

# POPULAR SECURITY SOFTWARE CAME UNDER RELENTLESS NSA AND GCHQ ATTACKS

BY ANDREW FISHMAN AND MORGAN MARQUIS-BOIRE @AndrewDFish @headhuntr YESTERDAY AT 1:03 PM



The National Security Agency and its British counterpart, Government Communications Headquarters, have worked to subvert anti-virus and other security software in order to track users and infiltrate networks, according to documents from NSA whistleblower Edward Snowden.

The spy agencies have reverse engineered software products, sometimes under questionable legal authority, and monitored web and email traffic in order to discreetly thwart anti-virus software and obtain intelligence from companies about security software and users of such software. One security software maker repeatedly singled out in the documents is Moscow-based Kaspersky Lab, which has a holding registered in the U.K., claims more than 270,000 corporate clients, and says it protects more than 400 million people with its products.

British spies aimed to thwart Kaspersky software in part through a technique known as software reverse engineering, or SRE, according to a top-secret warrant renewal request. The NSA has also studied Kaspersky Lab's software for weaknesses, obtaining sensitive customer information by monitoring communications between the software and Kaspersky servers, according to a draft top-secret report. The U.S. spy agency also appears to have examined emails inbound to security software companies flagging new viruses and vulnerabilities.

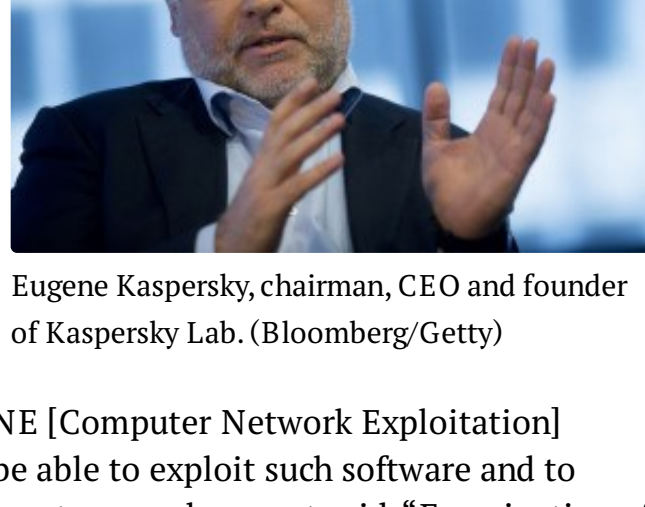
The efforts to compromise security software were of particular importance because such software is relied upon to defend against an array of digital threats and is typically more trusted by the operating system than other applications, running with elevated privileges that allow more vectors for surveillance and attack. Spy agencies seem to be engaged in a digital game of cat and mouse with anti-virus software companies; the U.S. and U.K. have aggressively probed for weaknesses in software deployed by the companies, which have themselves exposed sophisticated state-sponsored malware.

Anti-virus software is an ideal target for a would-be attacker, according to Joxean Koret, a researcher with Coseinc, a Singapore-based information security consultancy. "If you write an exploit for an anti-virus product you're likely going to get the highest privileges (root, system or even kernel) with just one shot," Koret told The Intercept in an email. "Anti-virus products, with only a few exceptions, are years behind security-conscious client-side applications like browsers or document readers. It means that Acrobat Reader, Microsoft Word or Google Chrome are harder to exploit than 90 percent of the anti-virus products out there."

(Disclosure: One of the authors of this report, Morgan Marquis-Boire, spoke at a Kaspersky Lab event in Puerto Rico in 2013 and at another in London in 2014. He was not paid for either event, but the cost of his travel and accommodation were covered by the company.)

## Reverse engineering Kaspersky software

According to a top-secret GCHQ warrant renewal request written in 2008 and published today by The Intercept, the British spy agency viewed Kaspersky software as an obstruction to its hacking operations and needed to reverse engineer it to find ways to neutralize the problem. Doing so required obtaining a warrant.



Eugene Kaspersky, chairman, CEO and founder of Kaspersky Lab. (Bloomberg/Getty)

"Personal security products such as the Russian anti-virus software Kaspersky continue to pose a challenge to GCHQ's CNE [Computer Network Exploitation] capability and SRE is essential in order to be able to exploit such software and to prevent detection of our activities," the warrant renewal request said. "Examination of Kaspersky and other such products continues." The warrant renewal request also states that GCHQ reverse engineers anti-virus programs to assess their fitness for use by government agencies.

The requested warrant, provided under Section 5 of the U.K.'s 1994 Intelligence Services Act, must be renewed by a government minister every six months. The document published today is a renewal request for a warrant valid from July 7, 2008 until January 7, 2009. The request seeks authorization for GCHQ activities that "involve modifying commercially available software to enable interception, decryption and other related tasks, or 'reverse engineering' software."

Software reverse engineering, or "reversing," is a collection of techniques for deciphering and analyzing how a program operates. The process can be as simple as observing the flow of data into and out of the program, or as complex as analyzing the machine code — 1s and 0s — to look into the software's inner workings, including portions of the code that are not explained in the manual or other program documentation. Put simply, it often means taking thousands of commands that instruct the computer exactly what to do and working backwards to translate them into a format that's more intelligible to a human being.

Reversing is a common, often benign practice among software developers that can be used to enable software from different companies to interoperate or to identify security vulnerabilities before they can be exploited by third parties. Software makers, fearing piracy, hacking and intellectual property theft, often forbid the practice in licensing agreements and sometimes protect the most sensitive inner workings of their software with encryption. Governments have passed laws, with digital media in mind, that strictly circumscribe tampering with this encryption. Software companies have also sued to block reverse engineering as copyright infringement, arguing that it is illegal to make a copy of a program in violation of their restrictions on such copying.

GCHQ felt it needed legal cover to conduct reverse engineering, writing in the warrant renewal application that the practice could otherwise be "unlawful" and amount to "a copyright infringement or breach of contract." As we explore in a related story today, the warrant is legally questionable on several grounds, in that it applies ISA section 5 to intellectual property for the first time, and GCHQ may be applying ISA section 5 to certain categories of domestic policing.

It is unclear what GCHQ accomplished in its analysis of Kaspersky software, but GCHQ has repeatedly reverse engineered software to discover vulnerabilities. Rather than report the vulnerabilities to the companies, spy agencies have quietly stockpiled numerous exploits for a wide range of commercial hardware and software, using them to hack adversaries.

## Collecting leaky data

The NSA, like GCHQ, has studied Kaspersky Lab's software for weaknesses. In 2008, an NSA research team discovered that Kaspersky software was transmitting sensitive user information back to the company's servers, which could easily be intercepted and employed to track users, according to a draft of a top-secret report.

The information was embedded in "User-Agent" strings included in the headers of Hypertext Transfer Protocol, or HTTP, requests. Such headers are typically sent at the beginning of a web request to identify the type of software and computer issuing the request.

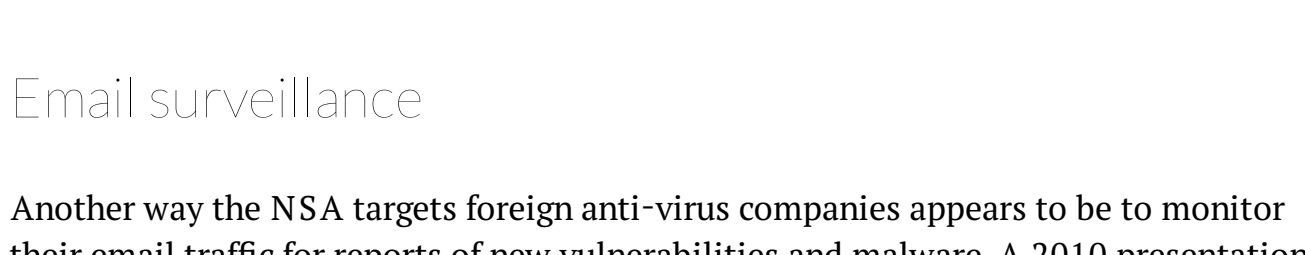
```
(U) User-Agent Strings
(TS//SI//REL) The Kaspersky client sends its own User-Agent strings when requesting updates. Some examples are
GET /diffs/bases/ids/i386/idsbase.kdz.7f- HTTP/1.0
Host: dnl-r01.kaspersky-labs.com
User-Agent: wnB4BwnB_ujCg31C0BANOC4wLjAuMzU3
GET /index/u0607g.xml.klz HTTP/1.0
Host: dnl-us5.kaspersky-labs.com
User-Agent: wnBAAAs9sHIBANOC4wLjAuNDU0
```

According to the draft report, NSA researchers found that the strings could be used to uniquely identify the computing devices belonging to Kaspersky customers. They determined that "Kaspersky User-Agent strings contain encoded versions of the Kaspersky serial numbers and that part of the User-Agent string can be used as a machine identifier." They also noted that the "User-Agent" strings may contain "information about services contracted for or configurations." Such data could be used to passively track a computer to determine if a target is running Kaspersky software and thus potentially susceptible to a particular attack without risking detection.

In a statement emailed to The Intercept, Kaspersky Lab denied that its "User-Agent" strings could be used against its customers. "The information is depersonalized and cannot be attributed to a specific user or company," the statement read. "We take all possible measures to protect this data from being compromised, for example through strong encryption."

But Kaspersky's measures sometimes appear to fall short. In 2014, Twitter user @cryptoOCDrob posted a screenshot of Kaspersky software leaking unencrypted data while checking website reputation. Two years later, another Twitter user, Christopher Lawson, claimed that his email address, license key and other details were being sent by Kaspersky without encryption.

Testing performed by The Intercept last month on a trial copy of "Kaspersky Small Business Security 4" determined that, while some traffic was indeed encrypted, a detailed report of the host's hardware configuration and installed software was relayed back to Kaspersky entirely unencrypted. By the time of publication, Kaspersky told The Intercept via email, it was unable to reproduce these results.



## Email surveillance

Another way the NSA targets foreign anti-virus companies appears to be to monitor their email traffic for reports of new vulnerabilities and malware. A 2010 presentation on "Project CAMBERDADA" shows the content of an email flagging a malware file, which was sent to various anti-virus companies by François Picard of the Montréal-based consulting and web hosting company NewRoma. The presentation of the email suggests that the NSA is reading such messages to discover new flaws in anti-virus software.

Picard, contacted by The Intercept, was unaware his email had fallen into the hands of the NSA. He said that he regularly sends out notification of new viruses and

malware to anti-virus companies, and that he likely sent the email in question to at least two dozen such outfits. He also said he never sends such notifications to government agencies. "It is strange the NSA would show an email like mine in a presentation," he added.

The NSA presentation goes on to state that its signals intelligence yields about 10 new "potentially malicious files per day for malware triage." This is a tiny fraction of the hostile software that is processed. Kaspersky says it detects 325,000 new malicious files every day, and an internal GCHQ document indicates that its own system "collect[s] around 100,000,000 malware events per day."

After obtaining the files, the NSA analysts "[c]heck Kaspersky AV to see if they continue to let any of these virus files through their Anti-Virus product." The NSA's Tailored Access Operations unit "can repurpose the malware," presumably before the anti-virus software has been updated to defend against the threat.

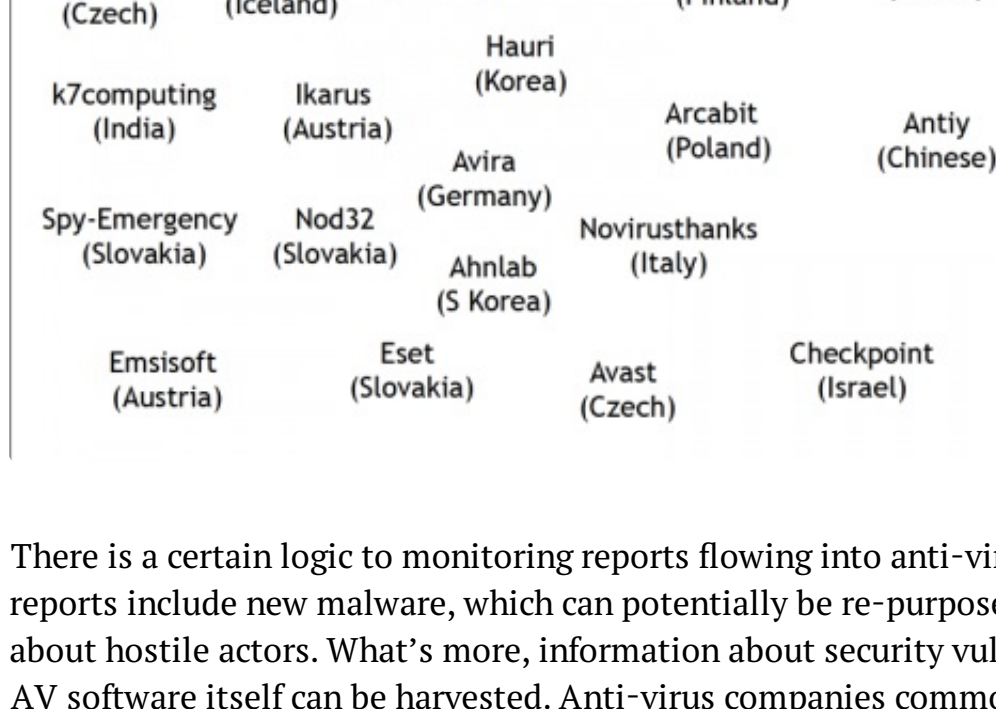
## What else can we do?

- TAO can repurpose the malware
- Check Kaspersky AV to see if they continue to let any of these virus files through their Anti-Virus product



The Project CAMBERDADA presentation lists 23 additional AV companies from all over the world under "More Targets!" Those companies include Check Point software, a pioneering maker of corporate firewalls based Israel, whose government is a U.S. ally. Notably omitted are the American anti-virus brands McAfee and Symantec and the British company Sophos.

## More Targets!



There is a certain logic to monitoring reports flowing into anti-virus companies. Such reports include new malware, which can potentially be re-purposed, and intelligence about hostile actors. What's more, information about security vulnerabilities in the AV software itself can be harvested. Anti-virus companies commonly, though not always, respond slowly to such reports, leaving a window in which spy agencies can potentially exploit these flaws. A 2012 report from Google security engineer Tavis Ormandy documented how, after alerting Sophos to multiple security vulnerabilities in its anti-virus software, the firm estimated it would require six months to patch all of the bugs. That estimate was later revised down 60 days for the entire set of fixes, according to Ormandy.

It's not clear exactly how many reports like Ormandy's have been piling up at anti-virus companies. But Koret, the security researcher, suggests that most AV companies have serious problems in this area. "During a period of ~1 year I researched more or less 17 AV engines," he wrote in an email. "I found vulnerabilities in 14 AV engines."

## Anti-virus firms vs. intelligence agencies

As government spies have sought to evade anti-virus software, the anti-virus firms themselves have exposed malware created by government spies. Among them, Kaspersky appears to be the sharpest thorn in the side of government hackers. In the past few years, the company has proven to be a prolific hunter of state-sponsored malware, playing a role in the discovery and/or analysis of various pieces of malware reportedly linked to government hackers, including the superviruses Flame, which Kaspersky flagged in 2012; Gauss, also detected in 2012; Stuxnet, discovered by another company in 2010; and Regin, revealed by Symantec. In February, the Russian firm announced its biggest find yet: the "Equation Group," an organization that has deployed espionage tools widely believed to have been created by the NSA and hidden on hard drives from leading brands, according to Kaspersky. In a report, the company called it "the most advanced threat actor we have seen" and "probably one of the most sophisticated cyber attack groups in the world."

Hacks deployed by the Equation Group operated undetected for as long as 14 to 19 years, burrowing into the hard drive firmware of sensitive computer systems around the world, according to Kaspersky. Governments, militaries, technology companies, nuclear research centers, media outlets and financial institutions in 30 countries were among those reportedly infected. Kaspersky estimates that the Equation Group could have implants in tens of thousands of computers, but documents published last year by The Intercept suggest the NSA was scaling up their implant capabilities to potentially infect millions of computers with malware.

Kaspersky's adversarial relationship with Western intelligence services is sometimes framed in more sinister terms; the firm has been accused of working too closely with the Russian intelligence service FSB. That accusation is partly due to the company's apparent success in uncovering NSA malware, and partly due to the fact that its founder, Eugene Kaspersky, was educated by a KGB-backed school in the 1980s before working for the Russian military.

Kaspersky has repeatedly denied the insinuations and accusations. In a recent blog post, responding to a Bloomberg article, he complained that his company was being subjected to "sensationalist ... conspiracy theories," sarcastically noting that "for some reason they forgot our reports" on an array of malware that trace back to Russian developers.

He continued, "It's very hard for a company with Russian roots to become successful in the U.S., European and other markets. Nobody trusts us — by default."

Kaspersky Lab openly cooperates with multiple international law enforcement agencies on cybercrime cases, but no inappropriate links to the FSB have ever been proven. Meanwhile, cozy relationships with intelligence agencies are not uncommon among Western technology companies. The CIA-backed venture capital firm In-Q-Tel has helped build over 200 tech start-ups, including cybersecurity firms FireEye and ReversingLabs and big data intelligence firms Palantir and Recorded Future. Previous reporting from the Snowden archive has shown that Microsoft, Google, Yahoo, Facebook, Apple, AOL and PalTalk all actively participated in the NSA's PRISM surveillance program.

No stranger to targeted cyberattacks, Kaspersky Lab announced earlier this month that it had been the victim of a sophisticated intrusion. In an email, Kaspersky Lab told The Intercept, "It is extremely worrying that government organizations would be targeting us instead of focusing resources against legitimate adversaries, and working to subvert security software that is designed to keep us all safe. However, this doesn't come as a surprise. We have worked hard to protect our end users from all types of adversaries. This includes both common cyber-criminals or nation state-sponsored cyber-espionage operations."

When asked for comment, the NSA and GCHQ declined to respond on the record to the specifics of this story.

Documents published with this article:

- Kaspersky User-Agent Strings — NSA
- Project CAMBERDADA — NSA
- NDIST — GCHQ's Developing Cyber Defence Mission
- GCHQ Application for Renewal of Warrant GPW/1160
- Software Reverse Engineering — GCHQ
- Reverse Engineering — GCHQ Wiki
- Malware Analysis & Reverse Engineering — ACNO Skill Levels — GCHQ

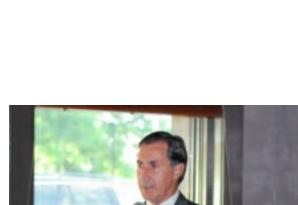


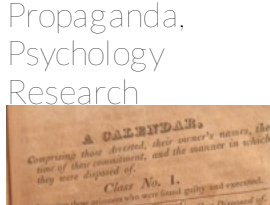
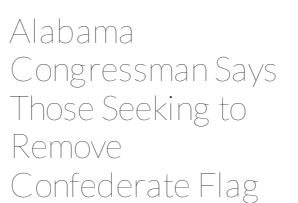

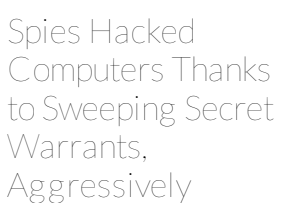

Photo: Shutterstock

✉ Email the authors: [fishman@theintercept.com](mailto:fishman@theintercept.com), [morgan@firstlook.org](mailto:morgan@firstlook.org)

36 DISCUSSING

+ ADD COMMENT      SHOW COMMENTS

## RECOMMENDED

 <p>Five More Things South Carolina Can Do After Taking Down the Confederate Flag</p>	 <p>Google Accused of "Abusive" Conduct in Privacy App Case</p>	 <p>Popular Security Software Came Under Relentless NSA and GCHQ Attacks</p>	 <p>Controversial GCHQ Unit Engaged in Domestic Law Propaganda, Online Psychology Research</p>
 <p>Alabama Congressman Says Those Seeking to Remove Confederate Flag Are "Beyond Contempt"</p>	 <p>Revealed: How DOJ Gagged Google over Surveillance of WikiLeaks Volunteer</p>	 <p>Spies Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law</p>	 <p>When South Carolina Massacred Members of the Emanuel AME Church</p>