# KASPERSKY'S CARROT-AND-STICK TAO COMPROMISE INCIDENT REPORT

Last week, Kaspersky released its investigation into the reported collection of NSA hacking tools off an employee's computer. Kim Zetter did an excellent story on it, so read that for analysis of what the report said.

The short version, though, is that Kaspersky identified a computer in the Baltimore, MD area that was sending a whole slew of alerts in response to a silent signature for Equation Group software from September to November 2014 — a year earlier than the leaked reports about the incident claimed the compromise had happened. Kaspersky pulled in an archive including those signatures as well as some associated files in the normal course of collecting analysis (and, according to Zetter, did not pull other archives of malware also associated with the machine). Kaspersky IDed it as irregular, and — so they're claiming — the analyst who found it told Eugene Kaspersky (referred to throughout in the third person "CEO" here), who told told the analyst to destroy the source code and related documents immediately. The report claims Kaspersky subsequently instituted a policy mandating such destruction going forward.

As Zetter notes, the timing of events gets awfully murky about when the file got destroyed and the new destruction policy was instituted.

> The company didn't respond to questions about when precisely it instituted this policy, nor did it provide a written copy of the distributed policy before publication of this article.

Meanwhile, during the same period this machine was sending out all the Equation Group alerts,

someone hacked it.

> It appears the system was actually compromised by a malicious actor on October 4, 2014 at 23:38 local time,

The report explains this compromise at length, providing (in addition to the precise time), the C&C server URL, a list of 121 other virus signatures found on the machine during the period the Equation Group signatures were alerting. It also links to Kaspersky's analysis of the backdoor in question, which was developed by Russian criminal hackers.

> "It looks like a huge disaster the way it happened with running all this malware on his machine. It's almost unbelievable," [Zetter quotes Kaspersky's director of the company's Global Research and Analysis Team Costin Raiu].

Thus far, consider what this report does: it makes it clear that Kaspersky has far more detail about the compromise than the anonymous sources leaking to the press are willing to share (all the time with Eugene Kaspersky inviting them to provide more details). It elaborates on the story it had already shared about who the likely culprit was to have stolen and used the files. And it suggests (though I'm not sure I believe it), that it's entirely the fault of the hacker who turned off Kaspersky's AV in order to run a pirated copy of Windows Office.

That's the carrot. Here, Kaspersky is saying, we've figured out who stole those files your idiot developer loaded onto his malware-riddled computer. Go get them. Free incident response, three years after the fact!

But it's the stick I'm just as interested in.

First, as part of its explanation of the process Kaspersky used to hone in on the incident, the

report includes a list of hits and false positives on NSA signatures just from September 2014 — effectively providing a list of (dated) malware signatures. While the report notes many of these alerts are false positives, Kaspersky is nevertheless saying, here's a list of all the victims of your spying we identified for just one month out of the 40 months we just analyzed. Presumably, the hits after September 2014 would have come to include far more true victims.

Then, the report provides a list of all the Equation Group signatures found on the TAO engineers' computer, providing a snapshot of what one person might work on, a snapshot that would provide useful for those trying to understand NSA's work patterns.

Even while it provides lists of signatures that will provide others some insight into NSA activity, the report makes a grand show of concern for privacy, redacting the name of the archive as [undisclosed] and including a discussion about how it could have — but chose not to — include the complete file paths of the archive.

> Looking at this metadata during current investigation we were tempted to include the full list of detected files and file paths into current report, however, according to our ethical standards, as well as internal policies, we cannot violate our users' privacy. This was a hard decision, but should we make an exception once, even for the sake of protecting our own company's reputation, that would be a step on the route of giving up privacy and freedom of all people who rely on our products. Unless we receive a legitimate request originating from the owner of that system or a higher legal authority, we cannot release such information.

Mind you, FSB is the "higher legal authority" in Russia for such things.

Then, in the guise of claiming how little information Kaspersky has on the individual behind all this, the report makes it clear it retains his IP, from which they could reconstitute his identity.

> **Q3** – Who was this person?
>
> **A3** – Because our software anonymizes certain aspects of users' information, we are unable to pinpoint specifically who the user was. Even if we could, disclosing such information is against our policies and ethical standards. What we can determine is that the user was originating from an IP address that is supposedly assigned to a Verizon FiOS address pool for the Baltimore, MD and surrounding area.

In short, along with providing a detailed description of what likely happened – the hacker got pwned by someone else – Kaspersky lays out all the information on NSA's hacking activities that it could, if it so chose, make public: who NSA hacked when, who the developer in question is, and more details on how the NSA develops its tools.

But (in the interest of privacy, you understand?) Kaspersky's not going to do that unless some higher authority forces it to.

Of course, Kaspersky's collection of all that data on NSA's hacking is undoubtedly one of the reasons the NSA would prefer it not exist.

A carrot, and a stick.

At the end of her piece, Zetter quotes Rob Joyce laying out the more modest attack on Kaspersky (this stuff shouldn't be run on sensitive government computers, which it shouldn't), even while admitting that other AV products have the same privileged access to collect such information on users.

> Asked about Kaspersky's discovery of multiple malware samples on the NSA

> worker's home computer, Rob Joyce, the Trump administration's top cybersecurity adviser who was head of the NSA's elite hacking division when the TAO worker took the NSA files home and put them on his work computer, declined to respond to Kaspersky's findings but reiterated the government's contention that Kaspersky software should be banned from government computers.
>
> "Kaspersky as an entity is a rootkit you run on a computer," he told Motherboard, using the technical term for stealth and persistent malware that has privileged access to all files on a machine.
>
> He acknowledged that software made by other antivirus companies has the same potential for misuse Kaspersky has but said, Kaspersky is "a Russian company subjected to FSB control and law, and the US government is not comfortable accepting that risk on our networks."

We shall see if this report serves to halt all the (inaccurate at least with respect to timing, if this report is to be believed) leaks to the press or even the other attacks on Kaspersky.

All that said, there are two parts of this story that still don't make sense.

First, I share Zetter's apparent skepticism about the timing of the decision to destroy the source code, which the report describes this way:

> Upon further inquiring about this event and missing files, **it was later discovered that at the direction of the CEO, the archive file, named "[undisclosed].7z" was removed from storage**. Based on description from the analyst working on that archive, it contained a collection of executable modules, four documents bearing classification markings, and other files

> related to the same project. The reason we deleted those files and will delete similar ones in the future is two-fold; We don't need anything other than malware binaries to improve protection of our customers and secondly, because of concerns regarding the handling of potential classified materials. Assuming that the markings were real, such information cannot and will not **[note this typo]** consumed even to produce detection signatures based on descriptions.
>
> This concern was later translated into a policy for all malware analysts which are required to delete any potential classified materials that have been accidentally collected during anti-malware research or received from a third party. Again to restate: to the best of our knowledge, **it appears** the archive files and documents were removed from our storage, and only individual executable files (malware) that were already detected by our signatures were left in storage.

The key sentence — "it was later discovered … the archive file … was removed" — is a master use of the passive voice. And unlike all the other things for which the report offers affirmative data, the data offered here is the absence of data. "It appears" that the archive is no longer in storage, without any details about when it got removed. The report is also silent about whether any of these events — the removal and claimed destruction and the institution of a new policy to destroy such things going forward — were a response to the Duqu 2 hack discovering such files, as well as the one silent signature integrating the word "secret" described elsewhere in the report, on Kaspersky's servers.

Then there's the implausibility of an NSA developer 1) running Kaspersky then 2) turning

it off 3) to load a bunch of malware onto his computer in the guise of loading a pirated copy of Office 4) only to have a bunch of other malware infect the computer in the same window of time, finally 5) turning the Kaspersky back on to discover what happened after the fact.

Really? I mean, maybe this guy is that dumb, or maybe there's another explanation for these forensic details.

In any case, the entire report is a cheeky chess move. I eagerly wait to see if the US' anonymous leakers respond.