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

zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped

Kim Zetter

Share this post

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

zetter.substack.com

Dozens of computers at two government agencies in Ukraine are now confirmed to have been wiped by malware known as WhisperGate. The web sites of the two agencies were also defaced last week.

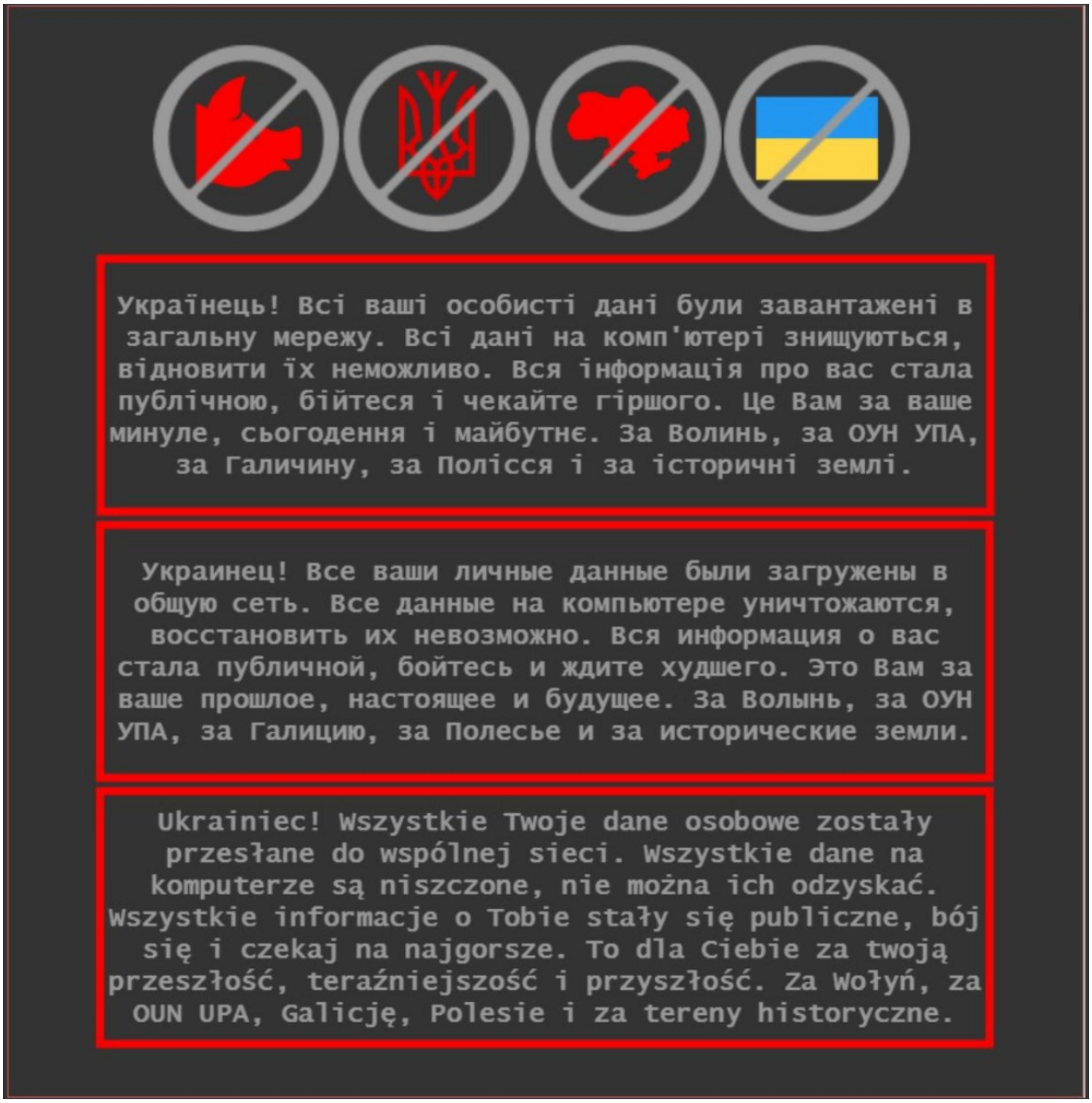
Kim Zetter
Jan 18

8

Share this post

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

zetter.substack.com



Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це Вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі.

Украинец! Все ваши личные данные были загружены в общую сеть. Все данные на компьютере уничтожаются, восстановить их невозможно. Вся информация о вас стала публичной, бойтесь и ждите худшего. Это Вам за ваше прошлое, настоящее и будущее. За Волынь, за ОУН УПА, за Галицию, за Полесье и за исторические земли.

Ukrainiec! Wszystkie Twoje dane osobowe zostały przesłane do wspólnej sieci. Wszystkie dane na komputerze są niszczone, nie można ich odzyskać. Wszystkie informacje o Tobie stały się publiczne, bój się i czekaj na najgorsze. To dla Ciebie za twoją przeszłość, teraźniejszość i przyszłość. Za Wołyń, za OUN UPA, Galicję, Polesie i za tereny historyczne.

Screenshote of defacement message that was placed on government web sites last week. Dozens of systems at two government agencies in Ukraine were wiped with a destructive tool that Ukraine now believes was part of a coordinated attack last week against systems in Ukraine, an official says.

The tool, called WhisperGate, wiped seven workstations at one government agency in Ukraine and wiped a combination of workstations and servers at the second agency.

The web sites of the same two agencies were also defaced last week in an operation that targeted at least 70 government web sites, and the official says the government now believes the defacements and wiper attack were part of the same multi-pronged operation.

“They were timed,” says Victor Zhora, deputy director of Ukraine's State Services for Special Communication and Information Protection. “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 it’s still unclear what level of coordination occurred between the attackers conducting the two operations but said the evidence connecting the two is both technical and intelligence in nature, though he wouldn’t elaborate on either.

Zhora wouldn’t identify the two agencies struck by the wiper but said that while they are “rather important” agencies, they are not critical.

“What we consider critical is systems that could significantly influence the whole political and economic situation in Ukraine in case of loss,” he said. “But these two cases are not critical considering what could be the loss if any register or any state-scaled database [were lost].”

Last Thursday dozens of government agencies in Ukraine were targeted in a web site defacement campaign in which hackers replaced the main web page at some of the sites with a politically charged message. On the same day the defacements occurred, Microsoft detected destructive wiper malware on dozens of systems belonging to several entities in Ukraine — including some whose web sites were defaced. Wipers delete or overwrite important system files, rendering systems unable to boot up or otherwise operate.

Microsoft never revealed how many entities were infected with the wiper, though someone familiar with the investigation told me just a “handful.” Microsoft also didn’t say if any systems infected with the WhisperGate wiper were actually damaged by the wiper. The news today is the first confirmation that the wiper was activated on the systems of government agencies.

The WhisperGate wiper 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."

In the meantime, the second and third stages occur — the malware has reached out to a Discord channel and pulled down another malicious component, which then corrupts numerous other files on the infected system. The attackers execute the operation by forcing 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.

Zhora said that the master boot record — the portion of the hard drive that is responsible for launching the operating system on a machine when it is booted up — was overwritten on the dozens of systems at the two government agencies now confirmed to have been affected by the wiper, and they also had data destroyed on the machines.

It wasn’t clear last week if the defacements and wiper operation were related, eventhough the timing of the two operations suggested they were.

If the defacements and wiper were meant to be coordinated and simultaneous it suggests that something might have gone wrong with the coordination. Generally hackers siphon data from machines before wiping them, then deface the machines or web site with a public message intended to taunt the victim and warn them that stolen data will soon be published.

In this case, the web sites of agencies were defaced with such a message warning that data had been destroyed and would soon be made public, but then nothing else appeared to happen, and web servers in themselves do not store the kind of information that is stored on email servers or internal networks.

Two days later, news broke that a wiper had also been found on the systems of dozens of systems belonging to several entities in Ukraine, including some of the same agencies whose web sites had been defaced. But it was never clear if the wiper had been activated on those systems or was simply sitting dormant on them waiting to be activated by the attackers. If the latter, this suggested that the coordination had perhaps failed and that the web sites had been defaced prematurely. The news today that workstations were wiped the same day the defacements occurred suggests the coordination may have been more successful than previously believed.

In addition to these two government agencies, the Ukrainian company Kitsoft also confirmed that it found the WhisperGate malware on some of its systems. Kitsoft develops and maintains web sites and at least 50 of the 70 sites targeted for defacement last week were Kitsoft customers. Investigators eventually determined that Kitsoft had been compromised, which allowed the hackers to gain access to Kitsoft’s administrator panel and use the company’s credentials to deface customer web sites.

Kitsoft spokeswoman Alevtina Lisniak confirmed to Zero Day today that the WhisperGate wiper was also found on some of their systems and that it had overwritten the master boot records on those machines. The company took the systems down to rebuild from scratch..

“We discovered some overwritten [master boot records] and then stopped the infrastructure to prevent further attack development,” Lisniak writes. This suggests that only the wiper’s first stage may have been activated, but this is still unclear.

Update: 1.19.22 To clarify that Microsoft found the wiper on dozens of systems, but those systems were at just a handful of entities.

For a full description of what occurred last week, see:

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

Also related:

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: