Kaspersky-Branded Products and Berkeley Research Group Independent Assessment

NCCIC

Background

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) reviewed the Independent Assessment, titled *Information Security Risks of Anti-Virus Software* (hereafter "BRG Assessment"), prepared by Berkeley Research Group, LLC (BRG), and dated November 10, 2017. Kaspersky Lab (hereafter "Kaspersky") submitted the BRG Assessment to DHS as an exhibit to Kaspersky's request for DHS to initiate a review of Binding Operational Directive (BOD) 17-01. The BRG Assessment, in part, responds to the *NCCIC Information Security Risk Assessment* (hereafter "NCCIC Assessment") on commercial off-the-shelf (COTS) anti-virus software and Kaspersky-branded products, dated August 29, 2017. The NCCIC Assessment was attached as Exhibit 1 to an Information Memorandum from the Assistant Secretary for DHS Cybersecurity and Communications (CS&C) to the Acting Secretary of DHS, dated September 1, 2017 (hereafter "Information Memorandum"). This document is a *Supplemental Information Security Risk Assessment* and will similarly be attached to an Information Memorandum from the Assistant Secretary for CS&C to the Acting Secretary of DHS.

1. File Access and High-Level Privileges

The BRG Assessment confirms the key conclusions of the NCCIC Assessment. Specifically, BRG explains, consistent with the NCCIC Assessment, that anti-virus software operates with "broad access to the computer's hardware and operating system" and that the software "runs with the same privileges as the user, as well as one or more underlying, highly-privileged software components, such as kernel-mode drivers or SYSTEM-level processes." BRG describes the "kernel" as a "core component of a computer's operating system and largely responsible for facilitating the interaction between other software running on the computer and the computer's central processing unit (CPU), memory, and other hardware devices (often via additional software called a "device driver")."[1] The "SYSTEM account" is "an internal account on Microsoft Windows operating systems that operates at the highest privilege level."[2] Most anti-virus software now also "intercepts and monitors network traffic on a user's computer, including encrypted web browsing traffic, in order to identify malicious code embedded in websites visited by the user."[3]

Based on its "limited technical analysis within the time available" of Kaspersky and other anti-virus products, BRG determined that all of the software that it analyzed, including Kaspersky-branded products, "contained components that operated with SYSTEM-level privileges." Additionally, BRG determined that "[e]ach installed multiple kernel drivers within our test systems for various anti-malware purposes, including file system monitoring, process monitoring, and network traffic interception and

[1] BRG Assessment, p. 8, n. 13.

[2] BRG Assessment, p. 8, n. 14.

[3] BRG Assessment, pp. 8-9.

inspection."[4] BRG states that, "[A] software vulnerability in any one of the kernel drivers or SYSTEM-level processes could reasonably result in a complete compromise of the user's computer."[5]

While BRG refers (above) to a "software vulnerability" in a kernel driver or SYSTEM-level process, as detailed in the NCCIC Assessment, DHS is concerned about the information security risks presented by the normal functionality of anti-virus software, apart from any specific "vulnerability" in the software. The Russian Government or Kaspersky—in collaboration with the Russian Government—can exploit this functionality, including broad access to files, high-level system privileges, and interception and inspection of encrypted web traffic.

2. BRG Preliminary Review of Kaspersky-Lab Software

Overview

The BRG Assessment states that BRG conducted a "preliminary review" of specific Kaspersky anti-virus products and solutions. BRG states that the BRG Assessment intended the review to address the following three high-level objectives:

1. Evaluate whether it is feasible for an intelligence agency to passively monitor and decrypt traffic between users of Kaspersky-branded products and the Kaspersky Security Network (KSN);
2. Determine whether turning KSN off—or using the Kaspersky Private Security Network (KPSN)—can reliability prevent potentially sensitive data from inadvertently being transmitted to Kaspersky; and
3. Evaluate whether there exists a mechanism by which a malicious actor leveraging KSN can conduct targeted searches of Kaspersky users for specific information.

NCCIC assesses each of these objectives in turn below.

Objective 1: Passive Interception and Decryption of Traffic between Kaspersky-Branded Products and KSN

Kaspersky's KSN infrastructure "supports several security-related services provided by Kaspersky software products, including file, website, and wireless network reputation services."[6] KSN also "has the ability to receive information from clients, such as statistics regarding malware detected on users' computers or samples of malicious files, to improve Kaspersky's malware detection capabilities."[7] These are all consistent with NCCIC's understanding of KSN functionality.

---

[4] BRG Assessment, p. 11.

[5] BRG Assessment, p. 11.

[6] BRG Assessment, p. 24.

[7] BRG Assessment, p. 24; see also p. 6, n. 6.

BRG indicates that it identified this objective because the NCCIC Assessment and the Information Memorandum "refer to KSN as a potential information security risk due to the presumed ability of a malicious third party to monitor and intercept communications between KSN and users of Kaspersky software."[8]

DHS notes two significant limitations in this portion of the BRG Assessment. First, as BRG states, "BRG has not yet independently reviewed any network protocols or other communications systems used *within* KSN or *between KSN and Kaspersky's non-KSN IT infrastructure* (e.g., Kaspersky offices or other datacenters)" (emphasis added by author).[9] It is this access to Kaspersky offices and datacenters in Russia—and communications between such offices and datacenters and KSN—that is a principal concern of DHS. In addition, BRG states that its objective is to evaluate the potential for "passive" monitoring and decryption by an intelligence agency or other third party. As explained in detail in the Information Memorandum, DHS is concerned—not only about such passive activities—but also about active operations involving Russian intelligence access to Kaspersky offices and datacenters, requests for decryption keys, and other abilities of Russian government agencies to compel or request assistance from Kaspersky.

On the specifics of what BRG did test, BRG states that it observed Kaspersky anti-virus software products "generally" using one of three network protocols for communicating with KSN infrastructure:

- Hypertext Transport Protocol (HTTP),
- HTTP Secure (HTTPS), and
- Kaspersky's proprietary KSN protocol.

Use of HTTP in Kaspersky Products

BRG states that Kaspersky client-side software uses HTTP to download product installation files during initial setup, to download software updates, and to download malware "record" updates. While other anti-virus vendors use the term "definition" or "signature," according to BRG, Kaspersky personnel internally use the term "record" to refer both to traditional signatures (used to identify malware on a user's computer) as well as more modern approaches to malware detection, such as heuristic methods, machine learning models, and behavioral methods.[10]

As BRG states, HTTP transmissions are unencrypted and unauthenticated. Nevertheless, BRG explains that all file types downloaded by Kaspersky software from Kaspersky servers are authenticated using "standard code- or package-signing mechanisms", including Microsoft's Authenticode and GOST 34.10.2001. Kaspersky software then "verifies the integrity of the bases or

[8] BRG Assessment, p. 24.

[9] BRG Assessment, p. 24, n. 71.

[10] BRG Assessment p. 8, n. 10.

index files prior to installation on the user's computer" and, consequently, users "would likely be able to detect attempts by a malicious actor to tamper with application-related files downloaded over HTTP."[11]

BRG does not explain exactly what error message would be presented to a user or any other mechanism by which a user would be alerted to a maliciously modified update. Moreover, BRG states that, "[d]ue to time constraints, we have not yet been able to include an assessment of Kaspersky's internal security processes and procedures regarding access to and use of [Kaspersky Lab Signer] and the keys used to sign bases, packages, or other updates distributed to Kaspersky software clients." [12] These are significant gaps in BRG's analysis. BRG's analysis of this use of HTTP therefore does not mollify DHS's concern that Kaspersky or Russian government actors could incorporate malicious functionality into Kaspersky software through the software or record update process.

Use of HTTPS in Kaspersky Products

BRG states that it observed Kaspersky software using HTTPS "in limited situations." Specifically, BRG explains that Kaspersky software will connect to KSN infrastructure:

- to activate the product;
- to obtain "in-product content" (such as Kaspersky Lab news);
- for communications about product license purchases and renewals; and
- for uploading "application crash dumps," which often include "the state of the application when the error occurred, possibly including memory contents, logs, or other information about the software on the system at the time of the application crash."[13]

BRG states that Kaspersky software "followed industry-standard best practices for SSL/TLS encryption," including using TLSv1.2 by default, properly validating the authenticity of server certificates, and using strong cipher suites for session key negotiation and encryption.[14]

DHS understands these uses of HTTPS and generally agrees with the use of HTTPS, if properly implemented, to protect web traffic. However, DHS notes that BRG states that it needs to "further validate the security of Kaspersky's client side SSL/TLS implementation (based on the open-source OpenSSL library), as well as the security processes used to manage the application servers."[15] Thus, if BRG identifies client-side implementation issues or issues with the security processes for management of Kaspersky application servers, these would present additional risks of concern to DHS.

---

[11] BRG Assessment, p. 25.

[12] BRG states that Kaspersky Lab Signer ("KLS") is Kaspersky's internal, centralized service "intended" to cryptographically sign the various file types used by Kaspersky software prior to distribution to users. BRG Assessment, p. 25.

[13] BRG Assessment, p. 25.

[14] BRG Assessment, p. 25.

[15] BRG Assessment, p. 26.

Breaking and Inspecting of HTTPS by Kaspersky Products

While BRG focuses on Kaspersky's use of HTTPS to encrypt communications between users and KSN, BRG does not address the risks created by the Kaspersky software's ability to break and inspect other HTTPS communications by the user's non-anti-virus applications.

As explained in the NCCIC Assessment, Kaspersky-branded products have the ability to decrypt encrypted HTTPS transmissions, inspect and analyze the contents, and then re-encrypt and forward on the traffic. Specifically, the NCCIC Assessment states, with respect to anti-virus products—including Kaspersky products that have this functionality—that 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 client to independently validate its connection to the server."[16] Furthermore, "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."[17] And, "[i]n 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 connection."[18]

Kaspersky's ability to break and inspect encrypted traffic is clearly described in publically-available Kaspersky documentation.[19] However, BRG's analysis does not address the above risks.

Use of Proprietary Encryption Protocol for Communications with the KSN

In addition to using HTTP and HTTPS, the BRG Assessment states that Kaspersky software uses "its own proprietary, encrypted protocol for communicating with KSN."[20] DHS understands that this custom protocol is the primary encryption method leveraged by Kaspersky products to protect sensitive customer information in-transit between the customer's Kaspersky software and KSN.

To analyze use of this protocol, BRG states that it reviewed a subset of the Kaspersky source code related to this protocol, communicated with a Kaspersky developer with knowledge of its implementation, and analyzed KSN network traffic generated by the Kaspersky products it was reviewing.[21] BRG then explains, at a high level, the various encryptions and decryptions—using certain public, private, and secret keys—that occur when Kaspersky client software first connects to KSN (e.g.,

---

[16] NCCIC Assessment, pp. 3-4.

[17] NCCIC Assessment, p. 4.

[18] NCCIC Assessment, p. 4.

[19] Kaspersky Lab, *How to scan encrypted connections in Kaspersky Internet Security 2012*, August 15, 2012, ID: 6271, https://support.kaspersky.com/us/6271.

[20] BRG Assessment, p. 26.

[21] *See* BRG Assessment, p. 26.

with a file reputation request), when the KSN server responds to the client software, and during future connections between the client and the KSN server.

BRG concludes that the KSN protocol "appears to be secure from decryption by a passive adversary who does not possess the server's RSA private key or secret [Advanced Encryption Standard] AES key ($\mathbf{K_s}$)." Significantly, the KSN protocol "does not provide forward secrecy"—i.e., "if the server's RSA private key [which is a long-term key shared across all KSN servers] is compromised, a malicious actor could decrypt the client-generated AES key ($\mathbf{K_c}$) and passively decrypt *all previous or subsequent data sent by or to a Kaspersky client*" (emphasis added by author).[22] Similarly, BRG states that "if the server's AES key [which is a secret key also shared across KSN servers and re-generated weekly] is compromised, a malicious actor could recover the client-generated AES key from the encrypted session token and use the decrypted AES key to passively decrypt *all previous or subsequent data sent by or to a Kaspersky client until the server rotates its AES key*" (emphasis added by author).[23]

BRG states that, according to Kaspersky, this proprietary, encrypted protocol is intended to "(a) reduce load on KSN clients and servers, (b) permit clients to continue an encrypted KSN session across multiple separate TCP connections, and (c) enable any KSN server to handle a client's request since the servers do not maintain any connection state."[24] However, as BRG explains, the encryption implementation creates significant risks to the confidentiality of the data transmitted between Kaspersky software and KSN servers, if a KSN RSA private key or an AES secret key is compromised or otherwise obtained. As DHS explains in the Information Memorandum to which this Supplemental NCCIC Assessment is attached, based on a report prepared by Professor Peter Maggs, Russian law requires Kaspersky—and all other companies that use encrypted communications—to provide to the Russian Federal Security Service (FSB) the keys or other information needed to decrypt the company's encrypted communications in Russia. Thus, DHS has significant concerns about the ability of FSB to obtain access to unencrypted transmissions between KSN and U.S. government customers that use Kaspersky-branded products and participate in KSN.

According to BRG, Kaspersky "has claimed that it is modifying its current KSN encryption protocol to incorporate a Diffie-Hellman key exchange protocol that would provide for forward secrecy."[25] The above issues nevertheless currently remain.

Objective 2: Turning KSN Off or Using the Kaspersky Private Security Network

As described in the NCCIC Assessment, DHS is aware of Kaspersky statements that user participation in KSN is voluntary and users can "disable telemetry [data] reporting completely at any given time."[26] However, BRG testing determined that this statement is inaccurate, at least with respect to Kaspersky

---

[22] BRG Assessment, pp. 26-27.

[23] BRG Assessment, pp. 26-27.

[24] BRG Assessment, p. 27.

[25] BRG Assessment, p. 27.

[26] NCCIC Assessment, p. 6.

consumer-oriented products; products which could be used by federal departments and agencies. Specifically, BRG observed that "Kaspersky consumer-oriented products (i.e., Kaspersky Anti-Virus, Kaspersky Internet Security, and Kaspersky Total Security), communicated with KSN to a limited degree *despite declining to agree to the KSN Statement during product installation and also disabling KSN within the application's user interface*" (emphasis added by author).[27] In particular, when the software detected sample malware, BRG inferred that "statistics" about the infection were uploaded to Kaspersky— although BRG does not appear to know what exact data was uploaded—and that the sample file was "likely uploaded" to Kaspersky when KSN was enabled.[28] Thus, even if a customer declines to participate in KSN and disables KSN in the user interface, some data is transferred to Kaspersky, and even a sophisticated user is unable to determine exactly what that data is.

The NCCIC Assessment also acknowledged the ability of government customers to deploy a local version of KSN on the customer's network, referred to as the Kaspersky Private Security Network (KPSN). Kaspersky markets KPSN as a way for customers' files and other objects to be analyzed locally, in an IT environment controlled by the customer, rather than sending the files back to KSN over the public Internet (using the proprietary, custom protocol described above).

BRG explains that KPSN can be installed in one of three configurations: "(a) Standard, which allows all on-premise KPSN servers to access Kaspersky servers directly; (b) Unidirectional Gateway, in which access to Kaspersky servers is managed through a gateway, installed and configured in an organization's [demilitarized zone] DMZ, that allows only inbound traffic to the on-premise KPSN servers, and (c) Proxy, where traffic from the local network to the Internet is routed through a proxy server configured at the network's perimeter."[29]

In its testing, BRG observed its test KPSN server downloading and updating its reputational databases using HTTPS and AMQPS, an encrypted version of the Advanced Message Queuing Protocol. In response to a sample malware infection, a Kaspersky enterprise-oriented product (Kaspersky Endpoint Security) communicated (presumably about the detection) to the KPSN server, and BRG did not observe any traffic from the KPSN server to KSN or any other Kaspersky servers.[30]

However, BRG did not address a main concern expressed in the NCCIC Assessment about the KPSN option. Specifically, the NCCIC Assessment explains that

- "even on-premise solutions require vendor updates to the anti-virus signatures and less frequent updates to the software itself,"
- "these updates are usually downloaded via temporary or indirect Internet connection or physical media like USB flash drives," and

[27] BRG Assessment, p. 28.

[28] BRG Assessment, p. 28.

[29] BRG Assessment, p. 28.

[30] BRG Assessment, p. 29.

- "[a]ny software update has the potential to add functionality or expand the attack surface of the host machine."[31]

The Kaspersky client software still receives record and software updates from Kaspersky through KPSN, and such software updates can contain malware or take another action that presents risks to federal information and information systems (e.g., by compromising the integrity of data or the availability of IT resources; in addition to other mechanisms for data exfiltration outside of the connection between the customer and KSN).

The NCCIC Assessment also notes that a vendor-withheld signature would make the endpoint remain vulnerable to a known threat.[32] DHS recognizes that Kaspersky has pointed to NIST Special Publication 800-83, Revision 1 to argue that the risk of Kaspersky intentionally withholding signatures to allow specific attacks can be mitigated by using anti-virus products from multiple vendors. However, the NIST publication that Kaspersky cites also states that "running multiple antivirus products on a single host simultaneously is likely to cause conflicts between the products" and that "if multiple products are used concurrently, they should be installed on separate hosts" (e.g., one anti-virus product on perimeter email servers and a different product on internal email servers).[33] NIST also notes that this "would necessitate increased administration and training, as well as additional hardware and software costs."[34] Finally, this suggestion does not address the risks of software updates including malware, the risks of the increased attack surface and risk of vulnerabilities that come with deploying multiple anti-virus products, or other risks.

Objective 3: Risk of Leveraging KSN to Conduct Targeted Searches of Kaspersky Users for Specific Information

BRG explains that Kaspersky Lab Anti-Virus Architecture (KLAVA) is the architecture for the core component of the Kaspersky anti-virus products, the anti-virus "engine." According to BRG, the KLAVA anti-virus engine, like most anti-virus engines, operates by ingesting a set of algorithms defined by Kaspersky malware analysts to detect and, in some cases, remediate, a malware infection.[35] Kaspersky refers internally to the implementation of a particular detection algorithm as a record, which may contain the name or other identifier assigned to the threat, its signature, or other means of detecting the threat, and an action (the "verdict") to take if the software identifies a file or process matching the threat.[36] BRG explains that, in addition to signatures and more advanced detection methods, records may also

---

[31] NCCIC Assessment, p. 6.

[32] NCCIC Assessment, p. 6.

[33] NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, p. 11, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[34] NIST Special Publication 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, p. 11, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[35] BRG Assessment, p. 29.

[36] BRG Assessment, p. 29.

include references (called “links”) to executable procedures implemented in C/C++ code, and these links “have nearly unrestricted access to the user’s system, including the ability to call operating system [Application Programming Interfaces] or other low-level system functions.”[37] Additionally, records can be used to update and patch Kaspersky software.[38] Individual records are compiled and aggregated into multiple database files (called “bases”), which are stored in Kaspersky’s proprietary KDC file format and distributed for ingestion into the KLAVA engines.

Significantly, BRG explains that KLAVA provides a function “which allows the analyst to upload a file processed by KLAVA to Kaspersky for further analysis,” as well as additional functions that can be used to retrieve and upload other information, such as Microsoft Windows registry keys.[39] Depending on the record’s “verdict” section, Kaspersky may—or may not—notify the user about the detection.[40] Furthermore, because Kaspersky uses a proprietary file format and encryption, a customer is unable to access the records to analyze whether any might be malicious.

BRG concedes that it anticipates doing, but has not yet completed,

1. “a more comprehensive assessment of the circumstances in which a file will be uploaded to Kaspersky from a user’s computer”; and
2. “a review of Kaspersky’s operational processes related to any controls surrounding the development, testing, deployment, and auditability of records given their capabilities and breadth of system access.”[41]

BRG has not yet addresses either of these areas, both of which are of significant areas of concern for DHS.

3. Conclusion

The NCCIC Assessment explained various risks to federal information and information systems presented by Kaspersky-branded products. As detailed in this Supplement, the BRG Assessment confirms NCCIC’s concerns about the broad file access and high-level system privileges of Kaspersky anti-virus products and BRG’s “Preliminary Review” of Kaspersky anti-virus software, across three objectives, does not meaningfully address the information security risks identified by DHS.

[37] BRG Assessment, pp. 29-30.

[38] BRG Assessment, p. 29.

[39] BRG Assessment, p. 30.

[40] BRG Assessment, p. 30.

[41] BRG Assessment, p. 30.