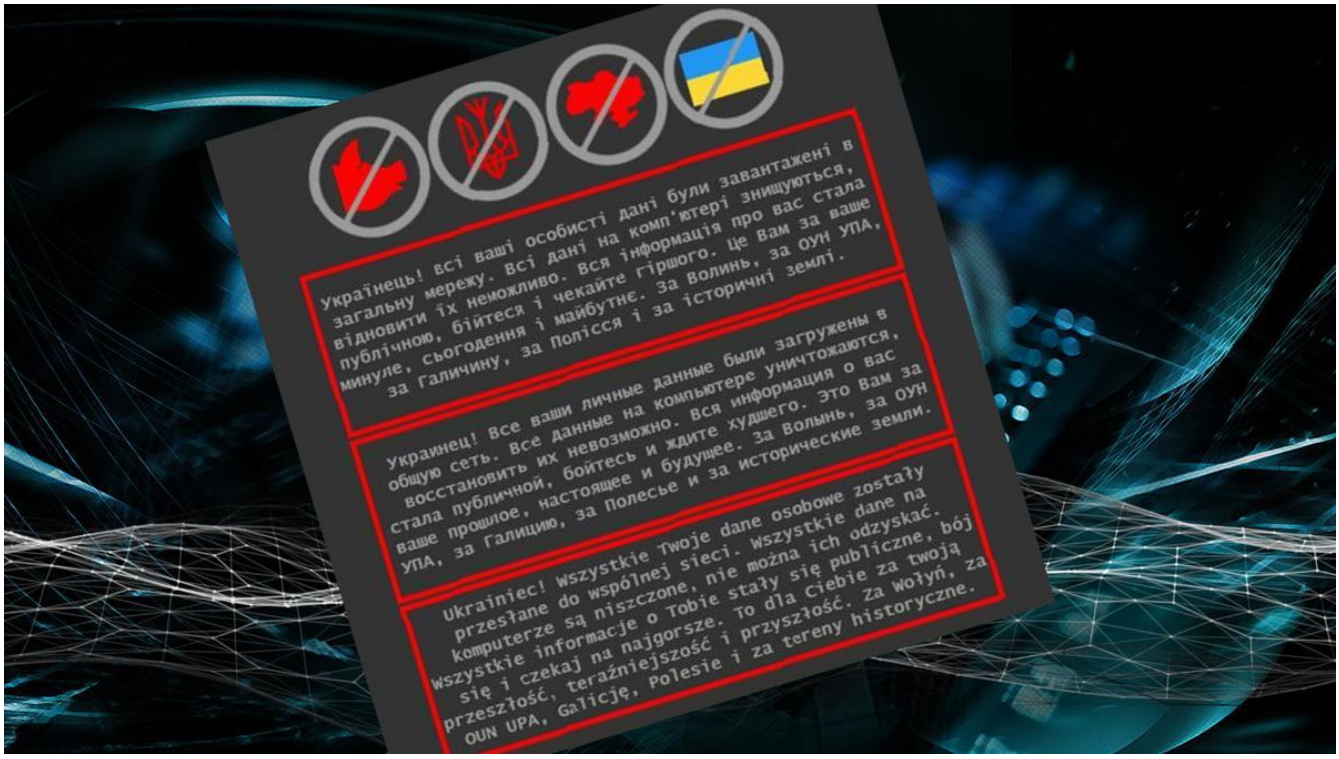
CSIRT MON - ANALYSIS OF THE CYBERATTACK ON UKRAINIAN GOVERNMENT RESOURCES

csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/analysis-cyberattack-ukrainian-government-resources/

22 stycznia 2022

ANALYSIS OF THE CYBERATTACK ON UKRAINIAN GOVERNMENT RESOURCES



On the night of January 13 – 14, 2022, many Ukrainian government websites were defaced. As a result of the attack, access to the Diia platform, which is the equivalent of the Polish mObywatel application, was also cut off. An initial vector that allowed the attacker to take control over the above-mentioned resources was the vulnerability of the October CMS application, used to manage the content of the websites.

The content of the defacement was published simultaneously in Ukrainian, Russian and Polish. The content of the prepared message used the theme of the Volhynia massacre and historical, controversial issues that may have negatively affect bilateral relations between Poland and Ukraine. In-depth analyses, the first results of which were published on January 15, 2022, showed that the compromise of websites was also aimed at distracting attention from the activities involving in the use of malware by the adversary, the purpose of which was to destroy data on the infected device. The exact scale of the damage is currently unknown, but the information shows that the same malware samples were also detected in many government organizations, non-profit organizations and private companies' networks in Ukraine.

According to the Ukrainian State Service for Special Communication and Information Protection, nearly 70 Ukrainian websites (domestic and international) were attacked on January 13-14, 2022. As a result of these attacks, numerous websites in the gov.ua domain were compromised (as of January 14, 2022):

- Government services portal "Diia" - diia.gov.ua (unavailable),
- Cabinet of Ministers - kmu.gov.ua (unavailable),
- Ministry of Foreign Affairs - mfa.gov.ua (defaced, unavailable),

- State Rescue Service - dsns.gov.ua (unavailable),
- Ministry of Education and Science - mon.gov.ua (unavailable),
- Ministry of Youth and Sport - sport.gov.ua (unavailable),
- Ministry of Energy - mpe.kmu.gov.ua (unavailable),
- Ministry of Agrarian Policy - minagro.gov.ua (unavailable),
- Ministry of Veterans Affairs - mva.gov.ua (unavailable),
- Ministry of Environment Protection and Natural Resources - mepr.gov.ua (unavailable),
- State Treasury Service - treasury.gov.ua (unavailable);

Other sites likely to be affected by this attack (status unknown):

- State Register of Court Orders - reyestr.court.gov.ua
- Ministry of Territories and Communities Development - minregion.gov.ua
- State Service for Special Communications and Information Protection - new.cip.gov.ua,
- Supreme Court of Ukraine - supreme.court.gov.ua,
- High Anti-Corruption Court of Ukraine - hcac.court.gov.ua,
- "Court system" official portal - court.gov.ua,
- National Civil Service Agency - nads.gov.ua,
- State Inspectorate of Nuclear Supervision - snriu.gov.ua,
- local authorities of Rivne - rv.gov.ua,
- local authorities of Transcarpathia - carpathia.gov.ua,
- local authorities of Donetsk - dn.gov.ua,
- State Agency for Forest Resources - forest.gov.ua,
- Ministry of Strategic Industry - mspu.gov.ua,
- local authorities of Mukachevo - mukachevo-rada.gov.ua,
- Social Protection Fund for the Disabled - ispf.gov.ua,
- Municipal Enterprise "KyivTeploEnergo" - teplo.org.ua,
- Antimonopoly Committee of Ukraine - amcu.gov.ua,
- National Sports Committee of People with Disabilities - paralympic.org.ua,
- State Sea and River Transport Service - marad.gov.ua,
- local authorities of Dnipro - adm.dp.gov.ua,
- Ukrainian State Center for Radio Frequencies - ucrf.gov.ua.

On January 14, 2022 the Ukrainian CERT issued a statement[1] which describes that, after preliminary analysis, it was determined that the probable attack vector was the vulnerability of the Octobercms platform used to manage the content of websites (CVE-2021-32648). Octobercms is a CMS platform based on the Laravel PHP framework. In vulnerable versions of the October package, an attacker could request for an account password reset and then access it with a specially crafted request. The bug has been fixed in Build 472 and v1.1.5.

A graphic file *(index.jpeg)* containing content written in Ukrainian, Russian and Polish was published on compromised websites where the content of the page was changed (Figure 1).

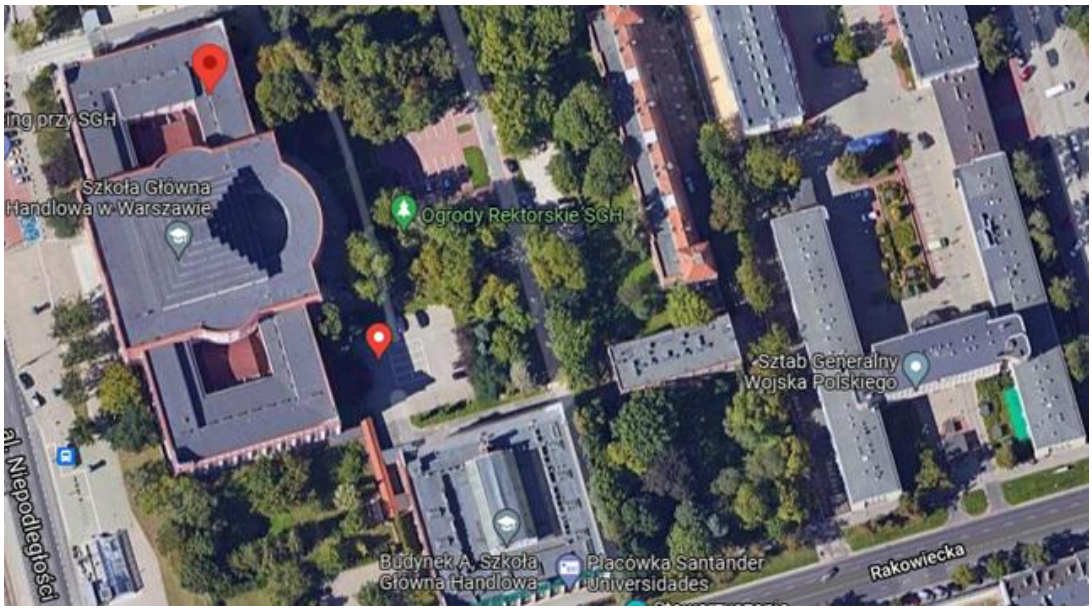
The metadata of the above image file contained the following coordinates:

Latitude: 52° 12' 31.1" N,

Longitude: 21° 0' 33.9" E,

GPS : 52.208630, 21.009427.

The above geographical data indicate a car park of the Warsaw School of Economics (Figure 2). However, it should be remembered that the graphic file in question, which appeared on the compromised pages, is not a photo, so the above geographical data was probably added manually.



On January 15, 2022, Microsoft published a report[2] in which it describes that the Microsoft Threat Intelligence Center (MSTIC) identified an operation involving the use of malicious software by an adversary (DEV-0586), aimed at destroying data on an infected device. The report indicates that the use of malware is related to a large-scale campaign targeting Ukrainian government entities and IT companies that are engaged in maintaining Ukrainian government websites[3]. The malware described in the report first appeared on the systems of Ukrainian victims on January 13, 2022. MSTIC estimates that malware (which is designed to appear ransomware) does not actually have a data recovery mechanism. So it was created for destructive purposes (wiper), the effect of which is to prevent the operation of target devices.

At the moment, the exact attribution is not known, however, according to the Deputy Secretary of the National Security and Defense Council of Ukraine (Serhiy Demediuk), the UNC1151 group may be responsible for the attack, and the malware used to destroy data resembles the tools used by the APT29 group, associated with the Russian SVR[4].

Particularly noteworthy is the fact that the attacker prepared metadata in the graphic file used for defacement. The location hidden under the given coordinates indicates the area of the Warsaw School of Economics. CSIRT MON suspects that the real intention of the adversary was to use the geolocation of the General Staff of the Polish Army to lead potential analysts and public opinion to a false, controversial trail.

Due to the situation in Ukraine, the CSIRT MON team warns about the potential risk of extending the attack to other countries in the region.

Recommendations

The CSIRT MON team recommends intensifying activities leading to the security of ICT systems used to provide key services and constituting critical infrastructure.

For this purpose, it is recommended:

1. Implementation of recommendations contained in the Mandiant report[5], reducing the risk of infection with the software used in this attack.
2. Analyzing own resources in terms of the presence of IoCs included in this announcement, as well as ongoing updating of signatures used by security tools such as antivirus software, EDR, IDS, IPS, etc.
3. In-depth monitoring of the security of ICT systems, in particular analyzing alerts generated by security tools such as antivirus software, EDR, IDS, IPS, firewalls, e-mail protection systems, etc.

4. Installing the latest security patches for all elements of the ICT infrastructure (including operating systems, application software, network devices) giving the highest priority to vulnerabilities that are actively exploited[6].
5. The use of multi-factor authentication in access control mechanisms, in particular for e-mail and critical resources.
6. Verification of the computer incident response plan and the resulting procedures.
7. Maintaining backup copies and verification of procedures allowing to restore the ICT system after a computer incident.
8. Reporting to the appropriate CSIRT team identified computer incidents that may have been caused by attacks.

Any new information on this subject will be updated on a regular basis.

Update of 18.01.2022 at 4:00 p.m.

On January 17, 2022, the Ukrainian SBU service reported that 95% of all attacked websites had been restored to operation[7]. In connection with the above-described attack, CSIRT MON together with CSIRT NASK and CSIRT GOV is working on the analysis of malware used for this attack. The preliminary findings show that malware consists of at least 3 different modules (executable files) that are launched on the victim's computer in a strictly defined order. The first module, called PAYWIPE[8],is malware disguised as ransomware. The following information is presented to infected victims, urging them to pay a ransom.

> Your hard drive has been corrupted.
>
> In case you want to recover all hard drives
>
> of your organization,
>
> You should pay us $10k via bitcoin wallet
>
> 1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
>
> tox ID
> 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
>
> with your organization name.
>
> We will contact you to give further instructions.

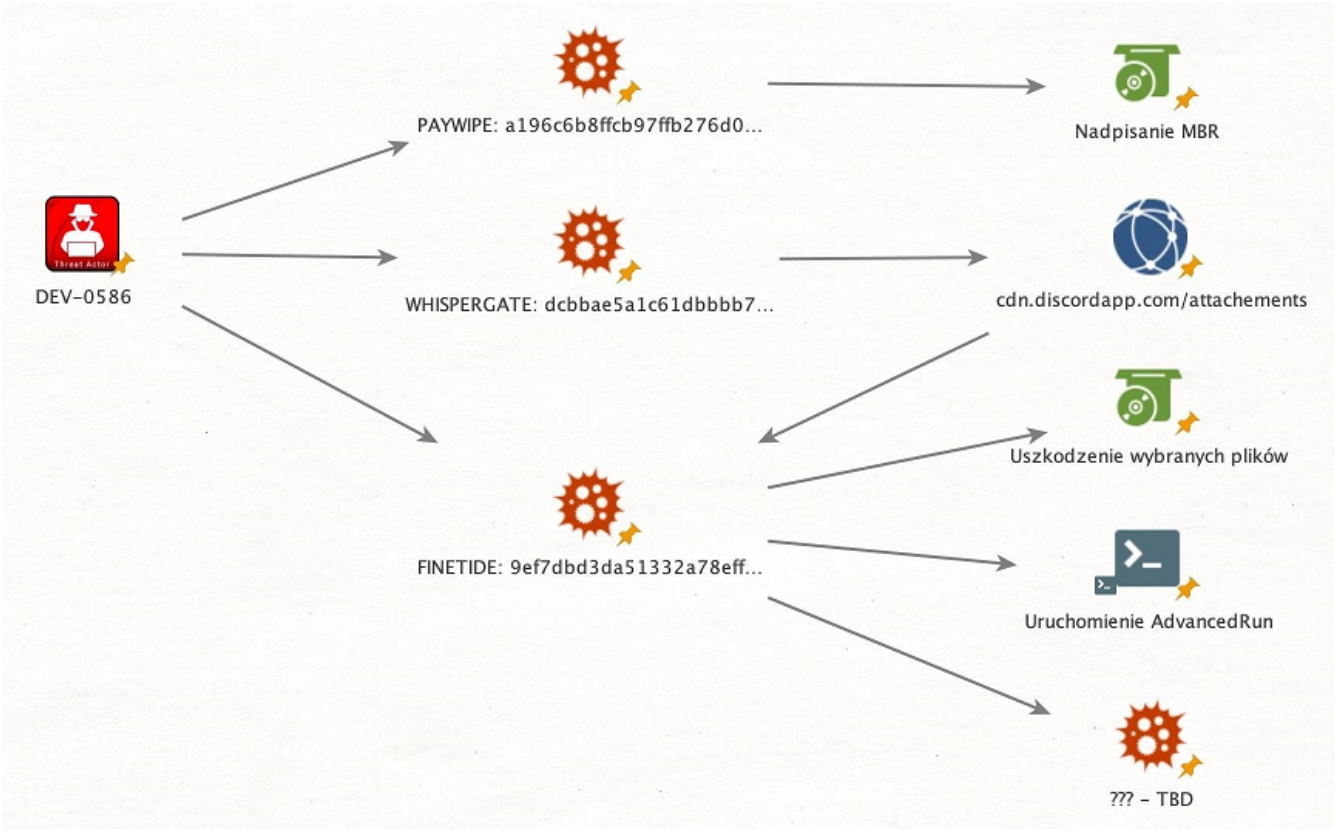
In fact, this malware is a wiper*,* so there are no functionalities implemented in it that allow you to restore the system to its original form. This module is designed to overwrite the *Master Boot Record,* which results in the deletion of information about system partitions and prevents the operating system from starting after reboot.

Another module called WHISPERGATE[9] is designed to download the next module called FINETIDE[10] using the resources uploaded by the adversary to Discord communication platform. The addresses of malicious resources hosted on Discord are listed in a table with indicators of compromise. The WHISPERGATE module is an application written in .NET. Downloading malicious content from Discord resources is preceded by running the *Sleep* command for 10 seconds by a PowerShell application with base64-encoded arguments. This operation is done to avoid potential detection mechanisms on the attacked machine. The FINETIDE module is downloaded as a file with a JPEG extension, while the task of WHISPERGATE is to read all bytes from the end to the beginning of the JPEG file and save them to a new DLL file. WHISPERGATE then executes a malicious DLL file (FINETIDE module) that is obfuscated using *the Eazfuscator* software[11].

There are three resources available within the DLL file. At the moment, only one of the resources has been analyzed. The analysis showed that it consists of the *AdvancedRun* and *Waqybg* module. The AdvancedRun module is a tool from Nirsoft[12], which is used in this case to disable Windows Defender, while the *Waqybg* module damages files with the following extensions by modifying their content and extension.

. HTML . HTM . PHTML . PHP . JSP . ASP . PHPS . PHP5 . ASPX . PHP4 . PHP3 . DOC . DOCX . XLS . XLSX . PPT . PPTX . PST . MSG . EML . TXT . CSV . RTF . WKS . WK1 . PDF . DWG . JPEG . JPG . DOCM . DOT . DOTM . XLSM . XLSB . XLW . XLT . XLM . XLC . XLTX . XLTM . PPTM . POT . PPS . PPSM . PPSX . HWP . SXI . STI . SLDX . SLDM . BMP . PNG . GIF . RAW . TIF . TIFF . PSD . SVG . CLASS . JAR . SCH . VBS . BAT . CMD . ASM . PAS . CPP . SXM . STD . SXD . ODP . WB2 . SLK . DIF . STC . SXC . ODS .3DM . MAX .3DS . STW . SXW . ODT . PEM . P12 . CSR . CRT . KEY . PFX . DER . OGG . JAVA . INC . INI . PPK . LOG . VDI . VMDK . VHD . MDF . MYI . MYD . FRM . SAV . ODB . DBF . MDB . ACCDB . SQL . SQLITEDB . SQLITE3 . LDF . ARC . BAK . TAR . TGZ . RAR . ZIP . BACKUP . ISO . CONFIG

The following graphic (Figure 3) illustrates how and in which sequence malware runs. Further analyses on the characteristics of the FINETIDE tool are currently underway.



Update of January 19, 2022 at 2:00 p.m.

As indicated by the Security Service of Ukraine[13] and the Cyber Police of Ukraine[14], the attack also exploited (in addition to vulnerabilities in content management systems - OctoberCMS) the Log4j vulnerability. In addition, according to the above-mentioned sources, the government websites were also compromised as a result of the takeover of the accounts of employees of the IT service provider that provided services to the Ukrainian government. In addition, the Cyber Police of Ukraine noted DDoS attacks on a number of Ukrainian government entities.

Update of January 20, 2022 at 3:00 p.m.

Considering the fact that the recent attacks on Ukrainian government websites exploited CVE-2021-32648 vulnerability (related to the OctoberCMS content management system), there is a risk of further exploitation of this software vulnerability..
In order to prevent the use of CVE-2021-32648 vulnerability, as well as to introduce additional security measures, it is recommended to:
1. Update October CMS to the latest version.

2. Allow access to the CMS login panel only through a trusted point-to-point connection or from a specific IP address.

3. Implement two-factor authentication login process.

4. Change the path to the OctoberCMS login panel from the default (/backend/*) to another path, which consists of a string of pseudo-random characters.

5. Uninstall any plugins that come from unknown sources. Install add-ons only from the official platform provided by the manufacturer, taking into account the need to update.

Embarrassment indicators

Sample

Indicator	**Value**	**Update date**
Registered command used to run stage1.exe via Impacket	cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1	16.01.2022 20:00
MS Defender Engine Signatures	DoS:Win32/WhisperGate.A!dha DoS:Win32/WhisperGate.C!. Dha DoS:Win32/WhisperGate.H!dha DoS:Win32/WhisperGate.X!dha	16.01.2022 20:00
Malicious resources downloaded from Discord	https://cdn.discordapp[.] com/attachments/926229413052420097/929804142480851064/Ckyds.jpeg https://cdn.discordapp[.] com/attachments/920038082684809226/929889321555738664/cmd.bin https://cdn.discordapp[.] com/attachments/870329984361824376/929834806672498789/menumod.jpeg	16.01.2022 20:00
Commands run by FINETIDE	*C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Set-MpPreference -ExclusionPath 'C:\'* *"C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run*	18.01.2022 16:00

PAYWIPE	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 (SHA256)	16.01.2022 20:00
WHISPERGATE	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 (SHA256)	16.01.2022 20:00
WHISPERGATE	2367511bfe58c927c3fd90d61b986e9fe1f5c4aa6a2340f376d158b24134b8ac (SHA256)	16.01.2022 20:00
FINETIDE	923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 (SHA256)	16.01.2022 20:00
FINETIDE	9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d (SHA256)	16.01.2022 20:00
WHISPERGATE	6ab08bc281b15935876936423b906c2bd8772ab1a6cb67a8fed2116e506fb7f8 (SHA256)	17.01.2022 15:21
PAYWIPE	22f1d202cd3c902a5d813b0be8a3bc3e61af31a3dcd799e6a63139d6ea888382 (SHA256)	17.01.2022 15:21
FINETIDE	706c36fc25013c285995bbaa46fb31400b122c09b13a0f7a1f5833d200c547a0 (SHA256)	17.01.2022 15:21
FINETIDE	b331613b3999e8e6e7def1768a7ceb6704784129da30b046858308035623b53a (SHA256)	17.01.2022 15:21
Muqirm-1.exe	9ae87c35d2a6209b208dcefea9785a31d69a1a9396a825883edddd3e030188e4 (SHA256)	17.01.2022 15:21
PAYWIPE	b50fb20396458aec55216cc9f5212162b3459bc769a38e050d4d8c22649888ae (SHA256)	17.01.2022 15:21
WHISPERGATE	1d776e7fb062e153d3a62e1ebe1f2eec30ea13fa4b1b8749935f1856be4182d9 (SHA256)	17.01.2022 15:21
WHISPERGATE	caddbd43356550c7c1bd5fb91665531fa43b55047412316d0a3042ddefbe81d1 (SHA256)	17.01.2022 15:21
PAYWIPE	67a7dc6405acc9887da45e7b5d57413157519265650fa6749b1b2c8c0a8f3d11 (SHA256)	18.01.2022 16:00

[1] https://cert.gov.ua/article/17899

[2] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[3] https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/

[4] https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

[5] https://www.mandiant.com/media/14506/download

[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[7] https://ssu.gov.ua/en/novyny/sbu-narazi-vidnovleno-robotu-95-saitiv-shcho-postrazhdaly-vid-kiberataky-na-derzhavni-resursy

[8] In line with Madiant nomenclature

[9] In line with Madiant and Microsoft nomenclature

[10] Według nomenklatury firmy Mandiant

[11] https://www.gapotchenko.com/eazfuscator.net

[12] https://www.nirsoft.net/utils/advanced_run.html

[13] https://ssu.gov.ua/novyny/sbu-narazi-vidnovleno-robotu-95-saitiv-shcho-postrazhdaly-vid-kiberataky-na-derzhavni-resursy

[14] https://www.cyberpolice.gov.ua/news/kiberpolicziya-derzhspeczzvyazku-ta-sbu-razom-iz-mizhnarodnymy-ekspertamy-vstanovlyuyut-dzherela-poxodzhennya-kiberatak-na-derzhavni-vebsajty-897/