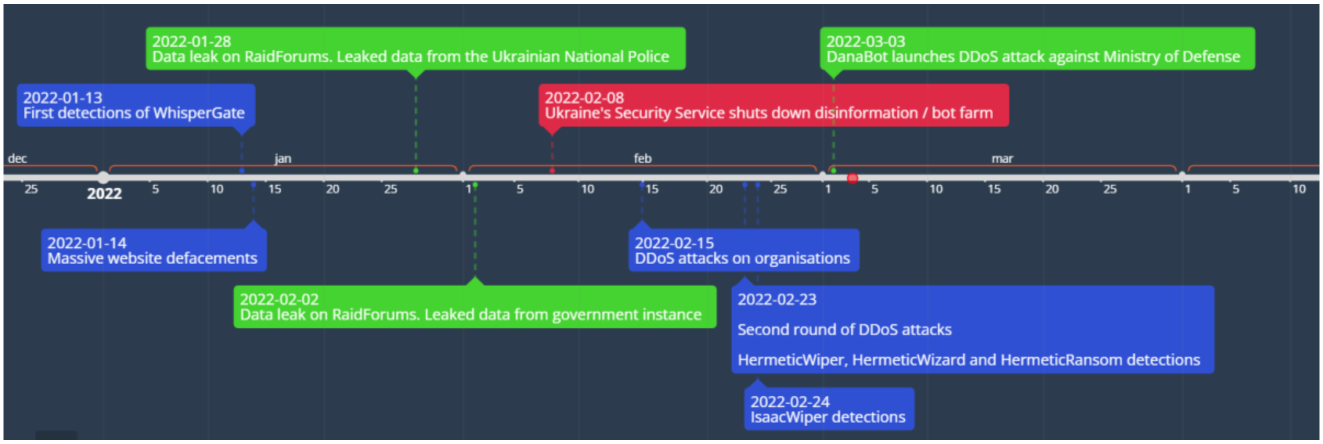
Threat Update – Ukraine & Russia war

blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/

February 24, 2022



Last updated on 2022-03-17/ 8am CET

2022-02-25: added key historical operation: Cyclops Blink
2022-03-02: added note on spillover and recommendation
2022-03-03: added further information on attacks, updated recommendations
2022-03-07: added info on HermeticRansom decrypter and our mission statement
2022-03-15: added info on CaddyWiper and fake AV update phishing campaign used to drop Cobalt Strike
2022-03-17: added info on the removal of a deepfake video of Ukrainian President Zelenskyy
2022-04-22: added info on Industroyer2 and generic scams

Introduction & background

In this report, NVISO CTI describes the cyber threat landscape of Ukraine and by extension the current situation. Understanding the threat landscape of a country, however, requires an understanding of its geography first and foremost.

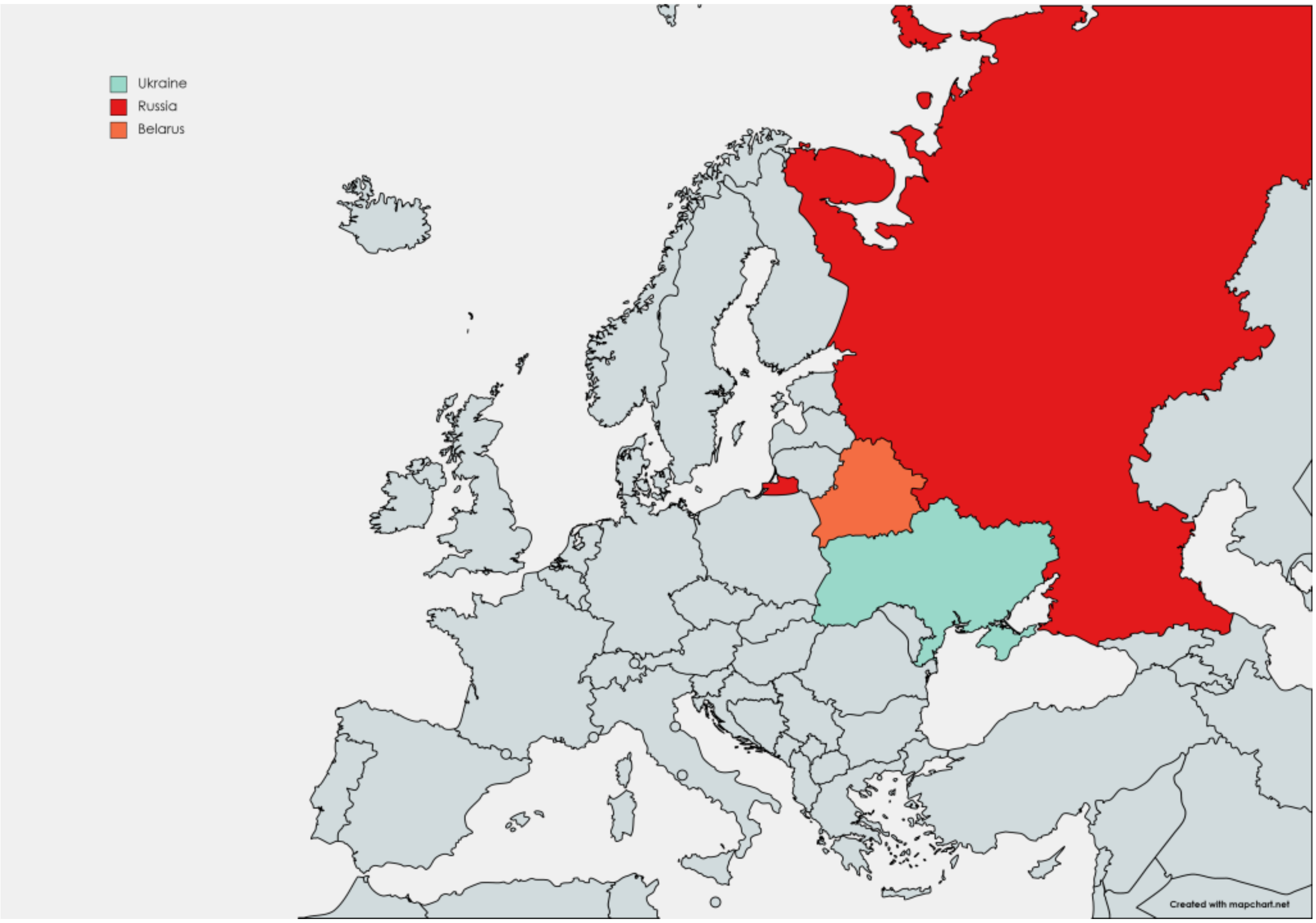


Figure 1 – Map of Ukraine and bordering countries

Ukraine, bordered by Russia as well as Belarus has seen its share of hostile intelligence operations and near declarations of war. The annexation of Crimea, a peninsula that was officially recognized as part of Ukraine, was annexed by Russia early 2014: this was one of the first and larger “turning points” in modern history.

More recently, in 2018, Russia took it one step further after several years of absorbing Crimea as part of Russia, by installing a border fence to separate Crimea from Ukraine.[1]

In 2020, during several Belarusian protests targeted at Belarus’ current president Lukashenko, Ukraine recalled its ambassador to assess the prospects, or lack thereof, regarding their bilateral relationship.[2] Tensions increased further, and in 2021, Ukraine joined the European Union (EU) in imposing sanctions on Belarusian officials.[3]

In 2022, this tension materialized by Russia actively performing military operations on Ukraine’s border, and in February, the bombardment of several strategic sites in Ukraine.[4]

Historical Cyber Attacks

As mentioned, to understand a country, one needs to understand its geography and geopolitical strategy. A remarkable initiative from Ukraine is their intent on joining NATO as well as becoming an official member of the EU. These initiatives are likely the trigger for the recent turmoil, in December 2021, where Russia became openly bold, more aggressive and with ultimate goal as explained by Putin: to unify or absorb Ukraine back into Russia. In that same month, Putin presented to the United States and NATO a list of security demands, including Ukraine not ever joining NATO.[5] The intent of Putin is, as always, likely to have multiple dimensions.

This report will describe further history of cyber-attacks on Ukraine, a timeline of current relevant events in the cyberspace, and finally some recommendations to ensure protection in case of "cyberwar spillover" as was in the case of NotPetya in 2017.

As mentioned in the introduction, Ukraine has seen its fair share of targeted cyber-attacks. The table below captures significant Advanced Persistent Threat (APT) campaigns / attacks against Ukraine specifically.

Attack Group	Attack Purpose	Malware / Toolset	Date
Black Energy (aka Sandworm)	Disrupt / Destroy	KillDisk / Black Energy	2015
Black Energy	Disrupt / Destroy	Industroyer	2016
Black Energy	Disrupt / Destroy	NotPetya	2017
Grey Energy (Black Energy successor)	Espionage	GreyEnergy	2018
Black Energy	Espionage	VPNFilter	2018
Unknown, likely DEV-0586 (aka GhostWriter)	Disrupt / Destroy	WhisperGate	2022
Unknown, likely DEV-0586	Disrupt / Destroy	HermeticWiper	2022
Black Energy	Disrupt / Destroy	Cyclops Blink	2022*
Black Energy	Disrupt / Destroy	Industroyer 2	2022

Table 1 – Key historic attacks

Other attacks have taken place, both cyber-espionage and cyber-criminal, but the threat group "Black Energy" is by far the most prolific in targeting Ukrainian businesses and governmental institutions.

Black Energy and its successors and sub-units are attributed to Russia's Intelligence Directorate or GRU (now known as the "Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation"). The GRU is Russia's largest foreign intelligence agency and has therefore access to a vast number of resources, capabilities, and certain freedom to execute more risky intelligence operations. Note that APT28, also known as Sofacy and "Fancy Bear" is also part of the GRU but resides in a different unit.[6]

Specifically looking at the attacks targeting Ukraine in 2022, a timeline can be observed below:

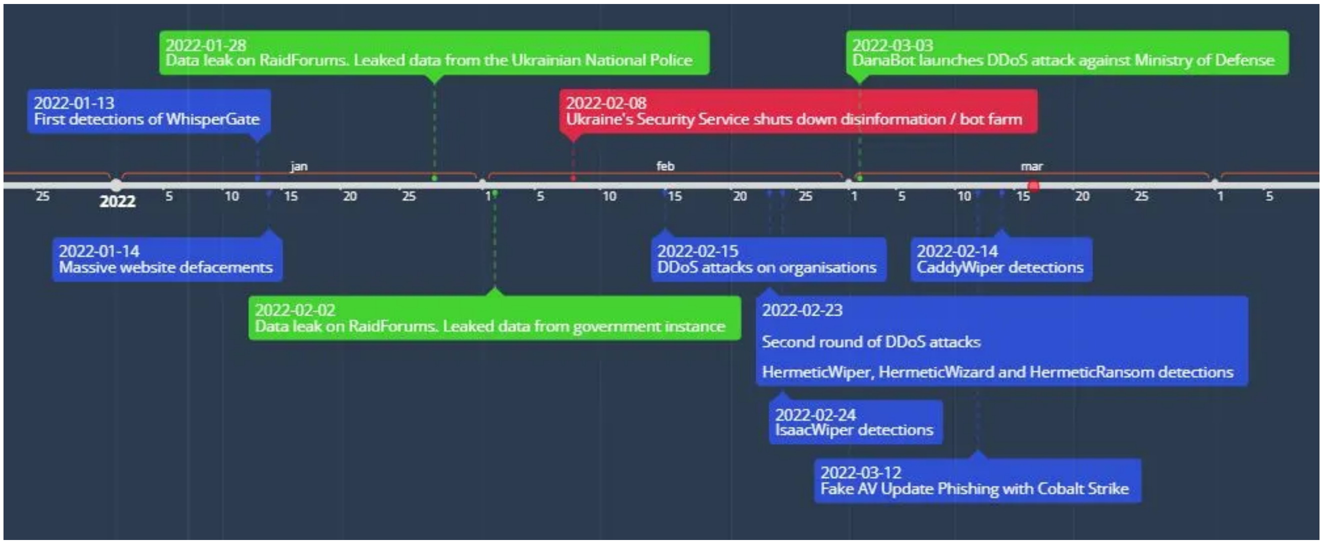


Figure 2 – Ukraine 2022 timeline

Highlighted in blue on the timeline, are suspected attack campaigns by nation states, likely either Russia or Belarus. Highlighted in green are suspected attack campaigns by cybercriminal actors in favor of Russia.

Highlighted in red on the timeline, is an intelligence counteraction by Ukraine's Security Service, known as the SSU or SBU. The SSU can be seen as Ukraine's main government agency protecting national interests, but also has a focus on counterintelligence operations. On February 8th 2022, the SSU shut down a Russian "trolling farm" that had as sole intent to distributed "fake news" to spread panic. The bots also published false information about bomb threats at various facilities.[7]

NVISO CTI assesses with moderate confidence Russia and Belarus will continue destructive or espionage operations on Ukraine's infrastructure and those who support Ukraine whether it be logistically, operationally, or otherwise publicly.

As of yet, spillover of these operations has not been observed in Belgium by organizations such as the Centre for Cyber security Belgium (CCB).[8] The UK's National Cyber Security Centre (NCSC) in turn advices "organizations to act following Russia's attack on Ukraine" and provides further guidance.[9]

Key historical operations

In a quick overview of the aforementioned pre-2022 attacks, the following are some of the key elements that contributed to their success, and which are important to take into account when building a detection strategy:

- The attack on the Ukrainian power grid was prefaced with a phishing attack against a number of energy distribution companies. The phishing email contained a Word document that, when Macros were enabled, dropped the **Black Energy** malware to disk. Using this malware the adversaries obtained credentials to access VPN and remote support systems that allowed them to open circuit breakers remotely. In order to prevent the operators from closing the circuit breakers remotely again, a wiper was deployed on the operator machines.
- **NotPetya** was initially deployed via a supply chain attack on Linkos Group. The NotPetya ransomware caused worldwide damages due to its highly effective spreading mechanism combining the EternalBlue (MS17-010) vulnerability, credential dumping from infected systems and PsExec for lateral movement.
- **GreyEnergy** and its accompanying toolset was typically prefaced with a phishing attack, containing malicious documents that would deploy “GreyEnergy mini”, a first-stage backdoor. A second point of entry was via vulnerable public-facing web services that are connected to the organization’s internal network. The attacker’s toolset also contained Nmap and Mimikatz for discovery and lateral movement.
- **VPNFilter** is a multi-stage, modular platform with versatile capabilities to perform a wide range of operations, primarily espionage but also destructive attacks. The malware installs itself on network devices such as routers and NAS, and can only be completely removed with a full reinstallation. Its current preface or infection vector is unknown, but it is assumed they target vulnerabilities in these network devices as an initial entrypoint. VPNFilter was a broad-targeting malware and campaign, but was responsible for multiple large-scale attacks that targeted devices in Ukraine.
- **Cyclops Blink** is the “replacement framework” of VPNFilter and has been active since at least June 2019, fourteen months after VPNFilter was disrupted. Just like VPNFilter, Cyclops Blink is broad-targeting, but might be targeting devices in Ukraine specifically. As opposed to VPNFilter, Cyclops Blink is only known to target WatchGuard network devices at this point in time. Its preface is WatchGuard devices that expose the remote management interface to the internet / external access.

Current Cyber Attacks (2022)

WhisperGate

Starting on January 13th, 2022, several Ukrainian organizations were hit with a destructive malware now known as WhisperGate. The malware was designed to wipe the Master Boot Record, MBR, and proceed to corrupt the files on disk, destroying all traces of the data.

Initial execution of the first stage was completed using the Python tool Impacket, this being widely used for lateral movement and execution. Initial access to run Impacket is believed to have occurred via insecure remote access channels and using stolen/harvested credentials.

Once the MBR is wiped, a fake ransom screen is displayed. This is just to distract while the third stage is downloaded from a Discord link. Then all data is overwritten on disk.

Massive web defacements

Between the 13th and 14th of January, a coordinated web defacement on several governmental institutions of Ukraine took place – all websites and their content were wiped and replaced with a statement[10]:

Ukrainian! All your personal data has been sent to a public network. All data on your computer is destroyed and cannot be recovered. All information about you stab (public, fairy tale and wait for the worst. It is for you for your past, the future and the future. For Volhynia, OUN UPA, Galicia, Poland and historical areas.[10]
The SSU assesses the attack happened via a vulnerable Content Management System (CMS), and that “in total more than 70 state websites were attacked, 10 of which were subjected to unauthorized interference”.[11]

DDOS attacks on organizations

On February 15th, Ukraine’s Ministry of Defence (MoD) tweeted[11] that “*The MOU website probably suffered a DDoS attack: an excessive number of requests per second was recorded.*

Technical works on restoration of regular functioning are carried out.”

The attack was carried out on the MoD itself and the Armed Forces of Ukraine, but also on two national banks, which had as result that internet banking was not available for several hours.

DDoS attacks & the “HermeticBunch”

On February 23rd, there were two newly reported cyber events: DDoS attacks and an attack campaign we could name “HermeticBunch”.

NetBlock, an internet observatory, noted the DDoS attacks on February 23rd around 4pm CET. The attacks were impacting the websites of Ukraine’s MoD, Ministry of Foreign Affairs (MoFA) and other governmental institutions.[12]

ESET initially reported[13] detecting a new wiper malware used in Ukraine. Their telemetry indicated the malware was installed on several hundreds of machines with first instances discovered around 4pm CET. Symantec posted an analysis[14] the next day corroborating

ESET's findings, and providing more insight into the attack: ransomware was initially deployed, as a smokescreen, to hide the data-wiping malware that was effectively used to launch attacks against Ukrainian organizations.

ESET reported on March 1st [15] that multiple Ukrainian organizations were targeted by an attack campaign comprising:

- **HermeticWiper**, a data-wiping malware;
- **HermeticWizard**, spreads HermeticWiper over the network (using WMI & SMB);
- **HermeticRansom**: likely a ransomware smokescreen for HermeticWiper.

These components indicate an organized attack campaign with as main purpose destruction of data. While the spreader malware, HermeticWizard, is worrisome, it can be blocked by implementing the advice from the Recommendations section below.

Note that AVAST Threat Labs has created a decrypter for files encrypted with HermeticRansom. [17]

IsaacWiper

IsaacWiper was first detected by ESET on February 24th [18], and was leveraged again for destructive attacks against the Ukrainian government. The wiper is less sophisticated than HermeticWiper, but not less effective.

DanaBot

DanaBot is a Malware-as-a-Service (MaaS) platform where threat actors ("affiliates") can purchase access to the underlying DanaBot platform. Zscaler reported on March 2nd [19] to have identified a threat actor targeting Ukraine's Ministry of Defense (MoD) using DanaBot's download and execute module.

Fake AV Update leading to Cobalt Strike

Phishing emails impersonating the Ukrainian government were seen during a campaign to deliver Cobalt Strike beacons and Go backdoors on the 12th of March. Reported by the Ukraine CERT (CERT-UA) [20], the emails were themed as "critical security updates" and contained links to download a fake AV update package. The 60 MB file was actually a downloader which then connected to a Discord CDN to download a file called one.exe. This being a Cobalt Strike beacon. It also downloads a Go dropper that executes and pulls down two more Go payloads, GraphSteel and GrimPlant. Both of these being backdoors.

CaddyWiper

CaddyWiper was discovered by ESET on March 14th [21] and it is the 4th data wiping malware to be used against Ukraine. It was deployed in the attacks via GPO, this showing that the threat actor already had a major foothold in the environment. It also has functions to cause it to not wipe Domain Controllers, this being the foothold the attackers would lose if destroyed.

Deepfake video

On 16 Mar 2022, Facebook removed a deepfake video of Ukrainian President Zelenskyy asking Ukrainian troops to surrender. The video initially appeared on the compromised website of news channel, Ukraine 24, before it was spread to other compromised websites, such as Segodnya. In response, Zelenskyy published a video of his own, asking Russian troops to surrender instead. [22]

Industroyer2

On 12 Apr 2022, Eset reported on Industroyer2. ESET researchers collaborated with CERT-UA to analyze the attack against an Ukrainian energy company. The destructive actions were scheduled for 2022-04-08 but artifacts suggest that the attack had been planned for at least two weeks
The attack used ICS-capable malware and regular disk wipers for Windows, Linux and Solaris operating systems. In addition to Industroyer2, Sandworm used several destructive malware families including CaddyWiper, ORCSHRED, SOLOSHRED and AWFULSHRED. Eset had first discovered CaddyWiper on 2022-03-14 when it was used against a Ukrainian bank (see also above).[23]

Note on scammers

Now that a lot of organizations are offering aid to Ukraine, it’s more than ever important to validate the source of the aid offering. This can translate into either:

- Scammers pretending to be humanitarian or aid organizations;
- Scammers pretending to be law enforcement or others offering direct help to Ukrainian citizens.

It’s highly recommended to always perform proper vetting of those offering aid, asking for aid or otherwise request for compensation. Unfortunately, even in these times, scammers will try to take advantage to fill their pockets. As a side note, CERT-UA had also reported on scammers impersonating the CIA.[24]

Recommendations

Based on the collective knowledge on adversary groups acting in the interests of the Russian state and the current ongoing events, it is important for organizations to use this momentum to implement a number of critical defenses and harden their overall environment.

Each organization should review their own threat model with regards to the potential threats facing them, however, the below is a good overview to improve your security posture against a variety of (destructive) attacks.

Your external exposure

It is advised to perform a periodic assessment on your external perimeter to identify what systems and services are exposed to the internet. Given the cloud first approach many organizations are taking, it has become less straight forward of identifying what services your organization is exposing to the internet, however, attack surface monitoring solutions can provide an answer to that by looking beyond the scope of your organization IP range.

For all identified services exposed to the internet, ensure:

- Validate these are actually required to be exposed to the internet;
- They are up to date with the latest security patches.

For all services for which authentication is required (e.g. VPN solutions, access to your client portal, etc.) it is strongly advised to enforce Multi Factor Authentication (MFA).

Abuse of (privileged) accounts

Once inside your network, threat actors are very frequently seen going after privileged accounts (can be local admin accounts or privileged domain accounts).

In terms of local admin accounts, it is important to ensure these accounts have strong passwords assigned to them, and that no password re-use is performed across different hosts. Each local administrator account as such should have a unique strong password assigned to it. Various tools exist that can support in the automated configuration of these unique passwords for each of these accounts. A good example that can be used is Microsoft’s Local Administrator Password Solution (LAPS).

For privileged domain accounts (e.g. a specific server administrator, the domain administrator or the accounts that have access to your security tooling such as EDR’s), it is strongly advised to implement MFA.

Lateral Movement

Once the adversary has obtained access into the environment, they’ll move laterally to eventually gain access to the critical assets of the organization. The following are a number of key recommendations to help in the prevention of successful lateral movement:

- Implement network segmentation and restrict the communication flows between segments only to the ones required for business reasons;

- Configure host-based firewalls to restrict inbound connections (depending on your business, a few questions to ask could be: should I allow inbound SMB on my workstations, should an inbound RDP connection be possible from another workstation, etc.)
- Harden RDP configuration by:

  Denying server or Domain Administrator accounts from authenticating to workstations;
  Enforcing Multi-Factor Authentication (MFA);
  Where possible, use Remote Credential Guard or Restricted Admin.

In addition to the implementation of key hardening principles, the lateral movement phase of an attack is also an opportunity in which adversaries can be detected. Monitoring should be performed on workstation-to-workstation traffic and authentications, usage of RDP and WMI, as well as commonly used lateral movement tools such as PsExec, WinRM and PS Remoting.

Mandiant has additionally provided guidance on protecting against destructive attacks [20] (PDF).

Critical Assets

In several cases, the adversaries have been observed conducting destructive attacks. As a proactive measure, ensure offline backups of your critical assets (such as your Domain Controllers) are created regularly. A frequent overlooked aspect of a backup strategy is the restore tests. On a frequent basis, it should be verified that the backup can effectively be restored to a known good state.

On a final note, given that the majority of systems are virtualized these days, it’s important to ensure the access to your back-end virtualization environment is properly segmented and secured.

Phishing Prevention

A number of the observed attacks that Russia linked threat actors have executed were initiated via a phishing campaign with the goal of stealing user credentials or executing malware on the systems. As such, it is important to verify the hardening settings of your mail infrastructure. Some key elements to take into account are:

- Enable MFA on all mailboxes;
- Disable legacy protocols that do not understand MFA and as such would allow an adversary to bypass this security control;
- Perform sandbox execution of all attachments received via mail;
- Enable safe links (various mail security provides provide this option) to have the URL checked for phishing markers once the user clicks.

Additionally, it is frequently observed that the adversaries are attempting to have a user enable Macros in the malicious office documents they send. It is advised to review if all users within your environment use Office Macros and whether or not these can be disabled. If Macros are used for business reasons, consider only allowing signed Macros.

DDOS Mitigations

Depending on your organization's risk profile, there is the potential threat of a DDoS attack, especially following sanctions imposed on Russia in specific sectors. It is advised to investigate and implement DDoS mitigations on critical public-facing assets. Noteworthy is Google's Project Shield [19], which is "a free service that defends news, human rights and election monitoring sites from DDoS attacks". Google has recently expanded protection for Ukraine, and is already protecting more than 150 websites hosted in Ukraine.

Crisis & Incident Management

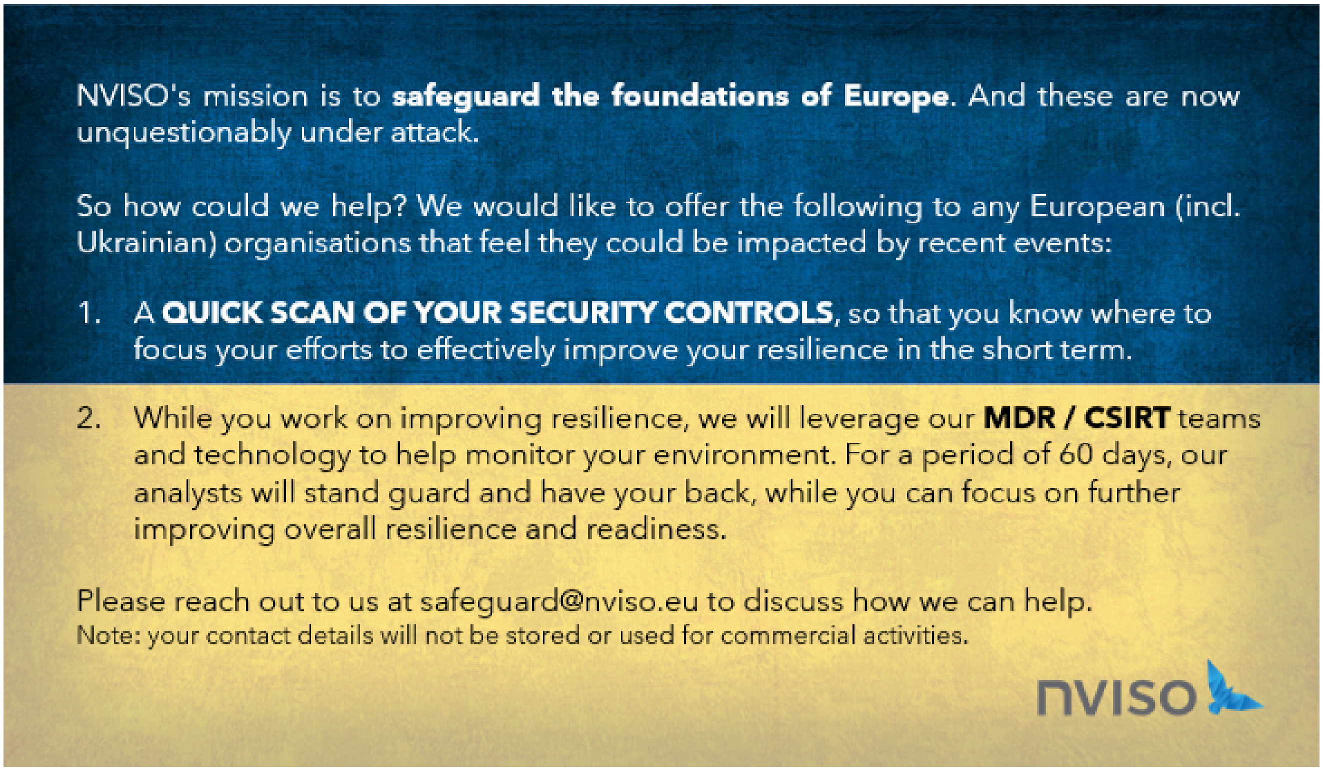
Tabletop exercises are a great way of measuring the crisis & incident management processes & procedures you currently have, and to identify any potential gaps that may be uncovered during a tabletop. Moreover, tabletops are cross-functional and can be used for both leadership, as well as anyone working with incidents on a day to day basis. The results of a tabletop exercise can ultimately be used as a platform to improve the current way of working, or to invest in new resources should there be a need.

About the authors

Bart Parys	Bart is a manager at NVISO where he mainly focuses on Threat Intelligence and Malware Analysis. As an experienced consumer, curator and creator of Threat Intelligence, Bart loves to and has written many TI reports on multiple levels such as strategic and operational across a wide variety of sectors and geographies.
Robert Nixon	Robert is a manager at NVISO where he specializes in Cyber Threat Intelligence at the tactical, organizational and strategic level. He also is an SME in automation, CTI infrastructure, malware analysis, DFIR, and SIEM integrations/use case development.
Michel Coene	Michel is a senior manager at NVISO where he is responsible for our CSIRT & TI services with a key focus on (and very much still enjoys hands on) incident response, digital forensics, malware analysis and threat intelligence.

Our goal is to provide fast, concise and actionable intelligence on critical cyber security incidents. Your comments and feedback are very important to us. Please do not hesitate to reach out to threatintel@nviso.eu.

About NVISO



NVISO's mission is to **safeguard the foundations of Europe**. And these are now unquestionably under attack.

So how could we help? We would like to offer the following to any European (incl. Ukrainian) organisations that feel they could be impacted by recent events:

1. A **QUICK SCAN OF YOUR SECURITY CONTROLS**, so that you know where to focus your efforts to effectively improve your resilience in the short term.
2. While you work on improving resilience, we will leverage our **MDR / CSIRT** teams and technology to help monitor your environment. For a period of 60 days, our analysts will stand guard and have your back, while you can focus on further improving overall resilience and readiness.

Please reach out to us at safeguard@nviso.eu to discuss how we can help.
Note: your contact details will not be stored or used for commercial activities.