Dynamic Malware Analysis Example #1

File Name: e-Archive Dekont.exe

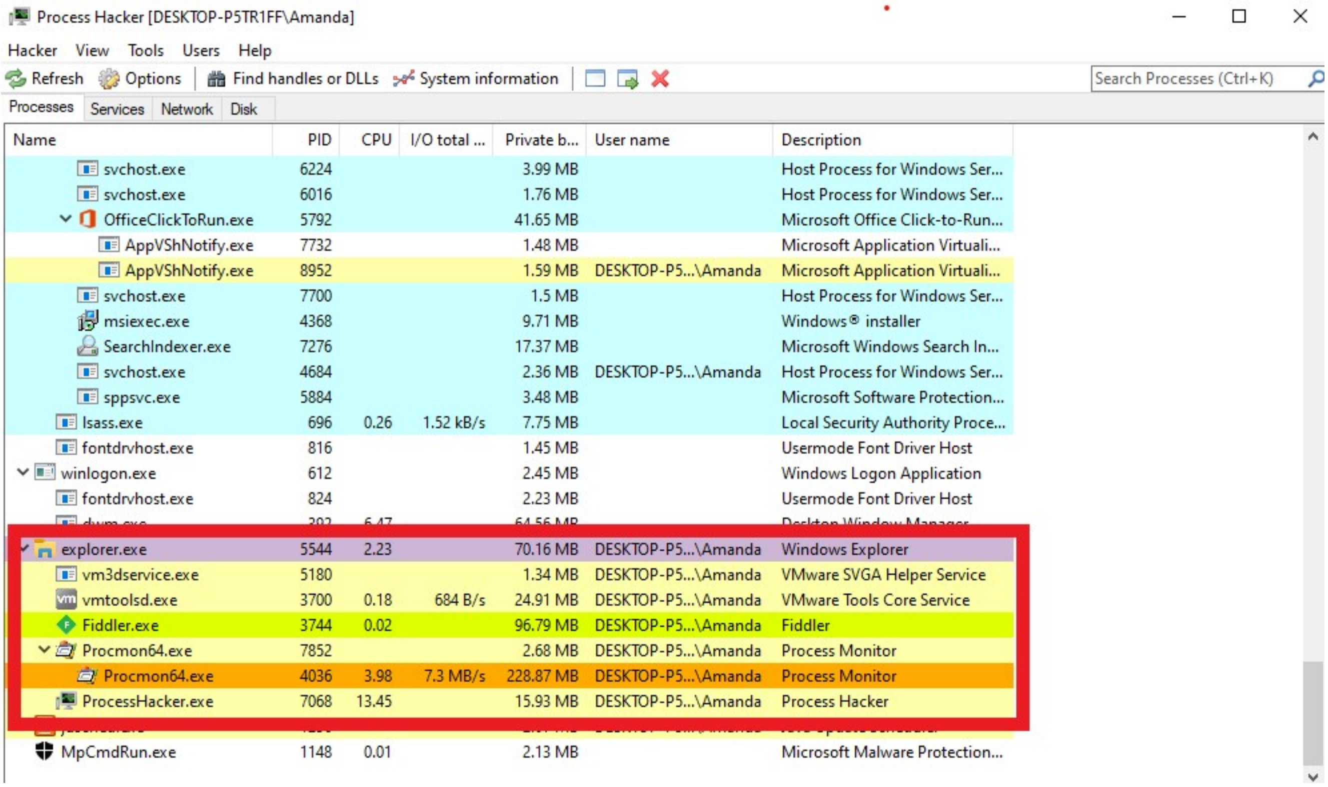
MD5 Hash: 7a0093c743fc33a5e111f2fec269f79b

SHA256 Hash: 722ef401e5cbb067c5c33faa402774d3c75ef08e0c8cc4d7e66a9cfa53684088

Preparing

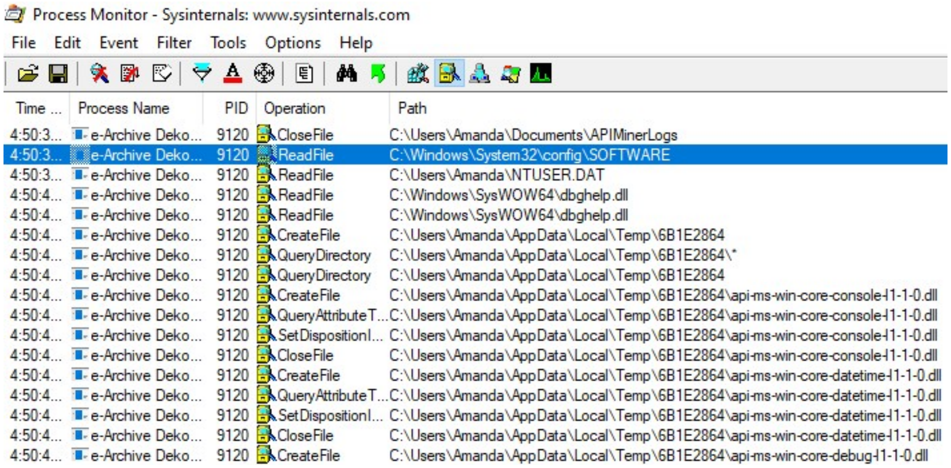
Because our monitoring tools list all the activities that have been done since the time the malware was run, we should run these tools before executing the suspicious program we have. Otherwise, we will not be able to see malicious activities on these tools even though they carry out malicious software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


Process Hacker [DESKTOP-P5TR1FF\Amanda]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

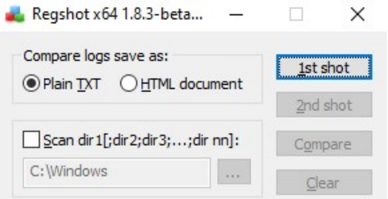
Name	PID	CPU	I/O total ...	Private b...	User name	Description
svchost.exe	6224			3.99 MB		Host Process for Windows Ser...
svchost.exe	6016			1.76 MB		Host Process for Windows Ser...
OfficeClickToRun.exe	5792			41.65 MB		Microsoft Office Click-to-Run...
AppVShNotify.exe	7732			1.48 MB		Microsoft Application Virtuali...
AppVShNotify.exe	8952			1.59 MB	DESKTOP-P5...\Amanda	Microsoft Application Virtuali...
svchost.exe	7700			1.5 MB		Host Process for Windows Ser...
msiexec.exe	4368			9.71 MB		Windows® installer
SearchIndexer.exe	7276			17.37 MB		Microsoft Windows Search In...
svchost.exe	4684			2.36 MB	DESKTOP-P5...\Amanda	Host Process for Windows Ser...
sppsvc.exe	5884			3.48 MB		Microsoft Software Protection...
lsass.exe	696	0.26	1.52 kB/s	7.75 MB		Local Security Authority Proce...
fontdrvhost.exe	816			1.45 MB		Usermode Font Driver Host
winlogon.exe	612			2.45 MB		Windows Logon Application
fontdrvhost.exe	824			2.23 MB		Usermode Font Driver Host
dwm.exe	392	6.47		64.56 MB		Desktop Window Manager
explorer.exe	5544	2.23		70.16 MB	DESKTOP-P5...\Amanda	Windows Explorer
vm3dservice.exe	5180			1.34 MB	DESKTOP-P5...\Amanda	VMware SVGA Helper Service
vmtoolsd.exe	3700	0.18	684 B/s	24.91 MB	DESKTOP-P5...\Amanda	VMware Tools Core Service
Fiddler.exe	3744	0.02		96.79 MB	DESKTOP-P5...\Amanda	Fiddler
Procmon64.exe	7852			2.68 MB	DESKTOP-P5...\Amanda	Process Monitor
Procmon64.exe	4036	3.98	7.3 MB/s	228.87 MB	DESKTOP-P5...\Amanda	Process Monitor
ProcessHacker.exe	7068	13.45		15.93 MB	DESKTOP-P5...\Amanda	Process Hacker
MpCmdRun.exe	1148	0.01		2.13 MB		Microsoft Malware Protection...

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!)


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
4:50:3...	e-Archive Deko...	9120	CloseFile	C:\Users\Amanda\Documents\APIMinerLogs
4:50:3...	e-Archive Deko...	9120	ReadFile	C:\Windows\System32\config\SOFTWARE
4:50:3...	e-Archive Deko...	9120	ReadFile	C:\Users\Amanda\NTUSER.DAT
4:50:4...	e-Archive Deko...	9120	ReadFile	C:\Windows\SysWOW64\dbghelp.dll
4:50:4...	e-Archive Deko...	9120	ReadFile	C:\Windows\SysWOW64\dbghelp.dll
4:50:4...	e-Archive Deko...	9120	CreateFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864
4:50:4...	e-Archive Deko...	9120	QueryDirectory	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\*
4:50:4...	e-Archive Deko...	9120	QueryDirectory	C:\Users\Amanda\AppData\Local\Temp\6B1E2864
4:50:4...	e-Archive Deko...	9120	CreateFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-console-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	QueryAttributeT...	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-console-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	SetDispositionI...	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-console-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	CloseFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-console-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	CreateFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-datetime-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	QueryAttributeT...	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-datetime-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	SetDispositionI...	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-datetime-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	CloseFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-datetime-l1-1-0.dll
4:50:4...	e-Archive Deko...	9120	CreateFile	C:\Users\Amanda\AppData\Local\Temp\6B1E2864\api-ms-win-core-debug-l1-1-0.dll

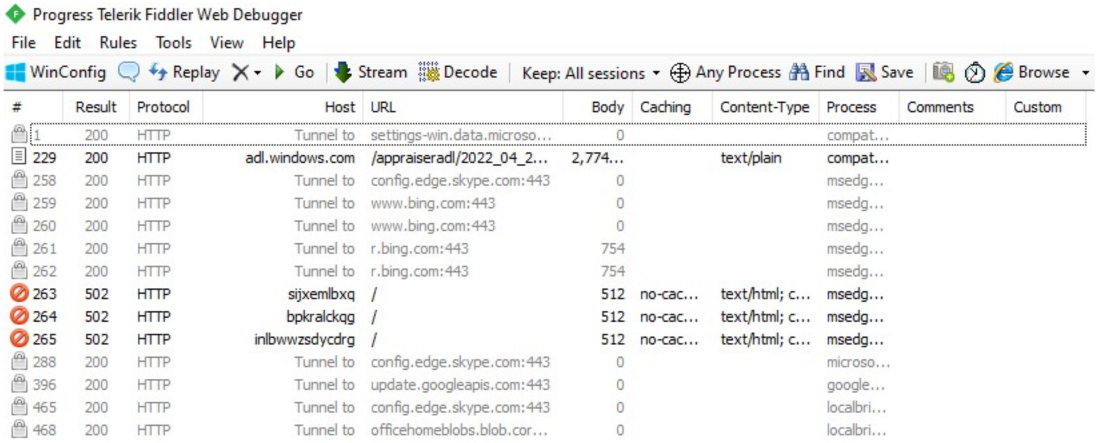
Run RegShot to see registry activities. Take a shot by pressing the “1st shot” button before running the malware. This process will take some time.



Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

You can use Wireshark and Fiddler to see network activities. Fiddler will suffice, as the malware we reviewed communicates over the HTTP protocol.


Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse

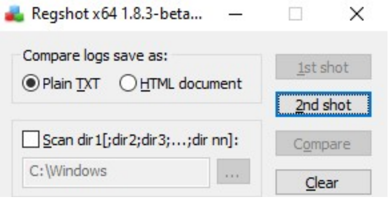
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	Tunnel to	settings-win.data.microso...	0			compat...		
229	200	HTTP	adl.windows.com	/appraiseradl/2022_04_2...	2,774...		text/plain	compat...		
258	200	HTTP	Tunnel to	config.edge.skype.com:443	0			msedg...		
259	200	HTTP	Tunnel to	www.bing.com:443	0			msedg...		
260	200	HTTP	Tunnel to	www.bing.com:443	0			msedg...		
261	200	HTTP	Tunnel to	r.bing.com:443	754			msedg...		
262	200	HTTP	Tunnel to	r.bing.com:443	754			msedg...		
263	502	HTTP	sijxemlbxq	/	512	no-cac...	text/html; c...	msedg...		
264	502	HTTP	bpkralckqg	/	512	no-cac...	text/html; c...	msedg...		
265	502	HTTP	inlbwwzsdycdrg	/	512	no-cac...	text/html; c...	msedg...		
288	200	HTTP	Tunnel to	config.edge.skype.com:443	0			microso...		
396	200	HTTP	Tunnel to	update.googleapis.com:443	0			google...		
465	200	HTTP	Tunnel to	config.edge.skype.com:443	0			localbri...		
468	200	HTTP	Tunnel to	officehomeblobs.blob.cor...	0			localbri...		

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.



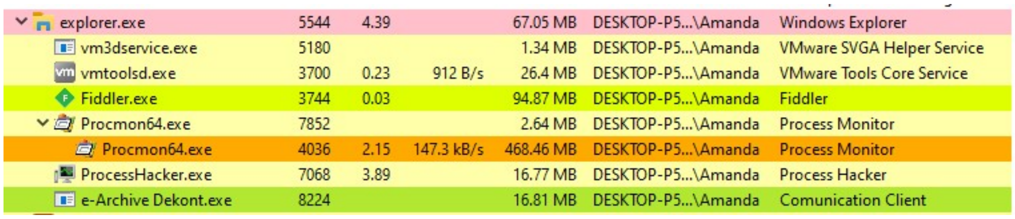
Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

Process Activities

As we mentioned earlier in our training series, there are some advantages of detecting process activities first. Since we will encounter a lot of logs and activities, the first step we need to do is to detect the processes belonging to the malware.

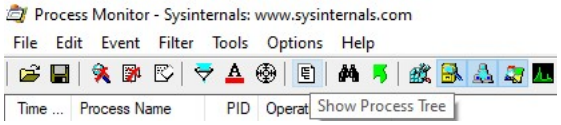
When we examine the processes occurred over Process Hacker, we see that only one process belonging to the malware is running.



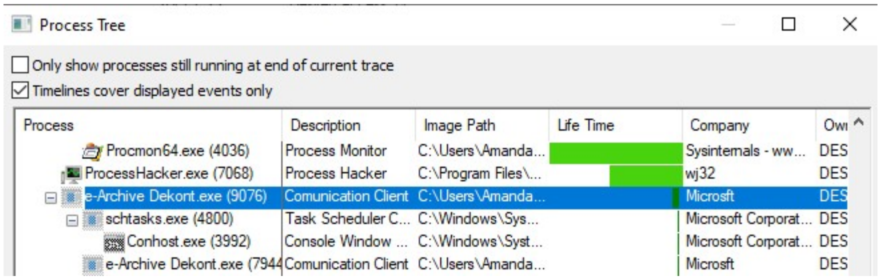
explorer.exe	5544	4.39		67.05 MB	DESKTOP-P5...\Amanda	Windows Explorer
vm3dservice.exe	5180			1.34 MB	DESKTOP-P5...\Amanda	VMware SVGA Helper Service
vmtoolsd.exe	3700	0.23	912 B/s	26.4 MB	DESKTOP-P5...\Amanda	VMware Tools Core Service
Fiddler.exe	3744	0.03		94.87 MB	DESKTOP-P5...\Amanda	Fiddler
Procmon64.exe	7852			2.64 MB	DESKTOP-P5...\Amanda	Process Monitor
Procmon64.exe	4036	2.15	147.3 kB/s	468.46 MB	DESKTOP-P5...\Amanda	Process Monitor
ProcessHacker.exe	7068	3.89		16.77 MB	DESKTOP-P5...\Amanda	Process Hacker
e-Archive Dekont.exe	8224			16.81 MB	DESKTOP-P5...\Amanda	Comunication Client

However, things are not always as they seem! Since Process Hacker only shows the processes that are running momentarily, the malware may have created a child process at a time we did not monitor and terminated it later.

At this point, the Procmon tool comes to our rescue. 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.



The process tree provided by Procmon completes this shortcoming of Process Hacker, as it also includes terminated processes.



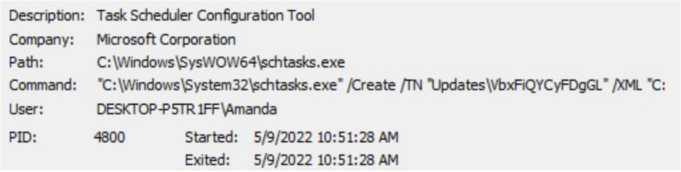
□ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owi
Procmon64.exe (4036)	Process Monitor	C:\Users\Amanda...		Sysinternals - ww...	DES
ProcessHacker.exe (7068)	Process Hacker	C:\Program Files\...		wj32	DES
e-Archive Dekont.exe (9076)	Comunication Client	C:\Users\Amanda...		Microsft	DES
schtasks.exe (4800)	Task Scheduler C...	C:\Windows\Sys...		Microsoft Corporat...	DES
Conhost.exe (3992)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DES
e-Archive Dekont.exe (7944	Comunication Client	C:\Users\Amanda...		Microsft	DES

When we go over the the image above, we see that the first process we run (9076 PID) runs the tool called “schtasks.exe” belonging to Windows Task Scheduler (PID 4800) and then runs its own malware (7944 PID) again.

Before moving on to other activities, let's examine the schtasks.exe process. Schtasks.exe is a tool that enables the Task Scheduler to be used via the command interface in the Windows operating system. Attackers ensure persistency by adding their own malware to scheduled tasks with the help of Task Scheduler.

In order to see what kind of scheduled task the attacker added, we must click on the "schtasks.exe" (4800 PID) in the process tree of procmon and examine its details.



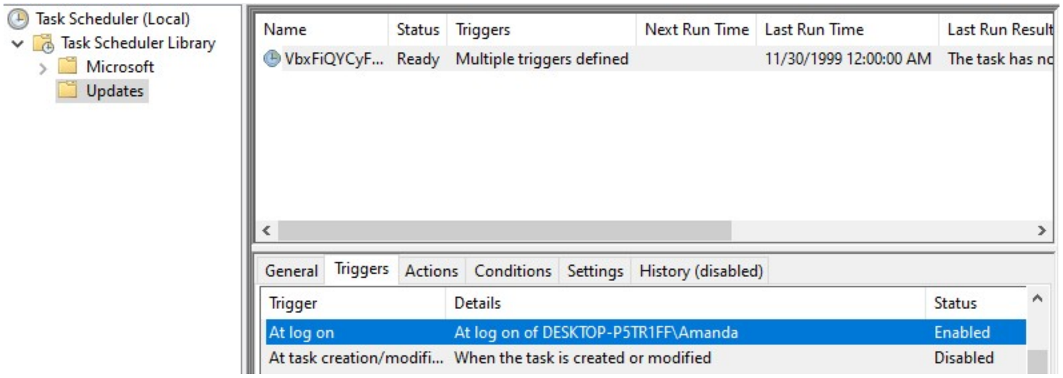
```
Description:  Task Scheduler Configuration Tool
Company:      Microsoft Corporation
Path:         C:\Windows\SysWOW64\schtasks.exe
Command:      "C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VbxFiQYCyFDgGL" /XML "C:
User:         DESKTOP-P5TR1FF\Amanda
PID:          4800       Started:  5/9/2022 10:51:28 AM
                         Exited:   5/9/2022 10:51:28 AM
```

When we examine the command-line arguments, we see that a scheduled task named "Updates\VbxFiQYCyFDgGL" has been created. However, the information of the scheduled task except for its name is in the XML file located at the following path:

“C:\Users\Amanda\AppData\Local\Temp\tmpCCF2.tmp”.

Click here to get information about the command-line arguments of the tool named Schtasks.exe.

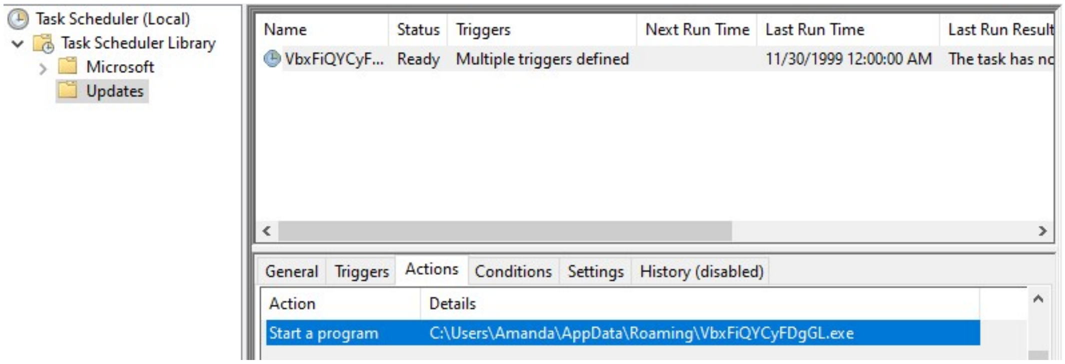
When you try to access the relevant file, you can see that the file is deleted. But don't worry, this scheduled task is now saved so we can see it through the Scheduler Task.



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
VbxFiQYCyF...	Ready	Multiple triggers defined		11/30/1999 12:00:00 AM	The task has no

Trigger	Details	Status
At log on	At log on of DESKTOP-P5TR1FF\Amanda	Enabled
At task creation/modifi...	When the task is created or modified	Disabled

On the Trigger tab, you can see in which situations this scheduled task added by the attacker will run. As it can be seen on the screenshot above this scheduled task will run at log on.



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
VbxFiQYCyF...	Ready	Multiple triggers defined		11/30/1999 12:00:00 AM	The task has nc

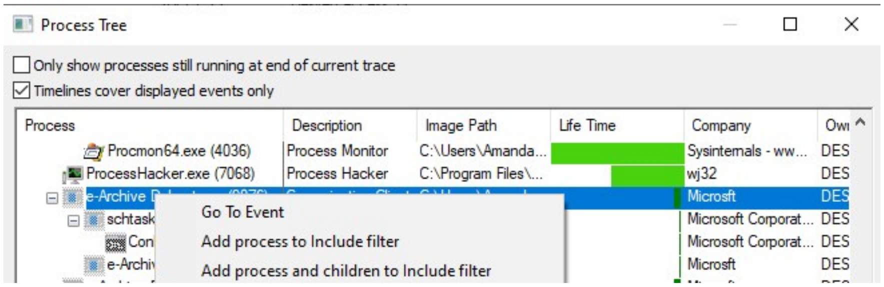
Action	Details
Start a program	C:\Users\Amanda\AppData\Roaming\VbxFiQYCyFDgGL.exe

You can see what action will run on the Actions tab. You can see on the above screenshot that the malicious software named “VbxFiQYCyFDgGL.exe” prepared by the attacker will run when this scheduled task runs.

This is how we have detected the scheduled task that the attacker added.

We detected malware processes (9076, 4800, 7944 PIDs) with the help of Procmon. Next, we need to detect the network, file and registry activities of these processes.

You filter down the processes with PID values of 9076, 4800, 7944 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.


Process Tree
Go To Event
Add process to Include filter
Add process and children to Include filter

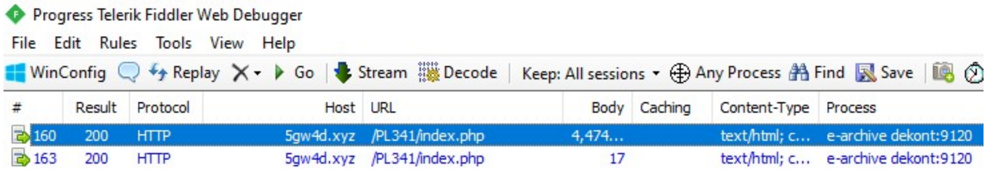
☐ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Ow
Procmon64.exe (4036)	Process Monitor	C:\Users\Amanda...		Sysinternals - ww...	DES
ProcessHacker.exe (7068)	Process Hacker	C:\Program Files\...		wj32	DES
e-Archive D				Microsft	DES
schtask				Microsoft Corporat...	DES
Con				Microsoft Corporat...	DES
e-Archiv				Microsft	DES

Network Activities

Since the malware we examined communicates over the HTTP protocol, you can detect the connections it establishes very easily using the Fiddler tool.

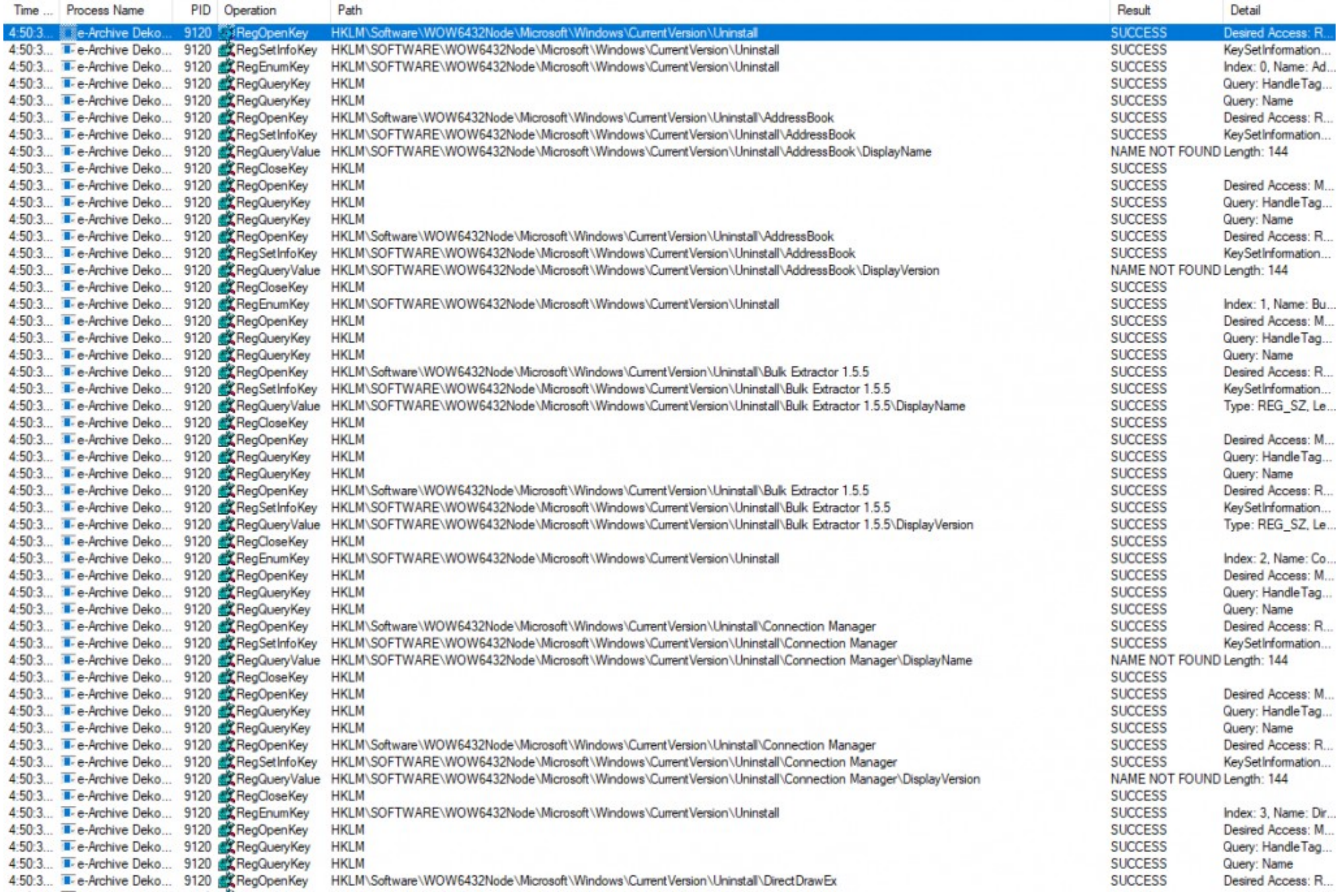
After running the malware, you can see that the process named “e-archive dekont.exe” on Fiddler communicates with the domain “**5gw4d[.]xyz**”.



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
160	200	HTTP	5gw4d.xyz	/PL341/index.php	4,474...		text/html; c...	e-archive dekont:9120
163	200	HTTP	5gw4d.xyz	/PL341/index.php	17		text/html; c...	e-archive dekont:9120

Registry Activities

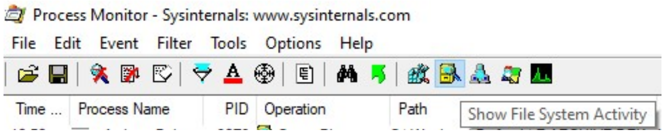
When we examine the registry activities, you can see that the keys under HKLM\Software\WOW6432Node\Microsoft\Windows\CurrrentVersion\Uninstall are queried. There are settings under this key that are left by the applications installed in the system for uninstall. It is often preferred to enumerate this key to detect applications installed on the system by attackers.



```
Time ...  Process Name        PID  Operation      Path                                                                                   Result          Detail
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegEnumKey     HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         Index: 0, Name: Ad...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook                       SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook                       SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName           NAME NOT FOUND  Length: 144
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook                       SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook                       SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayVersion        NAME NOT FOUND  Length: 144
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegEnumKey     HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         Index: 1, Name: Bu...
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5              SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5              SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5\DisplayName  SUCCESS         Type: REG_SZ, Le...
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5              SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5              SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Bulk Extractor 1.5.5\DisplayVersion SUCCESS        Type: REG_SZ, Le...
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegEnumKey     HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         Index: 2, Name: Co...
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager                SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager                SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName    NAME NOT FOUND  Length: 144
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager                SUCCESS         Desired Access: R...
4:50:3... e-Archive Deko...  9120  RegSetInfoKey  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager                SUCCESS         KeySetInformation...
4:50:3... e-Archive Deko...  9120  RegQueryValue  HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayVersion NAME NOT FOUND  Length: 144
4:50:3... e-Archive Deko...  9120  RegCloseKey    HKLM                                                                                                   SUCCESS
4:50:3... e-Archive Deko...  9120  RegEnumKey     HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall                                   SUCCESS         Index: 3, Name: Dir...
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM                                                                                                   SUCCESS         Desired Access: M...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: HandleTag...
4:50:3... e-Archive Deko...  9120  RegQueryKey    HKLM                                                                                                   SUCCESS         Query: Name
4:50:3... e-Archive Deko...  9120  RegOpenKey     HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx                      SUCCESS         Desired Access: R...
```

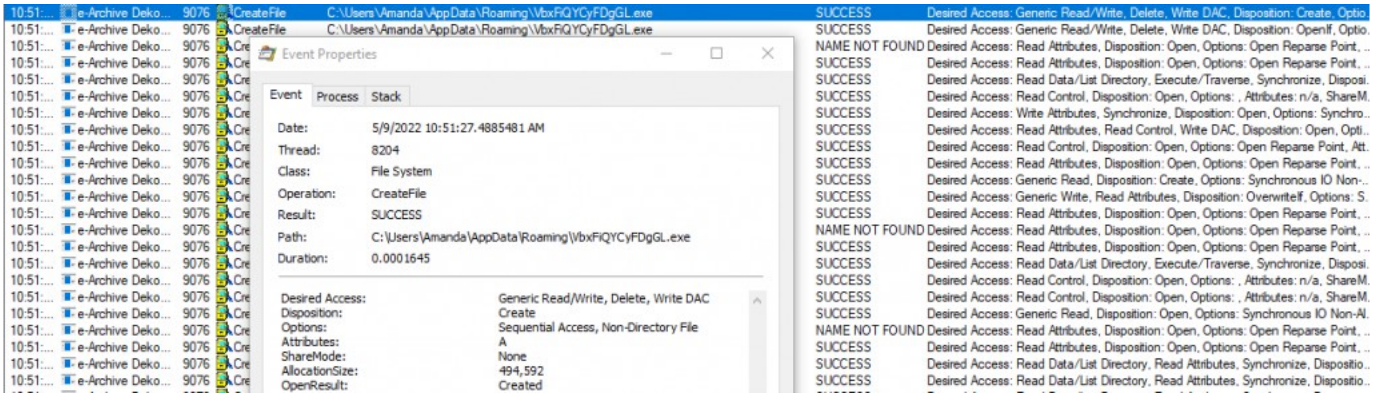
File Activities

To detect malware file activities, disable the other three activities in the top menu of procmon.


Process Monitor - Sysinternals: www.sysinternals.com
File
Edit
Event
Filter
Tools
Options
Help
Time ...
Process Name
PID
Operation
Path
Show File System Activity

You can enter a filter with Operation=CreateFile to see file creation activities.

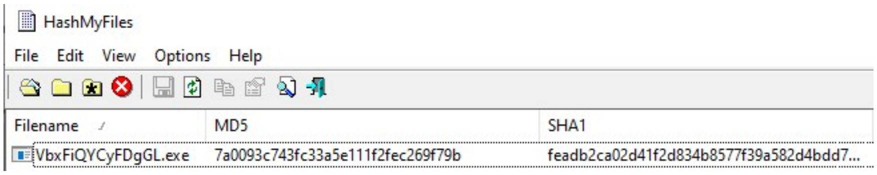
When we examine the logs, we see that an executable file named "VbxFiQYCyFDgGL.exe" is written under the "C:\Users\Amanda\AppData\Roaming\" directory.



```
10:51:...  e-Archive Deko...  9076  CreateFile  C:\Users\Amanda\AppData\Roaming\VbxFiQYCyFDgGL.exe  SUCCESS         Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: Create, Optio
10:51:...  e-Archive Deko...  9076  CreateFile  C:\Users\Amanda\AppData\Roaming\VbxFiQYCyFDgGL.exe  SUCCESS         Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: OpenIf, Optio.
10:51:...  e-Archive Deko...  9076  Cre                                                            NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposi.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareM.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Synchro..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Read Control, Write DAC, Disposition: Open, Opti..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Control, Disposition: Open, Options: Open Reparse Point, Att.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Generic Read, Disposition: Create, Options: Synchronous IO Non-..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: S.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposi.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareM.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareM.
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Al.
10:51:...  e-Archive Deko...  9076  Cre                                                            NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, ..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Dispositio..
10:51:...  e-Archive Deko...  9076  Cre                                                            SUCCESS         Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Dispositio..
```

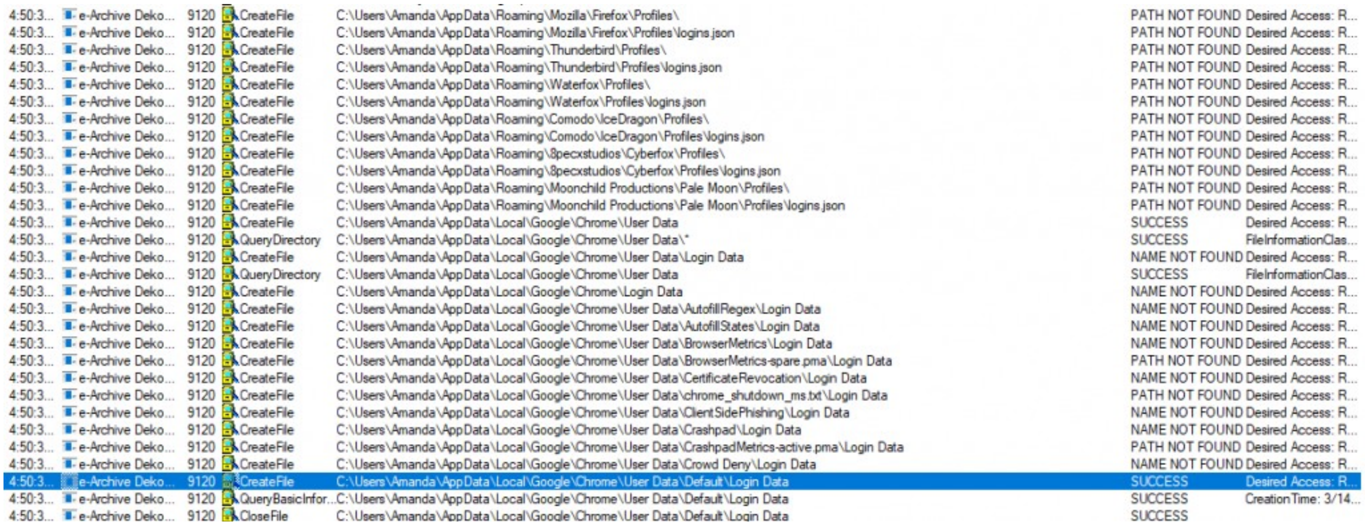
```
Event Properties

Event   Process   Stack

Date:        5/9/2022 10:51:27.4885481 AM
Thread:      8204
Class:       File System
Operation:   CreateFile
Result:      SUCCESS
Path:        C:\Users\Amanda\AppData\Roaming\VbxFiQYCyFDgGL.exe
Duration:    0.0001645

Desired Access:      Generic Read/Write, Delete, Write DAC
Disposition:         Create
Options:             Sequential Access, Non-Directory File
Attributes:          A
ShareMode:           None
AllocationSize:      494,592
OpenResult:          Created
```

When we look at the hash of the application named “VbxFiQYCyFDgGL.exe” with the tool called HashMyFiles, we see that it is actually the same file as the file we analyzed first. We see that the malware has copied itself to a different folder.



Filename	MD5	SHA1
VbxFiQYCyFDgGL.exe	7a0093c743fc33a5e111f2fec269f79b	feadb2ca02d41f2d834b8577f39a582d4bdd7...

When we examine the file activities further, we see that the malware reads the files to steal information from applications such as Firefox, Chome, Thunderbird. We have determined that the malware we have is information stealer.



```
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Mozilla\Firefox\Profiles\                                              PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Mozilla\Firefox\Profiles\logins.json                                   PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Thunderbird\Profiles\                                                  PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Thunderbird\Profiles\logins.json                                       PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Waterfox\Profiles\                                                     PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Waterfox\Profiles\logins.json                                          PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Comodo\IceDragon\Profiles\                                             PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Comodo\IceDragon\Profiles\logins.json                                  PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\8pecxstudios\Cyberfox\Profiles\                                        PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\8pecxstudios\Cyberfox\Profiles\logins.json                             PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\                              PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Roaming\Moonchild Productions\Pale Moon\Profiles\logins.json                   PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data                                                  SUCCESS         Desired Access: R...
4:50:3...  e-Archive Deko...  9120  QueryDirectory      C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\*                                                SUCCESS         FileInformationClas...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Login Data                                       NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  QueryDirectory      C:\Users\Amanda\AppData\Local\Google\Chrome\User Data                                                  SUCCESS         FileInformationClas...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\Login Data                                                 NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\AutofillRegex\Login Data                         NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\AutofillStates\Login Data                        NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\BrowserMetrics\Login Data                        NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\BrowserMetrics-spare.pma\Login Data              PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\CertificateRevocation\Login Data                 NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\chrome_shutdown_ms.txt\Login Data                PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\ClientSidePhishing\Login Data                    NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Crashpad\Login Data                              NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma\Login Data            PATH NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Crowd Deny\Login Data                            NAME NOT FOUND  Desired Access: R...
4:50:3...  e-Archive Deko...  9120  CreateFile          C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Default\Login Data                               SUCCESS         Desired Access: R...
4:50:3...  e-Archive Deko...  9120  QueryBasicInfor...  C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Default\Login Data                               SUCCESS         CreationTime: 3/14...
4:50:3...  e-Archive Deko...  9120  CloseFile           C:\Users\Amanda\AppData\Local\Google\Chrome\User Data\Default\Login Data                               SUCCESS
```

Result

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

- the malware has copied itself to the "C:\Users\Username\AppData\Roaming\" directory with the name "VbxFiQYCyFDgGL.exe",
- has used Task Scheduler to ensure persistence,
- has enabled its own malicious application to run at every logon by creating a scheduled task with the name "VbxFiQYCyFDgGL"
- communicates with the command & control server,
- the command control address is “5gw4d[.]xyz/PL341/index.php” and it communicates over the HTTP protocol,
- discovers the applications installed in the system with the help of the key under the "HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall" registry key,
- steals sensitive data from applications such as Chrome, Firefox, Thunderbird.

Artifacts

MD5: 7a0093c743fc33a5e111f2fec269f79b
SHA256: 722ef401e5cbb067c5c33faa402774d3c75ef08e0c8cc4d7e66a9cfa53684088
File Name: e-Archive Dekont.exe
File Name: VbxFiQYCyFDgGL.exe
Domain: 5gw4d[.]xyz
URL: http[:]//5gw4d[.]xyz/PL341/index.php