# A deeper look at hacking groups and malware targeting Ukraine

⋮ 4/27/2022

Ukraine's main cybersecurity incident response team released a list on Friday of the five most persistent hacking groups and malware families attacking Ukraine's critical infrastructure.

According to the Computer Emergency Response Team of Ukraine (CERT-UA), the country has recorded 802 cyberattacks since Russia invaded the country earlier this year. That compares to just 362 documented attacks during the same time last year, CERT-UA said. Here are the groups and malware behind some of the biggest attacks:

## Armageddon/Garmaredon

**Who:** A threat actor notorious for targeting Ukraine since 2014 and backed by the Russian Federal Security Service (FSB). Prior to 2022, the Security Service of Ukraine attributed around 5,000 cyberattacks to Armageddon and were able to identify five members of the group and trace the malware to Russian hacking platforms. The group has used a number of tactics over the years including Outlook macros, EvilGnome backdoor, planted malware, and exposed vulnerabilities. Despite Ukrainian efforts to thwart the group over the years, Armageddon has remained aggressive.

**What:** In April, CERT-UA attributed a number of phishing emails to Armageddon which were sent to Ukrainian organizations and other European government agencies. The emails lured recipients by using the subject line, "Information on war criminals of the Russian Federation," which provided a downloadable file. When the file was opened, a PowerShell script would run and infect the device.

https://youtu.be/Rci5xiyMv7k

In March a similar phishing email was sent to Latvian government officials with a file containing war information which allowed the malware to download. Most recently, on April 20, the group was linked to new variants of the "Backdoor.Pterodo" malware payload. Armageddon has used this payload in the past, however, by constantly creating new variants they are able to quickly shift to a new one after the previous one is detected and blocked. Although their tactics are not the most complex, their ability to remain persistent in efforts against Ukraine has made them a notable threat.

## UNC1151

**Who:** According to research published by Mandiant, UNC1151 is a Belarus-aligned hacking group who has been active since 2016. The group has previously targeted government agencies and private organizations in Ukraine, Lithuania, Latvia, Poland, and Germany — also attacking Belarusian dissidents

and journalists. Historically, UNC1151 has stolen victim credentials through registered credential theft domains that spoof legitimate websites. UNC1151 has also been linked to the Ghostwriter campaign based on research that suggests UNC1151 provided them with technical support and findings that show similarities in their narratives. Due to the fact that the group has never targeted Russia and based on the relationship between Belarus and Russia, UNC1151 has been tied to Russian operations.

**What:** Since Russia invaded Ukraine the group has remained aggressive through a variety of attacks. In January the group was linked to the defacement of multiple Ukrainian government websites which displayed a message claiming that personal data was made public. On February 25, CERT-UA warned the public of spearphishing campaigns targeting the email and facebook accounts of Ukrainian military personnel. The group was able to gain access to messages and were able to use the contacts of the accounts to send out more emails. On March 7, CERT-UA found the state organizations of Ukraine had devices infected with MicroBackdoor — a malicious program executed by UNC1151.

## APT28

**Who:** APT28 (also referred to as Fancy Bear) is backed by Russia's military intelligence service (GRU). According to Mandiant research, the group has conducted cyberespionage operations that align with the interests of the Russian government since 2007, however, the government ties were not confirmed until December, 2016 after an analysis by the Department of Homeland Security (DHS) and the FBI. ATP28 has been involved in a number of cyberattacks in which they have stolen highly sensitive information including; the conflict in Syria, NATO-Ukraine relations, the European Union refugee and migrant crisis, the 2016 Olympics and Paralympics Russian athlete doping scandal, public accusations regarding Russian state-sponsored hacking, and the 2016 U.S. presidential election, according to a report by Mandiant.

**What:** ATP28 was linked to the cyberattack on US satellite communications provider Viasat. The attackers gained access to Viasat's KA-SAT network in Ukraine on February 24, leaving many Ukrainians without internet access. Although ATP28's involvement in the attack has not been confirmed, SentinelOne has alluded to their involvement based on the similarities between the AcidRain malware used in the Viasat attack and a VPNFilter malware used in the 2018 disruption of hundreds of thousands of routers which the FBI confirmed. On April 6, Microsoft obtained a court order granting the company permission to take control of seven domains used by APT28 to conduct their attacks.

## AgentTesla/XLoader

**Who:** Russian hacktivists and threat actors everywhere have been using the AgentTesla and XLoader malwares for some time, according to Check Point Research. AgentTesla has been around since 2014, according to security firm TitanHQ, and is used as a program to steal passwords. It has grown in popularity as customers can pay subscription fees ranging from $15 to $69. XLoader is another malware that was rebranded in 2020 from the previous name, Formbook. XLoader targets Windows and Mac devices through phishing emails and can collect passwords and screenshots, log keystrokes, and plant malicious files for a fee of $49 on the dark web.

**What:** On March 9, CERT-UA released findings showing a mass-distributed malicious email thread that used the topic line, “letter of approval of cash security,” which was sent to a variety of Ukrainian state organizations. The email contained a file attachment which downloaded and ran the XLoader malware. Once infected, authentication data from the device was collected and sent back to the hackers. Other phishing campaigns have been linked to AgentTesla including emails sent to Ukrainian citizens containing files with the IcedID malware which operates as a banking trojan to steal credentials.

## Pandora hVNC, RemoteUtilities, GrimPlant, GraphSteel

**Who:** Russian hacktivists and cyber spies use GrimPlant and GraphSteel which function as downloaders and droppers and fall under the umbrella term “Elephant Framework” — tools that are written in the same language and are used to target government organizations through phishing attacks. Threat analysis firm, Intezer, details this framework and provides an in-depth analysis of the malwares. GrimPlant is not overly sophisticated and grants attackers remote control of PowerShell commands, while GraphSteel is used to exfiltrate sensitive data.

**What:** On March 11, CERT-UA revealed that “coordinating entities” had received emails regarding instructions to increase security protocol. The email contained a link which provided a “critical updates” download through a 60MB file. After further investigation, they found that the file prompted a chain of other downloads including the GrimPlant and GraphSteel backdoors. Hackers were then able to steal sensitive information.

On March 28, CERT-UA disclosed another phishing campaign that planted GrimPlant and GraphSteel on the devices of government officials using the subject “Wage arrears.” The attached document contained accurate information, however, the file also downloaded a program that ran both GrimPlant and GraphSteel. CERT-UA released a statement earlier this month alerting the public of the latest phishing email which downloaded GrimPlant and GraphSteel through an attachment labeled, “Aid request COVID-19-04_5_22.xls.”