U.S. Department of Homeland Security
National Cybersecurity and Communications Integrations Center

Information Security Risk Assessment:

COTS Antivirus Software and Kaspersky-Branded Products

August 29, 2017

NCCIC

PURPOSE

This assessment presents the inherent information security concerns and security ramifications associated with the use of any commercial-off-the-shelf (COTS) antivirus solution in devices with access to a federal network. It also addresses specific risks presented by Kaspersky-branded products, solutions, and services (collectively, "Kaspersky-branded products").

BACKGROUND

Many organizations deploy antivirus software solutions to user workstations as a base layer of security to detect and remove the most common threats, including Trojans, malware, worms, and adware. Antivirus solutions have become a default part of cyber hygiene at the workstation level, though security experts recommend antivirus software be deployed alongside a full security stack to more robustly protect the network, a practice referred to as layered security or "defense-in-depth."[1]

Antivirus solutions usually employ one or more of three signature detection methods: file scanning, heuristics, and emulation.[2] File scanning leverages full content inspection in order to detect malicious code in files downloaded, emailed, or transferred to the computer. Heuristic scanning monitors all processes and establishes baselines for a workstation's patterns of behavior in order to detect deviations from those baselines. Emulators use sandboxed virtual machines to test run suspicious or encrypted executables. Monitoring changes in the sandbox allows the antivirus software to make a determination of whether the suspicious process is safe to execute on the host system or if the process is deemed unsafe and should be deleted or quarantined.

In order to perform these functions and protect the workstation, antivirus software requires the highest level of system privileges, particularly to combat any malicious software that might try to remove the antivirus or interrupt kernel-level system calls as part of its attack kill-chain. Each antivirus product operates off an antivirus engine—the main kernel programmed to search for malicious activity using the methods described above. Multiple antivirus products from different antivirus companies may share the same antivirus engine if an antivirus company does not have the resources to build its own engine.[3]

---

1 Shenk, 2013.
2 Sanok Jr, 2005.
3 Koret, 2014.

GENERAL ANTIVIRUS SECURITY CONCERNS

Deploying an antivirus product increases that workstation's attack surface. Mitigating this risk requires:

- trust in the antivirus company not to abuse its privileges on the host; and
- trust in the product to capably resist hijacking by the attackers against which it defends.

Assessing the vendor's reputation for trustworthiness is a crucial part of any security product acquisition process.

In order to perform their basic functions, antivirus products operate with the highest level of system privileges, which is higher than any standard computer process. This gives the antivirus vendor system-level privileges on the customer endpoints it defends. An antivirus product also has full content inspection capabilities, and could remove or transmit anything—from a downloaded Trojan and routine detection metrics to Personally Identifiable Information (PII) and proprietary data—back to its home servers. Because antivirus processes are often white-listed by the other products in an organization's security stack, an immense level of trust is granted to the antivirus vendor not to abuse that level of access for economic, espionage, or destructive purposes.

Many antivirus vendors now provide a virtual machine known as a "cloud sandbox" to further analyze suspicious executables. When the antivirus software detects and quarantines a suspicious file, it uploads the suspicious file to the antivirus vendor's virtual machine sandbox, which is located on a remote server (requiring an upload over the Internet). Some sandboxes are self-contained to prevent malware samples from contacting their command-and-control servers, but others remain connected to the Internet to record and analyze the malware's unhindered execution and communications. Researchers from SafeBreach Labs found it possible to hijack these Internet-connected sandboxes for data exfiltration. They accomplished this by having the malware embed the desired data payload into a second malware sample before purposely triggering the antivirus quarantine function. The antivirus then uploads the data-infused malware to the cloud sandbox, where it can contact and exfiltrate the data to attacker-controlled servers with no interference from the passive sandbox.[4]

Another feature many antivirus products advertise is the capability to "break-and-inspect" Hyper Text Transfer Protocol Secure (HTTPS) traffic for malicious code by intercepting the traffic with a man-in-the-middle (MITM) connection.[5] The antivirus software uses its own certificate to sign outgoing traffic from the user and incoming traffic from the server in order to decrypt the content and determine whether malicious commands or software are part of the communication. However, this technique expands the attack surface further, because it leaves no way for the

[4] Klein and Kotler, 2017.

[5] Bachaalany and Koret, 2015.

client to independently validate its connection to the server and leaves it wholly dependent on the security product's validation.[6]

Additional concerns lie in flaws with the antivirus products themselves, as some "do not properly verify the certificate chain of the server,"[7] do not always forward certificate-chain verification errors to the client, and occasionally connect to servers using weaker encryption protocols than the client itself would allow.[8] Even with the antivirus product working securely, simply employing this function defeats the purpose of end-to-end encrypted HTTPS connections with an external server because a third party is allowed to read, manipulate, and forward any information in the connection. In the best case, an antivirus product would detect an encrypted malware callback and remove it from the outgoing traffic so the malware cannot contact the attacker's server. In the worst case, a product could store and exfiltrate sensitive information, including login credentials being transmitted from the client to the server, or otherwise compromise the integrity of the network communication.

Furthermore, any software that receives vendor-provided updates could disguise known malicious software via the antivirus update process. Just as antivirus companies like Webroot have accidentally released signature updates that mistakenly identify legitimate programs as malicious,[9] an antivirus company could just as easily provide signatures marking known malicious software as legitimate and safe. More subtly, the antivirus software could withhold signatures that would identify known malware. Additionally, even a correctly functioning antivirus update process can still fall victim to third-party attack, as Windows Update did in 2012 when the Flame virus spoofed a legitimate Microsoft certificate to trick the workstation into loading the malware launcher, which was disguised as a normal update.[10] While antivirus definitions are usually specially formatted and encrypted lists of pattern-match signatures, updates to the antivirus software itself modify the code the program runs on, and the updates themselves could potentially include malicious code.

Deployment of personal antivirus on employee bring-your-own-devices (BYOD) introduces additional security considerations because, while these devices are not subject to the same supplementary security restrictions and access controls as an enterprise workstation, they are often allowed to operate on the same enterprise data.

Like any software, antivirus products themselves are subject to exploitation, and any attacker with the ability to compromise the product has the ability to assume the security privileges of that running process. COSEINC security researcher and author of *The Antivirus Hacker's Handbook*, Joxean Koret presented multiple vulnerabilities, identified across a wide array of

[6] US-CERT, 2017.
[7] US-CERT, 2017.
[8] US-CERT, 2017.
[9] Sulleyman, 2017.
[10] Whitney, 2012.

different antivirus products, during his presentation to the information security conference 44CON in 2014.

While many of these security flaws were quickly patched by the antivirus companies in question, Koret also identified vulnerabilities inherent to using any commercial antivirus engine, such as:

- buffer overflows due to the properties of the programming languages used to code most engines;
- virus definition updates sent over HTTP and vulnerable to MITM attacks;
- libraries compiled without using address space layout randomization (ASLR); and
- other vulnerabilities.[11]

A security stack is only as strong as its weakest component, and antivirus solutions present a large vulnerability in the event that an attacker can compromise the software.

KASPERSKY-SPECIFIC CONSIDERATIONS

Based on publicly available information, Kaspersky-branded antivirus software and other Kaspersky-branded products and solutions that contain antivirus functionality appear to present the general antivirus software risks identified above. For example, the default installation of Kaspersky Internet Security scans all encrypted HTTPS connections using the interception technique described above in order to detect malicious activity.[12]

Additionally, Kaspersky customers may participate in the Kaspersky Security Network (KSN). KSN is a cloud-based network to which a wide range of data from customer devices may be transferred for the purpose of additional analysis. A list of such data is available in the KSN Statement, which users must agree to in order to participate.[13] Under the terms of the agreement, the information subject to transfer includes highly sensitive data collected from a user's device, such as information about the computer's hardware and software, files downloaded, certain websites visited, running applications, and user account names—essentially the full spectrum of forensic data a device produces. Furthermore, Kaspersky notes in the KSN Statement that it reserves the right to disclose any of the information processed "under confidentiality and licensing agreements with certain third parties which assist [Kaspersky] in developing, operating, and maintaining the Kaspersky Security Network."[14] These third parties may be trusted partners of Kaspersky, but that does not mean they are subject to the same vetting and rigorous suitability scrutiny as other companies with which the U.S. Government has entrusted its data.

[11] Koret, 2014.
[12] Kaspersky Labs 2017.
[13] Kaspersky Labs 2017.
[14] Kaspersky Labs 2017.

Kaspersky also notes that "no data transmission can be guaranteed secure"[15] and "[Kaspersky] cannot guarantee the security of any data [participants] transmit to [Kaspersky] or from [Kaspersky] products or services,"[16] with a final warning that participants "use all these services at [their] own risk."[17] Such data, whether provided to Kaspersky through normal course of operation, to third parties by Kaspersky as part of their sharing agreement, or to adversaries by in-transit interception techniques, could assist an attacker in obtaining sensitive files from government computers, targeting employees with precisely crafted spear-phishing attacks, and other information security risks.

Kaspersky has made statements that the risks of KSN can be mitigated by the customer or user. A May 9, 2017, Kaspersky press release states: "Unlike in many other products, Kaspersky Lab users have full control over telemetry (data) sharing with their participation being voluntary, and they can disable telemetry reporting completely at any given time. In addition, business and government users may choose to install a local and private Kaspersky Security Network (KSN) center on their premises to make sure the data never leaves their facility."[18]

The National Cybersecurity and Communications Integration Center (NCCIC) recognizes that Kaspersky may offer customers the ability to deploy a KSN center on the customer's local network and choose configuration settings that limit or eliminate the transfer of data to the KSN (among other potential options). However, assuming that the statements made by Kaspersky are fully accurate and it is possible to prevent any files from leaving a host or network, that assumption still does not address threats posed by the software itself as an on-premise solution. The level of system access granted to antivirus software would allow malicious activity to be conducted through the antivirus software itself, and even if the threat is not present in a current build of the software, it could be added through a future update or a third-party exploitation of the software. In order to stay up-to-date with the most advanced threats, even on-premise solutions require vendor updates to the antivirus signatures and less frequent updates to the software itself; and these updates are usually downloaded via temporary or indirect Internet connection or physical media like USB flash drives. Any software update has the potential to add functionality or expand the attack surface of the host machine. If a vendor withheld a signature update, the endpoints would remain vulnerable to a known threat. Furthermore, while the customer has the option of making configuration changes in the antivirus software, a configuration page is only a user interface, meaning it could display options as disabled while they remain enabled in the antivirus code.

Kaspersky also offers various cybersecurity services, including threat hunting, incident response, and security assessment. The information security risk presented by any service depends on the

[15] Kaspersky Labs 2017.
[16] Kaspersky Labs 2017.
[17] Kaspersky Labs 2017.
[18] Kaspersky 2017.

specifics of the service provided. In general, these services present various significant information security risks. For example, any service that involves direct or indirect access to a computer or network, such as through installation of endpoint software to conduct a hunt or incident response, or through other abilities to influence information security practices on a network, presents information security risks.

RECOMMENDATIONS

While new software acquisitions are primarily assessed for technical capability, effectiveness, and ease of use, vendors should undergo vetting separate from that of their products. Security vendors with access to sensitive federal data and networks must be confirmed as trustworthy partners who keep customer business independent of—and unaffected by—any obligations to the vendors' home government or commercial partners.

In response to concerns about the security of an antivirus product, some vendors may offer a government the opportunity to review the product's source code. The value of such a review should be viewed with caution. First, by its inherent nature, antivirus software has broad access rights and privileges (as described above), and it is this inherent functionality that presents information security risks. Thus, even if a source code review found no backdoors or other unusual code, these risks would remain. Apart from the inherent risks in the code (when exploited by a malicious actor), if a reviewer did review the code, the reviewer may not know or be able to confirm whether the provided source code is complete and unaltered. The code could also be updated at any time, and the reviewing party may not have the resources or ability to continually re-review the code. The review also may be incomplete or ineffective unless done by someone with deep familiarity with the software (such as one of its original developers).

WORKS CITED

Bachaalany, Elias, and Joxean Koret. “The Antivirus Hacker's Handbook”. Indianapolis: John Wiley & Sons, Inc., 2015.

Kaspersky Labs. "Kaspersky Internet Security 2018 release notes: commercial release of version 18.0.0.405." Kaspersky. August 14, 2017. http://support.kaspersky.com/13617#block1 (accessed August 18, 2017).

Kaspersky Labs. "Kaspersky Security Network Statement." Kaspersky. March 3, 2017. http://support.kaspersky.com/9365#block0 (accessed August 8, 2017).

Kaspersky. May 9, 2017 Statement Regarding Recent False Allegations about Kaspersky Lab. May 9, 2017. https://usa.kaspersky.com/blog/statement-regarding-false-allegations/11109/ (accessed August 23, 2017).

Klein, Amit, and Itzik Kotler. "The Adventures of AV and the Leaky Sandbox." SafeBreach. July 28, 2017. https://go.safebreach.com/rs/535-IXZ-934/images/Adventures_AV_Leaky_Sandbox.pdf (accessed August 23, 2017).

Koret, Joxean. "Breaking Antivirus Software." 44CON. 2014. 146. http://joxeankoret.com/download/breaking_av_software_44con.pdf (accessed August 18, 2017).

Sanok Jr., Daniel J. "An Analysis of How Antivirus Methodologies Are Utilized in Protecting Computers from Malicious Code." InfoSecCD '05 Proceedings of the second annual conference on Information security curriculum development. Kennesaw, GA: ACM New York, NY, USA, 2005. 142-144.

Shenk, Jerry. Layered Security: Why It Works. White Paper, SANS Institute, 2013. https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805 (accessed August 27, 2017).

Sulleyman, Aatif. "Windows Users Mystified As Antivirus Accidentally Cripples Computers." The Independent. April 25, 2017. http://www.independent.co.uk/life-style/gadgets-and-tech/news/windows-antivirus-software-malware-webroot-trojan-facebook-microsoft-a7701896.html (accessed August 18, 2017).

US-CERT. "HTTPS Interception Weakens TLS Security." National Cyber Awareness System (NCAS) Alert (TA17-075A). March 16, 2017. https://www.us-cert.gov/ncas/alerts/TA17-075A (accessed August 24, 2017).

Whitney, Lance. Flame virus can hijack PCs by spoofing Windows Update. June 5, 2012. https://www.cnet.com/news/flame-virus-can-hijack-pcs-by-spoofing-windows-update/ (accessed August 24, 2017).