

Threat Brief: Ongoing Russia and Ukraine Cyber Conflict

unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

Robert Falcone, Mike Harbison, Josh Grunzweig

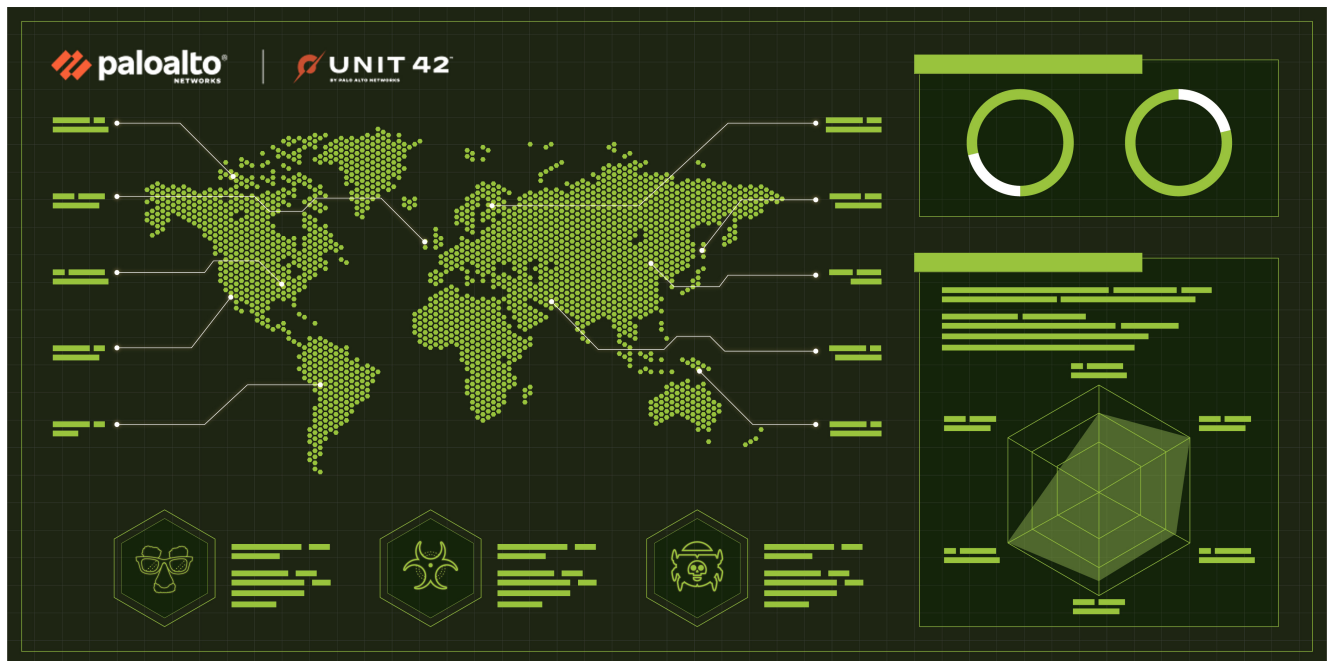
January 20, 2022

By [Robert Falcone](#), [Mike Harbison](#) and [Josh Grunzweig](#)

January 20, 2022 at 12:30 PM

Category: [Government](#), [Malware](#), [Threat Brief](#)

Tags: [Cortex](#), [CVE-2021-32648](#), [next-generation firewall](#), [OctoberCMS](#), [Russia](#), [threat brief](#), [threat prevention](#), [Ukraine](#), [vulnerabilities](#), [WhisperGate](#), [WildFire](#), [Windows](#)



This post is also available in: [日本語 \(Japanese\)](#)

Executive Summary

Beginning on Jan. 14, 2022, reports began emerging about a series of attacks targeting numerous Ukrainian government websites. As a result of these attacks, numerous government websites were found to be either defaced or inaccessible. As a result of this, the government of Ukraine formally accused Russia of masterminding these attacks against their websites.

A day later, public reporting outlined new malware called [WhisperGate](#) that originally was observed on Jan. 13, 2022. This malware disables Windows Defender Threat Protection, is destructive in nature and was discovered to have targeted multiple organizations in Ukraine. Microsoft has publicly attributed the use of this custom malware to a threat actor they refer to as DEV-0586.

Though both attacks have targeted Ukrainian organizations, the two threats have so far been implemented in separate situations.

As a result of these events, Palo Alto Networks researchers took immediate action to ensure that customers anywhere in the world can be appropriately protected against these reported threats, however they may be exploited. These attacks ultimately resulted in the investigation of the following two threats:

1. [CVE-2021-32648](#), a vulnerability in the OctoberCMS content management system (CMS) platform, which is believed to be behind the attacks against Ukrainian government websites.
2. The WhisperGate malware, attributed to the DEV-0586 threat actor.

Palo Alto Networks customers can use [Xpanse](#) or [Threat Prevention](#) for the Next-Generation Firewall to identify vulnerable and/or internet-facing instances of OctoberCMS. Protections against WhisperGate malware have been included in [Cortex XDR](#), as well as in the WildFire and Advanced URL Filtering [subscriptions for the Next-Generation Firewall](#). There is a [Cortex XSOAR](#) pack available to assist with detecting and mitigating both threats.

Threats targeting Ukraine discussed	Relevant CVEs/malware/affected software
Attacks against Ukrainian government websites	CVE-2021-32648 , affecting OctoberCMS
Attacks against multiple organizations in Ukraine	WhisperGate malware, disabling Windows Defender Threat Protection

Table of Contents

[CVE-2021-32648 Vulnerability](#)

[WhisperGate Malware Family](#)

[Mitigation Actions](#)

[Hunting for WhisperGate](#)

[Conclusion](#)

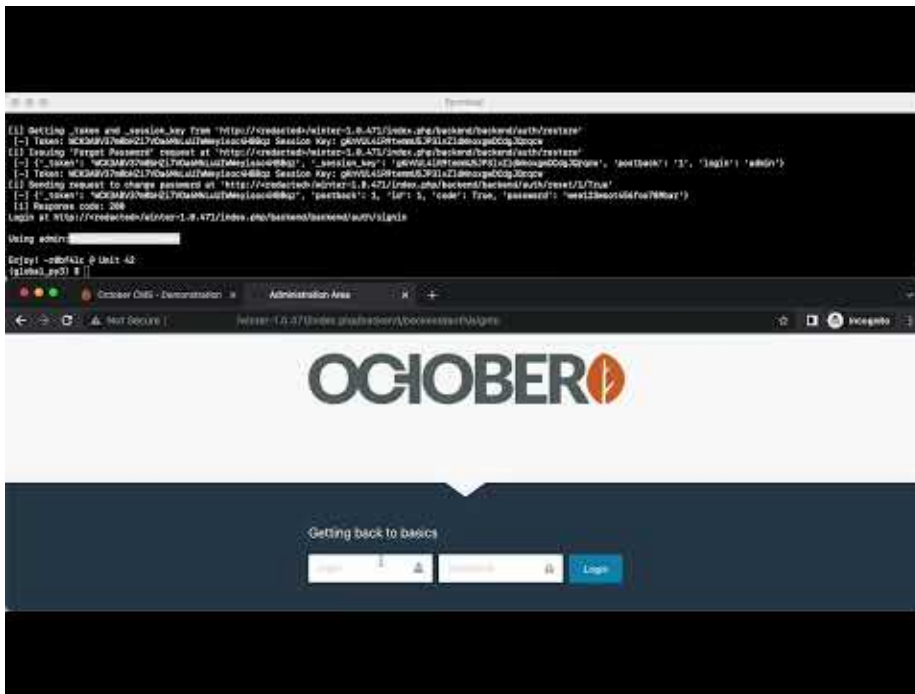
[Additional Resources](#)

CVE-2021-32648 Vulnerability

The CVE-2021-32648 vulnerability lies within the OctoberCMS platform prior to version 1.0.472 and results in an attacker gaining access to any account via a specially crafted account password reset request. This vulnerability is believed to have allowed threat actors to gain access to the underlying websites leveraged by the Ukraine government.

Once the vulnerability was discovered, Palo Alto Networks threat researchers quickly began reverse-engineering the patch that remediated this vulnerability and were able to produce a working proof of concept (PoC) in a very short time. Later that day, a [public PoC surfaced](#),

allowing organizations to better understand this vulnerability and how it is exploited. Using our PoC, we created the following demonstration video of how a malicious actor would exploit the CVE-2021-32648 vulnerability, log into the compromised OctoberCMS account and to deface a web page hosted by the server:



[Watch Video At:](#)

<https://youtu.be/0hDxZWGWZrM>

To determine how this vulnerability was exploited, we analyzed the patch that developers added to OctoberCMS version 1.0.472 to mitigate the CVE-2021-32648 vulnerability. We discovered that the vulnerable code existed in the Auth/Models/User.php file within the October Rain library of OctoberCMS. The code that exposes this vulnerability is within a function named checkResetPasswordCode, specifically, line 281 in User.php. The following line of code attempts to validate the inbound password reset request by comparing the reset code submitted within the HTTP request with the reset code generated by OctoberCMS during a legitimate reset process:

```
return ($this->reset_password_code == $resetCode);
```

To exploit this vulnerability, the actor would simply supply a boolean true value as the reset code within a custom-crafted HTTP request to reset the password of an account. By supplying the boolean true, the comparison between boolean true and the reset code string results in a boolean true, even though the two variables have different types. This effectively validates the actor's inbound password reset request, which allows the actor to then change the password

To fix this vulnerability in version 1.0.472, the OctoberCMS developer changed the line of code above to use `===` instead of `==` when comparing the values of the reset code provided by the user via an HTTP POST request. The difference between `===` and `==` involves the `===` comparing the value and type of value of the variable, not just the value, as happens when using


==. To demonstrate the difference, the following two commands run PHP code to show that a comparison of the string code with boolean true using == results in a boolean true, while the same comparison using === results in a boolean false:

```
$ php -r '$res="code"===true; echo($res." (".gettype($res).")"."\\r\\n");'  
1 (boolean)  
$ php -r '$res="code"==true; echo($res." (".gettype($res).")"."\\r\\n");'  
1 (boolean)
```

As a result of the analysis of the CVE-2021-32648 vulnerability, various product protections were created or enhanced. More information about these protections can be found within the [Mitigation Actions](#) section of the briefing.

WhisperGate Malware

First observed by Microsoft on Jan. 13, 2022, [WhisperGate](#) malware is computer network attack (CNA) malware aimed at deleting Microsoft Windows Defender and corrupting files on the target. It consists of two samples: One appears as ransomware while the other is a beaconing implant used to deliver an in-memory Microsoft Intermediate Language (MSIL) payload. The in-memory code uses Living Off the Land Binaries (LOLBINS) to evade detection and also performs anti-analysis techniques, as it will fail to detonate when certain monitoring tools exist. At the time of writing, there are two known samples identified as WhisperGate: Stage1.exe and Stage2.exe. Stage1.exe purports to be ransomware, as it overwrites the target's master boot record with 512 bytes and upon reboot displays the following ransom note:



```
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  
1AUNM68gj6PGPFcJuftrKATa4WLnzg8fpfv and send message via  
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496  
F65  
with your organization name.  
We will contact you to give further instructions.
```

Figure 1. Stage 1 ransom note.

Stage2.exe is a beaconing implant that performs an HTTPS connection to download a JPG file hosted on Discord's content delivery network (CDN). Discord's CDN is a user-created service that allows users to host attachments and is not malicious. The hosted file is retrieved from the following URL:

[hxxps://cdn.discordapp\[.\]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg](https://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg)

File Tbopbh.jpg is the malicious payload that is in-memory loaded and kicks off the destructive capabilities. The following patterns of activities are associated with this payload:

1. File InstallUtil.exe is copied to the host's %TEMP% directory, e.g. C:\Users\[USERNAME]\AppData\Local\Temp. This file is a legitimate Microsoft Windows binary.
2. Two instances of PowerShell are spawned with an encoded command to sleep for 10 seconds, e.g. C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
3. A Visual Basic Script (VBS) is created in C:\Users\[USERNAME]\AppData\Local\Temp named: Nmddfrqqrbyjeyggda.vbs
4. Process wscript.exe is used to execute the VBS script in step 3. The VBS script is used to call PowerShell to set Windows Defender exclusion path to C:\ e.g. C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Set-MpPreference - ExclusionPath 'C:'
5. AdvancedRun.exe is created and written to the C:\Users\[USERNAME]\AppData\Local\Temp directory.
6. AdvancedRun.exe is used to execute PowerShell.exe to delete and stop Windows Defender. The following command parameters are passed to AdvancedRun:

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run

"C:\Users\[USERNAME]\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run
7. PowerShell process used to delete Windows Defender, e.g. C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse
8. File InstallUtil.exe running from C:\Users\[USERNAME]\AppData\Local\Temp directory. The in-memory payload (Tbopbh.jpg) is running within the context of the InstallUtil.exe process
9. Multiple instances of cmd.exe calling Ping.exe to delete file InstallUtil.exe, e.g. cmd.exe /min /C ping 111.111.111[.]111 -n 5 -w 10 > Nul & Del /f /q %TEMP%\InstallUtil.exe
10. File AdvancedRun.exe is deleted from the C:\Users\[USERNAME]\AppData\Local\Temp directory by the stage2.exe binary.
11. ICMP traffic to host: 111.111.111[.]111
12. All files and directories, including those on mounted USB drives, excluding the floppy drive (A:) are targeted. The following file extensions are overwritten with a one-byte value of 0xCC.

```
.SHTML .HTML .XHTML .PHTML .PHPS .PHP5 .ASPX .PHP4 .PHP6 .PHP7 .PHP3 .DOCX .XLSX .PPTX .VSDX .ONETOC2
.JPEG .DOCB .DOCM .DOTM .DOTX .XLSM .XLSB .XLTX .XLTM .PPTM .PPSM .PPSX .PPAM .POTX .POTM .SLDX .SLDM
.TIFF .DJVU .SH .CLASS .LAY6 .JAVA .KDBX .VMDK .NVRAM .VMSD .VMSN .VMSS .VMTM .VMXF .VSWP .VMTX .VMEM
.ACCDB .SQLITEDB .SQLITE3 .BACKUP .CONFIG
```

Figure 2. Targeted file extensions.

13. Targeted files greater than one megabyte are truncated to one megabyte when overwritten.

14. Virus & Threat protection is no longer available from Windows Security.

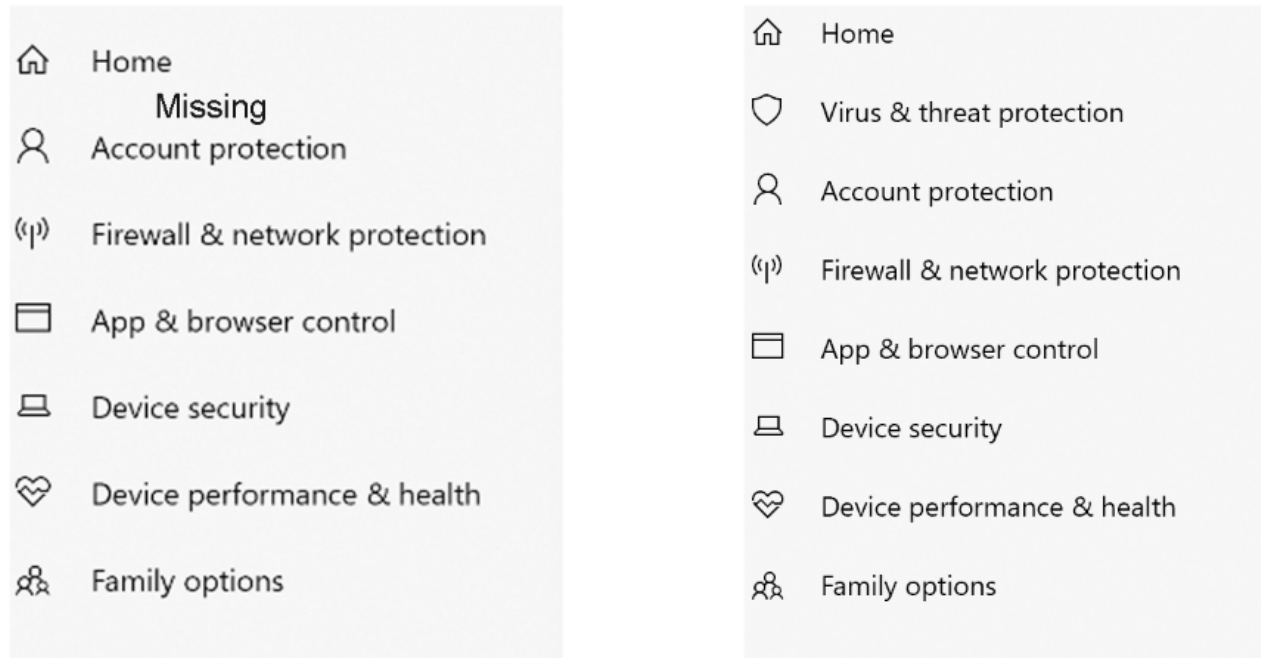


Figure 3. Virus & Threat Protection removed.

Mitigation Actions

Organizations running OctoberCMS prior to Build 472 and v1.1.5 are encouraged to update to the latest version. Additionally, in order for this vulnerability to be exploited, the web server must be running PHP below 7.4.

Palo Alto Networks customers receive protections against the OctoberCMS vulnerability in the following ways:

- Threat ID [92199](#) was released to identify this vulnerability
- Xpanse has a policy that customers can enable to detect internet-facing instances of OctoberCMS

Palo Alto Networks customers receive protections against WhisperGate malware in the following ways:

- [WildFire](#) appropriately identifies WhisperGate samples as malicious.
- All observed malicious Discord URLs have been flagged as malicious.

- [Cortex XDR](#) prevents this malware from executing using machine learning-based local analysis, the Behavioral Threat Protection module and the ransomware protection module.

The Cortex XSOAR "WhisperGate & CVE-2021-32648" pack can help automatically detect and mitigate the two threats. Read more on the [XSOAR marketplace](#).

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

Hunting for WhisperGate

Palo Alto Networks Cortex XDR customers may leverage the following XQL queries, written by the Cortex Managed Threat Hunting service experts, to hunt their datasets for indicators related to WhisperGate malware:

```
1 // Description: WhisperGate - Self Delete
2 config case_sensitive = false
3 |dataset = xdr_data
4 |filter event_type = ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START
5 |filter (action_process_image_name = "cmd.exe" OR action_process_image_name =
6 "ping.exe") and action_process_image_command_line contains "111.111.111.111 -n 5 -w
7 10"
8 |fields _time, agent_hostname, actor_effective_username, actor_process_image_path,
9 actor_process_image_sha256, action_process_image_path,
10 action_process_image_command_line, action_process_image_sha256
11
12 // Description: WhisperGate - PowerShell Sleep
13 config case_sensitive = false
14 |dataset = xdr_data
15 |filter event_type = ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START
16 |filter action_process_image_name = "powershell.exe" and
17 action_process_image_command_line contains
18 "UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA=="
19 |fields _time, agent_hostname, actor_effective_username, actor_process_image_path,
20 actor_process_image_sha256, action_process_image_path,
21 action_process_image_command_line, action_process_image_sha256
22
23 // Description: WhisperGate - InstallUtil (Wiper)
24 config case_sensitive = false
25 |dataset = xdr_data
26 |filter (event_type = FILE and (event_sub_type = ENUM.FILE_WRITE or event_sub_type
27 = ENUM.FILE_CREATE_NEW) and (action_file_name = "installutil.exe" AND
28 action_file_path contains "\\appdata\\local\\temp\\installutil.exe")) or ((event_type =
29 ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START) and
action_process_image_name = "installutil.exe" and action_process_image_path contains
"\\appdata\\local\\temp\\installutil.exe")
|dedup agent_id, actor_process_image_command_line, actor_process_image_sha256,
action_file_path, action_file_sha256, action_process_image_sha256,
action_process_image_command_line
```

```
|fields _time, agent_id, agent_hostname, actor_effective_username, action_file_name,
action_file_path, action_file_sha256, actor_process_image_path,
actor_process_image_command_line,
actor_process_image_sha256, action_process_image_path,
action_process_image_command_line, action_process_image_sha256

// Description: WhisperGate - Disable Defender
config case_sensitive = false
|dataset = xdr_data
|filter ((event_type = ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START)
and (action_process_image_name = "advancedrun.exe" and
(action_process_image_command_line contains "stop windefend" OR
action_process_image_command_line contains "mdir 'c:\programdata\microsoft\windows
defender") or (action_process_image_name = "wscript.exe" and
action_process_image_command_line contains "nmddfrrqbyjeyggda.vbs"))) or
(event_type = FILE and (event_sub_type = ENUM.FILE_WRITE or event_sub_type =
ENUM.FILE_CREATE_NEW) and (action_file_name = "nmddfrrqbyjeyggda.vbs"))
|dedup agent_id, actor_process_image_command_line, actor_process_image_sha256,
action_file_path, action_file_sha256, action_process_image_sha256,
action_process_image_command_line
|fields _time, agent_id, agent_hostname, actor_effective_username, action_file_name,
action_file_path, action_file_sha256, actor_process_image_path,
actor_process_image_command_line,
actor_process_image_sha256, action_process_image_path,
action_process_image_command_line, action_process_image_sha256
```

Conclusion

The Unit 42 Threat Intelligence team remains vigilant in monitoring this evolving situation, is actively hunting for known indicators from recent events and is ready to put protections in place to thwart attacks against our customers.

Product-specific protections have been implemented as a result of research performed in recent days, and those protections will be augmented as needed as more details come to light. Palo Alto Networks will update this Threat Brief with new information and recommendations as they become available.

Additional Resources

CVE-2021-32648 Information

WhisperGate Information

Updated March 4, 2022, at 6:15 a.m. PT.

**Get updates from
Palo Alto
Networks!**

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).