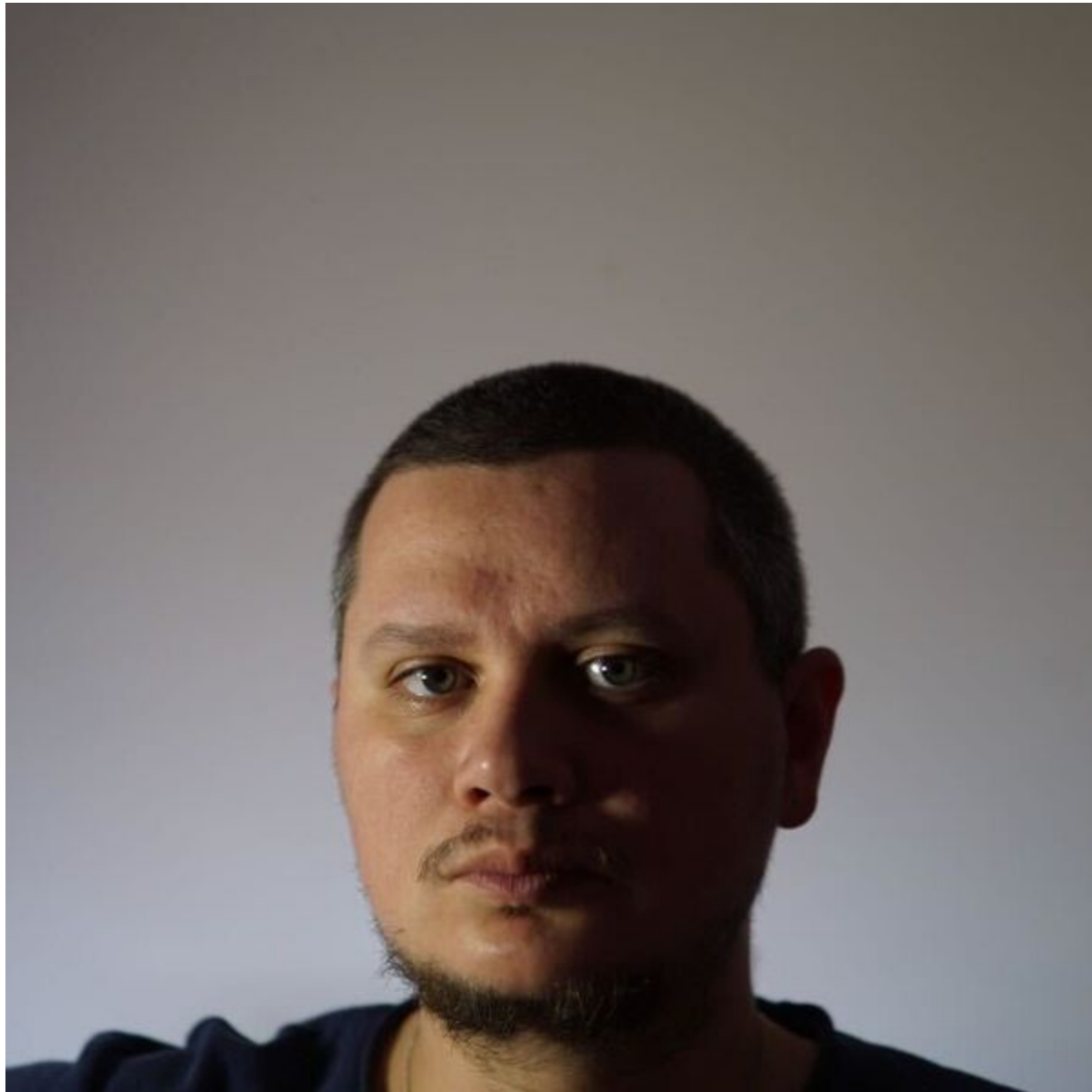


Five Things You Need to Know About the Cyberwar in Ukraine

B bitdefender.com/blog/hotforsecurity/five-things-you-need-to-know-about-the-cyberwar-in-ukraine/



Radu CRAHMALIUC

March 11, 2022

One product to protect all your devices, without slowing them down.

[Free 90-day trial](#)




Einstein once said he doesn't know what weapons will be used for the next World War, but he fears the war after it will be fought with sticks and stones. A new world confrontation is highly unlikely at this moment but the weapons used are as high-tech as it gets as some of them use code instead of gunpowder.

As the first Russian troops started rolling into Ukraine, cybersecurity experts everywhere braced for the worst -- some of the biggest cybercrime gangs in the world are known to have close ties with the Russian government and operate from so-called "hacker heavens" in the ex-Soviet space.

The fears came to life when the Conti ransomware group publicly pledged its support to the Russian cause. Several Ukrainian banks and public institutions were hit by DDoS attacks and data-erasing malware, but, retaliatory attacks against western public institutions and companies have remained scarce. For now.

“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/27/2022  9697 [READ MORE >>](#)

Is this a sign that most organizations have correctly assessed the danger and strengthened their security, or is it just the calm before the storm?

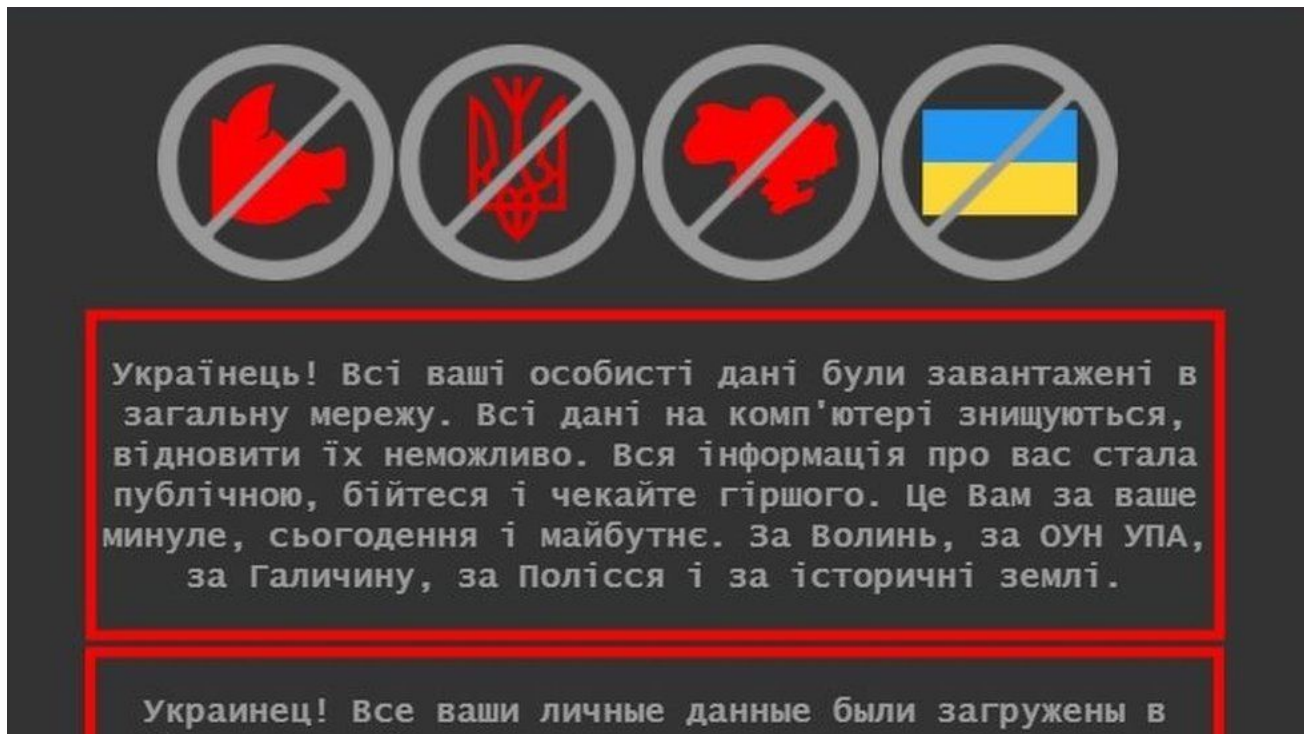
Here's what we know so far:

1. For now, Ukraine is the main target

Most of the cyberattacks so far have focused strictly on hitting Ukrainian organizations, in at least three separate waves:

- on Jan. 14, 70 government websites were defaced and taken offline, including the Ministry of Foreign Affairs and the Security and Defense Council. However, according to the reports no data was leaked, and downtime lasted a few hours. Almost at the same time, the Microsoft Threat Intelligence Center (MSTIC) reported active malware, dubbed WhisperGate, that was made to look like ransomware but lacked a recovery component. This meant it was actually designed to destroy data.
- on Feb. 15, Ukraine's two largest banks were taken offline by a massive Distributed Denial of Service (DDoS) attack that also affected mobile apps and ATMs.

- on Feb. 23, another DDoS attack took out military and government sites while a data wiper called HermeticWiper was detected on hundreds of computers belonging to various Ukrainian organizations. Simultaneously, MSTIC detected a trojan dubbed FoxBlade that can surreptitiously weaponize victims' computers and use them in DDoS attacks.



Despite the obvious interest in disrupting the Ukrainian infrastructure there's no guarantee malware like WhisperGate, HermeticWiper or FoxBlade can't spill over to computers in other countries too. Additionally, as more countries join the sanctions against Russia, Russian-backed hackers could shift their focus and retaliate.

2. Ukraine is fighting back

Kremlin-backed hackers may have had the benefit of surprise, but the cyberwar isn't one-sided at all. On the contrary, after the initial shock, the Ukrainian government called for the assembly of a volunteer IT army that quickly started retaliating: the hacker collective Anonymous took down the Belarussian Railways internal network and almost 300 company websites in Russia. Conti's internal messages and source code were leaked, the Kremlin site was hacked, the Russian Nuclear Institute and the Russian Space agency suffered data breaches and Russian tv channels were hacked to show real footage from Ukraine.

Дорогие граждане. Призываем вас прекратить это безумие, не отправляйте своих сыновей и мужей на верную смерть. Путин заставляет нас врать и подвергает опасности. Вы хотите ядерной войны? Вы хотите все умереть за него? Пора действовать! Выходите на улицы.



3. It's not just about companies

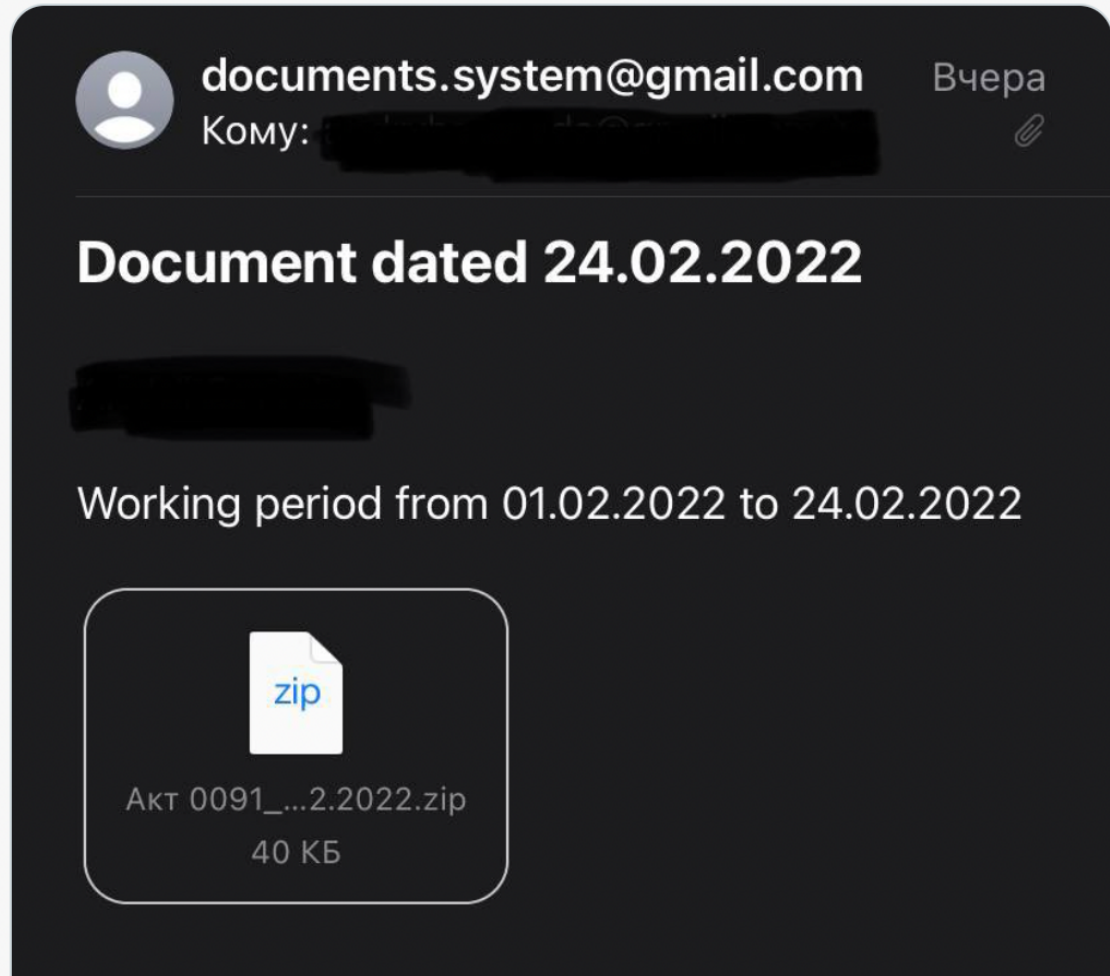
There's a general belief state actors only go after companies and public institutions, but that's not the case. Sometimes they also target regular people. In late February, the national Computer Emergency Response Team for Ukraine issued a warning of a major phishing campaign against military personnel. Even more worrying, European officials were targeted with malware in an apparent attempt to disrupt efforts to help Ukrainian refugees.



SSSCIP Ukraine  @dsszzi · Feb 25

Warning  A phishing [#attack](#) has started against Ukrainians! Citizens' e-mail addresses receive letters with attached files of uncertain nature. The mass distribution of such messages to messengers may happen.

[#cyberattacks](#) [#Ukraine](#)



Whether they're looking to gather intelligence, phish for credentials or obstruct humanitarian efforts, state actors don't discriminate when it comes to targeting regular people. Even if you're not directly involved in the current situation, it's always a good idea to protect your devices from malware, update them regularly, use strong passwords and watch out for scams and phishing emails.

4. There are third parties taking advantage of the situation

Researchers at Bitdefender Labs picked up [waves of fraudulent and malicious emails](#) exploiting the humanitarian crisis and charitable spirit of people across the globe. The conflict in Ukraine is a gold mine for scammers and criminal groups that aren't necessarily politically involved but love making money. One of the preferred methods is using fraudulent

emails asking recipients to donate money. Scammers are impersonating the Ukrainian government, international humanitarian agency Act for Peace, UNICEF, and the Ukraine Crisis Relief Fund to ask for crypto donations.



A donation campaign has been launched to support Ukraine and also help refugees fleeing from the conflict in Ukraine. The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT.

BTC - bc1qzvkyvkcrynnyye8nxv [redacted]
ETH, USDT, LUNA (ERC-20) - 0x4428a0f3029309a322bE [redacted]
SOLANA (SOL): 8YoCx8Hzcs8ig9tJRF4xp [redacted]
BINANCE (BNB): bnb15z8f3zxyn9r48mk9p [redacted] / 0x4428a0f3029309a322bE [redacted]

Kindly reply to this email if you need to donate with other token.

Best Regards
Ukraine
#BeautifulUkraine



5. Cyberwar could be the next cold war

The lack of devastating attacks on western targets on the scale of Colonial Pipeline or Kaseya doesn't mean the danger has passed. Even if the military conflict ends, the cyber conflict is likely to persist for years, and all parties involved, whether government agencies, private companies, or regular users, must come to terms with it.

Whether we like it or not, cyberattacks used for sabotage or spying aren't going away anytime soon for a number of reasons: they're cheap and efficient, they can be launched from anywhere in the world, they bring in good money, state responsibility is hard to prove and, most importantly, the number of potential targets is virtually unlimited.

For more tips, please check our dedicated [cybersecurity guide](#) in armed conflict zones.

In response to the military crisis and increased cybercriminal activity, Bitdefender & the Romanian National Cyber Security Directorate (DNSC) are offering **[free cybersecurity protection](#)** for any Ukrainian citizen, company or institution, as long as necessary.

TAGS

[ukraine](#) [industry news](#)

AUTHOR

Radu CRAHMALIUC

Radu is a tech-geek with 15 years of experience in writing, journalism and copywriting. When he's not writing he's probably taking something apart, trying to figure out how things work.

[View all posts](#)

