

Dynamic Analysis Workflow

Follow sequence exactly

1. Start procmon, then pause and clear
2. Start Fakenet
3. Start Regshot, then take 1st shot
4. Once 1st shot completes, Resume procmon
5. Run Malware for about 1 – 3 mins and study fakenet output
6. After about 3 mins pause procmon
7. Use Regshot, to take 2nd shot
8. Once 2nd shot completes, click Compare->Compare and show output
9. Study Regshot output

Work flow sequence continued

- In procmon apply these filters:
- ProcessName is: malware-name
- Operation is:
 - WriteFile
 - SetDispositionInformationFile
 - RegSetValue
 - ProcessCreate
 - TCP
 - UDP

Procmon filters

ProcMon Operations

File Operations	Registry Operations
CreateFile	RegCreateKey
ReadFile	RegQueryValue
<u>WriteFile</u>	<u>RegSetValue</u>
<u>SetDispositionInformationFile</u>	<u>RegDeleteKey</u>
	<u>RegDeleteValue</u>

ProcMon Operations

Process Operations	Network Operations
ProcessStart	TCP*
<u>ProcessCreate</u>	UDP*

Procmon filters continued

```
on="1.3.35.441" ismachine="1" sessionid="{17E1747A-52B8-47F7-B928-FD1F
741AC5F-P58B-4465-B35F-EABA43833282}" dedup="cr" domainjoined="0"><hw
sse41="1" sse42="1" avx="1"/><os platform="win" version="6.1.7601.0"
4D0-B729-4F61-AA34-91526481799D)" version="1.3.36.72" nextversion="" 1
ec3=202113R" installage="391" installdate="4823" cohort="1:9co:" cohor
ping_freshness="{29B71476-CE97-4220-B92E-197B967BD96F}"/></app><app
sion="89.0.4389.114" nextversion="" lang="en" brand="GGLS" client="" e
installdate="4823" cohort="1:gu:zi300.5" cohortname="Stable"><updateche
80658-B767-4D68-BF34-7413AF300A50>"/></app></request>
Storing HTTP POST headers and data to http_20210415_132913.txt.
POST /service/update?cup2key=10:3144470437&cup2hreq=785ab222d9ae0
HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
```

Process Monitor Filter

Display entries matching these conditions:

Operation is Process Create then Include

Reset Add Remove

Column	Relation	Value	Action		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process N...	is	financials-xls.exe	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	WriteFile	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	SetDispositionInformationFile	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	RegSetValue	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	TCP	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	UDP	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Operation	is	Process Create	Include
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	Procexp.exe	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	Autouns.exe	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	Procmon64.exe	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	Procexp64.exe	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Process N...	is	System	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Operation	begins with	IRP_MJ_	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Operation	begins with	FASTIO_	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Result	begins with	FAST IO	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Path	ends with	pagefile.sys	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Path	ends with	\$Mft	Exclude
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Path	ends with	\$MftMir	Exclude

OK Cancel Apply

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

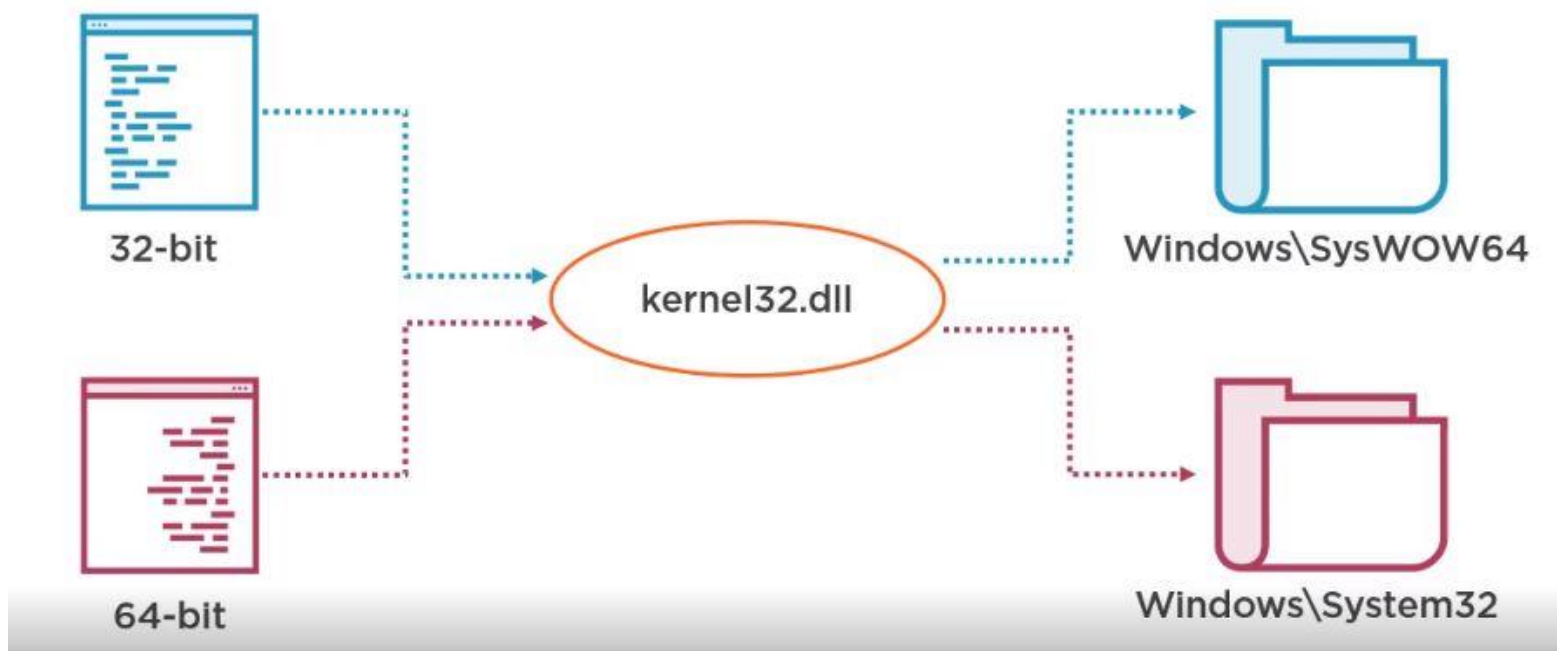
Time ...	Process Name	PID	Operation	Path	Result
1:00:3...	financials-xls.exe	2132	WriteFile	C:\Windows\xpupdate.exe	SUCCESS
1:00:3...	financials-xls.exe	2132	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS
1:00:4...	financials-xls.exe	2132	WriteFile	C:\Users\pc\AppData\Roaming\Install...	SUCCESS
1:00:4...	financials-xls.exe	2132	RegSetValue	HKCU\Software\Install\Version	SUCCESS
1:00:4...	financials-xls.exe	2132	RegSetValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS

Showing 5 of 108,933 events (0.0045%) Backed by virtual memory

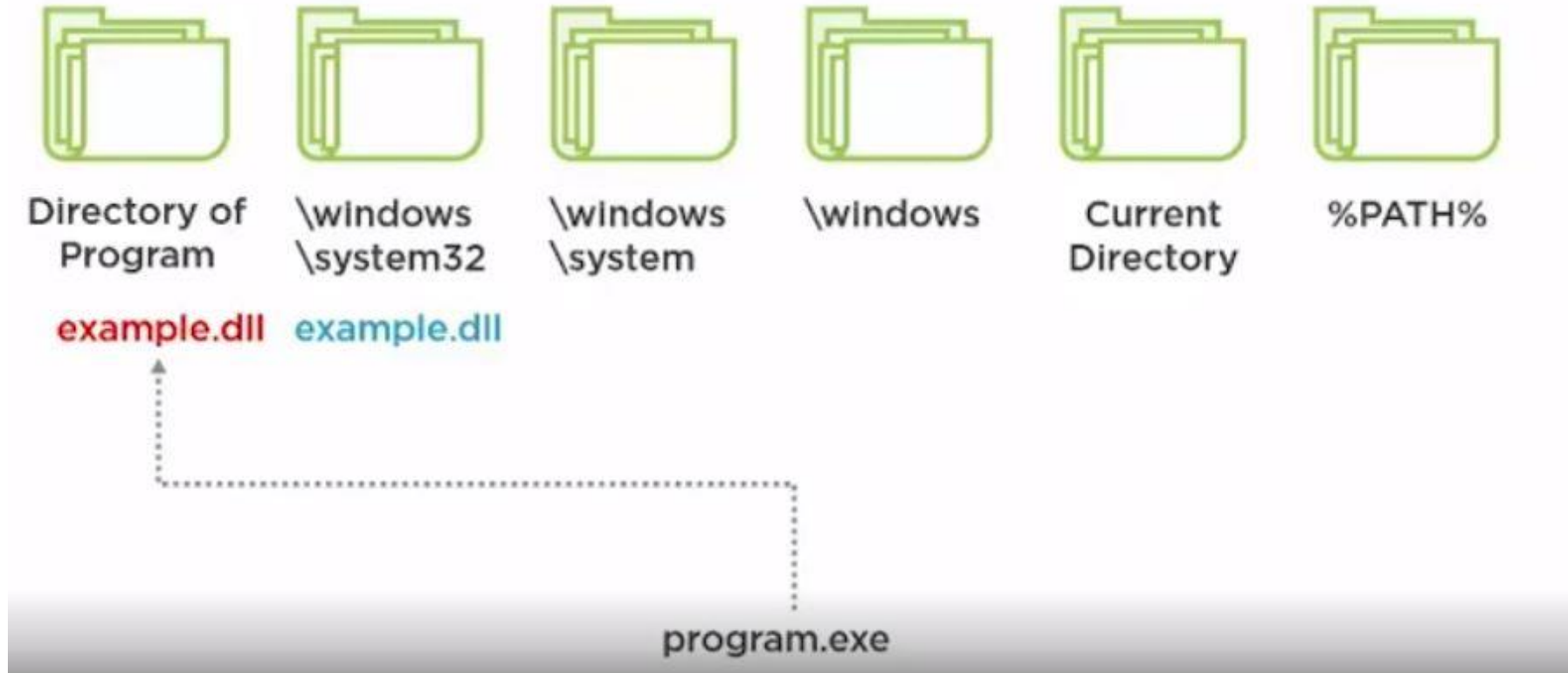
Registry Persistence

	<code>\Software\Microsoft\Windows\CurrentVersion\Run</code>
	<code>\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>
HKLM	<code>\Software\Microsoft\Windows\CurrentVersion\RunServices</code>
HKU	<code>\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
HKCU	<code>\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>
	<code>\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs</code>

32-bit Programs on 64-bit Windows



DLL Search Order



Network Analysis

- Fakenet will save a pcap file in the logs folder
- Use Wireshark to open it
- Filter out http
- Trace the TCP stream

Thank you