SHORTER KASPERSKY: OUR HOME AV FOUND NSA'S LOST TOOLS SIX MONTHS BEFORE NSA DID

Kaspersky has what it calls a preliminary investigation into the allegations that it obtained NSA tools by taking them from an NSA hacker who loaded them onto his home computer. It follows by just a few days and directly refutes the silly accusations made by Rick Ledgett the other day in Lawfare, most notably that Kaspersky found the tools by searching on "TS/SCI," much less the "proprietary" Ledgett claimed. I assume the word "preliminary" here means, "Okay, you've made your public accusation, now Imma badly discredit you, but I'm holding other details back for your next accusation."

Instead of finding the hacking tools in early 2015, Kaspersky says, they found the GrayFish tool back on September 11, 2014, probably six months before the anonymous government sources have been saying it was discovered.

And they found it with their home AV.

> - *The incident where the new Equation samples were detected used our line of products for home users, with KSN enabled and automatic sample submission of new and unknown malware turned on.*
> - *The first detection of Equation malware in*

> *this incident was on September 11 2014. The following sample was detected:*
>
> - *44006165AABF2C39063A419BC73D790D*
> - *mpdkg32.dll*
> - *Verdict: HEUR:Trojan.Win32.GrayFish.gen*

After that, what Kaspersky describes as "the user" disabled the AV and downloaded a pirated Microsoft copy onto his computer, which created a backdoor that could have been used by anyone.

> - *After being infected with the* ***Backdoor.Win32.Mokes.hvl*** *malware, the user scanned the computer multiple times which resulted in detections of new and unknown variants of Equation APT malware.*

Once that backdoor was loaded, "the user" scanned the computer and found other Equation Group tools.

What Kaspersky is *not* saying is that this probably wasn't the TAO hacker, but probably was someone pretending to be the user (perhaps using NSA's own tools?!), who stole a slew of files then.

Two other points: Kaspersky claims to have called the cops — or probably the FBI, which would have been the appropriate authority, and

he claims to call the cops whenever they find malware in the US.

> - *Some of these infections have been observed in the USA.*
> - *As a routine procedure, Kaspersky Lab has been informing the relevant U.S. Government institutions about active APT infections in the USA.*

It's possible that Kaspersky did inform the FBI, and that FBI routinely gets such notice, but that FBI routinely ignores such notice because they don't care if NSA is hacking people in the US (which given what we know, is at least sometimes, and would have been during this period, Americans approved for 705(b) surveillance that doesn't get turned off as is legally required when they return to the US).

In other words, it's possible that FBI learned about this, but ignored it because they ignore NSA's illegal hacking the US. Only this time it wasn't NSA's illegal hacking, but NSA's incompetence, which in turn led an NSA hacker to get hacked by … someone else.

Finally, there's this bit, which is the least credible thing in this announcement. The Kaspersky statement says Eugene himself was informed of the discovery, and ordered the tool (in a kind of one-man Vulnerabilities Equities Process) to be destroyed.

> - *After discovering the suspected Equation malware source code, the analyst reported*

> *the incident to the CEO. Following a request from the CEO, the archive was deleted from all our systems. The archive was not shared with any third parties.*

I don't so much doubt *that* Eugene ordered the malware to be destroyed. Once Kaspersky finished its analysis of the tool, they would have no use for it, and it would add to risk for Kaspersky itself. I just find it remarkable that he would have made the personal decision to destroy this malware at some point after its discovery, but not have raised it until now.

Unless, of course, he was just waiting for someone like Rick Ledgett to go on the sort of record.

Though note how Kaspersky gets conspicuously silent about the timing of that part of the story.

One final point: this new timeline doesn't explain how Israel (possibly with the involvement of the US) would have found this tool by hacking Kaspersky (unless the decision to destroy the tool came after Kaspersky discovered the hack). But it does suggest the Duqu chicken was chasing the TAO hacker egg, and not vice versa as anonymous sources *have* been claiming.

That is, the scenario laid out by this timeline (which of course, with the notable exceptions of the Duqu hack and the destruction date for GrayFish, comes with dates and file names and so at least looks more credible than Rick Ledgett's farcical "proprietary" claims) is that Kaspersky found the file, reported it as an infection to the cops, which likely told NSA about it, leading to the attack on Kaspersky to go try to

retrieve it or discover how much else they obtained. That is, Duqu didn’t hack Kaspersky and then find the file. They hacked Kaspersky to find the file that some dopey TAO hacker had made available by running Kaspersky home AV on his computer.

Update: Changed “probable” involvement of US in Duqu hack to “possible.”

Update: Changed “stolen” in title to “lost.”