New Ransomware Linked to NotPetya Sweeps Russia and Ukraine

wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/

Andy Greenberg October 24, 2017

Just four months ago, a massive ransomware attack known as NotPetya ripped through Ukraine, Russia, and some multinational companies, infecting thousands of networks and eventually causing hundreds of millions of dollars in damages. Now, an apparent aftershock of that attack is reverberating through the region, as a new variant of that code locks up hundreds of machines and handicaps infrastructure.

On Tuesday, the security community began tracking a new outbreak of ransomware tied to NotPetya's authors. Known as BadRabbit, the the strain has infected hundreds of computers —mostly in Russia, but with some victims in Ukraine, Turkey, Bulgaria, and Germany— according to security firms including ESET and Kaspersky. For now, the outbreak remains only a small fraction of the size of the NotPetya epidemic. But it has nonetheless hit several Russian media outlets, including the newswire Interfax, according to the Russian security firm Group-IB, and also infected Ukraine's Odessa airport and Kiev subway system, partially paralyzing their IT systems and disabling the subway system's credit card payments, according to one Ukrainian government official.

"The dangerous aspect is the fact that it was able to infect many institutions which constitute critical infrastructure in such a short timeframe," says Robert Lipovsky, a malware researcher at ESET, "which indicates a well-coordinated attack."

Kaspersky also found strong evidence tying the new attack to the creators of NotPetya. After the June NotPetya outbreak, the company's analysts found that one Ukrainian news site, Bahmut.com.ua, had been hacked to deliver the malware, along with dozens of other sites that were similarly corrupted—but hadn't yet been activated to start infecting victims. Now Kaspersky has found that 30 of those hacked sites began to distribute the BadRabbit malware on Tuesday.

"This indicates that the actors behind ExPetr/NotPetya have been carefully planning the BadRabbit attack since July," writes Costin Raiu, the director of Kaspersky's global research and analysis team, in a note to WIRED.

ESET

While Kaspersky counts just under 200 victims among its users so far, roughly 50 or 60 Ukrainian computers in the Ukrainian government alone have been infected with the ransomware, according to Roman Boyarchuk, head of the Center for Cyber Protection within Ukraine's State Service for Special Communications and Information Protection. Possibly more devices are affected in Ukrainian private-sector networks. Given that ESET estimates that only 12.2 percent of victims are in Ukraine and 65 percent are in Russia, those numbers suggests several hundred infections in Russia.

"A lot of systems have been manually disconnected because of the attack," in part to control the spread of the ransomware, says Boyarchuk. But that disruption still represents only a fraction of the damage Ukraine suffered from the earlier NotPetya malware attack in June—or in several other waves of attacks in the country's three-year, ongoing cyberwar with Russia. "The scope of the territory and coverage is not that serious according to the information we have right now," Boyarchuk adds. "We can’t see any massive distribution."

Further links to NotPetya stand out to malware analysts as well. Kaspersky notes that like NotPetya, the new ransomware spreads by using the Windows Management Instrumentation Command-Line, or WMIC, in combination with credentials it steals using the open-source tool Mimikatz. Like NotPetya, BadRabbit also spreads using Microsoft's Server Message Block (SMB) protocol, ESET says, though it uses credentials hardcoded into its software to spread between computers, rather than the leaked NSA tool known as EternalBlue that NotPetya used. Cisco's Talos research division found Thursday that BadRabbit uses a different leaked NSA hacking tool known as EternalRomance, which also allows infections to spread automatically through a network via SMB.[2]

If BadRabbit and NotPetya were in fact created by the same hackers, their shared origins raise significant questions about the ransomware's motives. After reverse-engineering NotPetya, some researchers found that it wasn't in fact ransomware at all, and offered victims no way to recover their files even if they paid a ransom Instead, it appeared to be thinly disguised, destructive malware launched by state-sponsored (likely Russian) hackers,

and meant only to cause maximum disruption to Ukrainian targets. But given that the majority of BadRabbit's victims are Russian themselves, the new incident may raise doubts about NotPetya's suspect Russian government roots.

BadRabbit demands users pay .05 bitcoins, or about $286, to have their files decrypted. But with its link to NotPetya's fake ransomware, whether that payment actually gets results is so far unclear. Both ESET and Kaspersky's researchers declined to comment for now on the BadRabbit hackers' motives.

Unlike NotPetya, which was mostly delivered to victim networks through tainted updates to the Ukrainian accounting software MeDoc, researchers have so far found only a more run-of-the-mill infection method used to install BadRabbit: ESET and Kaspersky found that hackers had infected Russian and Ukrainian news sites to deliver the malware via a fake Flash update, tricking victims into manually installing it themselves.

> 'The actors behind ExPetr/NotPetya have been carefully planning the BadRabbit attack since July.'

Costin Raiu, Kaspersky Lab

But ESET's Robert Lipovsky remains wary that the malware may have also been injected into target networks with another, more devious infection trick. "While this may very well be *an* infection vector, it is doubtful that this was *the* main infection vector...and quite possibly a smoke screen," he says.

The Ukrainian government's Boyarchuk pointed to an alert from the Ukrainian Computer Emergency Response Team indicating that a Microsoft Office Dynamic Data Exchange vulnerability was also used to infect victims with malicious Word, Excel, and Outlook files, but other researchers have yet to confirm those findings. Later on Tuesday, the Ukrainian CERT published a notice attributing the infections to phishing emails impersonating Microsoft technical support.[1]

All of that leaves plenty of unanswered questions around the mechanics and motivation of this latest ransomware flareup. But whether BadRabbit turns out to be a targeted state-sponsored cyberattack or merely a callous for-profit operation, it's already making its presence felt.

[1]*Updated 10/25/2017 9:00 pm EST to include more information from the Ukrainian CERT.*[2]*Updated 10/26/2017 3:25 pm EST to include BadRabbit's use of the NSA exploit EternalRomance.*