engine further highlight the diligence enterprises must have when managing systems and choosing a solution.

This tip will explore how host-based antivirus tools operate and the enterprise management considerations for these tools.

Host-based antivirus tool operations

Tavis Ormandy, a Google Project Zero researcher, has been keeping the information security industry honest and pointing out the inconsistencies between the marketing and reality in security tools. Ormandy has found numerous critical vulnerabilities in antivirus tools recently, one of them being the vulnerability in Symantec Antivirus products. The intent of antivirus tools is to scan and work with malicious files. It is reasonable to expect the software to be secure and that any malicious file would not cause a problem for the software. Standard secure development recommendations are to distrust the input from an end user and antivirus tools should also distrust that a file is not malicious. The software should assume the file could cause a problem for the tool, and include functionality to prevent exploitation of vulnerabilities in the tool.

The vulnerability is a classic buffer overflow. It is triggered when scanning a malformed file that could be received via email or browsing the web on an endpoint, or on a server when it accesses a file, such as when the server saves a file, processes a file attached to an email or downloads a file. Email systems or systems that operate on files from uncontrolled sources are at the highest risk, since a file could be sent from anywhere to be processed by the antivirus software. The buffer overflow allows for remote code execution as system or root -- depending on the platform and user of the software executing the scan.

On Windows, Symantec loads itself into the operating system to intercept all file system activities and runs as an administrative account -- or system. Symantec also loads itself into the kernel to prevent modifications to its configuration by unsuspecting users or malware. Symantec is not unique in these decisions -- many antivirus tools implement these kinds of operation techniques.

In this e-guide

Enterprise management considerations for antivirus tools

Not much has changed since November 2011 when I wrote about a vulnerability in a Sophos antivirus product, which had been researched by Ormandy. The same enterprise protection steps of keeping core operating systems and applications updated are still necessary, and the same must be done with all of the other software on an endpoint, especially security critical software like antivirus software. Given how long enterprises have been using antivirus software and using centralized management of antivirus software, they should already have in place a regular cycle for updating the endpoint software, deploying patches, monitoring the environment, automating definition updates and monitoring the logs. Performing this at scale consistently is difficult, but critical to good security hygiene to protect the enterprise.

If an enterprise decides to keep using antivirus tools, it should evaluate thoroughly existing and potential vendors. There are AV comparison or test guides which have focused primarily on features, functionality and detection coverage. These are potentially the most important aspects of any tool, but the security of the tool also shouldn't be overlooked. It is necessary to understand the additional risk from any piece of software so integrated into the operating system. Evaluating the software development practices of the vendor, or better yet, having a third party that focuses on secure software development and application security, could help with understanding the severity of future antivirus vulnerabilities in a particular product or from the vendor.

Enterprises may want to perform these same steps on security tools periodically as part of critically evaluating their information security programs and identifying areas of improvement. As a community, customers must advocate for secure development practices from their software providers, and this could improve the state of software security. If we continue paying maintenance or subscription fees for insecure software, software vendors will not make the necessary changes.

Antivirus software is dead; long live antivirus software! The core functionality of antivirus software as an independent operating system security monitor will continue to be necessary and evolve over time. However, the critical nature of antivirus software requires antivirus vendors to perform at a higher standard of security. The continued embarrassment of antivirus vendors by the poor state of security and the decreasing efficacy of their tools should drive more enterprises to critically evaluate if traditional antivirus vendors are performing adequately for their information security programs, and replace these vendors if they are not meeting the enterprise's needs. The funds devoted to antivirus could then be used elsewhere to better protect the enterprise.

↘ Next article

In this e-guide

Recent ransomware attacks: Data shows 50% growth in 2016

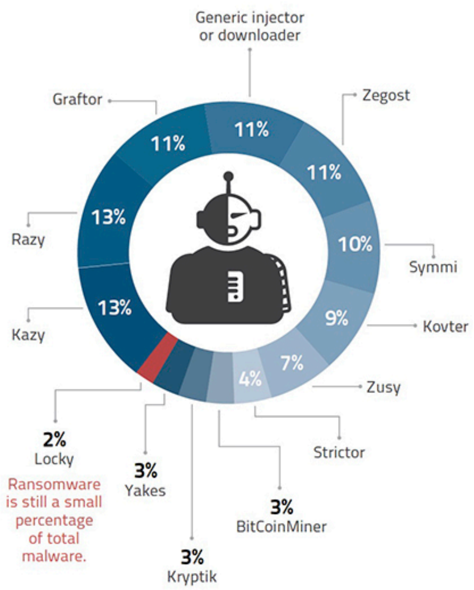
Kathleen Richards, Editor - *Information Security* magazine

Ransomware is the fastest growing malware across industries, up 50% in 2016 compared to 2015, according to new data from endpoint security provider Carbon Black. Criminal use of malicious software to encrypt files or hard drives of unsuspecting victims is so widespread that some states are enacting legislation to make recent ransomware attacks easier to prosecute. In September, California became the latest state to offer specific anti-extortion guidelines to prosecute criminals who demand ransoms, usually in bitcoins, to unlock victims' systems. But even with the rise in recent ransomware attacks, these viruses represent only a small percentage of total malware.

Malware continued to target all industries in 2016, with manufacturing companies (21.8%), non-profit organizations (16.4%) and utilities and energy (15.6%) hardest hit, according to Carbon Black, which based its findings on data from more than 1,000 organizations, representing 2.5 million endpoints. Of the dozen or more malware families tracked, Locky, which was used in one of four recent ransomware attacks, accounted for 2.17% of total malware.

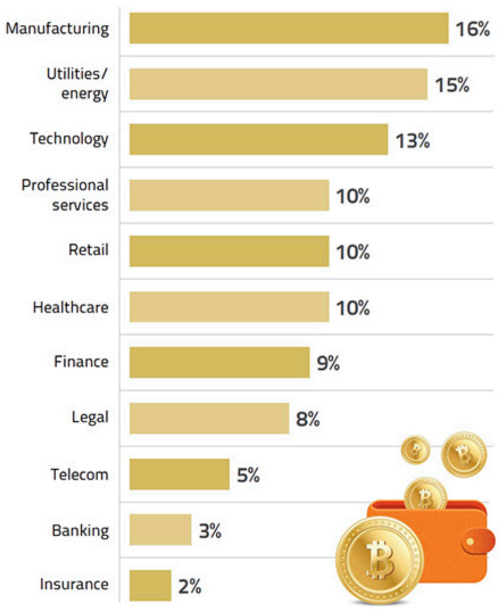
In this e-guide

Families to Watch Out for
Percentage of malware by identification



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016; NUMBERS HAVE BEEN ROUNDED; ART: JORGE REYES, HTTPS://CREATIVECOMMONS.ORG/LICENSES/BY/3.0/US/

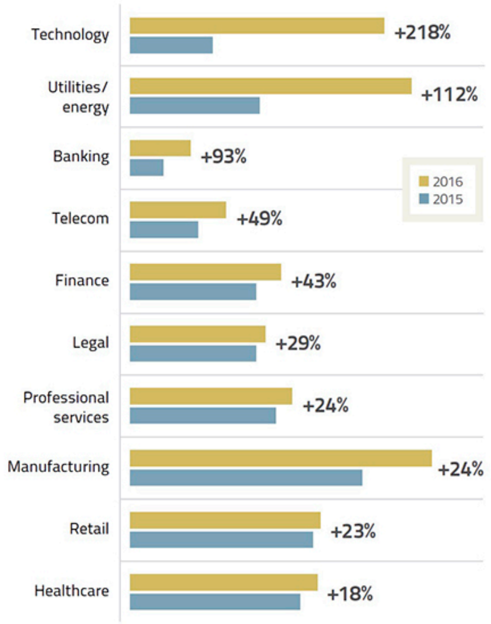
'That'll Be Thousands of Please'
Total ransomware by industry



SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016; NUMBERS HAVE BEEN ROUNDED; BITCOIN ART: DIBRONZINO/FOTOLIA

Technology (218%), utilities and energy (112%) and banking (93%) saw the highest year-over-year ransomware growth, the data showed. In addition to Locky variants, other ransom families in the top five included CryptoWall (based on CryptoLocker), CryptXXX, Bitman and Onion, which is also known as CTB-Locker.

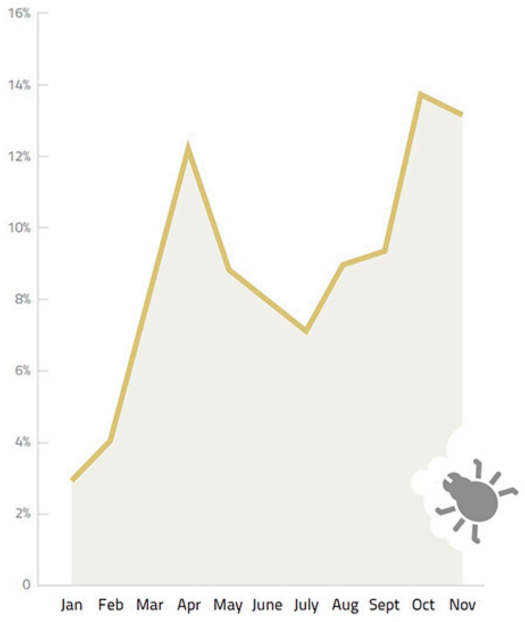
In this e-guide



Targeted More in 2016

Year-over-year ransomware growth by industry

SOURCE: CARBON BLACK THREAT REPORT, DECEMBER 2016



Rise in Attacks Beyond Malware

Microsoft PowerShell and WMI-based attacks in 2016

SOURCE: CARBON BLACK THREAT REPORT,DECEMBER 2016; WMI STANDS FOR WINDOWS MANAGEMENT INSTRUMENTATION

Malware was not the only way that criminals gained control of systems last year. According to Carbon Black, a rise in nonmalware attacks that used Microsoft PowerShell and Windows Management Instrumentation (WMI) increased in Q2 and never really lost momentum.

Fundamentals of endpoint security: Antimalware protection in the enterprise

Ed Tittel, Writer, Trainer, Internet Consultant

Endpoint antimalware protection is a type of application that actively works to prevent malware from infecting a computer. In many such products, the security technology extends to virtual desktops and mobile devices, as well as workstations and laptops.

Common types of malware that affect computers and all kinds of mobile devices include viruses, Trojan horses, worms, spyware, rootkits and the like.

The term "endpoint" with "antimalware" usually implies a product is designed for use within an organization (versus individual consumer use on a one-off or household basis), which could mean a small business, branch office, midsize company, government agency or enterprise.

With hundreds of thousands of different kinds of malware in the wild, and with cyberattacks on the rise, one hyper-critical issue for organizations of any size is ensuring strong protection against malware. Plus, organizations that fall under the regulatory umbrella of laws like the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, or adhere to PCI DSS standards for accepting payment cards, must run antimalware software as a part of their compliance requirements.

In this e-guide

The beauty of endpoint antimalware software suites

Endpoint protection must be able to prevent malware attacks, protect users (while exchanging emails, browsing the Web or connecting devices), and stop the proliferation of any attacks that manage to succeed. To meet those goals, today's endpoint antimalware suites provide layered protection in the form of robust antivirus functionality -- with the ability to shield against new or otherwise unknown threats, aka zero-day threats -- antispyware, email inbox protection, host-based firewall, data loss prevention, warnings when visiting websites that could pose safety risks, and much more.

The beauty of such antimalware suites is that a single package with multiple functionalities presents a cohesive defense between external malware and internal systems and data. This type of in-depth defense uses different methods to stop malware so an attempted attack or intrusion is unlikely to succeed simply by making its way through a single layer of protection. Plus, a suite is easier for IT to manage than a collection of different applications from different vendors.

Think of a computer or device with endpoint antimalware installed as a heavily fortified castle with thick walls, a moat, steel gates and drawbridges. Guards -- inside and out -- constantly watch for suspicious activity, ready to block or slay the "dragons."

Characteristic features of endpoint antimalware protection

Here are some typical features found in these kinds of software suites:

- **Antivirus:** Malware writers go to great lengths to create malware that can avoid detection and resist removal. Today's antimalware products typically combine signature-based scanning with heuristics technology and cloud-based global threat intelligence to recognize and root out malware on systems and prevent infections in the first place. (Heuristics is the practice of identifying malware based on previous experience, observations of malware behavior and typical points of attack.) This combination of antivirus technologies is also effective against zero-day threats, which have historically posed major challenges to IT security teams.
- **Antispyware:** A malicious spyware infection is probably easier to pick up than a common cold, and it's a major threat to protecting sensitive or confidential data. Antispyware software runs constantly in the background to block spyware installation, regardless of the source.
- **Data loss prevention (DLP):** The technologies involved in DLP aim to protect data that leaves the security of the internal business network, whether it's via email messages, USB drives, on a laptop or mobile device, or uploaded to the cloud.
- **Desktop firewall:** Although a network should always be protected by a firewall, having a second firewall running on the endpoint is another layer of defense against malware that finds any cracks in the armor.

- **Device control:** Malware can infect a computer that isn't connected to a network or the Internet. Connecting a USB device to a computer or installing software from a CD or DVD always runs the risk of transferring an infected application to the target machine. Device control allows IT to restrict or block user access by setting and enforcing device access rules.
- **Email protection:** This component of antimalware suites attempts to filter out phishing emails, spam and other messages that carry malicious or otherwise suspect content.
- **Website browsing protection:** Also referred to as reputation technology, most antimalware suites consult some type of ratings database that indicates whether a website is safe to browse or not. With this type of protection in place, those websites that are indicated as not safe will not be opened. Users will receive warn-off messages instead.

In addition to the above features, some endpoint antimalware suites roll in intrusion detection and prevention functionality, application control and network access control. Some packages also perform patch assessment and management, in which system threats are assessed and the most critical patches are applied first, as well as vulnerability assessments and even full-disk encryption to protect stored data.

In this e-guide

Deploying and managing endpoint antimalware products

Typically, endpoint antimalware products require an administrator to install a management console on a server to help manage clients, product licenses and logs.

This step also creates a database containing settings, privileges, events and security policies. An organization that's very large or has multiple sites may need to install additional management servers for performance reasons, as well as to replicate data. The next step is to install software (sometimes referred to as an "agent") on client computers and devices, either directly or across the network.

Regardless of the approach taken, clients must be configured for client software updates (automatic or pushed from the server) and virus definition updates, at a minimum.

Overall, endpoint antimalware protection is an important and necessary element in any organization's security infrastructure -- though it shouldn't be the only element organizations implement. Before diving in, IT managers and security specialists should assess their environments to determine what they need specifically to protect, and should look ahead three to five years at how their environment is expected to change.

It's also a good idea to research several highly rated endpoint antimalware packages to see how their features compare, determine which packages are most suitable to the organization's size and needs, and keep an eye on costs to get the best product for the budget.

↘ Next article

In this e-guide

Removing malware: What are the best methods?

Nick Lewis, Program Manager for Trust and Identity - Internet2

Ever since the first viruses were detected, there has been a constant battle of deciding between the most appropriate responses to detected malware. Should security teams clean up the malware and move on or format the hard drives to start over with a clean system? Both options have their place and the right one for an organization depends heavily on the enterprise's risk tolerance, the type of system and many other factors.

This tip will explore the process of removing malware from client devices and potential best practices.

Process of removing malware from client devices

Malware appears to be becoming harder to detect and remove from client devices, but the fundamental issues have not changed. The questions of if a system was infected, what the malware is, what the malware did, where the malware hid and if it can be removed still remain. Malware, specifically rootkits, have been around since the 1990s and can burrow deep into the operating system to hide its activities. Malware has become harder to detect as malware authors make an effort to hide their activities rather than announcing that they love you. Malware has become more difficult to remove with the emergence of fileless malware, DLL injection and other advancements.

While the questions in the age of ransomware are the same, the risk of choosing the incorrect response has never been higher. If a system is infected with ransomware and the owner pays the ransom, it's possible the malware won't be removed and the criminal will come back to re-encrypt the data and ask for a new ransom. Even APT-style attacks could be persisting on a network if not completely removed from a compromised system.

One change is the depth of hardware infiltrations. If your enterprise is defending against state-sponsored attackers like the NSA, their hardware implants appear to be significantly more advanced than the attacks of the 1990s. The hardware implements have been accompanied by malware targeting firmware.

The security tools in the last 20 years have improved significantly. The standard install of most operating systems still needs additional security tools, but file integrity monitors like Tripwire, OSSEC and Samhain, as well as host-based intrusion detection system tools and whitelisting tools provide significant protection and visibility into files executing on a system.

Potential best practices for removing malware

Antimalware tool customers expect to receive instructions on removing malware, and most antimalware vendors provide some guidance. Some vendors even produce tools to remove specific pieces of malware like

Microsoft's Malicious Software Removal Tool, Apple's antimalware functionality and others for Android/iOS, along with commercial tools. Every antimalware vendor will give some instructions on how to remove detected malware, so if a customer wants to try to remove the malware, they can do so. This has been true for as long as there have been antivirus tools. Enterprises that want to first try to remove malware should develop standardized procedures for helpdesk and incident responders to use when responding to a malware infection. This could include requiring password changes, using a limited admin account to investigate a system, offline investigation and more.

With the advancements in hardware implants and malware targeting firmware, it is even more difficult to determine if a system has been compromised. If your enterprise has been targeted with this level of attack, it may not be possible to recover the infected hardware. Even if an attacker isn't using this level of sophistication, it may still not be possible to fully remove malware and may be a very time consuming process. A complete reinstall may not even remove malware hidden in the boot sector of a hard drive, so a complete wipe of a system might be necessary before reinstalling or reimaging a system. In the worst case where the firmware is infected, it may be necessary to replace the hardware.

Developing an automated procedure for reinstalling an operating system is a best practice from a system deployment aspect, but also significantly aids in reinstalling a system after a malware infection. One reason why enterprises try to repair a system after a malware infection is because of the length of time it takes to rebuild a system. A completely automated reinstall could address this concern and is more secure.

One absolute best practice is ensuring proper planning for incident response. It is critical to know what tools can be used to monitor a system to detect suspicious activity on the system or on the network. These detection tools are critical for evaluating if a system is compromised. Using a host-based system or security monitor, like the previously mentioned file integrity monitoring or whitelisting tools, to monitor activities on the local system, as well as a network monitor from a separate system to monitor all network traffic, can identify any suspicious behavior. Your enterprise should determine which of these tools work best when establishing procedures.

Conclusion

Understanding the risk tolerance for an enterprise is critical to the efficient functioning of an information security program. It may not be possible to know exactly what happened on a malware-infected system even with careful monitoring of the system. An enterprise with a low tolerance for risk may want to require that a system is reformatted if suspicious activity is detected and an enterprise with a higher risk tolerance might find it acceptable for a professional helpdesk technician using approved procedures to remediate a malware-infected system when it doesn't have sensitive data.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia