The Secret Service Tried to Catch a Hacker With a Malware Booby-Trap

vice.com/en/article/wxqz54/secret-service-network-investigative-technique-ransomware

A Seattle Police Department officer tried to unmask a ransomware attacker by deploying his own hack, according to newly unsealed court records.

Although in this case the officer's attempt didn't work, the news shows that the use of so-called network investigative techniques (NITs)—the U.S. government's general term for hacking tools deployed by law enforcement—is not limited to the FBI. Here, the Seattle Police Department official was working in their capacity as a Task Force Officer for the U.S. Secret Service.

Seamus Hughes, deputy director of the program on extremism at George Washington University, discovered and shared the court docket with Motherboard.

In 2016 the South Correctional Entity (SCORE) Jail in Des Moines, Washington found ransomware on its computer network, according to the warrant application written by Chris Hansen, the Seattle Police Department detective and Secret Service Task Force Officer. Ransomware is a type of malware that generally encrypts files on a target's system and then demands a bounty payment in cryptocurrency to unlock them. In some cases, ransomware attackers will offer to unlock a limited number of victim's files to prove they do have the capability to recover the data.

Hansen spoke to the information technology director for the jail who's listed in the court docket as "A.M.", and reported that a user "was unable to access the user's computer files on a server that the SCORE Jail uses to facilitate remote searches of jail records by law enforcement officers with accounts on the SCORE Jail computer system," the document reads. The ransomware appeared to have infected the system through the account of an Auburn, Washington police officer who had been hacked himself.

> **Do you know anything about law enforcement hacking? Who is using the tools, and who is selling them? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.**

The impact was sizable, and majorly disrupted work for over 12 hours, infected a network share used by every employee in the jail, and the ransomware also "infected a software program used by several law enforcement agencies to create lineup montages, infecting the image files used for creating these lineups and preventing law enforcement officers from accessing the system to look up inmate booking photos and tattoo images," the document reads.

Along with the bevvy of encrypted material on the system sat another, new file.

"hallo, our dear friend! looks like you have some troubles with your security. all your files are now encrypted," the message from the ransomware attackers read, which added they would only keep the keys to decrypt the files for no more than 72 hours.

While Hansen and A.M. were on the phone, the ransomware kept spreading. As A.M. took a RAM image (essentially preserving what was currently in the system's memory) of a computer with a suspicious process running on it, the ransomware then started locking down that system's files too, the document reads. At Hansen's direction, A.M. contacted one of the email addresses provided by the attackers in their original message, lavandos@dr.com, and asked for more information on how to retrieve the files. The ransomware attacker replied, and asked A.M. to send three of the encrypted files, the complaint adds.

Hansen checked the email headers of the reply, and found the attacker's related IP address was a Tor exit node. Tor is an anonymity network that routes a user's traffic through computers spread throughout the world. Because this clearly wasn't an IP address that would help identify who the ransomware attacker really was, Hansen hatched a plan.

Hansen first took a NIT, which in this case was a program that once run on a target's computer would connect back to a Secret Service server and reveal the IP address of the suspect's machine. He then compressed the file, and with the cooperation of the jail, placed the file on the jail's compromised network, deliberately exposing it to the ransomware and encrypting it.

The idea was that the jail would send this booby-trapped file, along with two others, to the attackers to decrypt, the document explains. Once the ransomware author sent back the unencrypted versions, the jail would reply saying that one of them—the one including the NIT—is not working, and ask the attackers to examine the unzipped file and repair it. The jail would also send them another, unencrypted copy of the file in case the attackers didn't retain one.

"If the perpetrator(s), in fact, examine(s) the unzipped file, and in doing so attempt(s) to run the file, the action of pressing the 'run' button will launch the NIT," the complaint reads. Once activated, the NIT would not only tip-off investigators to the target's IP address, but also collect some other basic information like the computer's open communication ports, the type of operating system it was running, its language, timezone, wireless network information, and host and usernames. Armed with that sort of information, investigators may be able to identify where the attackers are located, or eventually who they are.

But this rather convoluted plan didn't play out.

"DEPLOYMENT OF NIT UNSUCCESSFUL; NO EVIDENCE SEIZED," another document reads. The documents don't elaborate why the NIT did not work.

U.S. law enforcement has increasingly turned to NITs, especially in cases that involve the Tor network or other anonymity systems. The FBI has used NITs to unmask people making bomb threats, other financially-driven cybercriminals, and child predators. Whereas some cases are highly targeted in nature, some operations have also been exceptionally broad. Motherboard previously revealed how the FBI hacked over 8,000 computers based in 120 countries based on one warrant.

That was a legally contentious warrant, as many defense lawyers argued that the judge who signed it did not have the authorization to green-light searches outside of her own district. Shortly after in December 2016, long-planned changes to the rules around warrants came into effect, meaning that magistrate judges could authorize hacking operations anywhere in the world.

> "DEPLOYMENT OF NIT UNSUCCESSFUL; NO EVIDENCE SEIZED."

Hansen deployed his NIT a few weeks after those changes, according to the court records.

Ahmed Ghappour, associate professor of law at Boston University, who has studied the legal issues around NITs and in particular their geopolitical ramifications, previously told Motherboard that hacking suspects who use Tor is "like playing Russian Roulette with cross-border cyber operations," primarily because investigators ultimately don't know where the NIT is going to end up, outside the United States or otherwise.

And law enforcement NITs have failed in the past. When trying to unmask Buster Hernandez, a particularly egregious child abuser targeting people on Facebook, the FBI tried, and failed, to unmask him with a NIT. But as Motherboard revealed last month, Facebook's own security team then purchased a much more effective piece of malware and provided it to the FBI, which successfully deployed it against Hernandez.

The Seattle Police Department did not respond to a request for comment. The Department of Homeland Security, of which the Secret Service is a part, also did not respond.

Subscribe to our cybersecurity podcast, CYBER.