Russia-Ukraine Cyberattacks (Updated): How to Protect Against Related Cyberthreats Including DDoS, HermeticWiper, Gamaredon, Website Defacement, Phishing and Scams

By Unit 42

Published: 2022-02-22 · Archived: 2026-04-05 19:01:49 UTC

Executive Summary

Over the past several weeks, Russia-Ukraine cyber activity has escalated substantially. Beginning on Feb. 15, a series of distributed denial of service (DDoS) attacks commenced. These attacks have continued over the past week, impacting both the Ukrainian government and banking institutions. On Feb. 23, a new variant of wiper malware named HermeticWiper was discovered in Ukraine. Shortly after, a new round of website defacement attacks were also observed impacting Ukrainian government organizations.

Consistent with our previous reporting on the topic, several western governments have issued recommendations for their populations to prepare for cyberattacks that could disrupt, disable or destroy critical infrastructure. We have already observed an increase in Russian cyber activity, which we reported on in our initial Threat Brief published last month and our recent report on the Gamaredon group. Future attacks may target U.S. and Western European organizations in retaliation for increased sanctions or other political measures against the Russian government. We recommend that all organizations proactively prepare to defend against this potential threat.

This post was substantially updated on Feb. 24 to add information on the recent DDoS attacks, HermeticWiper malware and website defacement; update our recommendations for how organizations should prepare for potential cyber impact; and provide additional details for our customers and clients on how we can help. This post was substantially updated March 31 to add information on phishing and scam attacks, cybersquatting trends, fake donation websites, DoS attacks on Ukrainian news sites and distribution of malicious binaries.

Full visualization of the techniques observed, relevant courses of action and indicators of compromise (IoCs) related to this report can be found in the Unit 42 ATOM viewer.

We will continue to provide updates with new information and recommendations as they become available.

Attack Types Discussed in Relation to Russia-Ukraine Cyber Activity	DDoS, website defacement, wiper
Named Threat Groups and Malware	HermeticWiper, Gamaredon, WhisperGate, OctoberCMS vulnerability
Types of Protections Covered	Best Practices, Proactive Assessments, Ransomware Readiness, WildFire, Threat Prevention, XSOAR, Cortex Xpanse

DDoS Attacks Impacting Ukrainian Government and Banking Institutions

On Feb. 15, the Cyberpolice of Ukraine reported that residents were actively receiving fake SMS text messages. These messages were likely intended to cause alarm among the population, as they claimed that ATMs were malfunctioning.

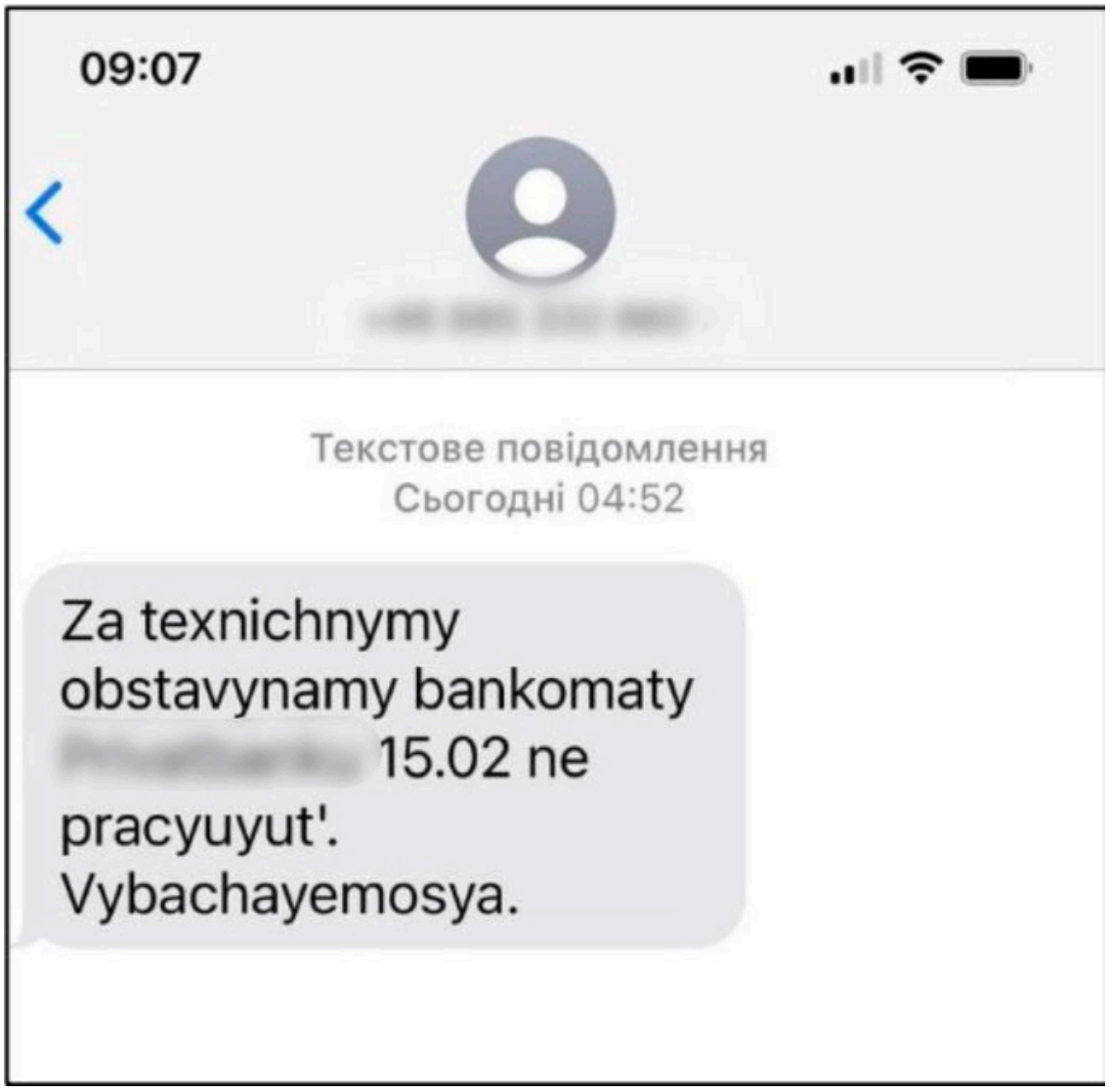


Figure 1. Example text message provided by the Cyberpolice of Ukraine.

Shortly after the text messages were observed, several DDoS attacks occurred. These attacks impacted Ukrainian government organizations including the Ministry of Defense, Ministry of Foreign Affairs, Armed Forces of Ukraine and the publicly funded broadcaster Ukrainian Radio. Additionally, the attacks targeted two banking institutions, PrivatBank and Oschadbank. An initial investigation into the DDoS attacks suggested that Mirai and Meris bot networks may have been leveraged in the attacks.

On Feb. 18, both the United States and the United Kingdom attributed these DDoS attacks to Russia's Main Intelligence Directorate (GRU).

Over the past week, Ukraine has continued to observe a relatively constant flow of DDoS attacks targeting its government and financial institutions. However, at this time, attribution for the ongoing attacks has not been

established. The Ukrainian CERT did identify a post on RaidForums from a user named “Carzita” that suggested that additional actors may also be launching DDoS and defacement attacks for undisclosed reasons.

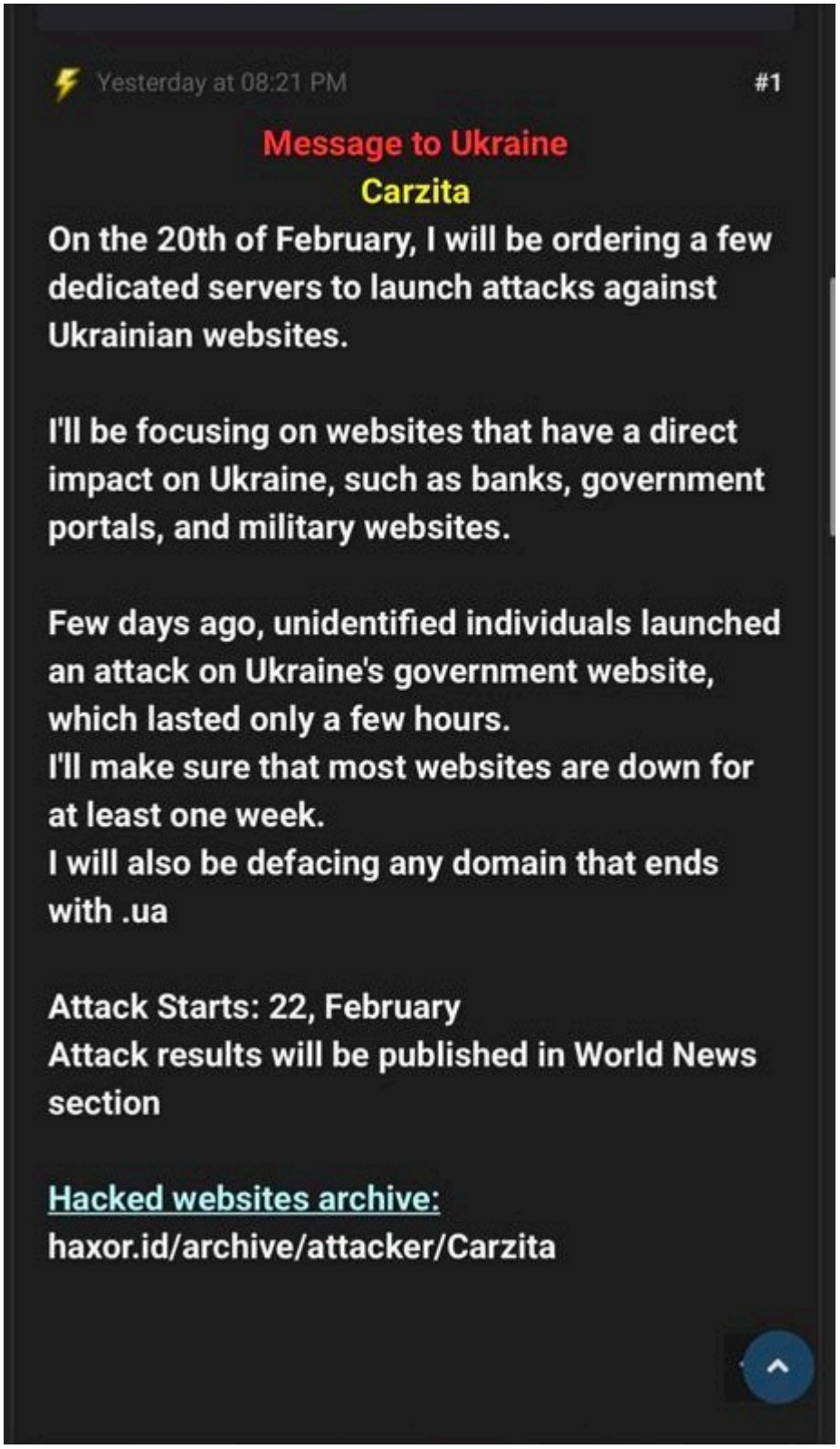


Figure 2. Carzita post on RaidForums.

HermeticWiper Malware

On Feb. 23, a malicious file named conhosts._exe (SHA256: 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591) was uploaded to a public malware repository from an organization in Kyiv, Ukraine. This executable is a signed file with a valid signature from an organization named Hermetica Digital Ltd. This signing certificate has since been explicitly revoked by its issuer. Upon execution, this file enumerates all files on a hard drive, wipes the partition info and then forces a system reboot, which predictably results in the following screen:

Figure 3. Missing operating system after hard drive is wiped.

Further analysis has confirmed that the malware accepts command-line arguments allowing an attacker to instruct the malware to sleep for a period of time or to shut down the system.

Additionally the kernel module responsible for the actual wiping activity is from a legitimate application called EaseUS Partition Master. This software is designed as free partition software that can reorganize disk space for better performance.

In tracking this threat, early reports show that the malware has been deployed against a financial institution in Ukraine as well as two contractors in Latvia and Lithuania that provide services to the Ukrainian Government. Additionally, ESET researchers have warned that they found this malware installed across “hundreds of machines” in Ukraine.

Figure 4. ESET research warning.

Website Defacement

Concurrent with the discovery of wiper malware, we also witnessed a second round of website defacements on Feb. 23. These attacks appear to have copied the messaging template observed in attacks exploiting the OctoberCMS vulnerability a month earlier on Jan.14, while adding a .onion web address and a message in red font that translates to, “Do you need proof, see the link at the end.”

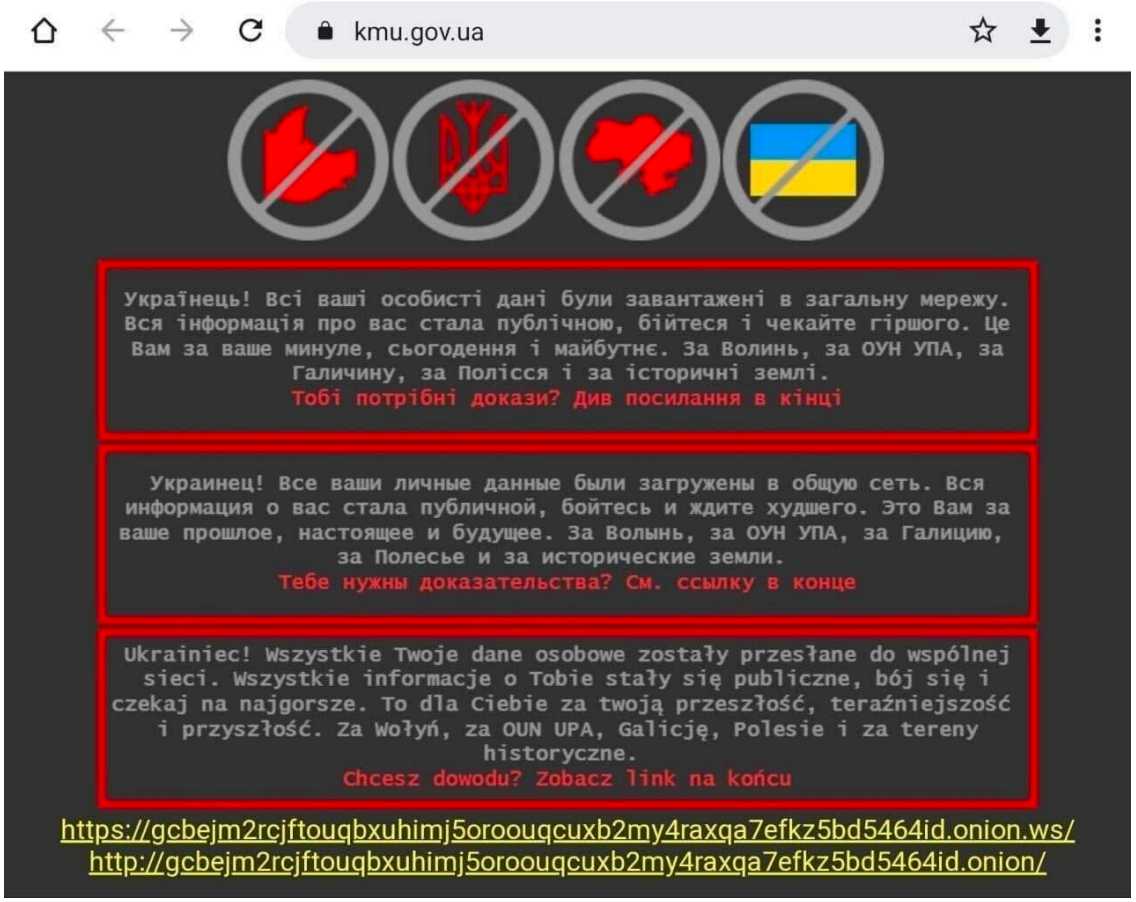


Figure 5. Website defacement message. A new message in red font translates to “Do you need proof, see the link at the end.”

The .onion site links to an entity calling themselves “Free Civilian” and offering to sell databases containing the personal data of Ukrainian citizens. Over the past 24 hours, the list of entities on the leaks section has expanded to 48 gov.ua domains and one Ukranian company (motorsich[.]com) that builds engines for airplanes and helicopters.

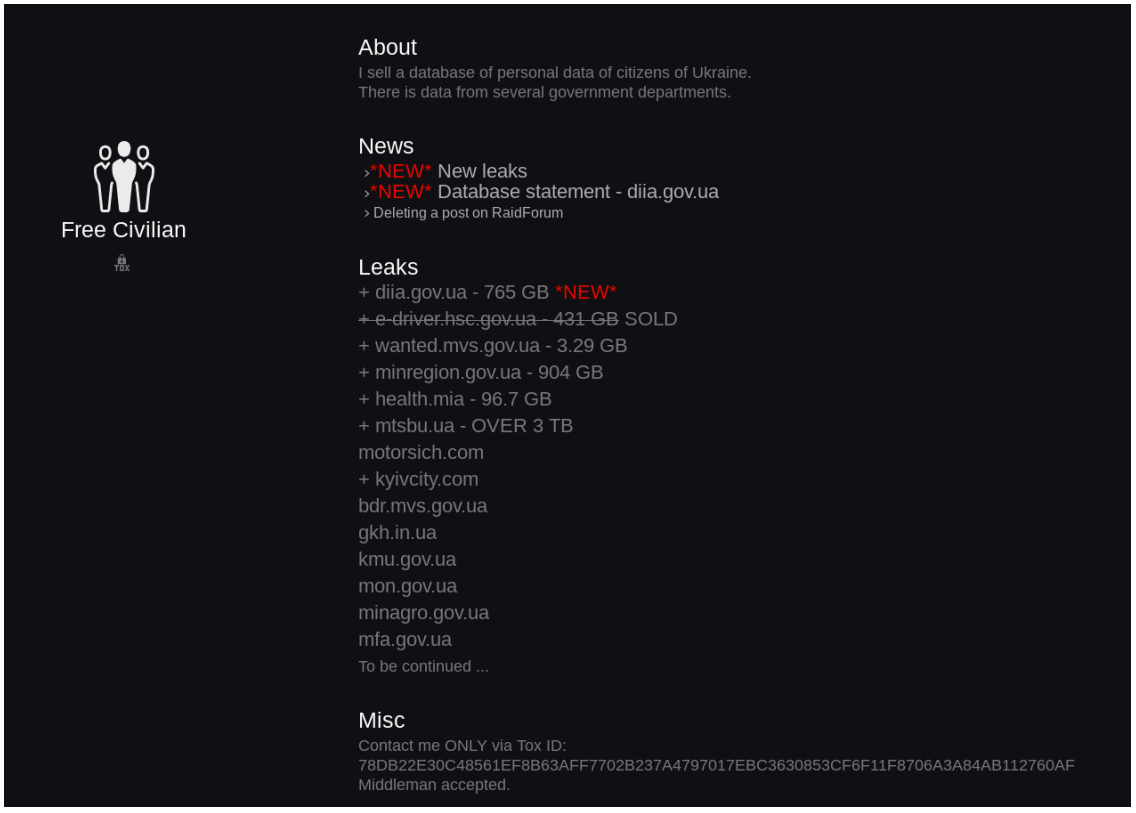


Figure 6. Free Civilian .onion site.

Figure 7. New leaks offered on the Free Civilian .onion site.

Rise in Phishing and Scam Attacks

Our team analyzed the larger trends regarding Ukraine-related phishing and scam URLs detected by Advanced URL Filtering. We noticed an overall increase in the detection of websites that host phishing and scam URLs on domains using Ukraine-related TLDs such as gov.ua and com.ua, or containing popular Ukraine-related keywords such as "ukraine" and "ukrainian". This trend correlates with an increase in Google searches for terms like "Ukraine aid." The increase in online searches containing Ukraine-related keywords likely makes such URLs a

more lucrative target for attackers, and past examples show that attackers are known for taking advantage of current events.

From January to late February, it appears that the number of Ukraine-related phishing and scam sites largely followed a similar trend as Ukraine-related internet searches; however, the number of phishing and scam sites has continued to rise through mid-late March as the situation remains ongoing. Figure 8 shows that the number of Ukraine-related phishing/scam sites is currently continuing to rise about a month after the “Ukraine aid” search term started trending in Google search.

Figure 8. Comparison of the number of websites (hostnames) hosting Ukraine-related phishing and scam URLs and worldwide search interest in “Ukraine Aid” as reported by Google Trends.

Among these phishing and scam URLs, we found a targeted phishing attack. On March 16 while ingesting a third-party data feed, our in-house machine learning models detected a phishing webpage targeting a Ukrainian state administration employee. The webpage is imitating a popular cloud file storage site. Upon visiting the webpage, the “Username” field is pre-populated with the targeted employee’s email address, and the user is then prompted to enter in their password in order to view a sensitive document as shown in Figure 9.

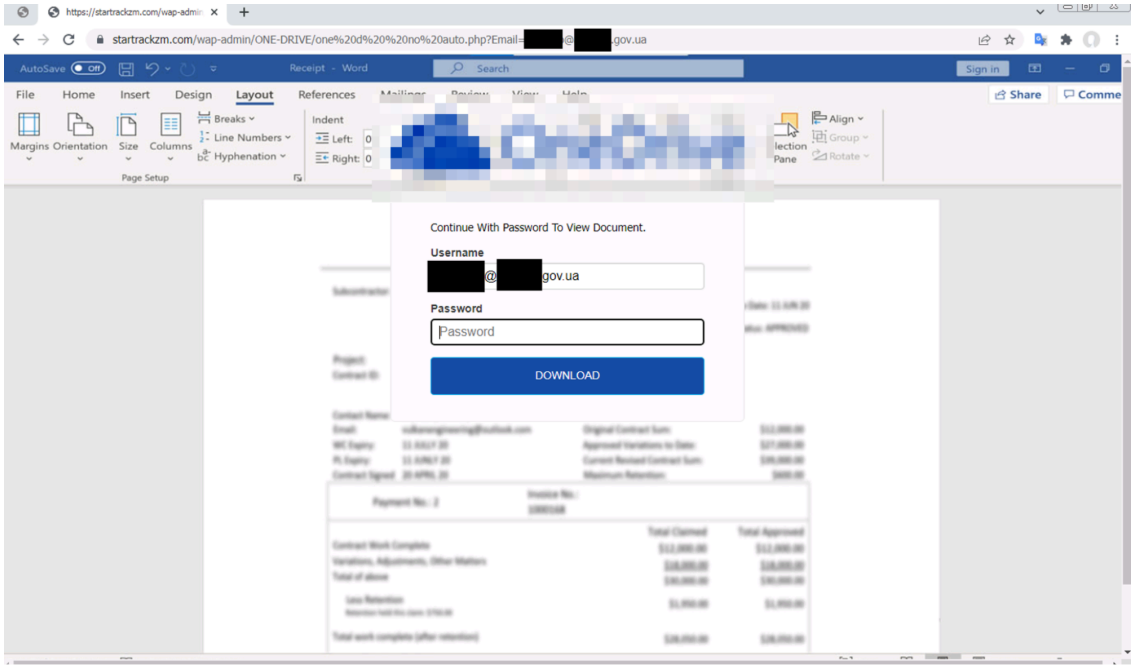


Figure 9. hxxps://startrackzm[.]com/wap-admin/ONE-DRIVE/one%20d%20%20no%20auto.php?Email=REDACTED@REDACTED.gov.ua. A phishing webpage targeting a Ukrainian state administration employee, detected by our in-house machine learning models on March 16.

Our teams at Palo Alto Networks are actively monitoring the phishing landscape surrounding Ukraine-related URLs and are sharing this threat intelligence with relevant authorities in Ukraine and internationally. We are also sharing a list of IoCs that were detected as phishing and scam URLs. Palo Alto Networks customers who subscribe to Advanced URL Filtering are already protected from these IoCs.

Increase in Cybersquatting Trends

We monitored a list of 50 legitimate Ukraine-related domains (e.g., popular news and donation websites) and keywords (e.g., Ukraine, refugee) as targets for cybersquatting. We detected 11,637 cybersquatting newly registered domains (NRDs) during February and March. In particular, we noticed a sharp increase in the number of cybersquatting domains that were registered close to Feb. 24, as shown in Figure 10 below.

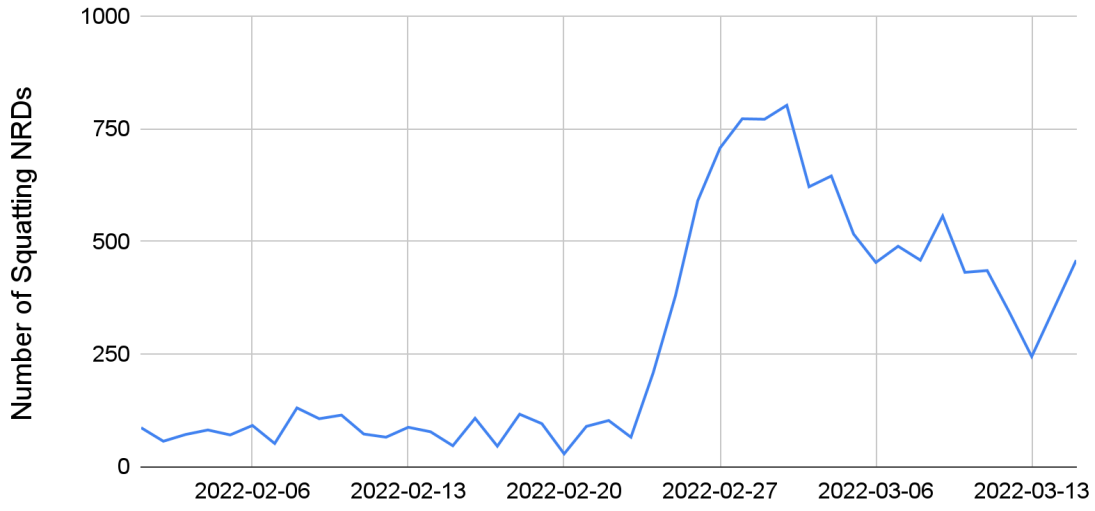


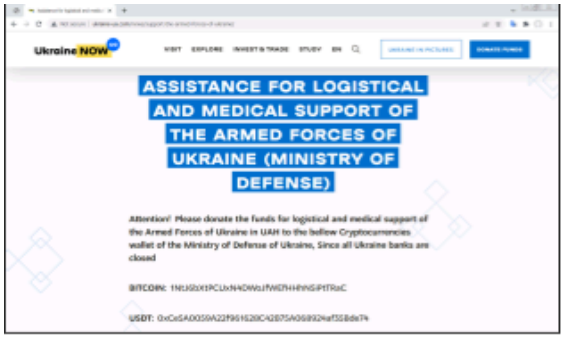
Figure 10. A spike in the number of squatting NRDs close to Feb. 24.

We manually analyzed a sample set of these cybersquatting domains. Below we share some interesting case studies.

Fake Donation Websites

We identified more than two dozen domains requesting donations to support Ukraine. A detailed analysis of these domains revealed that many of them are fake. These donation websites provide little to no information about the associated organization and distribution of funds. Many of these websites use cryptocurrency wallets (e.g., BTC, ETH) to accept payment (likely because these wallets are easy to set up and require no verification).

We also find that some websites are mimicking popular donation websites or organizations to trick users into paying them money. We show some examples in Figure 11. For instance, donatetoukraine[.]com is pretending to be associated with the popular Come Back Alive campaign. While the banking information shared on the donation website matches the original campaign website, we confirmed that the BTC wallet address is different from the actual.



Ukraine-ua[.]com is impersonating the official website of Ukraine, and asking for donations to an unofficial Bitcoin address.

ukraine[.]donatetounhrc[.]com is pretending as UNHCR. We confirmed that this domain is not affiliated with UNHCR and was recently registered on 9th March, 2022.

donatetoukraine[.]com is pretending to be part of a widely known Come Back Alive campaign. While the banking information shared on the donation website matches the original campaign website, the BTC wallet address is different from the actual.

Figure 11. The screenshots show various examples of websites impersonating legitimate Ukraine-related entities, asking for donations.

DoS Attacks on Ukrainian News Sites

We found a cybersquatting domain – save-russia[.]today – that is launching DoS attacks on Ukrainian news sites. Once a user opens the website in the browser, it starts making requests to various Ukrainian news sites and lists the number of requests made to each new site on the home page, as shown in Figure 12 below.

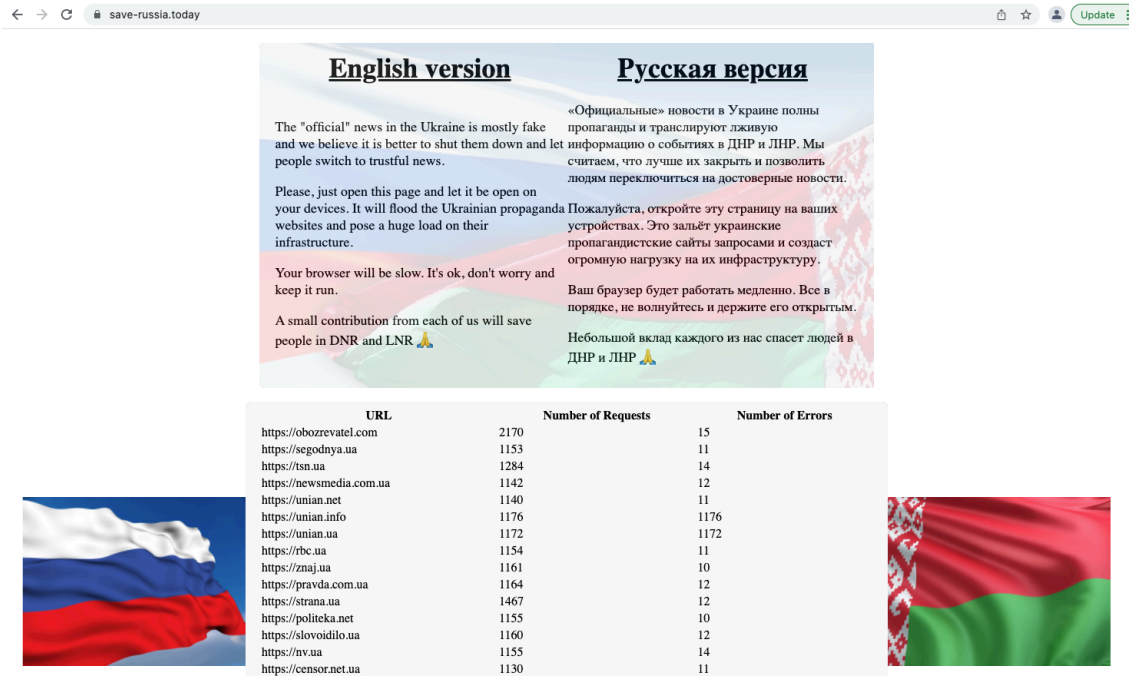


Figure 12. A cybersquatting domain save-russia[.]today is launching DoS attacks on Ukrainian news sites.

We strongly recommend that users be alert to the possibility of cybersquatting domains. In particular, fake donation websites mimicking popular websites can be misleading, as described earlier. Before donating money, we recommend checking whether the website is referenced and shared by the official charity or government organization. Our teams at Palo Alto Networks will continue monitoring domain squatting attacks and work to protect customers against them. We are also sharing a list ofIoCs publicly and have shared this threat intelligence with relevant authorities in Ukraine.

Distribution of Apps

We detected campaigns of fake downloads where threat actors have set up web pages to host malicious binaries. We found that these campaigns were targeting Ukrainian users. Most of these web pages show malicious binaries as popular browsers or communication apps in order to deceive users. For example, we detected a website that was distributing a malicious binary by masquerading as a popular global communication app targeting users in Ukraine. This domain is still active and trying to target Ukrainian users at the time of writing this post. Note that Palo Alto Networks customers receive protections against such domains from the Next-Generation Firewall via Advanced URL Filtering, DNS Security and WildFire URL Analysis subscriptions.

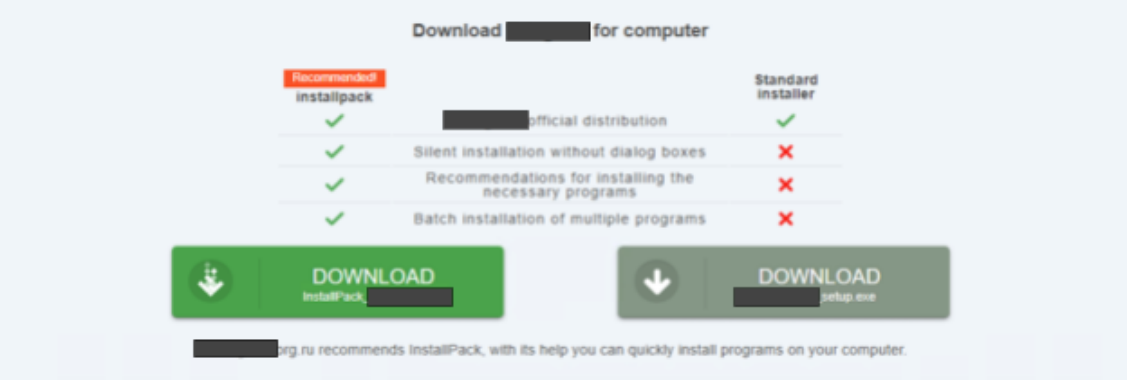


Figure 13: A website distributing a malicious binary by masquerading as a popular global communication app.

We also found that these fake download campaigns rotate domains to distribute the same malicious binaries. For example, we detected two domains distributing the same malicious binary where one domain was impersonating a popular, widely used video conferencing application and the other a widely used internet browser.

The distribution of fake browsers and communication apps targeting Ukrainian users at this time is concerning. Our teams at Palo Alto Networks will continue to monitor and work to protect our customers against such attacks. We are publicly sharing a list of IoCs and shared this threat intelligence with relevant authorities in Ukraine. We also advise Ukrainian users to only install software and apps from verified and official websites.

How Palo Alto Networks Is Working to Keep You Safe

Consistent with our previous reporting on the situation, Unit 42 continues to lead a company-wide effort to collect, evaluate and disseminate the latest intelligence on cyber activity related to Russia and Ukraine. We are actively collaborating with our partners in industry and governments to share our analysis and findings based on our global threat telemetry network.

These efforts have enabled us to make near-daily updates to our platform to ensure our customers have the best protection possible. This includes blocking hundreds of domain names, IP addresses and URLs for our customers related to newly discovered attacks. We've updated and added signatures to the WildFire analysis and Cortex XDR Prevent and Pro products to block newly discovered vulnerabilities and malware including HermeticWiper. Read more about Cortex XDR protections. Our Threat Prevention and Web Application and API Security products added coverage for the OctoberCMS vulnerability exploited in the WhisperGate attacks, and we released an XSOAR Playbook to help organizations hunt for this threat. Cortex Xpanse can assist with understanding and managing your organization's attack surface as well as identifying vulnerable resources.

We have released public reports on the WhisperGate attacks and the infrastructure and tactics used by the Gamaredon group. On the Unit 42 website, you will also find a free ATOM which contains a structured mapping of the Gamaredon group's tactics aligned to MITRE's ATT&CK framework.

As the situation continues to develop, we'll continue to update our blog with the latest information.

How You Should Prepare for an Increase in Cyberthreats Such as Wipers, DDoS, Website Defacement and Other Related Attacks

There is no single action you can take to protect your organization against this threat. Unlike a new malware family or vulnerability in the wild, the attacks we expect could come in many forms. Several western governments have proposed broad recommendations focused on technical hygiene. We consider these appropriate given the variety of tactics that Russian actors have used in the past.

We recommend organizations prioritize actions in the following four areas:

1. **Patch Internet-Facing and Business Critical Software**: Apply patches for any software containing vulnerabilities – not just those known to be exploited in the wild. This is most urgent for software that is internet-facing and necessary for your business's operations, such as webmail, VPNs and other remote access solutions.
2. **Prepare for Ransomware and/or Data Destruction**: A likely form of disruptive cyberattack will either use ransomware or a destructive attack that poses as ransomware. As we saw with the NotPetya attacks in 2017 and the WhisperGate attacks just last month, an attack that demands a ransom may not actually be "ransomware." The malware used in these attacks destroyed data without any chance of recovery, using the ransom demand simply to cover its true intention. The use of HermeticWiper further demonstrates this point. The preparation required to prevent and recover from these attacks is similar in either case. Testing back-up and recovery plans is critical, as well as testing your continuity of operations plan in case your network or other key systems are disabled in the attack.
3. **Be Prepared to Respond Quickly:** Ensure that you designate points of contact across your organization in key areas in case of a cybersecurity incident or disruption in critical infrastructure. Test your communication protocol (and backup protocols) to avoid being caught without a clear mechanism to disseminate critical information. Perform a table-top exercise with all of the key parties to walk through how you would respond in the event the worst happens.
4. **Lock Down Your Network: Making small policy changes can decrease the likelihood of a successful attack against your network. Many applications can be abused, even though the application itself may not be malicious. If your organization doesn't require their functionality, blocking them will improve your security posture. For example, recent attacks have abused popular applications – like Trello and Discord – to distribute malicious files. Users didn't need to use the software to be impacted, the attackers simply used the platforms to host links to files.**

There is no way to know for certain what shape an attack may take, but taking these steps will help provide broad protection against what we expect to come.

How Unit 42 Threat Intelligence and Security Consulting Can Help

Unit 42, the threat intelligence and security consulting arm of Palo Alto Networks, has a team of experts who can help your organization assess and test your security controls with proactive assessments and incident simulation services. Because of the likelihood of ransomware attacks – or destructive attacks that pose as ransomware – it may be beneficial to focus on preparing in this area, particularly ensuring backup and recovery plans are in place.

We have distilled the knowledge we've gained from responding to hundreds of ransomware incidents into our Ransomware Readiness Assessment offering, which is designed to help organizations strengthen their processes and technology to mitigate threats like the ones we expect in the coming days and weeks.

If you think you may have been compromised by wiper attacks, Gamaredon, DDoS attacks or other cyber activity related to Russia-Ukraine, or have an urgent matter, get in touch with the Unit 42 Incident Response team or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Indicators of Compromise

HermeticWiper SHA256

1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397

Certificate

Name Hermetica Digital Ltd
Thumbprint 1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
Serial Number 0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC

Website Defacement Domain

gcbejm2rcjftouqbxuhimj5oroouqcuxb2my4raxqa7efkz5bd5464id[.]onion

Scam and Phishing URLs, Fake Donation Sites, Fake Browser or Messenger

Please see the IoCs on GitHub.

Appendix A: Cortex Xpanse: Identifying Assets That May Be Impacted by CISA's Known Exploited Vulnerabilities

In Alert AA22-011A (updated March 1, 2022), the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS/CISA) identifies a selection of vulnerabilities that Russian advanced persistent threat (APT) groups are assessed to have exploited in the past, but recommends that users take action against a much broader list of known exploited vulnerabilities (KEVs). The cited KEVs and their impacted devices – all of which can be identified using Cortex Xpanse – are:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router

- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 Multiple Vmware Products
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange

Cortex Xpanse's ability to index the entire internet helps organizations discover, prioritize, and remediate significant exposures on their attack surfaces – including all of the impacted services listed above. We routinely observe vulnerable devices across the global internet, despite the fact that most of these CVEs are more than two years old.

Beyond Alert AA22-011A, CISA's overarching guidance for attack surface reduction includes hardening of forward-facing network services, with prioritized patching of KEVs, as documented in Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV). This directive requires agencies to remediate all vulnerabilities that CISA includes in their KEV catalog based on an assessment that the vulnerabilities "carry significant risk to the federal enterprise." Learn more and see a detailed workflow example on the Palo Alto Networks SecOps blog, "How Xpanse Can Identify CISA-Identified Known Exploited Vulnerabilities."

Updated April 1, 2022, at 11 a.m. PT.
