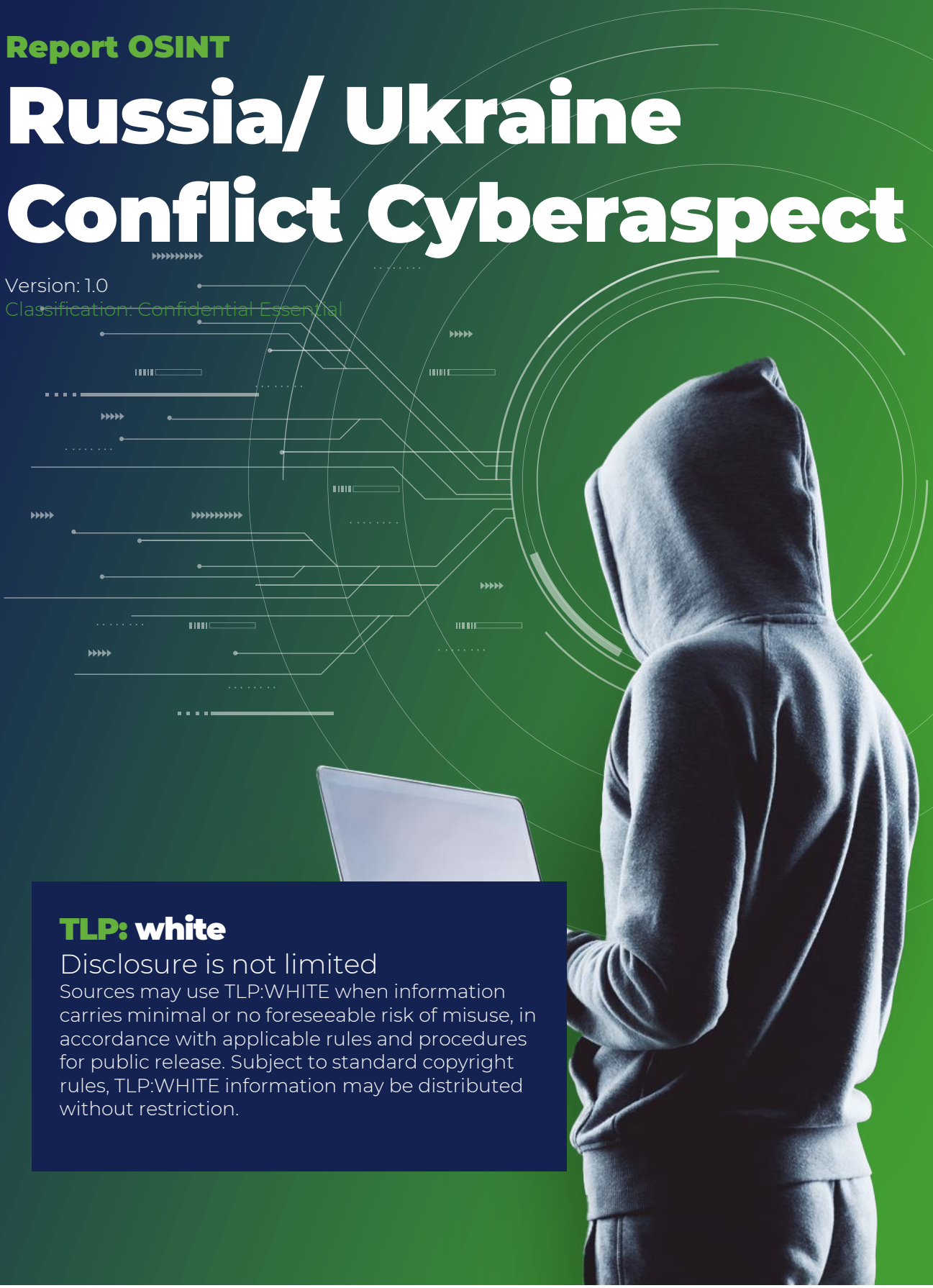
Report OSINT

Russia/ Ukraine Conflict Cyberaspect

Version: 1.0

Classification: Confidential Essential



TLP: white

Disclosure is not limited

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

TESORION

Fokkerstraat 4
3833 LD Leusden
The Netherlands
www.tesorion.com

Preface

Following the recent attacks affecting mainly Ukraine and the Baltic States, this document provides an OSINT scan on the cyber aspects of the Russia-Ukraine conflict.

For example, last month large numbers of infections were observed, related to the WhisperGate/Hermetic Wiper trojans, intended to make infected systems unusable, as well as the Cyclops Blink malware. The most commonly mentioned threat actor behind these malware attacks is the SandWorm APT group. This group was also responsible for previous large-scale malware attacks on Ukraine, such as NotPetya, which also caused a lot of damage in Western Europe.

With regard to the threat posed by the malware families and threat actors mentioned in this report, Tesorion is assuming on the one hand that infections will spread unintentionally to other countries, for example in Western Europe, and on the other hand that parties in this region will also be active.

There is also a risk of further escalation in which the Netherlands and other EU countries, possibly as a result of sanctions or other punitive measures, become the deliberate target of threat actors behind these malware families. For example, when the EU decides to exclude Russia and the SWIFT payment system.

The information in this report is derived from OSINT sources and public information published during the past month. The technical indicators such as IP addresses, malware hashes and Yara signatures can be used for the purpose of detecting and blocking malicious traffic.

The remainder of this report thus provides more information on the following topics:

- Malware Families & Threat Actors
- Indicators of Compromise
- Newsarticles & Security Advisories

Tesorion does not own the copyright for the technical information provided. This information originates from various IT Security companies and National CERTs.

Our Security Monitoring Services is closely monitoring the geopolitical conflict. The current situation is monitored through various threat intelligence feeds that are continuously updated. We make every effort to process this rapidly changing data. For those clients whom we are servicing with Immunity Services, Managed Firewall and other services, please note that the IOC's (Indicators of Compromise) are added to our services.

Author: *Tesorion Nederland B.V.*
Classification: *Public*
Published *2022*
Version *1.0*
:

Malware Families & Threat Actors

Malware Families
- BlackEnergy (Sandworm Tool 2015)
- Industroyer (Sandworm Tool 2016)
- NotPetya (Sandworm Tool 2017)
- WhisperGate (Wiper)
- HermeticWiper / Killdisk.NCV (Wiper)
- Cyclops Blink (Sandworm Tool)
- VPNFilter (Replaced by Cyclops Blink)
- Katana (DDoS Botnet)

Threat Actors
- Sandworm APT

Indicators of Compromise

Malware Hashes

1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 (unknown, wiper)
912342F1C840A42F6B74132F8A7C4FFE7D40FB77 (HermeticWiper/Killdisk.NCV)
61B25D11392172E587D8DA3045812A66C3385451 (HermeticWiper/Killdisk.NCV)
3F4A16B29F2F0532B7CE3E7656799125 (HermeticWiper/Killdisk.NCV)
5d5c99a08a7d927346ca2dafa7973fc1 (WhisperGate)
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 (WhisperGate)
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 (WhisperGate)
ff17ccd8c960594617107111fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6 (Cyclops Blink)
4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1 (Cyclops Blink)
50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86 (Cyclops Blink)
c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862 (Cyclops Blink)
82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf (Katana DDoS Botnet)
978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed (Katana DDoS Botnet)

IP Addresses

Katana Botnet Indicators of Compromise

- 5.182.211[.]5 on the port 60195 / http://5.182.211[.]5/rip.sh
    - Cyclops Blink Indicators of compromise

- 100.43.220[.]234
- 96.80.68[.]193
- 188.152.254[.]170
- 208.81.37[.]50
- 70.62.153[.]174
- 2.230.110[.]137
- 90.63.245[.]175
- 212.103.208[.]182
- 50.255.126[.]65
- 78.134.89[.]167
- 81.4.177[.]118

- 24.199.247[.]222
- 37.99.163[.]162
- 37.71.147[.]186
- 105.159.248[.]137
- 80.155.38[.]210
- 217.57.80[.]18
- 151.0.169[.]250
- 212.202.147[.]10
- 212.234.179[.]113
- 185.82.169[.]99
- 93.51.177[.]66
- 80.15.113[.]188
- 80.153.75[.]103
- 109.192.30[.]125

Yara Signatures

Yara Rule Katana DDoS Botnet

```
rule Ddos_Linux_Katana {
   meta:
     description = "Detects Mirai variant named Katana"
     date = "2022-02-19"
     license = "Apache License 2.0"
     hash = "82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf"
   strings:
     $ = "[http flood] fd%d started connect"
     $ = "Failed to set IP_HDRINCL. Aborting"
     $ = "[OVH] DDoS Started"
     $ = "[vega/table] tried to access table.%d but it is locked"
     $ = "Cannot send DNS flood without a domain"
   condition:
     all of them
}
```

Yara Rule Cyclops Blink

```
rule CyclopsBlink_notable_strings
{
 meta:
 author = "NCSC"
 description = "Detects notable strings identified within the Cyclops
Blink executable"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Process names masqueraded by implant
 $proc_name1 = "[kworker/0:1]"
 $proc_name2 = "[kworker/1:1]"
 // DNS query over SSL, used to resolve C2 server address
 $dns_query = "POST /dns-query HTTP/1.1\x0d\x0aHost:
dns.google\x0d\x0a"
 // iptables commands
 $iptables1 = "iptables -I %s -p tcp --dport %d -j ACCEPT &>/dev/null"
 $iptables2 = "iptables -D %s -p tcp --dport %d -j ACCEPT &>/dev/null"
 // Format strings used for system recon
 $sys_recon1 = "{\"ver\":\"%x\",\"mods\":["
 $sys_recon2 = "uptime: %lu mem_size: %lu mem_free: %lu"
 $sys_recon3 = "disk_size: %lu disk_free: %lu"
```

```
 $sys_recon4 = "hw: %02x:%02x:%02x:%02x:%02x:%02x"
 // Format string for filepath used to test access to device
filesystem
 $testpath = "%s/214688dsf46"
 // Format string for implant configuration filepath
 $confpath = "%s/rootfs_cfg"
 // Default file download path
 $downpath = "/var/tmp/a.tmp"
 condition:
 (uint32(0) == 0x464c457f) and (8 of them)
}
rule CyclopsBlink_module_initialisation
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to initialise the modules
built into Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Module initialisation code bytes, simply returning the module ID
 // to the caller
 $ = {94 21 FF F0 93 E1 00 08 7C 3F 0B 78 38 00 00 ?? 7C 03
 03 78 81 61 00 00 8E EB FF F8 7D 61 5B 78 4E 80 00 20}
 condition:
 (uint32(0) == 0x464c457f) and (any of them)
}
rule CyclopsBlink_modified_install_upgrade
{
 meta:
 author = "NCSC"
 description = "Detects notable strings identified within the modified
install_upgrade executable, embedded within Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 hash3 = "7d61c0dd0cd901221a9dff9df09bb90810754f10"
 hash4 = "438cd40caca70cafe5ca436b36ef7d3a6321e858"
 strings:
 // Format strings used for temporary filenames
 $ = "/pending/%010lu_%06d_%03d_p1"
 $ = "/pending/sysa_code_dir/test_%d_%d_%d_%d_%d_%d"
 // Hard-coded key used to initialise HMAC calculation
 $ = "etaonrishdlcupfm"
 // Filepath used to store the patched firmware image
 $ = "/pending/WGUpgrade-dl.new"
 // Filepath of legitimate install_upgrade executable
 $ = "/pending/bin/install_upgraded"
 // Loop device IOCTL LOOP_SET_FD
 $ = {38 80 4C 00}
 // Loop device IOCTL LOOP_GET_STATUS64
 $ = {38 80 4C 05}
 // Loop device IOCTL LOOP_SET_STATUS64
 $ = {38 80 4C 04}
 // Firmware HMAC record starts with the string "HMAC"
 $ = {3C 00 48 4D 60 00 41 43 90 09 00 00}
```

```
 condition:
 (uint32(0) == 0x464c457f) and (6 of them)
}
rule CyclopsBlink_core_command_check
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to test the command ID
being sent to the core component of Cyclops Blink"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Check for command ID equals 0x7, 0xa, 0xb, 0xc or 0xd
 $cmd_check = {81 3F 00 18 88 09 00 05 54 00 06 3E 2F 80 00
 (07|0A|0B|0C|0D)}
 condition:
 (uint32(0) == 0x464c457f) and (#cmd_check == 5)
rule CyclopsBlink_config_identifiers
{
 meta:
 author = "NCSC"
 description = "Detects the initial characters used to identify
Cyclops Blink configuration data"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Main config parameter data starts with the string "<p: "
 $ = "<p: " fullword
 // RSA public key data starts with the string "<k: "
 $ = {3C 00 3C 6B 60 00 3A 20 90 09 00 00}
 // X.509 certificate data starts with the string "<c: "
 $ = {3C 00 3C 63 60 00 3A 20 90 09 00 00}
 // RSA private key data starts with the string "<s: "
 $ = {3C 00 3C 73 60 00 3A 20 90 09 00 00}
 condition:
 (uint32(0) == 0x464c457f) and (all of them)
}
rule CyclopsBlink_handle_mod_0xf_command
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to check module ID 0xf
control flags and a format string used for file content upload"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Tests execute flag (bit 0)
 $ = {54 00 06 3E 54 00 07 FE 54 00 06 3E 2F 80 00 00}
 // Tests add module flag (bit 1)
 $ = {54 00 06 3E 54 00 07 BC 2F 80 00 00}
 // Tests run as shellcode flag (bit 2)
 $ = {54 00 06 3E 54 00 07 7A 2F 80 00 00}
 // Tests upload flag (bit 4)
 $ = {54 00 06 3E 54 00 06 F6 2F 80 00 00}
 // Upload format string
```

```
 $ = "file:%s\n" fullword
 condition:
 (uint32(0) == 0x464c457f) and (all of them)
}
rule CyclopsBlink_default_config_values
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to set default Cyclops
Blink configuration values"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Unknown config value set to 0x19
 $ = {38 00 00 19 90 09 01 A4}
 // Unknown config value set to 0x18000
 $ = {3C 00 00 01 60 00 80 00 90 09 01 A8}
 // Unknown config value set to 0x4000
 $ = {38 00 40 00 90 09 01 AC}
 // Unknown config value set to 0x10b
 $ = {38 00 01 0B 90 09 01 B0}
 // Unknown config value set to 0x2711
 $ = {38 00 27 11 90 09 01 C0}
 condition:
 (uint32(0) == 0x464c457f) and (3 of them)
}

rule CyclopsBlink_handle_mod_0x51_command
{
 meta:
 author = "NCSC"
 description = "Detects the code bytes used to check commands sent to
module ID 0x51 and notable strings relating to the Cyclops Blink update
process"
 hash1 = "3adf9a59743bc5d8399f67cab5eb2daf28b9b863"
 hash2 = "c59bc17659daca1b1ce65b6af077f86a648ad8a8"
 strings:
 // Check for module command ID equals 0x1, 0x2 or 0x3
 $cmd_check = {88 1F [2] 54 00 06 3E 2F 80 00 (01|02|03}
 // Legitimate WatchGuard filepaths relating to device configuration
 $path1 = "/etc/wg/configd-hash.xml"
 $path2 = "/etc/wg/config.xml"
 // Mount arguments used to remount root filesystem as RW or RO
 $mnt_arg1 = "ext2"
 $mnt_arg2 = "errors=continue"
 $mnt_arg3 = {38 C0 0C 20}
 $mnt_arg4 = {38 C0 0C 21}
 condition:
 (uint32(0) == 0x464c457f) and (#cmd_check == 3) and
 ((@cmd_check[3] - @cmd_check[1]) < 0x200) and
 (all of ($path*)) and (all of ($mnt_arg*))
}
```

Newsarticles & Advisories

23-Feb-2022
Alert (AA22-054A) New Sandworm Malware Cyclops Blink Replaces VPNFilter
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
Another round of 'wiper' malware appears in Ukrainian networks
https://www.cyberscoop.com/ukraine-wiper-malware-eset-sentinelone-whispergate/
Attack on Ukrainian Government Websites Linked to Russian GRU Hackers
https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/
Companies warned to boost cyber defence in wake of Ukraine crisis escalation
https://www.zdnet.com/article/companies-warned-to-boost-cyber-defence-in-wake-of-ukraine-crisis-escalation/
Cyclops Blink Malware Analysis Report
https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
DHS warns of urgent cyberattack threat as Russia tensions escalate
https://www.msn.com/en-us/news/other/dhs-warns-of-urgent-cyberattack-threat-as-russia-tensions-escalate/vi-AAUb86f
Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In
https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine
Dutch village 'played key role in Russian cyber attacks on Ukraine'
https://www.dutchnews.nl/news/2022/02/dutch-village-played-key-role-in-russian-cyber-attacks-on-ukraine/
ESETResearch: HermeticWiper Twitter Thread
https://twitter.com/ESETresearch/status/1496581903205511181
How to Prepare as Russia-Ukraine Situation Escalates
https://securityboulevard.com/2022/02/how-to-prepare-as-russia-ukraine-situation-escalates/
Looking into HermeticWiper Twitter Thread
https://twitter.com/juanandres_gs/status/1496581710368358400
Malware Analysis Report: Cyclops Blink
https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
Malware Detected in Ukraine as Invasion Threat Looms
https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/malware-detected-in-ukraine-as-invasion-threat-looms-NaVfMTy8x0v41PyZNuzo
New Sandworm Malware Cyclops Blink Replaces VPNFilter (1)
https://www.cisa.gov/uscert/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter
New Sandworm Malware Cyclops Blink Replaces VPNFilter (2)
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-054A%20New%20Sandworm%20Malware%20Cyclops%20Blink%20Replaces%20VPN%20Filter.pdf
Russia's Sandworm Hackers Have Built a Botnet of Firewalls
https://www.wired.com/story/sandworm-cyclops-blink-hacking-tool/
Second data wiper attack hits Ukraine computer networks
https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/
Technical Analysis of the DDoS Attacks against Ukrainian Websites
https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/
Ukraine hit by DDoS attacks, Russia deploys malware
https://www.theregister.com/2022/02/23/ukraine_ddos_russia_malware/
Ukraine: EU deploys cyber rapid-response team
https://www.bbc.com/news/technology-60484979

Ukrainian gov't sites disrupted by DDoS, wiper malware discovered
https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/
US, UK detail malware tied to Russian hacking group Sandworm that targets Linux
https://www.scmagazine.com/analysis/apt/us-uk-detail-malware-tied-to-russian-hacking-group-sandworm-that-targets-linux
Will Russia's invasion of Ukraine trigger a massive cyberwar?
https://www.newscientist.com/article/2309369-will-russias-invasion-of-ukraine-trigger-a-massive-cyberwar/
22-Feb-2022
6 EU Countries Extend Cyber Support To Ukraine As Conflict With Russia Escalates
https://www.forbesmiddleeast.com/innovation/cybersecurity/6-eu-countries-dispatched-experts-to-bolster-ukraine-in-dealing-with-cyber-threats
Ukraine accepts Dutch offer of help against cyber attacks
https://nltimes.nl/2022/02/22/ukraine-accepts-dutch-offer-help-cyber-attacks
18-Feb-2022
Information on cyberattacks on February 15, 2022
https://cert.gov.ua/article/37139
White House attributes Ukraine DDoS incidents to Russia's GRU
https://www.cyberscoop.com/ukraine-ddos-russia-attribution-white-house-neuberger/
16-Feb-2022
The Anatomy of the DDoS Attack Campaign Targeting Organizations in Eastern Europe
https://www.netscout.com/blog/asert/anatomy-ddos-attack-campaign-targeting-organizations-eastern
15-Jan-2022
Destructive malware targeting Ukrainian organizations
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

About Tesorion

Tesorion is a 100% Dutch company whose primary focus is on cybersecurity and on helping our customers combat all kinds of cybercrime and minimize their operational risks. The company's objective is to make the Netherlands more secure, with a particular focus on Managed Cybersecurity services. It achieves this using, among other things, SOC services, Behavior & Security Awareness, Digital Risk Protection and Offensive Security. Tesorion also offers specialist 24/7 support in the event of cyber incidents. When, for example, an organization is affected by a cybersecurity incident, Tesorion's digital forensics specialists can offer support. Every day more than four million devices are protected on behalf of customers in the healthcare, education, transport and logistics, corporate services, the financial sector, and industry.

If you are hacked, or if you think you might be,

never hesitate to contact the Tesorion Cyber Emergency Hotline **24/7**.

In case of **emergency**

+31 88 27 47 800

T·CERT
POWERED BY TESORION

24/7
Beschikbaar

180+
Specialisten

500+
Klanten

1000+
Sensoren

4+ miljoen
Beschermde Apparaten

100%
Europees

TESORION

Fokkerstraat 4
3833 LD Leusden
Nederland
www.tesorion.com