KASPERSKY AND THE THIRD MAJOR BREACH OF NSA'S HACKING TOOLS

The WSJ has a huge scoop that many are taking to explain why the US has banned Kaspersky software.

Some NSA contractor took some files home in (the story says) 2015 and put them on his home computer, where he was running Kaspersky AV. That led Kaspersky to discover the files. That somehow (the story doesn't say) led hackers working for the Russian state to identify and steal the documents.

> Hackers working for the Russian government stole details of how the U.S. penetrates foreign computer networks and defends against cyberattacks after a National Security Agency contractor removed the highly classified material and put it on his home computer, according to multiple people with knowledge of the matter.
>
> The hackers appear to have targeted the contractor after identifying the files through the contractor's use of a popular antivirus software made by Russia-based Kaspersky Lab, these people said.
>
> The theft, which hasn't been disclosed, is considered by experts to be one of the most significant security breaches in recent years. It offers a rare glimpse into how the intelligence community thinks Russian intelligence exploits a widely available commercial software product to spy on the U.S.
>
> The incident occurred in 2015 but wasn't discovered until spring of last year,

> said the people familiar with the matter.
>
> The stolen material included details about how the NSA penetrates foreign computer networks, the computer code it uses for such spying and how it defends networks inside the U.S., these people said.
>
> Having such information could give the Russian government information on how to protect its own networks, making it more difficult for the NSA to conduct its work. It also could give the Russians methods to infiltrate the networks of the U.S. and other nations, these people said.

Way down in the story, however, is this disclosure: US investigators believe Kaspersky's AV identified the files, but isn't sure whether Kaspersky told the Russian government.

> U.S. investigators believe the contractor's use of the software alerted Russian hackers to the presence of files that may have been taken from the NSA, according to people with knowledge of the investigation. Experts said the software, in searching for malicious code, may have found samples of it in the data the contractor removed from the NSA.
>
> But how the antivirus system made that determination is unclear, such as whether Kaspersky technicians programed the software to look for specific parameters that indicated NSA material. Also unclear is whether Kaspersky employees alerted the Russian government to the finding.

Given the timing, it's worth considering several other details about the dispute between the US and Kaspersky. (This was all written for another

post that I'll return to.)

The roots of Kaspersky's troubles in 2015

Amid the reporting on Eugene Kaspersky's potential visit to testify to Congress, Reuters reported the visit would be Kaspersky's first visit to the US since spring 2015.

> Kaspersky told NBC News in July that he was not currently traveling to the United States because he was "worried about some unexpected problems" if he did, citing the "ruined relationship" between Moscow and Washington.
>
> Kaspersky Lab did not immediately respond when asked when its chief executive was last in the United States. A source familiar with U.S. inquiries into the company said he had not been to the United States since spring of 2015.

A link in that Reuters piece suggests Kaspersky's concern dates back to August 2015 Reuters reporting, based off leaked emails and interviews with former Kaspersky employees, that suggests the anti-virus firm used fake files to trick its competitors into blocking legitimate files, all in an effort to expose their theft of Kaspersky's work. A more recent reporting strand, again based on leaked emails, dates to the same 2009 time period and accuses Kaspersky of working with FSB (which in Russia, handles both spying and cybersecurity — though ostensibly again, that's how the FBI works here).

But two events precede that reporting. In June 2015, Kaspersky revealed that it (and a bunch of locales where negotiations over the Iran deal took place) had been infected by Duqu 2.0, a thread related to StuxNet.

> Kaspersky says the attackers became entrenched in its networks some time last year. For what purpose? To siphon intelligence about nation-state attacks the company is investigating—a case of the watchers watching the watchers who are watching them. They also wanted to learn how Kaspersky's detection software works so they could devise ways to avoid getting caught. Too late, however: Kaspersky found them recently while testing a new product designed to uncover exactly the kind of attack the intruders had launched.
>
> [snip]
>
> Kaspersky is still trying to determine how much data the attackers stole. The thieves, as with the previous Duqu 2011 attack, embedded the purloined data inside blank image files to slip it out, which Raiu says "makes it difficult to estimate the volume of information that was actually transferred." But at least, he says, it doesn't appear that the attackers were out to infect Kaspersky customers through its networks or products. Kaspersky claims to have more than 400 million users worldwide.

Which brings us to what the presumed NSA hackers were looking for:

> The attackers were primarily interested in Kaspersky's work on APT nation-state attacks—especially with the Equation Group and Regin campaigns. Regin was a sophisticated spy tool Kaspersky found in the wild last year that was used to hack the Belgian telecom Belgacom and the European Commission. It's believed to have been developed by the UK's intelligence agency GCHQ.
>
> The Equation Group is the name Kaspersky gave an attack team behind a suite of

> different surveillance tools it exposed earlier this year. These tools are believed to be the same ones disclosed in the so-called NSA ANT catalogue published in 2013 by journalists in Germany. The interest in attacks attributed to the NSA and GCHQ is not surprising if indeed the nation behind Duqu 2.0 is Israel.

Kaspersky released its Equation Group whitepaper in February 2015. It released its Regin whitepaper in November 2014.

One thing that I found particularly interesting in the Equation Group whitepaper — in re-reading it after ShadowBrokers released a bunch of Equation Group tools — is that the report offers very little explanation of how Kaspersky was able to find so many samples of the NSA malware that the report makes clear is almost impossible to find. The only explanation is this CD attack.

> One such incident involved targeting participants at a scientific conference in Houston. Upon returning home, some of the participants received by mail a copy of the conference proceedings, together with a slideshow including various conference materials. The compromised CD-ROM used "autorun.inf" to execute an installer that began by attempting to escalate privileges using two known EQUATION group exploits. Next, it attempted to run the group's DOUBLEFANTASY implant and install it onto the victim's machine. The exact method by which these CDs were interdicted is unknown. We do not believe the conference organizers did this on purpose. At the same time, the super-rare DOUBLEFANTASY malware, together with its installer with two zero-day exploits, don't end up on a CD by accident.

But none of the rest of the report explains how Kaspersky could have learned so much about NSA's tools.

We now may have our answer: initial discovery of NSA tools led to further discovery using its AV tools to do precisely what they're supposed to. If some NSA contractor delivered all that up to Kaspersky, it would explain the breadth of Kaspersky's knowledge.

It would also explain why NSA would counter-hack Kaspersky using Duqu 2.0, which led to Kaspersky learning more about NSA's tools.

So to sum up, Eugene Kaspersky's reluctance to visit the US dates back to a period when 1) Kaspersky's researchers released detailed analysis of some of NSA and GCHQ's key tools, which seems to have led to 2) an NSA hack of Kaspersky, which in turn shortly preceded 3) some reporting based off unexplained emails floating accusations of unfair competition dating back to 2009 and earlier.

We now know all that came after Kaspersky *found* at least some of these tools sitting on some NSA contractor's home laptop.

This still doesn't explain how Russian hackers figured out precisely where Kaspersky was getting this information from — which is a real question, but not one the WSJ piece answers.

But reading those reports again, especially the Equation Group one, should make it clear how the Russian government could have discovered that Kaspersky had discovered these tools.