Webinar on cyberattacks in Ukraine – summary and Q&A

securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/

Authors

Expert GReAT

About the webinar

On March 10, 2022 Kaspersky's Global Research and Analysis Team (GReAT) shared their insights into the current (and past) cyberattacks in Ukraine. In this post we address the questions that we did not have the time to answer and provide the Indicators of Compromise (IoCs) that can help you defend against the identified threats. You can watch the full recording of the webinar here: 'A look at current cyberattacks in Ukraine'

The webinar included an historical overview of attacks on Ukraine; and an overview of current cyber-activity in the country, which comprises known APT activity, unknown parties carrying out DDoS attacks and leveraging commodity RATs, hacktivism, activities by cybercriminals and unattributed attacks.

In the webcast, we also provided an analysis of attacks identified using Kaspersky's honeypot network in Ukraine; as well as an analysis of the APT attacks by Gamaredon, Cyclops Blink, Hades/Sandworm and unknown groups, using commodity malware such as PandoraBlade. We also looked into different wipers that have been used against organizations in Ukraine, including HermeticWiper, WhisperGate, IsaacWiper and HermeticRansom. We also covered unknown and unattributed attacks and hacktivist activity taking place in the same timeframe.

We assess that the number of cyber attacks in Ukraine will increase during the next six months. While most of the current attacks are of low complexity – such as DDoS or attacks using commodity and low-quality tools – more sophisticated attacks exist also, and more are expected to come. Current complex activities include the employment of HermeticWiper, which stands out due to its sophistication, as well as the Viasat 'cyber event' – the partial network outage that impacted internet service for fixed broadband customers in Ukraine and elsewhere on the European KA-SAT network that affected over 30,000 plus terminals in Europe.

Currently, we assess that the risk of the cyber component of this conflict spilling over to Europe is medium-high.

We advise organizations to:

- Take typical measures against DDoS attacks, ransomware and destructive malware, phishing, targeted attacks, supply-chain attacks and firmware attacks
- Make sure that any and all internet-facing systems are up-to-date with all the latest patches installed
- Install security software on endpoints
- Set up extensive logging that will allow defenders to be alerted about suspicious events

- Establish strict application white-listing on all machines
- Actively hunt for attackers inside the company's internal network
- Integrate Threat Intelligence into SOC, EDR and leverage IOCs, YARA, Suricata and Sigma rules. We would also refer you to Kaspersky's Threat Intelligence Resource Hub, which currently provides free access to independent, continuously updated and globally-sourced information on ongoing cyberattacks and threats.

Q&A

Due to time limitations, we could not address all questions during the webinar, so here are our answers for the remaining questions we received in the live session:

Q: What are the chances that we'll see attacks using enterprise resources to launch attacks?

A: Depending on the nature of the attack, actors may not differentiate between home, SMB and enterprise systems. For example, infected IoT and network devices such as IP-cameras may be used by anyone, and may be infected and abused by attackers to launch attacks such as DDoS attacks. Attackers will use and abuse any resources they require in order to conduct their attack. If this includes enterprise resources then they will be included in the attackers scope.

Q: Currently we have seen massive connection outbreaks in many different services over TOR-exits located in the German region. Does this provide a "true" picture of the threat landscape, since many attackers seem to be from – in this instance – Germany but might originate from regions that are very interested in causing damage to Europe or Ukraine specifically right now?

A: We commonly take TOR and other anonymizing services into account when it comes to the origin of attacks. Not all attacks, for example on our honeypot infrastructure, are easily possible through TOR due to enforced policies on exit-nodes.

Q: I'm wondering what you can say about the attacks on Russian targets, both from "hacktivists" and others? Can you help us separate the hype and exaggerations from attacks that are having a real impact?

A: We have seen several public "hack" announcements. Most of them don't include enough evidence to confirm a real hack; nor do we have the abilities or resources to verify most of them as they are very specific and "targeted".
The most important suggestion is to not blindly trust all messages, reports and claims – especially unverified content or if it's from unverified channels/accounts.

Q: We all know of REvil group activity and the Kaseya case. REvil members were arrested by the Russian FSB a few months ago. Do you believe that these people might be "employed" by the Kremlin to organize an attack against Ukraine? Or you

think it might be possible to determine if any attackers are former REvil members?

A: We don't have any insights into the employment of criminals or other threat actors; nor into plans and strategies of any government or related organizations. Our focus is on the technical aspects only, which is where our expertise and focus lies. The real world identity of criminals and other threat actors is the focus area of law enforcement and related agencies.

Q: How may this conflict between Russia and Ukraine affect financial operations? Are firewalls and antivirus tools enough to defend against a cyberattack that comes from Europe?

A: Financial transactions and other operations are handled through the networks of financial institutions. These are usually secured using many different methods. The origin (that is, region or country) is usually not the first question in regards to defense, but rather technical aspects and targets. Depending on that, particular methods and policies should be applied to protect against attacks.

Q: Do you have any current readings on attacks on NGOs?

A: Several investigations reveal that targets include NGOs – these are accessible through our Threat Intelligence Reporting Service.

Q: How can we use the Kaspersky honeypot and sandbox?

A: Our honeypots are not part of any Kaspersky products. They are dedicated systems where specific sensors are installed in order to monitor attacks. However, you may join our honeypot initiative (for details, email us at honeypots@kaspersky.com).
You may access and use the Kaspersky Sandbox within our Product & Service offerings: Kaspersky Sandbox and Kaspersky Threat Intelligence. File analysis can also be conducted through OpenTIP.

What follows is the list of IoCs we derived from our honeypot-sensors in Ukraine. These are the observed, most prominent and relevant attacking IP addresses.

Indicators of Compromise (IoCs)

IPs found attacking Ukraine honeypot assets
185[.]252[.]232[.]67
133[.]242[.]129[.]39
120[.]48[.]3[.]144
178[.]62[.]81[.]147
159[.]203[.]71[.]145
116[.]105[.]72[.]113
182[.]59[.]88[.]117
27[.]6[.]204[.]233

115[.]48[.]212[.]167
42[.]227[.]250[.]181
219[.]157[.]145[.]211
182[.]119[.]167[.]53
42[.]224[.]124[.]173
125[.]40[.]19[.]101
196[.]70[.]116[.]243
125[.]41[.]141[.]113
219[.]157[.]59[.]51
14[.]106[.]231[.]203
87[.]150[.]3[.]191
152[.]32[.]180[.]171
192[.]241[.]221[.]199
121[.]229[.]44[.]136
192[.]241[.]220[.]251
192[.]241[.]220[.]48
192[.]241[.]220[.]47
192[.]241[.]218[.]100
62[.]16[.]2[.]14
152[.]32[.]135[.]202
139[.]162[.]8[.]54

Hashes
ecce8845921a91854ab34bff2623151e IsaacWiper

d5d2c4ac6c724cd63b69ca054713e278 HermeticRansom

3f4a16b29f2f0532b7ce3e7656799125 HermeticWiper
84ba0197920fd3e2b7dfa719fee09d2f HermeticWiper
517d2b385b846d6ea13b75b8adceb061 HermeticWizard

5d5c99a08a7d927346ca2dafa7973fc1 WhisperGate
14c8482f302b5e81e3fa1b18a509289d WhisperGate
e61518ae9454a563b8f842286bbdb87b WhisperGate
3907c7fbd4148395284d8e6e3c1dba5d WhisperGate
e5071ccd626ad4ef8b0be7561c50f1ac WhisperGate
238bf5d26e338ca205b269ca4a9f57a8 WhisperGate

033fa3ae260e465da3d541bc138d2e1d WhiteBlackCrypt x32
4a6bec571521881b387b9de3d7b06aa0 WhiteBlackCrypt x32
072da4148add1d8ee1e691cb94b31737 WhiteBlackCrypt x32
99bd77ae4a287904c813960727046d80 WhiteBlackCrypt x32
b36e5c508efea796731d444c189b413c WhiteBlackCrypt x64

490d8cdaf68619f23a2e03f55fd9e33e Pandora hVNC
6942546805623a1648960ffdc91d1cff Pandora hVNC
c2cbd5caa9012e4878ff35c31cb2122f Pandora hVNC
02190c8c52bfafe4fa69b2972f867c1b Pandora hVNC

e34d6387d3ab063b0d926ac1fca8c4c4 MicroBackdoor spearphishing ZIP archive
2556a9e1d5e9874171f51620e5c5e09a MicroBackdoor CHM dropper
bc6932a0479045b2e60896567a37a36c MicroBackdoor JS dropper

More IOCs are available to customers of the Kaspersky Intelligence reporting service. Contact: intelreports@kaspersky.com

- APT
- Cyber weapon
- DDoS-attacks
- Hackers
- Targeted attacks

Authors

GReAT

Webinar on cyberattacks in Ukraine – summary and Q&A

Your email address will not be published. Required fields are marked *