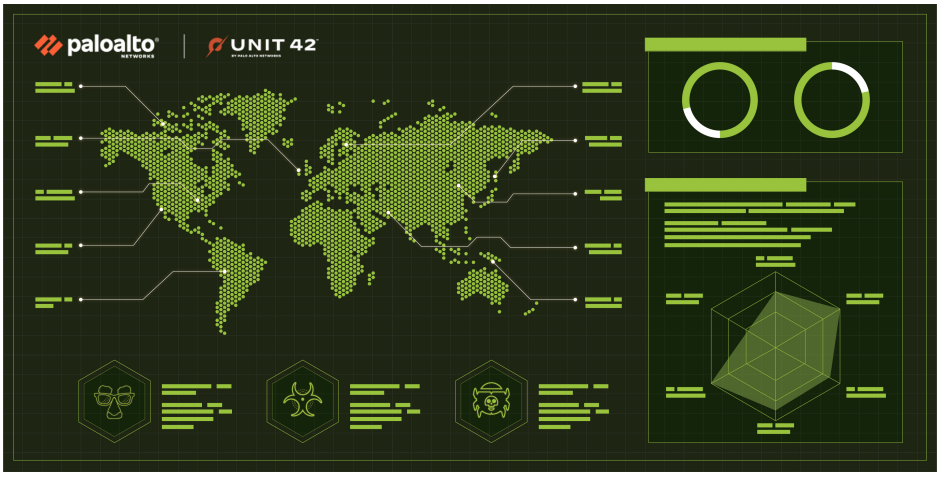
Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive

Mike Harbison, Peter Renals ⋮⋮ 7/19/2022

By Mike Harbison and Peter Renals

July 19, 2022 at 3:00 AM



Executive Summary

Organizations around the world rely on the use of trusted, reliable online storage services – such as DropBox and Google Drive – to conduct day-to-day operations. However, our latest research shows that threat actors are finding ways to take advantage of that trust to make their attacks extremely difficult to detect and prevent. The latest campaigns conducted by an advanced persistent threat (APT) that we track as Cloaked Ursa (also known as APT29, Nobelium or Cozy Bear) demonstrate sophistication and the ability to rapidly integrate popular cloud storage services to avoid detection.

The use of trusted, legitimate cloud services isn't entirely new to this group. Extending this trend, we have discovered that their two most recent campaigns leveraged Google Drive cloud storage services for the first time. The ubiquitous nature of Google Drive cloud storage services – combined with the trust that millions of customers worldwide have in them – make their inclusion in this APT's malware delivery process exceptionally concerning.

When the use of trusted services is combined with encryption, as we see here, it becomes extremely difficult for organizations to detect malicious activity in connection with the campaign.

The cybersecurity industry has long considered Cloaked Ursa to be affiliated with the Russian government. This aligns with the group's historic targeting focus, dating back to malware campaigns against Chechnya and other former Soviet bloc countries in 2008. In recent years, the hack of the United States Democratic National Committee (DNC) in 2016 has been attributed to this group, as well as the SolarWinds supply chain compromises in 2020. Increasing the specificity of the attribution, both the United States and the United Kingdom have publicly attributed this group to Russia's Foreign Intelligence Service (SVR).

The most recent campaigns by this actor provided a lure of an agenda for an upcoming meeting with an ambassador. These campaigns are believed to have targeted several Western diplomatic missions between May and June 2022. The lures included in these campaigns suggest targeting of a foreign embassy in Portugal as well as a foreign embassy in Brazil. In both cases, the phishing documents contained a link to a malicious HTML file (EnvyScout) that served as a dropper for additional malicious files in the target network, including a Cobalt Strike payload.

Palo Alto Networks customers receive protections from the indicators of compromise (IoCs) described in this blog through Cortex XDR, Advanced URL Filtering, DNS Security and WildFire malware analysis.

Full visualization of the techniques observed, relevant courses of action and IoCs related to this report can be found in the Unit 42 ATOM viewer.

Palo Alto Networks disclosed this activity to both Google and DropBox, and they have taken action to block the activity.

Names for threat actor group discussed	Cloaked Ursa, APT29, Nobelium, Cozy Bear

Table of Contents

Latest Campaigns

On May 13, 2022, Cluster25 published a report that outlined Cloaked Ursa's inclusion of DropBox services in their malware campaigns for the first time. (Here, we refer to this as campaign 1.) Searching for similar techniques, we have seen the actors continue to evolve their tactics, including by incorporating popular online storage services in their campaigns.

Less than two weeks after the Cluster25 report, on May 24, 2022, Unit 42 identified a new campaign targeting a NATO country in Europe. (We refer to this as campaign 2.)

The campaign oddly consisted of two emails to the same target country a few hours apart. Both emails contained the same lure document named Agenda.pdf, which provided a link to an agenda for an upcoming meeting with an ambassador in Portugal.

Portuguese Embassy

Convenient time for H.E Ambassador in May is here

Convenient time for H.E. Ambassador in June is here

Meeting agenda is here

Figure 1. Portuguese Embassy lure file.

Examining the two emails sent to the targeted nation provided clues as to why two emails were sent. The first email was sent at 2022-05-24T11:41:55Z with an Agenda.pdf hash of a0bdd8a82103f045935c83cb2186524ff3fc2d1324907d9bd644ea5cefacbaaf. This PDF had the following traits:

Created: 2022:04:04 13:51:53+02:00
Modified: 2022:05:24 13:28:23+02:00
Producer: 2.4.12 (4.3.5)
PDF Version: 1.5
Link: www.dropbox[.]com/s/dhueerinrg9k97k/agenda.html?dl=1

Interestingly, this sample was last modified roughly two hours before it was sent to its target. Additionally, this sample was designed to call out to DropBox to retrieve an EnvyScout payload.

The second email was sent at 2022-05-24T13:46:54Z with an Agenda.pdf hash of f9b10323b120d8b12e72f74261e9e51a4780ac65f09967d7f4a4f4a8eabc6f4c. This PDF had the following traits:

Created: 2022:04:04 13:51:53+02:00
Modified: 2022:05:24 14:27:02+02:00
Producer: 2.4.14 (4.3.5)
PDF Version: 1.5
Link: wethe6and9[.]ca/wp-content/Agenda.html

Similarly, this second sample was last modified less than an hour before it was sent to its target. Comparing the two samples, we see that the creation times remained consistent while the modification times aligned to the dates when the samples were used. The producer version in the second sample is incrementally higher, climbing from 12 to 14. Additionally, we see that the link in the document was updated to point to a legitimate web and digital marketing company in Toronto (wethe6and9[.]ca).

While speculative, one likely scenario is that the recipient could not access the file hosted in DropBox. There could be various reasons for this, including restrictive government network policies blocking access to cloud storage services. Regardless of the reason, the actors were compelled to rapidly build and send a second spear phishing email the same day with a link to an EnvyScout HTML file with the same name hosted on a legitimate website.

Pivoting on the creation time, producer and PDF version metadata in the two samples, we were able to quickly identify several additional suspicious documents in VirusTotal dating back to early April 2022. Many of these documents appear to be phishing documents associated with common cybercrime techniques. This suggests that there is likely a common phishing builder being leveraged by cybercrime and APT actors alike to generate these documents.

File Name	Created	Modified	Producer	Version
PURCHASE DETAILING INFO_001.pdf	2022:04:04 13:51:53+02:00	2022:04:11 17:51:32+02:00	2.3.5 (4.2.16)	1.5
Order-handling-depo_7754.pdf	2022:04:04 13:51:53+02:00	2022:04:18 16:41:15+02:00	2.3.5 (4.2.16)	1.5
HELP-DESK-BILLING-SLIP0092.pdf	2022:04:04 13:51:53+02:00	2022:04:19 16:50:44+02:00	2.3.5 (4.2.16)	1.5
Agenda.pdf	2022:04:04 13:51:53+02:00	2022:05:24 13:28:23+02:00	2.4.12 (4.3.5)	1.5
Agenda.pdf	2022:04:04 13:51:53+02:00	2022:05:24 14:27:02+02:00	2.4.14 (4.3.5)	1.5
JUNE_INVOICE00008488.pdf	2022:04:04 13:51:53+02:00	2022:06:10 15:51:29+02:00	2.4.18 (4.3.6)	1.5
Fifth-Third Confidential File.pdf	2022:04:04 13:51:53+02:00	2022:06:11 14:55:03+02:00	2.4.18 (4.3.6)	1.5
INV 32.pdf.remove	2022:04:04 13:51:53+02:00	2022:06:12 23:04:50+02:00	2.4.18 (4.3.6)	1.5
www.bankbri.co.id.pdf	2022:04:04 13:51:53+02:00	2022:06:25 17:26:51+02:00	2.4.19 (4.3.6)	1.5
Agenda.pdf	2022:04:04 13:51:53+02:00	2022:06:30 10:02:03+02:00	2.4.20 (4.3.10)	1.5

Table 1. Samples with similar metadata.

Reviewing this list, we identified a third Agenda.pdf created on June 30, 2022 that we assess to be part of a second phishing campaign by Cloaked Ursa. Examining the file, we found that its lure was consistent with the previous campaign. Specifically, the lure contained the same language and a similar link to an EnvyScout dropper hosted on a legitimate domain (porodicno[.]ba/wp-content/Agenda.html). Where the two campaigns differed was their target. While the first two lures were addressed to a Portuguese Embassy, this third lure was addressed to an embassy in Brazil.

Brzail Embassy

Convenient time for H.E Ambassador in July is here

Convenient time for H.E. Ambassador in August is here

Meeting agenda is here

Figure 2. Campaign 2 lure file Agenda.pdf

Finally, in comparing both campaigns, we found that Cloaked Ursa had evolved their use of cloud storage services in their delivery tactics. Notably, rather than continuing their use of the DropBox services, identified by Cluster25 in early May, these new campaigns incorporated Google Drive storage services as a means to obfuscate their actions and deploy additional payloads into target environments. A detailed analysis of both campaigns can be found below, particularly starting with the sections on Campaign 2 and Campaign 1.

Recent Related Cloaked Ursa Campaigns

The May campaign using Agenda.pdf represents repeat targeting of a particular NATO country. On Jan. 17, 2022, just days after the WhisperGate attacks in Ukraine, this NATO country was targeted in a Cloaked Ursa phishing campaign using a lure with the subject line of "*Note Verbal - Ambassador Absence*."

Additionally, this is not the first time we have seen Portugal serve as a focus for Cloaked Ursa campaigns. On Feb. 8, 2022, a phishing campaign targeted the Austrian Ministry of Foreign affairs. This campaign used a lure of "*NV - Non-working days of the Embassy of Portugal*" and originated from a potentially compromised Portuguese government email account.

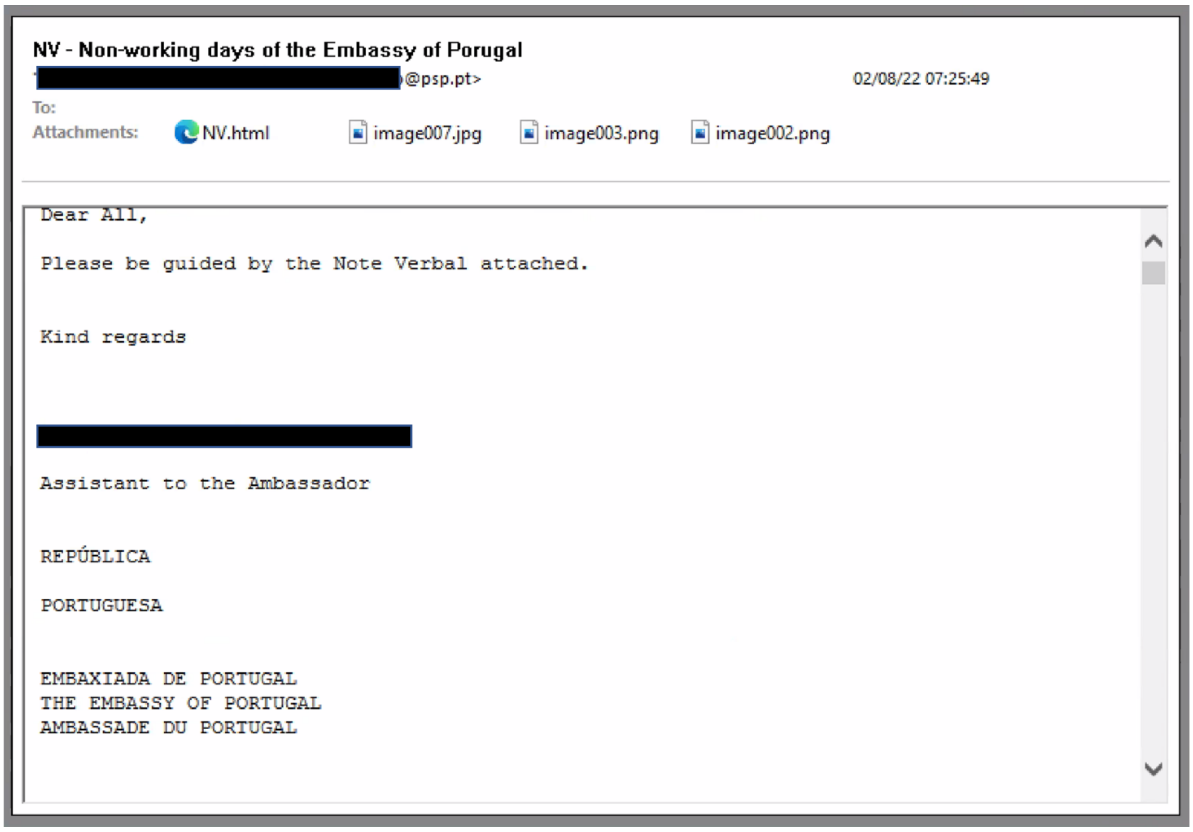


Figure 3. Email to Austrian Ministry of Foreign Affairs.

Days later, on Feb. 17, 2022, another phishing campaign was discovered with a lure of *"Embassy closure due to COVID-19*." The text of the email stated that the Embassy of the Republic of Turkey was being transferred to a state of isolation and was closing to the public. While the target of that campaign remains unknown, the original email was eventually seen by an employee of the Portuguese Ministry of Foreign Affairs who promptly forwarded the malicious email to their embassy staff in Egypt. Both of these email campaigns contained the malicious EnvyScout dropper.

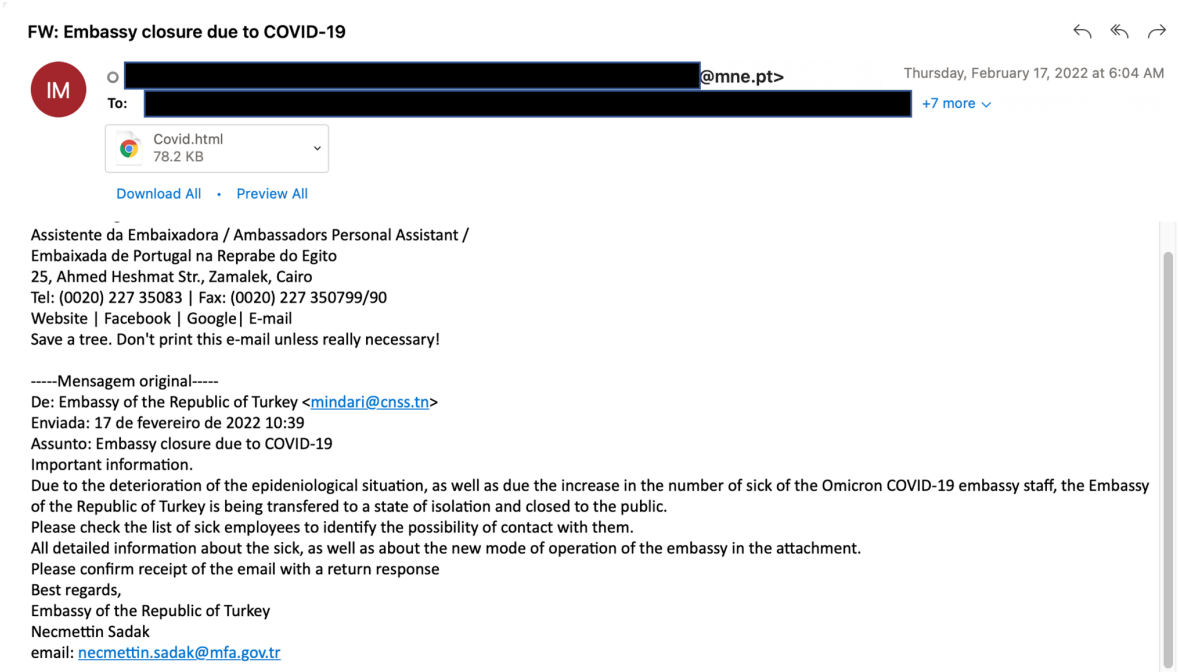


Figure 4. Email to Portuguese Embassy in Egypt.

Campaign 2

Beginning with the most recent spear phishing activity first, we analyzed a diplomatic-themed PDF file named Agenda.pdf (SHA256: ce9802b22a37ae26c02b1f2c3225955a7667495fce5b106113434ab5a87ae28a).

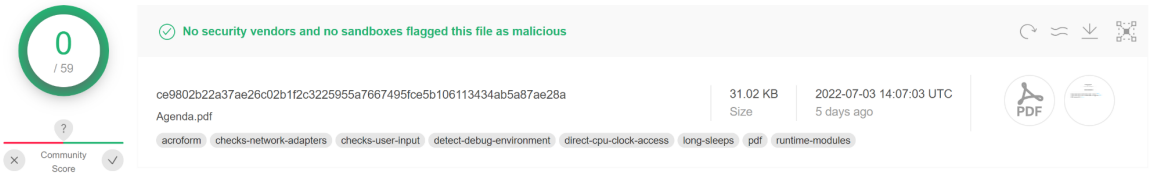


Figure 5. VirusTotal detections for campaign 2 lure file Agenda.pdf

This PDF document contains information that appears to address a foreign embassy in Brazil while using Brazil's official logo and notably misspelling “Brazil” as “Brzail.” The document was created on April 4, 2022, and later modified on June 30, 2022. All three URL links in the document point to an internet-facing web server that is hosting a file named Agenda.html. This file is EnvyScout, a malicious HTML document. The contents of Agenda.pdf are shown in Figure 6 below.

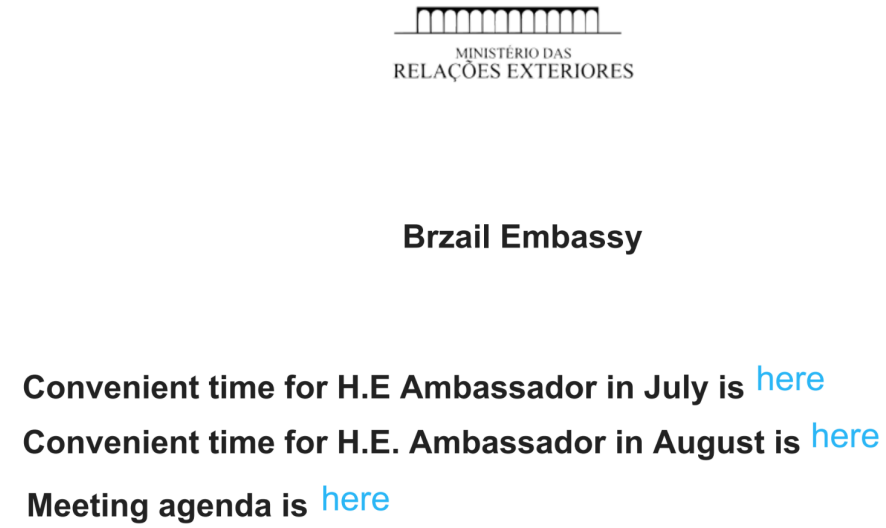


Figure 6. Campaign 2 lure file Agenda.pdf

A high-level overview of campaign 2 is depicted below in Figure 7.

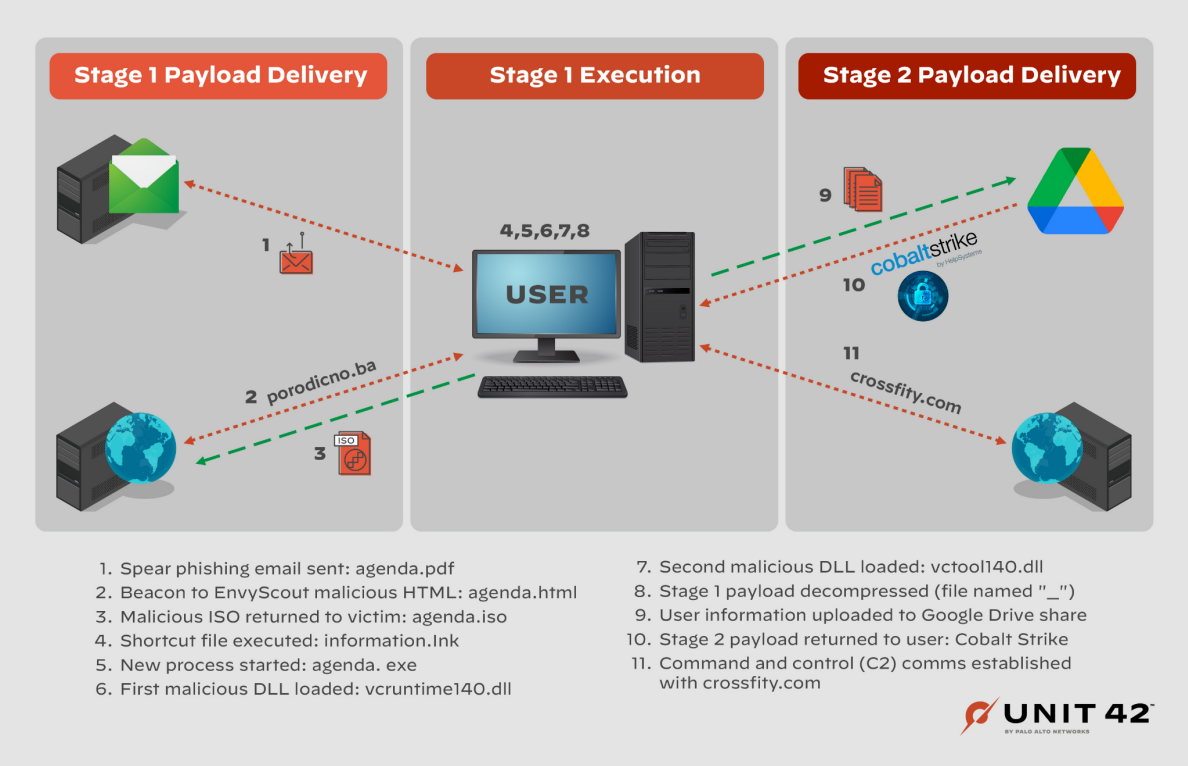


Figure 7. Campaign 2 overview.

EnvyScout – Agenda.html, Malicious HTML File

EnvyScout can be described as an auxiliary tool that is used to further infect the target with the actor's implant. It is used to deobfuscate the contents of the secondary malware, which is a malicious ISO file. This technique is known as HTML Smuggling. In this case, the file Agenda.html is responsible for deobfuscating a payload, and also for writing a malicious ISO file to the intended target hard drive. The payload file is an ISO file named Agenda.iso. It should be noted that the word “Agenda” is used throughout this attack, starting with the lure file, Agenda.pdf, and then carrying through to the named files on the target's hard drive.

The deobfuscation of the embedded payload is performed by subtracting 17 from each value. Once complete, the data is saved as Agenda.iso.

```
for(var i = 0x0; i < d['length']; i++) {
    d[i]=d[i] -17;
}

var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/octet-stream"});

var fileName = 'Agenda.iso';
```

Figure 8. Deobfuscation routine in EnvyScout Campaign 2.

The saving of the ISO is performed via JavaScript with the first attempt using the msSaveOrOpenBlob method. This method is the same as a user using Internet Explorer wanting to download and save/open a file from the internet. In the event this fails, a second file save method is used, console.save. This method creates a FileBlob from the input, and then automatically downloads it to the target. At this stage of infection, the user is prompted to open Agenda.iso by double clicking it.

```
var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/octet-stream"});

var fileName = 'Agenda.iso';

if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(f,fileName);
} else {
    var a = document.createElement('a');
    console.log(a);
    document.body.appendChild(a);
    a.style = 'display: none';
    var url = window.URL.createObjectURL(f);
    a.href = url;
    a.download = fileName;
    a.click();
    window.URL.revokeObjectURL(url);
}
```

Figure 9. Agenda.html ISO download.

Layers to Code Execution

Once the ISO has been downloaded, user interaction is required in order to achieve code execution on the victim machine. The user must double-click the ISO file and subsequently double-click the shortcut file, Information.lnk, to kick off the unpacking and infection process.

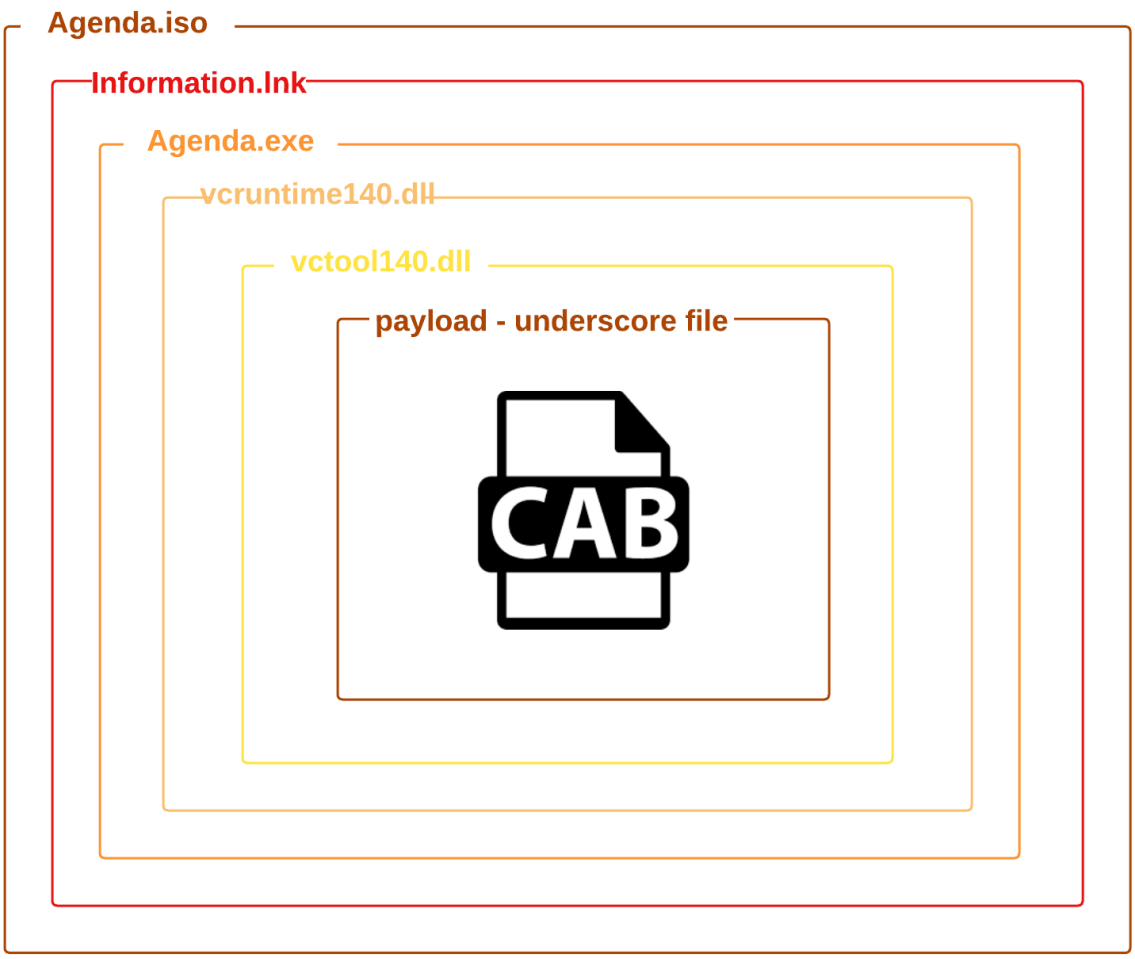


Figure 10. Layers to Stage 2 payload.

Agenda.iso - Malicious ISO Image

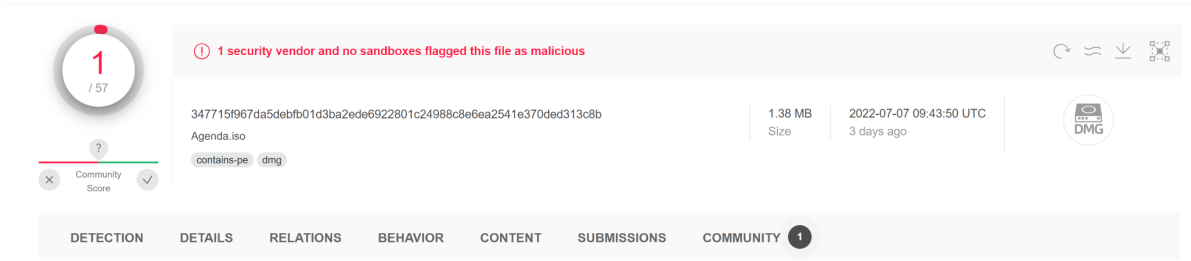


Figure 11. Agenda.iso

Agenda.iso (SHA256: 347715f967da5debfb01d3ba2ede6922801c24988c8e6ea2541e370ded313c8b) is the malicious ISO file created by EnvyScout (Agenda.html). At the time of writing, only one vendor on VirusTotal identified this sample as malicious.

Once double-clicked by the user and mounted by the operating system, the following is displayed to the user via Windows File Explorer:

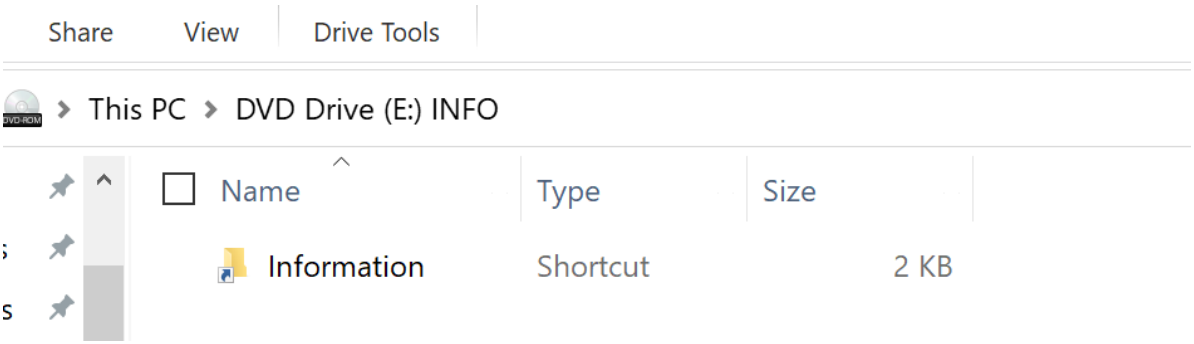


Figure 12. Agenda.iso contents; hidden files not enabled.

By default, Windows File Explorer doesn't show hidden files. The only file presented is Information.lnk. If "show hidden items" is selected, Windows File Explorer displays the following:

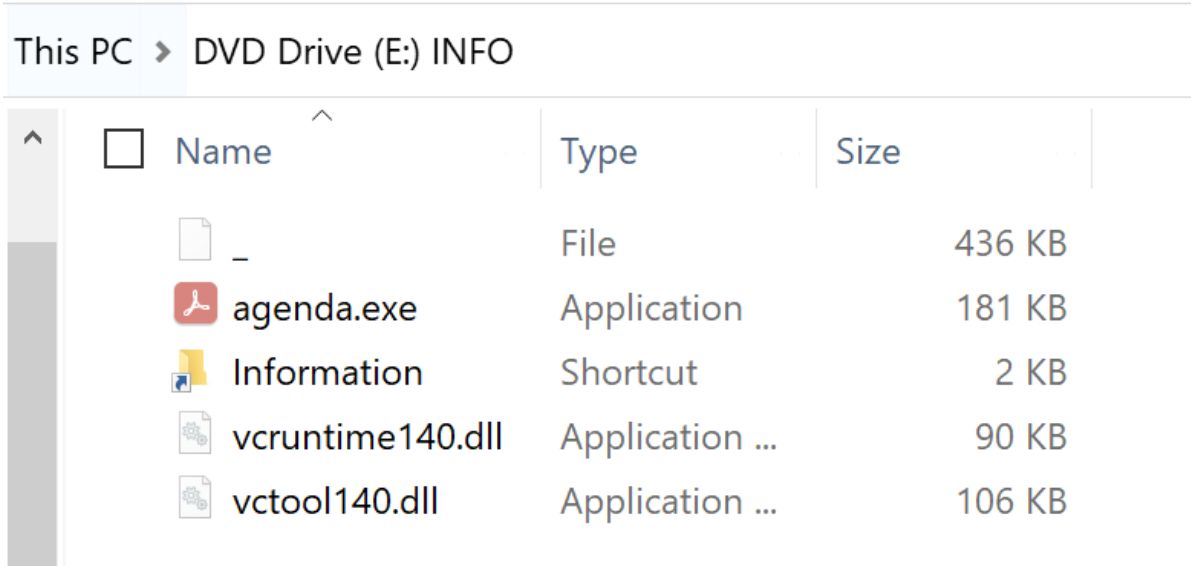


Figure 13. Agenda.iso contents; hidden files is enabled.

File Name	SHA-256	Description
_	09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677	File name is underscore. This is a compressed file (MSZIP) that is loaded by vctool140.dll
Information.lnk	32E1EEBF2AF8D36857B3A9EA3A2653E8E7AD6B6EAB8CA4665B252B5FB609D993	Windows shortcut file.
agenda.exe	E8E63F7CF6C25FB3B93AA55D5745393A34E2A98C5AEACBC42F1362DDF64EB0DA	Digitally Signed file by Adobe, Inc.
vcruntime140.dll	A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF	DLL loaded by agenda.exe
vctool140.dll	9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D	Actors DLL used to decompress and in-memory load payload

Table 2. Agenda.iso embedded file properties – Campaign 2.

Agenda.iso has the following properties:

- Created on: 6/29/2022 3:27:43 PM
- Label: INFO
- Application ID: IMGBURN V2.5.8.0 - THE ULTIMATE IMAGE BURNER!
- Volume Set ID: UNDEFINED

Information.lnk – Microsoft Shortcut File

This file is responsible for starting the infection chain on the target machine. It has the following properties:

- Link CLSID: 00021401-0000-0000-C000-000000000046
- Command line arguments: /k start agenda.exe
- Icon location: %windir%/system32/shell32.dll
- Target ansi: %windir%/system32/cmd.exe
- Creation, Modified, Accessed: None
- MS-PROPSTORE value: 46588ae2-4cbc-4338-bbfc-139326986dce
    - Converts to: S-1-5-21-2842427291-3266668846-140208303-1103

*Note about the SID in this lnk file. The SID has been found in other APT29 sample lure files (lnk) bundled with Cobalt Strike.

Once the shortcut file is double-clicked by the user, cmd.exe is used to execute agenda.exe in the current working directory. The /k parameter passed to cmd.exe instructs cmd.exe to carry out the execution and wait for agenda.exe to complete.

Agenda.exe – Adobe Executable

Agenda.exe is part of Adobe software, and is originally named WCChromeNativeMessagingHost.exe. It is digitally signed by Adobe, Inc., and is being used to evade detection from endpoint protection and antivirus software by abusing the trust of digitally signed applications. The technique is commonly referred to as DLL Side Loading.

Vcruntime140.dll – DLL loaded by agenda.exe

Vcruntime140 is a dependency file for agenda.exe. Since it exists in the same directory as agenda.exe, Windows will load it, making the APIs it contains available to it. Vcruntime140.dll is a common runtime library for Microsoft Visual Studio (Visual C++) versions 2015/2017/2019. Visual C++ runtime libraries are used for running programs developed in Microsoft Visual Studio. However, this file is not the legitimate Microsoft file, as it has been altered to load the actor's malicious DLL, vctool140.dll. Hijacking a common library file, such as vcruntime140.dll, avoids obvious detection, as one would assume the file is legitimate.

Vctool140.dll – DLL loaded by vcruntime140.dll

Vctool140.dll is the actor's core file. It searches for a payload file named underscore (_), decompresses it in memory into a .Net x64 executable and loads it. The file compression algorithm is Microsoft Zip (MSZIP), which requires the dependency file of cabinet.dll. Cabinet.dll is a Microsoft Windows library that is used to decompress Windows cabinet files, and it is typically installed on all Windows operating systems.

The technical details of how code execution is achieved are beyond the scope of this blog. In summary, it is achieved by instantiating the .Net Common Language Runtime (CLR) and using the ICorRuntimeHost interface to execute the loaded assembly. The technique is loading the CLR using native code. The in-memory code is an x64 .Net binary that is named GoogleDrive.

Payload – GoogleDrive

The decompressed payload is that of a .Net X64 executable that has been named GoogleDrive. It has the following properties:

```
// Drive, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null

// Entry point: GoogleDrive.Program.Main
// Timestamp: 62BC751F (6/29/2022 3:51:59 PM)

using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Runtime.Versioning;

[assembly: AssemblyVersion("1.0.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable(DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("GoogleDrive")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("")]
[assembly: AssemblyProduct("GoogleDrive")]
[assembly: AssemblyCopyright("Copyright ©  2022")]
[assembly: AssemblyTrademark("")]
[assembly: Guid("16396f7f-3b80-45dc-a570-641458b402de")]
[assembly: AssemblyFileVersion("1.0.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.7.1", FrameworkDisplayName = ".NET Framework 4.7.1")]
[assembly: ComVisible(false)]
```

Figure 14. GoogleDrive metadata.

It was compiled on June 29, 2022, and masquerades as a Google product. The binary is using Google Drive API to communicate with a Google account for uploads and downloads to a Google Drive share. It uses the following to authenticate to Google's services:

- Client_Id = 477421423157-doqkohd8ihvnpgtsnbld4e4kd1lbs01b.apps.googleusercontent.com
- Client_Secret = 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
- Refresh_Token = 1//0czAXEdbKrikVCgYIARAAGAwSNwF-L9IrjcOVo9aYPFogMEutV6W3cSJMh195N7Ty2cHvtpXf3FNQ9QKDHwN5SKG9FmrMSw5fnsI

Google Drive network authentication example, as shown below:

```
POST /token HTTP/1.1
User-Agent: google-api-dotnet-client/1.0.0.0 (gzip)
Content-Type: application/x-www-form-urlencoded
Host: oauth2.googleapis.com
Content-Length: 279
Connection: Keep-Alive

refresh_token=1%2F%2F0czAXEdbKrikVCgYIARAAGAwSNwF-
L9IrjcOVo9aYPFogMEutV6W3cSJMh195N7Ty2cHvtpXf3FNQ9QKDHwN
5SKG9FmrMSw5fnsI&grant_type=refresh_token&client_id=477
421423157-
doqkohd8ihvnpgtsnbld4e4kd1lbs01b.apps.googleusercontent
.com&client_secret=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
```

Figure 15. GoogleDrive authentication.

The sample has the following PDB string:

```
C:\Users\user\source\repos\GoogleDriveSucks\src\GoogleDriveSucks
\Drive.pdb
```

Figure 16. PDB string.

Once authenticated with Google, the following events occur:

1. For runtime persistence, checks if the registry key AgendaE exists in: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2. If the key does not exist, it is created with the following values:
    1. C:\Users\[USERNAME]\AppData\Roaming\agenda.exe
    2. Copies the following files to C:\Users\[USERNAME]\AppData\Roaming\
        1. _
        2. agenda.exe
        3. vcruntime14.dll
        4. vctool140.dll
3. Generates a random number.
4. Retrieves the username from the running process.
5. Computes the SHA256 of the username.
6. Retrieves information from the victim such as: running processes, machine name and network IP information.
7. Encrypts the data collected in step 6 via the following:
    1. XOR encrypt using a 44-byte key of 0x8F380CDA296F34DE27697A1A53051849B69D59E528D7E669F17CF8D3CF220B6696DA776534401C8A0F0C31C6
    2. Base64 encoded step a.
8. Uploads the data collected from step 7 to the Google Drive share with a unique client ID and a .txt file extension.
9. Creates a comment for the file uploaded in step 8.
10. Checks to see if any files are available to download for the current user ID.
    1. If any files exist, download them – these are payloads.
    2. Payload files are AES-CBC encrypted.
        1. AES key:0x9ECD936FE845D4B20175880E74410851EC3DB30412CB0E57BA6A8E958CB87E21
        2. AES IV: 0x4F083C8599B2F330694A38CA9741409C
    3. Payloads are .Net assembly files
11. Loads and executes downloaded payload file in memory.
12. Finishes.

Campaign 1

For the first campaign observed in late May 2022, the target was a NATO country's Ministry of Foreign Affairs. Similar to the campaign described above, this campaign also used lure files named Agenda.pdf. While two files were delivered to the intended target, for the purpose of this section, we provide analysis on the execution flow for SHA256 a0bdd8a82103f045935c83cb2186524ff3fc2d1324907d9bd644ea5cefacbaaf.

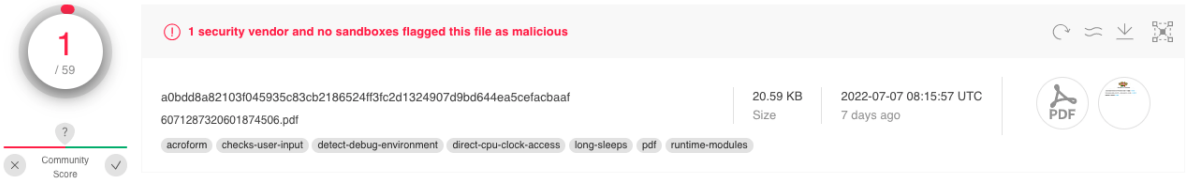


Figure 17. VirusTotal detections for campaign 1 lure file Agenda.pdf

This sample was sent to the target on May 24, 2022 with the following information:

- Email Sender: matysovi@seznam[.]cz
- Email Subject: Meeting request - Ambassador of Portugal
- Source IP: 77.75.78[.]212
- Source Country: Czech Republic (CZ)

This PDF document contains information that appears to address a foreign nation's embassy in Portugal, and even uses an official Portuguese government logo. The document was created on April 4, 2022, and later modified on May 24, 2022. All three URL links in the document point to a DropBox URL that is hosting a file named, Agenda.html. Similar to the campaign above, Agenda.html is EnvyScout, a malicious HTML document. The contents of Agenda.pdf are shown in Figure 18 below.

Figure 18. Campaign 1 lure file Agenda.pdf

A high level overview of campaign 1 is depicted below in figure 19 below.

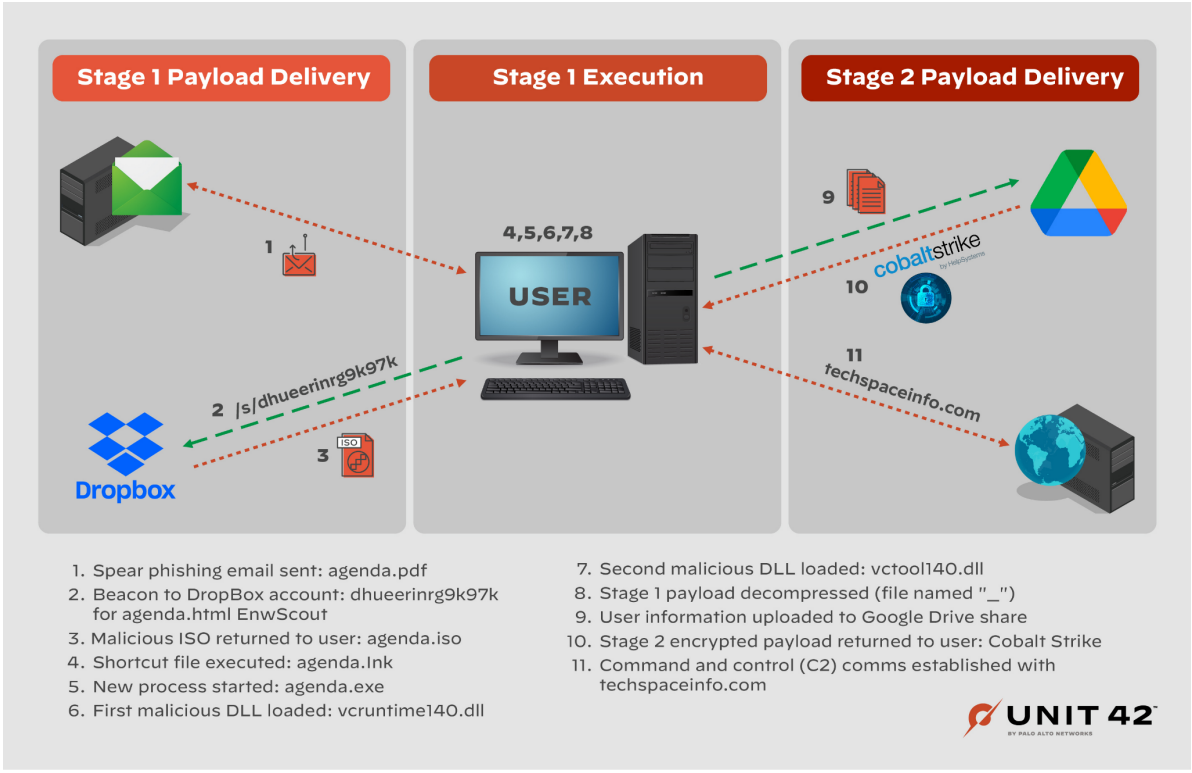


Figure 19. Campaign 1 overview.

The naming convention for the files involved in both campaigns is the same. For brevity, we will focus on the differences between the two campaigns.

Agenda.html (SHA256: cbe92abb2e275770fdff2e9187dee07cce1961b13c0eda94237aceeb06eefbbd) is a malicious HTML file (EnvyScout) that is hosted on DropBox and is identical to the file used in campaign 2 with the exception of the deobfuscation routine that is used to build the malicious ISO file. In campaign 1, the malicious ISO file is generated by subtracting 13 from each value (instead of 17), as shown below.

```
for(var i = 0x0; i < d['length']; i++) {
    d[i]=d[i] -13;
}

var e = new Uint8Array(d);
var f = new Blob([e], {type: "application/octet-stream"});

var fileName = 'agenda.iso';
```

Figure 20. Deobfuscation routine in EnvyScout campaign 1.

The deobfuscated payload, agenda.iso (SHA256: de06cf27884440f51614a41623a4b84e0cb3082d6564ee352f6a4d8cf9d92ec5) has the same file names and hidden file attributes as campaign 2. However, the Windows shortcut file is now named Agenda.lnk versus Information.lnk. A complete file listing is shown below in table 3.

File Name	SHA-256	Description
_	56CFFE5E224ACBE5A7E19446238E5BB9110D9200B6B1EA8B552984D802B71547	File name is underscore. This is a compressed file (MSZIP) that is loaded by vctool140.dll
Agenda.lnk	3C74BB7976B09FE7930D8B66F9E455A36F372696D2C6D64F7A9AE497E17D3E29	Windows shortcut file.
agenda.exe	E8E63F7CF6C25FB3B93AA55D5745393A34E2A98C5AEACBC42F1362DDF64EB0DA	Digitally Signed file by Adobe, Inc.
vcruntime140.dll	A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF	DLL loaded by agenda.exe
vctool140.dll	FBA3A311A4C0A283753B5A0CDCADD3FE19F5A1174F03CB966F14D04BBF3D73EE	Actors DLL used to decompress and in-memory load payload

Table 3. Agenda.iso embedded file properties - Campaign 1.

Agenda.iso has the following properties:

- Created on: 5/24/2022 1:56:19 PM
- Label: AGENDA
- Application ID: IMGBURN V2.5.8.0 - THE ULTIMATE IMAGE BURNER!
- Volume Set ID: UNDEFINED

Once a user double-clicks the Windows shortcut file, Agenda.lnk, the same runtime artifacts occur as in campaign 2, as depicted below:

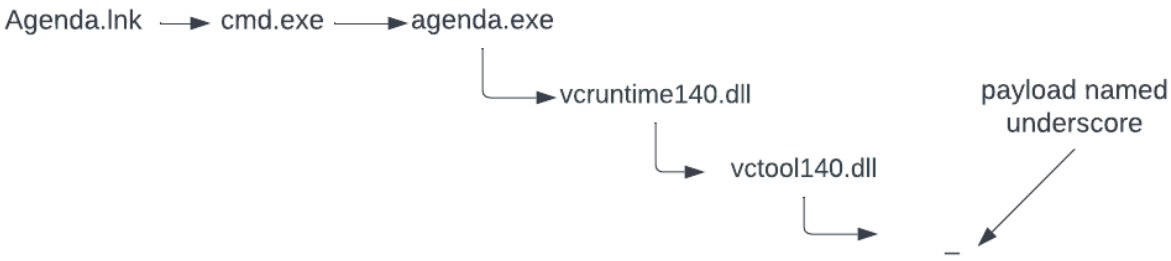


Figure 21. Depiction of runtime artifacts.

The underscore file is the MSZIP compressed payload. It is in-memory loaded by the actor's loader, vctool140.dll. Once decompressed, it is the same code base as in campaign 2, a Google Drive x64 .Net binary. The differences between this Google Drive binary and campaign 2 are:

- It was compiled on May 24, 2022.
- For persistence, creates the following registry key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**AdobeUpdate**
- The credentials for the Google Drive account are:
  - ClientId: 891757970989-9ejifbns5l2to04dtp4uofsi1jtuuftk.apps.googleusercontent.com
  - ClientSecret: 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
  - RefreshToken: 1//09QkhnFYvBS_uCgYIARAAGAkSNwF-L9IrMBe27bDvHC1mqbkHJ3_W4xZRd2sT8G04Ibff4U_fFBIrvYKtWQ1CJKm4FxPnfHUGFAI
- XOR key: 0xDDE5C7BB5B3A13E63A46D9BA9586B86A0BFAE23B6160DF7B14DE5AF187A96F15686034B506EE787E886238
- AES-CBC key: 0x5F7C003E182BBC08B66717894AC934E54FDA2C809391A3FC09CDB7563B707811
- AES IV: 0x4E8E525004C2DBFFFED47E9C087EBA4C

Like campaign 2, both samples share the same PDB string of:

```
C:\Users\user\source\repos\GoogleDriveSucks\src\GoogleDriveSucks\Drive.pdb
```

Figure 22. PDB string.

Conclusion

Cloaked Ursa has been attributed to Russia's Foreign Intelligence Service (SVR) by both the United States and the United Kingdom. Over the past six months, they have launched several phishing campaigns targeting foreign diplomatic missions.

Since early May, Cloaked Ursa has continued to evolve their abilities to deliver malware using popular online storage services. Their two most recent campaigns demonstrate their sophistication and their ability to obfuscate the deployment of their malware through the use of DropBox and Google Drive services. This is a new tactic for this actor and one that proves challenging to detect due to the ubiquitous nature of these services and the fact that they are trusted by millions of customers worldwide.

We encourage all organizations to review their email policies and the IoCs provided in this report in order to address this threat.

Special thanks to Google's Threat Analysis Group (TAG) and DropBox for their collaboration and support for this research.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

WildFire cloud-based threat analysis service accurately identifies the known samples as malicious.

Threat Prevention provides protection against Cobalt Strike Beacon traffic.

Advanced URL Filtering and DNS Security identify domains associated with this group as malicious.

Cortex XDR prevents the execution of known malware samples as malicious and also prevents the execution of Cobalt Strike using Behavioral Threat Protection.

If you think you may have been impacted 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
- Japan: +81.50.1790.0200

Indicators of Compromise

Lure File Samples-PDFs:

CE9802B22A37AE26C02B1F2C3225955A7667495FCE5B106113434AB5A87AE28A
F9B10323B120D8B12E72F74261E9E51A4780AC65F09967D7F4A4F4A8EABC6F4C
A0BDD8A82103F045935C83CB2186524FF3FC2D1324907D9BD644EA5CEFACBAAF

ISO File Samples:

347715F967DA5DEBFB01D3BA2EDE6922801C24988C8E6EA2541E370DED313C8B
DE06CF27884440F51614A41623A4B84E0CB3082D6564EE352F6A4D8CF9D92EC5

EnvyScout Samples-HTML Files:

0ED71B0F4F83590CCA66C0C9E9524A0C01D7A44CF06467C3AE588C1FE5B13118
CBE92ABB2E275770FDFF2E9187DEE07CCE1961B13C0EDA94237ACEEB06EEFBBD

Malicious DLLs:

A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF
9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D
FBA3A311A4C0A283753B5A0CDCADD3FE19F5A1174F03CB966F14D04BBF3D73EE

Compressed Payload Files-Underscore Files:

09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677
56CFFE5E224ACBE5A7E19446238E5BB9110D9200B6B1EA8B552984D802B71547

Decompressed in-memory payload:

295452A87C0FBB48EB87BE9DE061AB4E938194A3FE909D4BCB9BD6FF40B8B2F0
BC9AD574C42BC7B123BAAAFB3325CE2185E92E46979B2FAADDD4BC80DDFAC88A

Infrastructure linked to samples:

porodicno[.]ba/wp-content/Agenda.html
wethe6and9[.]ca/wp-content/Agenda.html
dropbox[.]com/s/raw/dhueerinrg9k97k/agenda.html

Cobalt Strike C2s:

crossfity[.]com
techspaceinfo[.]com

Cobalt Strike IPs:

185.47.128[.]39
31.31.74[.]79

Registry Keys:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AgendaE
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdobeUpdate

Email Senders:

matysovi@seznam[.]cz

Emails:

761ED73512CB4392B98C84A34D3439240A73E389F09C2B4A8F0CCE6A212F529C
4C1ED0F6470D0BBE1CA4447981430E8CEB1157D818656BE9C8A992C56C10B541

XQL Hunting Queries for Cortex XDR

Query 1:

```
// Description: Detect execution of legitimate Adobe binary renamed to Agenda.exe and abused for DLL Side Loading

dataset = xdr_data
| filter
    event_type = PROCESS and
    (
       action_process_signature_vendor = "Adobe Inc." or
       action_process_signature_vendor contains "Adobe Systems"
    ) and
    action_process_image_name = "Agenda.exe"
| fields agent_hostname, actor_effective_username, actor_process_image_path, actor_process_command_line, action_process_image_path, action_process_signature_vendor, action_process_signature_status, action_process_image_command_line
```

Query 2:

```
// Description: Search for registry key indicator matches

dataset = xdr_data
| filter event_type = ENUM.REGISTRY and action_registry_key_name contains """\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run""" and
   (
      action_registry_value_name = "AgendaE" or
      action_registry_value_name = "AdobeUpdate"
   )
| fields event_type, event_sub_type, agent_hostname, actor_effective_username, actor_process_command_line, action_registry*
```

Query 3:

```
// Description: Search for SHA256, IP, or domain indicator matches

dataset = xdr_data | filter
action_file_sha256 in
("09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677","56CFFE5E224ACBE5A7E19446238E
OR
action_module_sha256 in
("09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677","56CFFE5E224ACBE5A7E19446238E
OR
dst_action_external_hostname ~=".*crossfity.com|.*techspaceinfo.com" OR
dns_query_name ~=".*crossfity.com|.*techspaceinfo.com" OR
```

```
action_external_hostname ~=".*crossfity.com|.*techspaceinfo.com" OR
action_remote_ip in ("185.47.128.39","31.31.74.79")
| fields agent_hostname, agent_version,causality_actor_process_image_path, actor_process_image_path, action_file_path, acti
```