Ukrainian government calls out false flag operation in recent data wiping attack

By Catalin Cimpanu

Published: 2023-01-20 · Archived: 2026-04-05 15:24:28 UTC

The Ukrainian government said today that it found evidence meant to connect the data wiping attack that hit its own systems two weeks ago to a pro-Ukrainian hacking group in what security researchers typically describe as a "false flag" meant to distract investigators from the real culprits of the attack.

To better understand what the Ukrainian government is saying, a summary of the original attack is required, rewritten with the malware nomenclature and timeline presented by Ukrainian authorities:

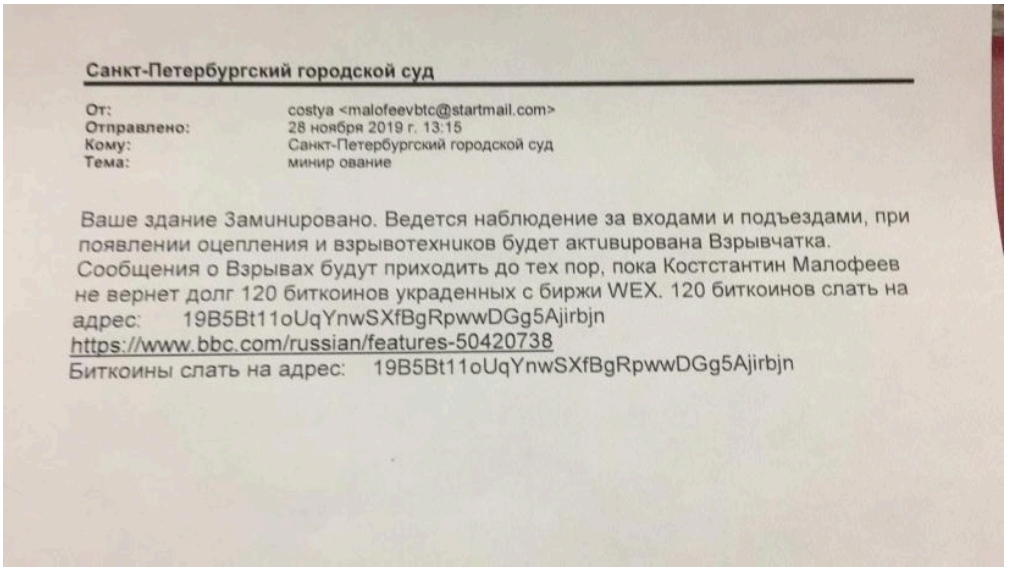
- On the night between January 13 and January 14, unidentified attackers attempted to gain access and deface the websites of more than 70 Ukrainian government agencies.
- The attack successfully defaced 22 websites and severely damaged six.
- Most of the government sites were managed by a local IT firm named KitSoft and ran on top of the October CMS website builder.
- The attackers used vulnerabilities in the CMS and KitSoft employee accounts to access servers hosting the sites to carry out the defacements.
- Besides altering websites, the attackers also deployed a malware strain named WhisperGate on servers and government systems they had previously compromised months before.
- This malware downloaded and ran two components.
- The first was named BootPatch and worked by rewriting the master boot record (MBR) of an infected computer, preventing it from booting and showing a ransom demand instead.
- The second component was named WhisperKill and worked by trashing files by rewriting their content with a 0xCC character sequence.
- Because the attackers did not include a data recovery mechanism, the attack was deemed to have been intentionally designed to be destructive and subsequently blamed on hackers tied to the Russian government.

But in a report published today by one of the agencies investigating the attacks, Ukraine's State Service for Communications and Information Protection (CIP) said that they found that the WhisperKill component contained more than 80% of code that was similar to a ransomware strain named WhiteBlackCrypt, suggesting that the attackers had re-used code from the public domain.

But while this is a common tactic for nation-state threat actors, CIP doesn't believe the choice to use code from WhiteBlackCrypt was an accident and was actually chosen on purpose, based on several factors.

First, officials said pointed out that the WhiteBlackCrypt is known to use an ASCII depiction of a trident, Ukraine's official coat of arms, in the ransom note it shows to users.

Second, officials say the ransomware also reused the same Bitcoin address to gather ransom payments as an address that used in email bomb threats sent to Russian organizations in 2019. According to reports in Russian media, some of the funds gathered through this campaign were allegedly sent to a group associated with Ukrainian special services.



Санкт-Петербургский городской суд

От: costya <malofeevbtc@startmail.com>
Отправлено: 28 ноября 2019 г. 13:15
Кому: Санкт-Петербургский городской суд
Тема: минир ование

Ваше здание Заминировано. Ведется наблюдение за входами и подъездами, при появлении оцепления и взрывотехников будет активирована Взрывчатка.
Сообщения о Взрывах будут приходить до тех пор, пока Костстантин Малофеев не вернет долг 120 биткоинов украденных с биржи WEX. 120 биткоинов слать на адрес: 19B5Bt11oUqYnwSXfBgRpwwDGg5Ajirbjn
https://www.bbc.com/russian/features-50420738
Биткоины слать на адрес: 19B5Bt11oUqYnwSXfBgRpwwDGg5Ajirbjn

Third, CIP says that several Russian Telegram channels have used these two incidents to incorrectly but formally link the WhiteBlackCrypt ransomware to Ukraine's Special Services and Armed Forces.

And last but not least, CIP says that an individual who posed as the same person who blackmailed Russian organizations in 2019 came back to life again in January 2022 when it mass-messaged and urged Ukrainian organizations to mount attacks against Russia.

All of this has led CIP and the Ukrainian government to believe that all of this is somehow a false flag operation meant to blame a "fake" pro-Ukrainian group for an attack on their own government, rather than the common assessment that Russian threat actors are behind the attack.

"The deliberate use of the WhisperKill malware on January 13-14, 2022, which is morphologically similar to the WhiteBlackCrypt malware and manipulatively associated with the SSO of the Armed Forces of Ukraine, is an attempt to provoke and distort reality in order to accuse Ukraine of attacks on January 13-14, 2022 year," CIP officials said today.

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
