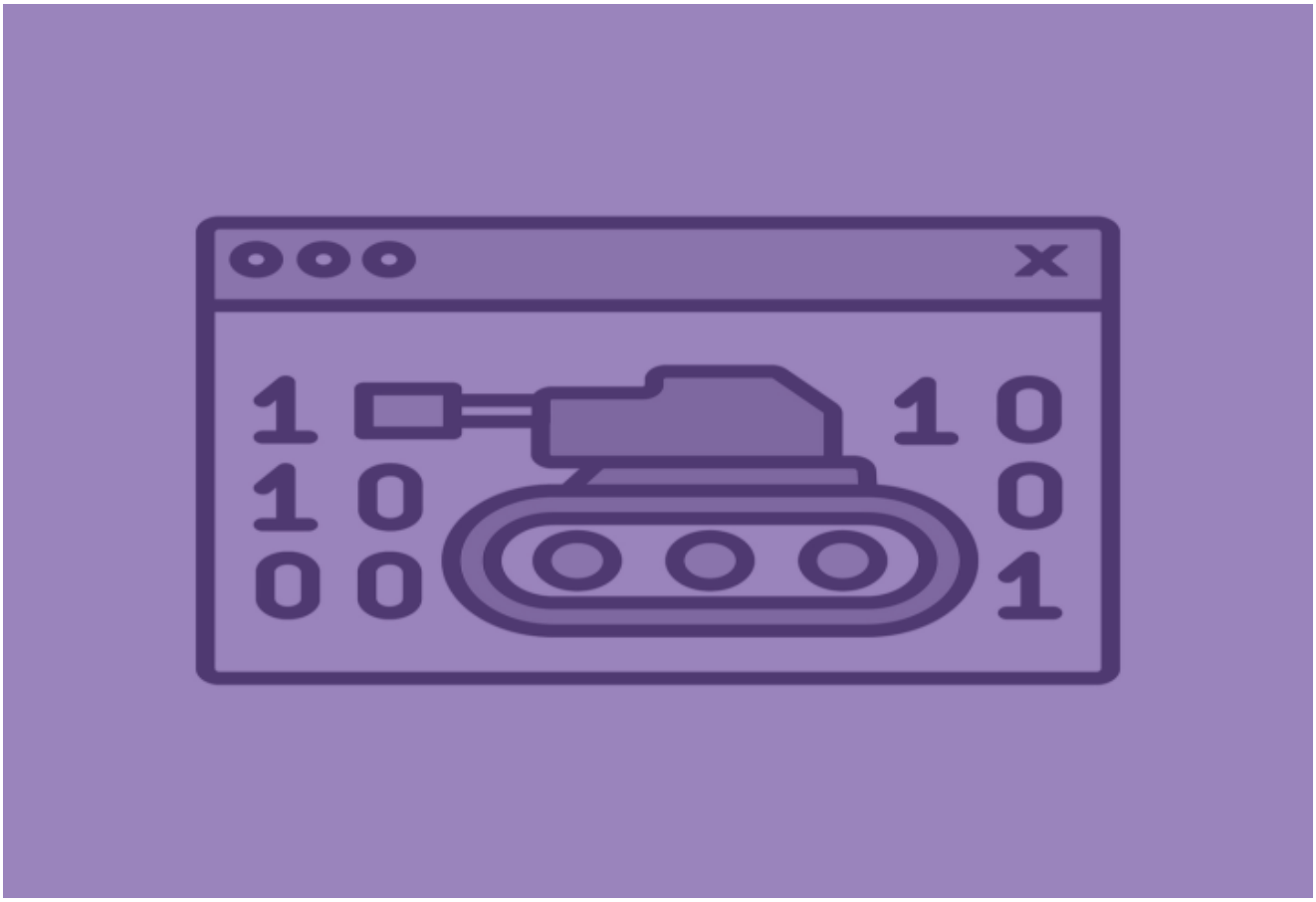
A Closer Look at the Russian Actors Targeting Organizations in Ukraine

lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/

March 3, 2022



In the context of the ongoing war between Russia and Ukraine, we have reviewed the cyberattacks against the Ukrainian organizations that occurred in January and February 2022. We have already provided a detailed analysis of the WhisperGate wiper here.

The Russian APT group Gamaredon (Primitive Bear, ACTINIUM) was attributed to the Russian Federal Security Service (FSB) and was identified by Unit 42 researchers [1] and Microsoft [2] targeting Ukrainian organizations in the last few months. Unit 42 collected three significant clusters of infrastructure (malicious domains, IP addresses, and malware samples).

The first cluster represents the Gamaredon downloader infrastructure. The threat actor deployed the UltraVNC software to connect back to a remote system (reverse tunnel). The second cluster contains C2 domains associated with Gamaredon's file stealer tool. The last cluster serves as the C2 infrastructure for a custom RAT called Pteranodon. We recommend blocking the IoCs reported by Unit 42 [3] [4].

An example of a lure document used by Gamaredon in the past is displayed in figure 1.


World Health Organization

COVID-19 Weekly Epidemiological Update

Edition 50, published 27 July 2021

In this edition:

- Global overview
- Special focus: Evaluations of the effectiveness of COVID-19 vaccines in real-world settings
- Special focus: Update on SARS-CoV-2 Variants of Interest and Variants of Concern
- WHO regional overviews
- Key weekly updates

Global overview

Data as of 25 July 2021

The global number of new cases reported last week (19-25 July 2021) was over 3.8 million, an 8% increase as compared to the previous week (Figure 1); an average of around 540 000 cases were reported each day over the past week as compared to 490 000 cases reported daily the week before. This trend is largely attributed to substantial increases in the Americas and Western Pacific Regions. The number of deaths reported this week increased sharply with over 69 000 deaths, a 21% increase when compared to the

Figure 1 (Source: Microsoft)

After the WhisperGate attacks that occurred in January 2022, several cybersecurity companies reported about a new wiper called HermeticWiper [5] [6] [7]. Before deploying the wiper, multiple DDoS attacks took place against Ukrainian organizations that were attributed to Russia's Main Intelligence Directorate (GRU).

The wiper was signed with a certificate issued to a Cyprus-based company called Hermetica Digital Ltd. Legitimate drivers from a tool called EaseUS Partition Master were utilized to corrupt the MBR (Master Boot Record) and MFT (Master File Table) for every physical drive. After a system reboot, the user is presented with the following screen:

Figure 2 (Source: Unit 42)

CISA also issued an alert regarding the WhisperGate and HermeticWiper wipers [8]. We recommend implementing the mitigation techniques presented in the alert to prevent similar attacks.

UAC-0056 (Lorec53) is another threat group that recently attacked organizations in Ukraine [9]. The infection vector is a spear-phishing email with a document attached containing three embedded objects. The malicious document's purpose is to write a JavaScript file that uses PowerShell to download a payload known as SaintBot (downloader) and OutSteel (document stealer). The malicious document used in this campaign is displayed below:

Figure 3

ESET researchers documented a new wiper called IsaacWiper, and a worm that spreads HermeticWiper in the LAN called HermeticWizard [10]. HermeticWiper is spread across a local network via WMI and SMB. IsaacWiper wipes the first 0x10000 bytes of each physical disk using the ISAAC pseudorandom generator and all files on logical drives with random bytes generated by the same generator. A timeline of the events is shown below:

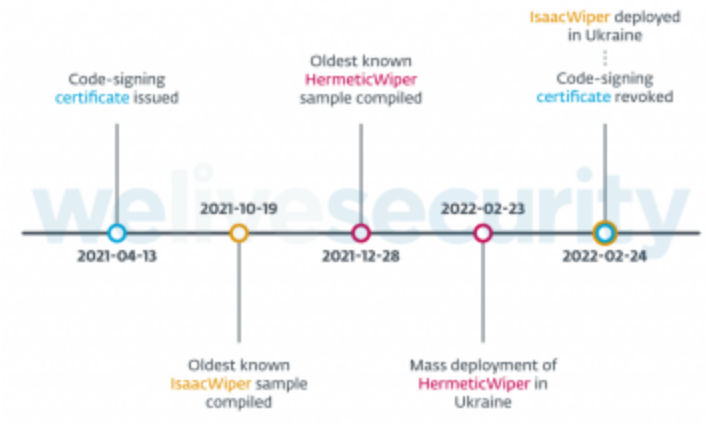


Figure 4 (Source: ESET)

Any Ukraine-based company for the next 6 months can get entirely free access to SecurityScorecard's enterprise license to protect themselves from malware resilience in light of ongoing cyber-attacks. We are also providing them with free access to SecurityScorecard forensics remediation team to deal with ransomware issues or to recover from any outage. Simply email Ukraine@securityscorecard.io.

References:

[1] https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/

[2] https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

[3] https://github.com/pan-unit42/iocs/blob/master/Gamaredon/Gamaredon_IoCs_JAN2022.txt

[4] https://github.com/pan-unit42/iocs/blob/master/Gamaredon/2022_02_Gamaredon_UPDATE.txt

[5] https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/

[6] https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[7] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

[8] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

[9] https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

[10] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/