RUSSIA'S SNAKES GOT DEPLANED

The US Attorney's Office in Brooklyn, EDNY, had a busy day on Tuesday. In addition to indicting George Santos for various kinds of fraud, EDNY's US Attorney, Breon Peace, got to take credit for the "remediation" of a peer-to-peer network of compromised computers exploited by Russian hacking group "Turla" to hack collection targets around the world.

For geeks, the claimed effect of the operation was pretty cool. The FBI developed code (or had a contractor do it for them) that would exploit the very thing that makes the Snake malware so tricky — the proprietary communications sessions it uses to run a global network of relay nodes through which it launches collection attacks.

> The majority of compromised systems serve as relay nodes (referred to as "hop points") in the Snake network, that route traffic from the FSB's ultimate target systems (referred to as "endpoints") through the network back to Turla operators in Russia.

The FBI code was designed to command Snake to overwrite its operational components.

> [A]n FBI-created tool named PERSEUS [] issued commands that caused the Snake malware to overwrite its own vital components.
>
> [snip]
>
> [T]hrough analysis of the Snake malware and the Snake network, the FBI developed the capability to decrypt and decode Snake communications. With information gleaned from monitoring the Snake network and analyzing Snake malware, the FBI developed a tool named PERSEUS which establishes communication sessions with

> the Snake malware implant on a particular computer, and issues commands that causes the Snake implant to disable itself without affecting the host computer or legitimate applications on the computer.
>
> [snip]
>
> Specifically, the FBI has developed a technique that exploits some of Snake's built-in commands, discussed above, which, when transmitted by PERSEUS from an FBI-controlled computer to the Snake malware on the Subject Computers, will terminate the Snake application and, in addition, permanently disable the Snake malware by overwriting vital components of the Snake implant without affecting any legitimate applications or files on the Subject Computers..

We'll see whether the operation was as successful as DOJ and NSA claimed. But the government at least claims to have significantly neutralized a hacking platform that has been a complex challenge for two decades.

A quote from a specialist on this hacking group made me want to look closer to understand what DOJ did, both technically and legally. Juan Andres Guerrero-Saade complained to CNN that the FBI had taken down the peer-to-peer network, rather than just sat on it to continue to observe what Russia's FSB was doing.

> Turla operatives are "genuine professionals," Juan Andres Guerrero-Saade, a researcher who has tracked Turla for years, told CNN.
>
> "They're not traipsing around breaking things or calling attention to themselves in stupid ways," said Guerrero-Saade, who is senior director of SentinelLabs, the research arm of security firm SentinelOne. He said that's what you'd "expect from the GRU,"

> referring to Russia's military intelligence agency, whose hackers are generally more conspicuous. "You don't see that out of Turla."
>
> [snip]
>
> While the FBI touted the action as another example of the bureau's strategy to protect hacking victims, Guerrero-Saade wondered what visibility the FBI might have lost into Turla's operations by exposing the network of hacked computers.
>
> "The FBI has a hammer and they've decided this is just another nail," Guerrero-Saade said. "And I don't think espionage operations should be handled the same way that criminal operations are."

But the search warrant affidavit suggests that's what the FBI has been doing since 2016.

The materials released by the government provide a very selective narrative both of the hacking group and the intervention:

> May 4, 2023: Search warrant affidavit
>
> May 8, 2023: Planned operation
>
> May 9, 2023: DOJ Press release; NSA press release; Joint Cybersecurity Advisory

The narrative starts in 2004, when investigators first started tracking Turla, ignores a 2008 Turla compromise of DOD computers, only names one collection target (a journalist) that might be in the US, and only describes likely German and French collection targets in passing.

As the affidavit describes, the FBI's understanding of Turla derived from both "sensitive sources" and the monitoring of victims.

> [T]hrough existing legal authorities, the cooperation of several U.S. victims[,] and sensitive sources, the FBI and U.S. Intelligence Community have obtained significant insight into the FSB's cyberespionage activities against the United States and its allies using Snake.

A key part of the affidavit's narrative describes that monitoring process. The FBI discovered that Turla compromised computers at US Victim A in San Jose, which let the FBI monitor how the malware worked. Using US Victim A, Turla compromised US Victim B in Syracuse, which in turn let the FBI monitor what happened from there. Using both US Victims A and B, Turla compromised US Victim D in Columbia, SC, which in turn let the FBI monitor traffic. Using Victim B, Turla compromised US Victim C, in Boardman, OR, which in turn let the FBI monitor traffic.

Over seven years, then, the FBI has been monitoring communications traffic from a growing number of US victim companies that Turla used as nodes. The affidavit emphasizes that these sites were used to attack *overseas* targets — like the presumed German and French targets mentioned in the affidavit. Aside from the journalist working for a US outlet (who could be stationed overseas), the affidavit doesn't mention any US collection targets. Nor does it explain whence Turla targets US collection targets.

2004: Investigation begins

2008: Turla compromises US military computer via thumb drive (not mentioned in affidavit)

2015 to 2017: FBI monitored communication between US-compromised computer and Minister of Foreign Affairs in NATO member-state, collected and decrypted

> Turla operators used Snake in an attempt

> to exfiltrate a large volume of what they believed to be internal United Nations and NATO documents sent from the NATO Victim-1

By description — particularly the reference to what hackers *thought* they were getting — this is likely Germany, as described in this report on the group.

> It was Tuesday, Dec. 19, 2017, when German security officials received the tipoff. A foreign intelligence service informed the Bundesnachrichtendienst (BND), Germany's foreign intelligence service, that somebody had hacked into the IT system belonging to Germany's Foreign Ministry.
>
> [snip]
>
> And the hackers hadn't actually stolen all that much by the beginning of 2018 — a total of six documents, only one of which was classified. Nevertheless, the BSI decided to throw the hackers out of the network. A short time later, public prosecutors launched an official investigation into the cyberintrusion.

2016: After finding IP address in Queue File on computers belonging to US Victim A in San Jose, CA, victim permitted FBI to do custom scan and monitor communication traffic to ID other hop points and victims

2017: FBI provides victim notification of earlier version of Snake on US Victim E computers in Van Nuys, CA

2017 to 2020: FBI monitored communications between US-compromised computer and NATO Victim-2 (possibly France)

2018: EDNY grand jury seated

2018: FBI observed communications between US Victim A and computers in Syracuse, NY, owned by

US Victim B and performed custom scan and monitored traffic

2018 to 2022: FBI identified traffic between US Victims A and B and computers in Columbia, SC owned by US Victim D; FBI performed a scan and monitored traffic

January 2020: FBI identified communication between US Victim B and cloud provider US Victim C in Boardman, OR; FBI performed custom scan and monitored ongoing traffic

2020 to 2021: FBI identified traffic between US Victim A and computer located in Hicksville, NY owned by US Victim F

2021 to 2022: FBI observes traffic between US Victims D and US Victim E; FBI provided custom scan but Victim E did not permit ongoing monitoring

2022: By the time FBI alerts US Victim E, it had ceased operation and discarded the computers

February to March 2022: FBI identified communication between US Victim A and computers in Gaithersburg, MD owned by US Victim G, which refused to cooperate with the FBI

nd: Turla used Snake to target journalist for US news media company (country location not stated)

As this timeline lays out, in the last two years, Turla exploited three US victim companies — US Victim E and G, both of which refused full cooperation, as well as the defunct one, US Victim F, in Hicksville, NY, that might be how EDNY would claim to establish venue if you ignore that that hack happened after the grand jury that conducted this investigation was seated in 2018 — from which the FBI was unable to get the kind of voluntary cooperation that US Victims A, B, C, and D offered. At first I mistakenly thought that FBI might have acted now because they were finding less success with the monitoring approach they've used since 2016.

But those computers are a different set (though possibly overlapping) than the set of computers targeted by this warrant. While Subject Computers 2 and 3 listed in the affidavit, both located in Columbia, SC, could be owned by US Victim D, US Victims E and G are not targeted. The additional targeted computers are located in Portland (Subject Computers 1 and 2), Atlanta (Subject Computer 4), Windsor, CT (Subject Computer 5), and Rancho Cordova, CA (Subject Computers 6, 7, and 8). If Subject Computers 2 and 3 do belong to US Victim D, including them might serve primarily to qualify this for remote search under 41(b)(6)(B) (which requires 5 districts).

For US purposes, the more important part of the operation may be parallel efforts done overseas. The affidavit suggests that the FBI will only execute the search within the US and foreign governments will only execute the search within their jurisdictions.

> On or about May 8, 2023, the FBI, in coordination with certain foreign governments acting outside of the United States, intends to execute a technical operation, codenamed MEDUSA, to disable Snake malware on numerous computers worldwide. Specifically, at a chosen time, FBI personnel will use PERSEUS to authenticate and establish sessions with the Snake malware on the Subject Computers, and send to the Snake implants on the Subject Computers built-in commands that will terminate the Snake application and, in addition, permanently disable the Snake malware by overwriting vital components of the Snake implant without affecting any legitimate applications or files on the Subject Computers. At the same time that the FBI executes the remote search technique described in this Affidavit to disable the Snake malware on computers located in the United States, certain foreign government authorities will take

> action to remediate Snake-compromised computers within their territories.

The press release is a bit more vague about that (and there are probably nodes in countries that the US IC would not trust enough to coordinate such an operation).

> For victims outside the United States, the FBI is engaging with local authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance.
>
> [snip]
>
> The FBI and U.S. Department of State are also providing additional information to local authorities in countries where computers that have been targeted by the Snake malware have been located.

As the affidavit described it, the FBI used a Rule 41(b)(6)(B) warrant permitting the government to search remotely in more than one District at a time so as to allow for the simultaneous worldwide operation.

> The FBI believes that use of the remote search technique described in this Affidavit is necessary to ensure the success of the coordinated technical operation to disrupt the Snake malware network worldwide. As detailed above, the Subject Computers are located in geographically disparate locations throughout the United States. There are not sufficient FBI personnel available who possess the specialized training and experience with the sophisticated Snake malware to physically travel to each location to disable the Snake malware on each of the Subject Computers simultaneously. Thus, without authorization to use the remote search technique requested in this Affidavit,

> the FBI would not be able to timely disable the Snake malware on the Subject Computers as part of a coordinated operation against the worldwide Snake network.

Whatever the case, the press release speaks in fairly expansive terms about neutralizing the entire network, not just some nodes in it.

To cycle back to Guerrero-Saade's complaint, then, it seems that FBI has been monitoring this network for years. Indeed, one wonders how much of the roll-up of Russian spying in recent years has benefitted from doing so.

But it seems that the US and its partners decided they had the capability and the will to attempt to shut down this network now (at a time, it should be said, when Russia is ratcheting up attacks on Ukraine and in advance of Ukraine's planned counterattack). Perhaps it is just part of the larger response rolled out in the wake of Russia's attack on Ukraine.