Hackers Were in Ukraine Systems Months Before Deploying Wiper

Kim Zetter

According to researchers from Cisco, evidence shows the intruders were in a few government systems late last summer, but didn't deposit their malicious wiper on the systems until recently.

Kim Zetter
Jan 21

Tower blocks pictured at dawn in Kyiv, capital of Ukraine. (Evgen Kotenko/ Ukrinform/Barcroft Media via Getty Images)

The hackers who breached Ukrainian government systems and installed a wiper on some of them were in the systems months before dropping their malicious code onto the networks, according to researchers with Cisco's Talos Intelligence Group.

The researchers found indicators of compromise — artifacts that tell investigators when and how attackers breached a system — which revealed that they were in the networks late last summer. But the intruders waited until months later to deposit a wiper on those same systems, which Microsoft discovered on the systems last week.

Matthew Olney, director of threat intelligence and interdiction at Cisco, didn't say when the wiper was deposited on systems. But the wiper's components were only compiled a few days before they were discovered on systems last week. The compilation date is visible in the code. Compilation is when the source code that a programmer writes is turned into binary code that a machine can read.

The wiper is capable of overwriting critical system files and rendering infected computers inoperable.

It wiped seven workstations at one government agency in Ukraine and a combination of workstations and servers at another agency. The web sites of the same two agencies were also defaced in operations that investigators now believe were coordinated.

Cisco has been assisting Ukraine with security and forensic analysis for five years, beginning after hackers tied to Russia's GRU intelligence agency took down the electric grid in parts of that country in late 2015 and again in 2016. The company has also been helping Ukraine investigate the attacks that occurred last week.

Olney didn't have details about the nature of the indicators of compromise, since his team is still digging through logs and images from the infected systems. Nor does he know what additional activity occurred inside the infected networks during the four to five months the actors sat in them before deploying the wiper.

From his experience, however, it appeared that the breaches may have been more opportunistic than extensively planned.

"If I were working for a national security organization, knowing that we were going to potentially be in conflict with another country, I would get access [to systems] without knowing what we're going to do with it," he said. "Here [it seems] they got access, and then decided what to do with it."

Researchers at the security firm Stairwell showed that individual components of the wiper were compiled and built on January 10, just days before the malware was deployed on systems and discovered. And researchers at the security firm ESET said the attackers used a crypting service called FUD on one of the wiper components in an attempt to make it undetectable. FUD is a popular service used by cybercriminals to obfuscate their malicious code in order to hide it from anti-virus programs. Anton Cherepanov, a researcher with ESET, told Zero Day that they may have used FUD to make it look like the attacks were conducted by cybercriminals instead of state-supported actors.

The intrusions were only discovered last week when dozens of government agencies in Ukraine were suddenly targeted in a defacement campaign in which hackers replaced the main web page of about a dozen sites with a politically charged message and attempted to deface others. The same day the defacements occurred, Microsoft discovered the destructive wiper code on the systems of a handful of entities in Ukraine — this included government agencies and at least one IT company now believed to be the Ukrainian software and web site development firm called Kitsoft.

The infection of Kitsoft was important. Once inside the company's network, the attackers didn't just deploy the wiper, they also gained access to the administrative panel where Kitsoft manages the web sites of a number of government agencies, and used this access to deface some of those sites. The company only learned later that a wiper had also been deployed on some of its own systems to destroy files.

The tool, called WhisperGate, works in three stages. In the first stage, the hackers load WhisperGate onto a system and the malware overwrites the portion of the hard drive responsible for launching the operating system when the machine is booted up. It overwrites

it with a ransom note demanding Bitcoin worth $10,000, though the message doesn't immediately appear on machines.

"Your hard drive has been corrupted," the note reads. "In case you want to recover all hard drives of your organization, You should pay us $10k via bitcoin wallet. We will contact you to give further instructions."

The ransom demand is a ruse, however, because the true intent of the malware is to destroy the machines. The malware reaches out to a Discord channel and pulls down another malicious component, which then corrupts numerous other files on the infected system.

The attackers then force the machine to power down. When it turns on again, the ransom message appears onscreen. The user sees the message and believes they just need to pay money to get the system decrypted — when in fact their system has already been rendered inoperable and unrecoverable.

Microsoft didn't say how many government agencies were infected with the wiper. But on Tuesday, a Ukrainian official told Zero Day that systems at two government agencies in Ukraine are known to have been wiped with the destructive tool, though the investigation is still ongoing.

Victor Zhora, deputy director of Ukraine's State Services for Special Communication and Information Protection, said the master boot record was overwritten on dozens of the systems and data had also been destroyed on the machines.

Zhora told Zero Day he believed the defacements and wiper operations were timed.

"It happened the same day and apparently at the same time [at both agencies]…. The probability of coincidence is much lower than if it happened only in one institution," he said.

Cisco's Olney says the defacements and wiper amount to a "confusing episode but not an alarming one," given the potential for worse attacks.

"What we have seen in [attacks in Ukraine] in the past have had real-world impact," in which government systems didn't work and lines formed at banks and stores because systems were down and people couldn't buy groceries. By comparison, the attacks last week amount to just another "winter in Ukraine," he says, when systems are traditionally targeted.

"It makes me wonder about what the intent of these events were," Olney says. "You have an actor who's methodology is to create chaos." But the events so far don't have "the impact we would have expected…. I'm left confused."

Although Ukrainian officials have attributed the attacks to Belarus and Russia, investigators say they haven't seen evidence pointing to a specific group of hackers or country yet. Russia, however, is a prime suspect given its past hacking operations in Ukraine, which

included taking out the power in parts of the country at the height of winter in 2015 and 2016, and its recent military aggressions against Ukraine, including the build up of troops on Ukraine's border.

Related:

What We Know and Don't Know about the Cyberattacks Against Ukraine - (updated)

Dozens of Computers in Ukraine Wiped with Destructive Malware in Coordinated Attack

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The Ukrainian Power Grid Was Hacked Again

If you like this story, feel free to share with others.

Share

If you'd like to receive future articles directly to your email in-box, you can also subscribe: