Software Reverse Engineering

COMP 272 | Spring 2022 | University of the Pacific | Jeff Shafer

Behavioral Analysis

Malware

Dark Caracal – January 2018

- "Dark Caracal" is name of *spyware campaign*
- Operations observed (w/ different malware) since 2012
  - Publically disclosed in 2018 in joint report by EFF and Lookout
- Advanced Persistent Threat (APT) surveillance targeting individuals and institutions (utilities, financial institutions, defense contractors, …)
  - Observed operations exfiltrating "hundreds of gigabytes of data"
- Authors: Lebanese General Security Directorate (alleged)
  - Attack infrastructure correlated to building they own
  - *So we have to watch out for* Lebanon *now too??*

Dark Caracal – January 2018

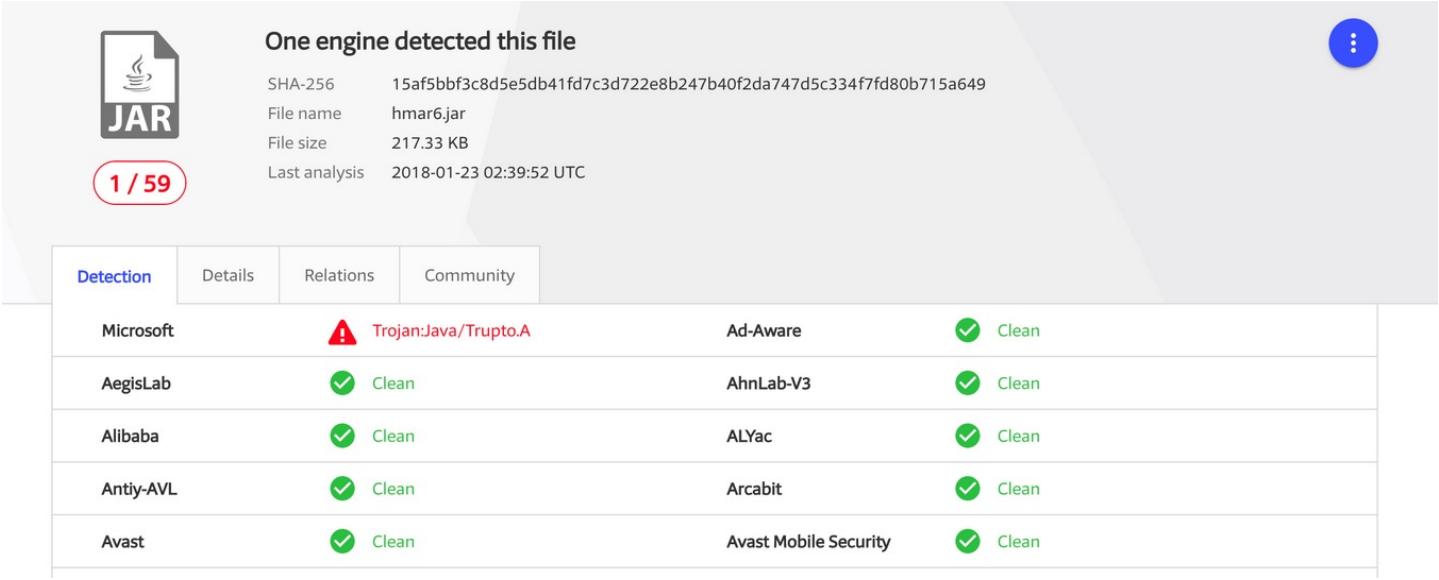
- Multiple tools in use since inception
  - *FinFisher* – “lawful intercept” tool sold to governments for “legitimate purposes”
  - *Bandook RAT* - Original RAT, Windows-only
  - *CrossRAT* – New RAT? Cross platform! (Windows, OSX, Linux) Written in Java
  - *Pallas* – Android malware in trojanized apps
- Capture documents, messaging clients (contacts and messages), audio, …
  - Mobile component

Dark Caracal

- SHA256 for CrossRAT:
  15af5bbf3c8d5e5db41fd7c3d722e8b247b40f2da747d5c334f7fd80b715a649

VirusTotal detection on 1/23/2018

Thanks to digitalsecurity.com



Dark Caracal

- Dark Caracal: Cyber-espionage at a Global Scale
  - https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
- **Very good report – you should at least read the executive summary**
  - 11 Android malware IOCs
  - 26 desktop malware IOCs
  - 60 domains and IP addresses
  - Lots of hashes to search for

Dark Caracal

- Analyzing CrossRAT: A cross-platform implant, utilized in a global cyber-espionage campaign
  - https://digitasecurity.com/blog/2018/01/23/crossrat/

Analysis Tools

Build Your Own: Malware Analysis Lab

- **What tools do we need in the lab?**
- **Static property analysis** (program *not* running)
  - PEStudio, Strings, BinText, …
- **Interactive behavioral analysis** (program *is* running)
  - Process Hacker, RegShot, Wireshark, API Monitor, …
- **Code analysis/reversing (We 🖤 Assembly)**
  - IDA Pro, Ghidra, x64dbg, OllyDbg, …

pestudio 8.72 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\cyberlab\desktop\ma
- indicators (1/11)
- virustotal (42/67 - 04.11.20
- dos-stub (!This program c
- file-header (Jun.2014)
- optional-header (GUI)
- directories (2)
- sections (99.34%)
- libraries (kernel32)
- imports (1/1/0/1)
- exports (0)
- tls-callbacks (n/a)
- resources (n/a)
- strings (1/1/0/721)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
md5	24CE99418862CB0C04E46FBA245596AB
sha1	7AFFA14EC4892FD3924E9B2E0FF66FA496303336
sha256	5B59DCF29F8271EBD0AC6D64EE02E8B1A15CF5D030CC098E9A903960685D6C97
first-bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00
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
file-description	n/a
file-type	executable
subsystem	GUI
compiler-stamp	Tue Jun 03 11:36:59 2014
debugger-stamp	n/a

sha256: 5B59DCF29F8271EBD0AC6D64EE02E8B1A15CF5D030CC098E9A903960685D6C97 | cpu: 32-bit | file-type: exe

- **PEStudio**
  - Static analysis
- Hash values
  - MD5
  - SHA1
  - SHA256
- 32 or 64 bit

pestudio 8.72 - Malware Initial Assessment - www.winitor.com

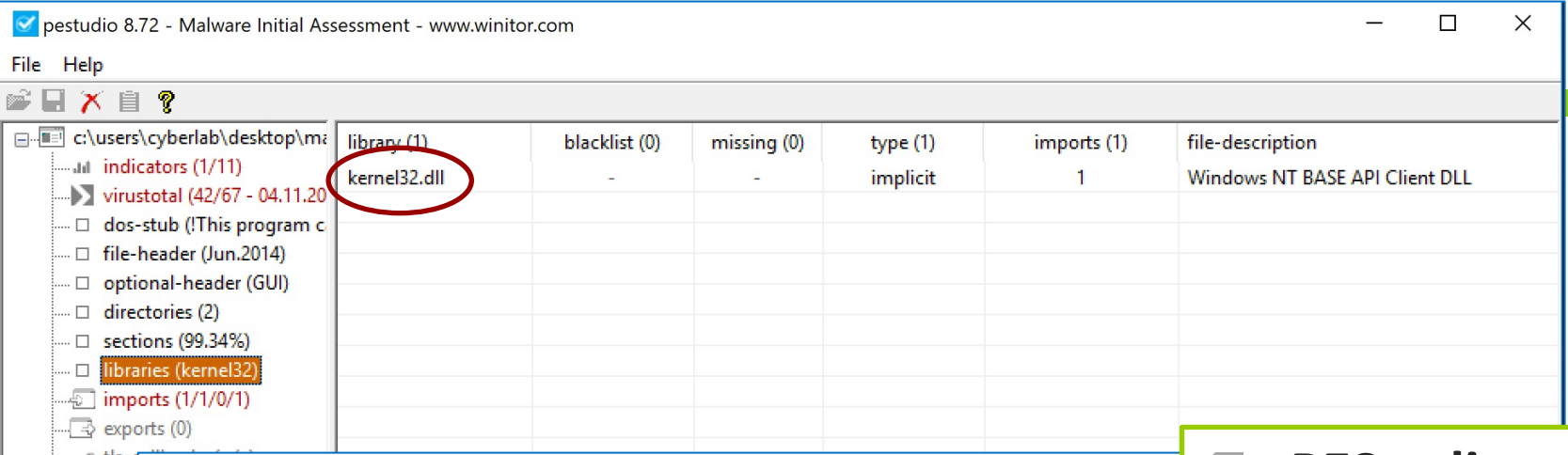
File Help

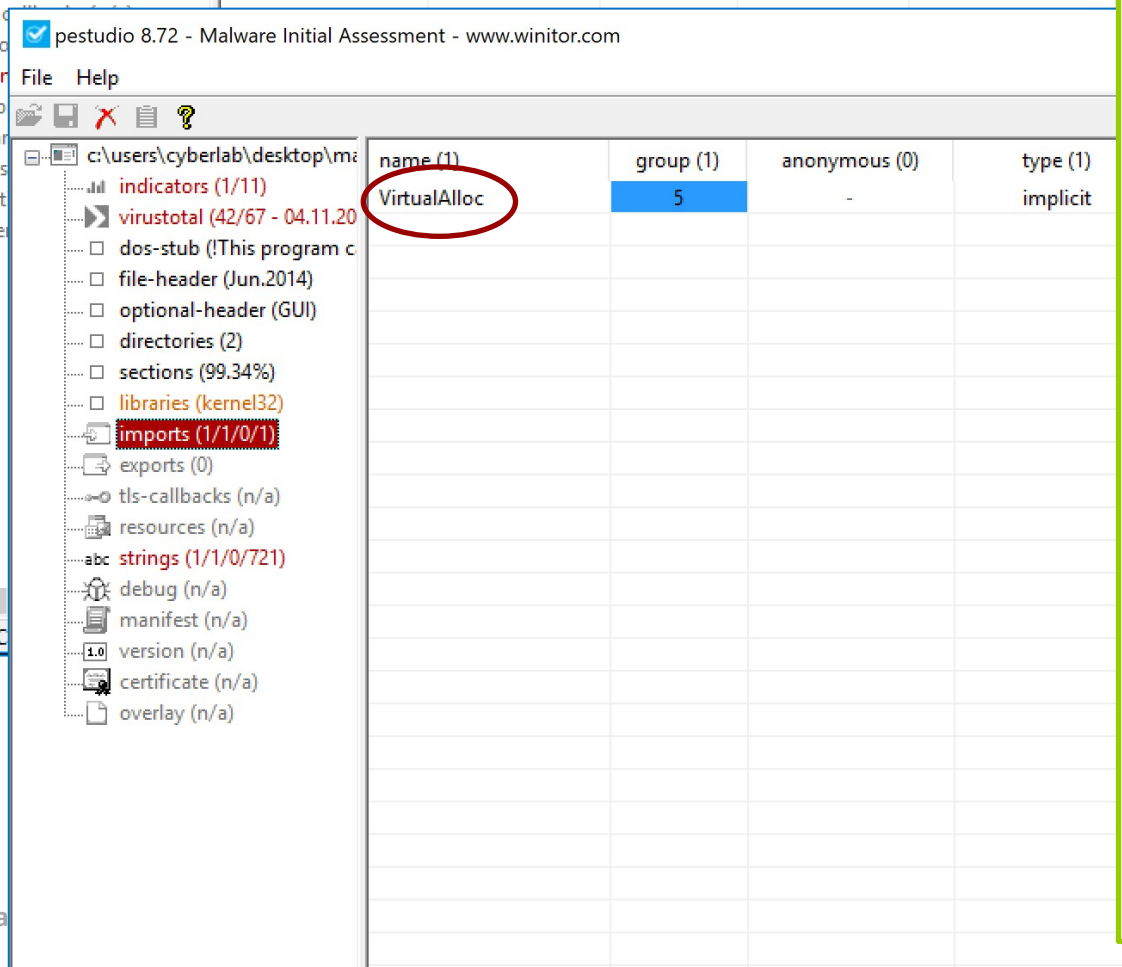
c:\users\cyberlab\desktop\ma
- indicators (1/11)
- virustotal (42/67 - 04.11.20
- dos-stub (!This program c
- file-header (Jun.2014)
- optional-header (GUI)
- directories (2)
- sections (99.34%)
- libraries (kernel32)
- imports (1/1/0/1)
- exports (0)
- tls-callbacks (n/a)
- resources (n/a)
- strings (1/1/0/721)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

engine (66)	positiv (42)	date (dd.mm.yyyy)	age (days)
Microsoft	Backdoor:Win32/Unskal.gen!A	04.11.2017	91
McAfee	EncBackOff!24CE99418862	31.10.2017	95
McAfee-GW-Edition	EncBackOff!24CE99418862	04.11.2017	91
MicroWorld-eScan	Gen:Variant.Graftor.149316	04.11.2017	91
BitDefender	Gen:Variant.Graftor.149316	04.11.2017	91
Ad-Aware	Gen:Variant.Graftor.149316	04.11.2017	91
F-Secure	Gen:Variant.Graftor.149316	04.11.2017	91
ALYac	Gen:Variant.Graftor.149316	04.11.2017	91
GData	Gen:Variant.Graftor.149316	04.11.2017	91
Emsisoft	Gen:Variant.Graftor.149316 (B)	04.11.2017	91
Qihoo-360	HEUR/QVM20.1.F6E3.Malware.Gen	04.11.2017	91
Kaspersky	HEUR:Trojan.Win32.Generic	04.11.2017	91
ZoneAlarm	HEUR:Trojan.Win32.Generic	04.11.2017	91
VBA32	Malware-Cryptor.General.3	04.11.2017	91
TrendMicro-HouseCall	TSPY_POSLOGR.SM	04.11.2017	91
TrendMicro	TSPY_POSLOGR.SM	04.11.2017	91
Yandex	Trojan.Agent!UQWAOXhxly0	02.11.201	
Zillya	Trojan.Agent.Win32.480368	04.11.201	
Symantec	Trojan.Backoff	03.11.201	
DrWeb	Trojan.Backoff.3	04.11.201	
Arcabit	Trojan.Graftor.D24744	04.11.201	
ViRobot	Trojan.Win32.Agent.77312.BI	04.11.201	
NANO-Antivirus	Trojan.Win32.Agent.ddkyih	04.11.201	
VIPRE	Trojan.Win32.Generic!BT	04.11.201	
AVware	Trojan.Win32.Generic!BT	04.11.201	
Antiy-AVL	Trojan/Win32.Agent	03.11.201	
Jiangmin	TrojanSpy.Recam.v	04.11.201	
Comodo	UnclassifiedMalware	04.11.201	

sha256: 5B59DCF29F8271EBD0AC6D64EE02E8B1A15CF5D030CC098E9A903960685D6C97 | cpu: 32-bit | file-type: executabl

- **PEStudio**
  - Static analysis
  - What do VirusTotal AV scanners think?





- **PEStudio**
  - Static analysis
- Only *one* library? (kernel32.dll is always loaded)
- Only *one* function imported? (allocates memory)

pestudio 8.72 - Malware Initial Assessment - www.winitor.com

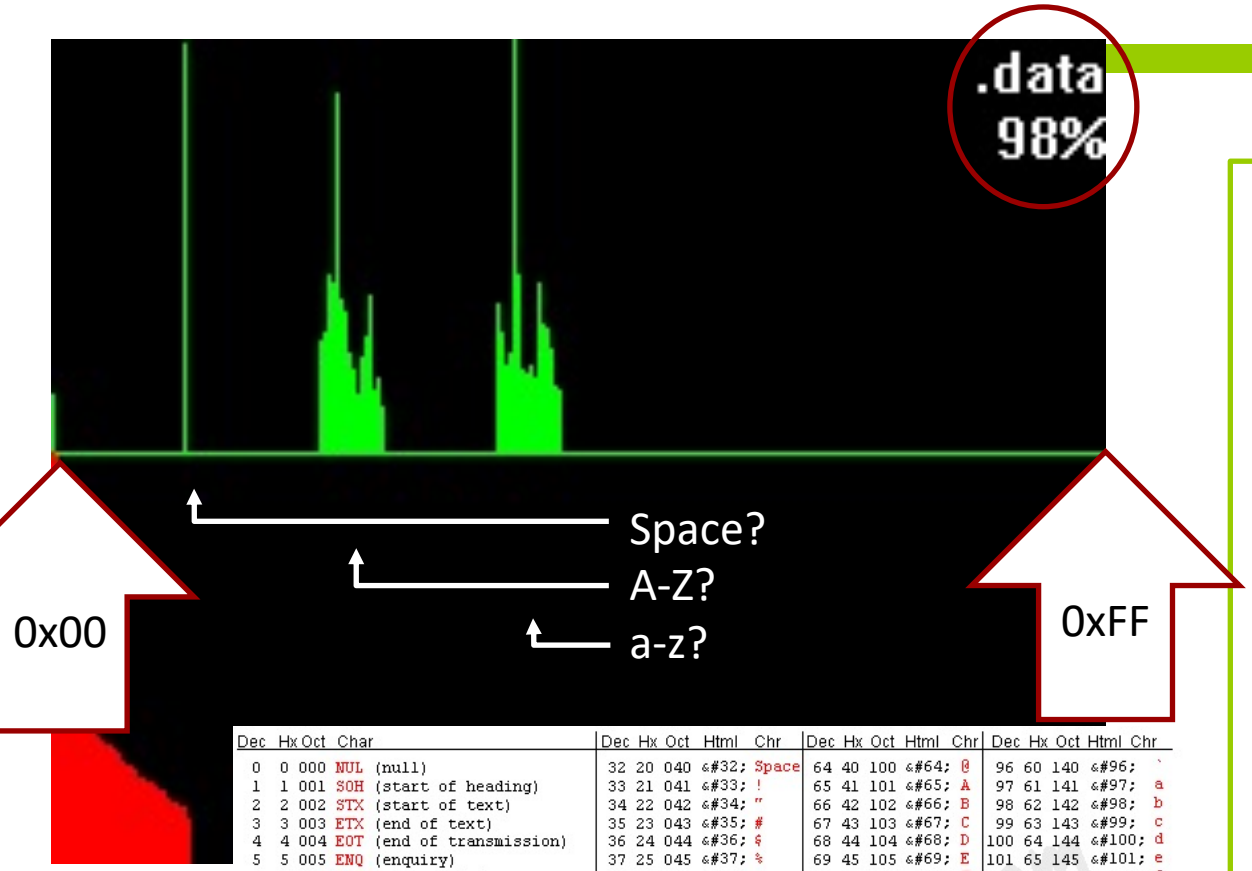
File Help

- c:\users\cyberlab\deskt
  - indicators (1/11)
  - virustotal (42/67 - 04
  - dos-stub (!This prog
  - file-header (Jun.2014
  - optional-header (GU
  - directories (2)
  - sections (99.34%)
  - libraries (kernel32)
  - imports (1/1/0/1)
  - exports (0)
  - tls-callbacks (n/a)
  - resources (n/a)
  - strings (1/1/0/721)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

type	size	blacklist (1)	hint (1)	whitelist (0)	value (721)
ascii	131	-	-	-	uvMKwr MMuxKK qxLLwwLK xylEyuCGqpHK xslBpnMKuwMOIuFC vuOHm{ BLmwBPuuBG...
ascii	93	-	-	-	qvEDrylExs LLqyDEquMlmI EBpoHCtpMMuoLB{I MOmsFN{qACyoJLvx PAwoLNvqPKlp EFp...
ascii	89	-	-	-	qxHE tpMLtyLAzzMM IuLC ymEAtqKFpsML quMLIsBF xylA uwKJpxMN msBDyo lBtq KPqp ...
ascii	94	-	-	-	MK muBAx{ AGpIMKmuBH xylHtqKlqnMLms BAxylA uwKJqpMNmsBE uwKLqx MNIs BFys...
ascii	88	-	-	-	LNymAA pxMNpn MJmu ELtqKNpxMKmx ECpwPCIsElynAFpr EK{nABqmMLIn EGx{ABqrM...
ascii	101	-	-	-	EN xxAEq{EM{oAG pvMKmxEF pwPD IsENyn AFpoMOIsFCynAF pxMOIsFCuwKLpx MNInEL...
ascii	129	-	-	-	Elx{AG qlMK mxEPx{AGqlIDwnEL xxADpuEN zyAA qnMNInEMqq PFIsFCxxAE qqPKrn EFppE...
ascii	112	-	-	-	ECqvMl muENxyJNrwlD xslMww LA{p LEuq MloyLNysPG mtLKwwLNyoHHrl KNwxLPvqLM...
ascii	80	-	-	-	rlEB x{AH qrMK plGBvxNEvpLM wwMEtIOO qvED ppBOmvBNIslA mmMMvmBFluMC vtlFp...
ascii	104	-	-	-	lu FBsqlCymDO qpLGzzMPxsCD wwLKww MLprGHvxOO wuLN vqMllmEJxyAG szELx{AApx...
ascii	126	-	-	-	GHplMlxm BCvq LMwwMMplGGwnADwv LKwwHD tmEM{nMBquBCvqLM wwMM IlGGqr...
ascii	129	-	-	-	vu LNvqAAxsLOqpDH tvMCtlIFppEC qvBlmwBltsNC l{MKvmBCmn BByw KPltEEppEC uyA...
ascii	114	-	-	-	ww DBnylFy{lDwvLKww GKqwED ppMlyulC vpLMwwMMmtGGqzMK plGBvxMJ plEDppBD ...
ascii	121	-	-	-	yoEHrlKN vrlDvqLMxm lFomFDyoHPrl KNsz FLqvEDmqMOxm lKvpLMwwKO quMLlrGH pl...
ascii	106	-	-	-	BD sqlF xuCHvzBlmv BKmulB l{MK vmBCmnBByuKPstMO muEKymDOqplCIlGG pvADppEF...
ascii	111	-	-	-	GHplEFppECqv MKqtGBvxHDplED ppMGvtFGyolFxm lFomEGrwlDv{BOxu AHwvMKlIGBqp...
ascii	81	-	-	-	rlKKqpFJpp EFxs KOpzMG tpDB uoMPm{Kl
ascii	114	-	-	-	DGsz EPtoABrlEKqvEDpp EFtoAGszEHppEF
ascii	82	-	-	-	IlGGqz EDppEF pplFqzGHpqEFqwEC wnPE
ascii	139	-	-	-	KJqtHCtp lMtsBHyoKG msMEvtHGqtEDpp
ascii	114	-	-	-	KJwuLN vqMKlIGBpx MPy{KL wuLKww ML
ascii	84	-	-	-	KP wuLK wwMLmzGHplMOxmKK vsLMwv
ascii	83	-	-	-	pplFmz GHpxEFppECqvlEIl GBplFlqvED pp
ascii	92	-	-	-	szELplEEpp ECuyAHrlEBvnMG mvEDxuNlw
ascii	82	-	-	-	AHrlENpl EDqvEDxyBJrl EGuyEH rlKK xlAC
ascii	125	-	-	-	ppKOz{lFmz GHplMFppECqv MKqtGBvxLl
ascii	127	-	-	-	EG ysNOwlLLwwLNyo FPrlKNqrlKvqLMxl Il
ascii	94	-	-	-	xyEGszKLspFCpp ECyuKPptlCpl GGvyMHl

sha256: 5B59DCF29F8271EBD0AC6D64EE02E8B1A15CF5D030CC098E9A903960685D6C97 | cpu: 32-bit | file-type: executable

- **PEStudio**
  - Static analysis
- Many strings, but none are human readable



ASCII Table

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	[illegible]	[illegible]	84	54	124	T	[illegible]	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	[illegible]	85	55	125	U	[illegible]	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	[illegible]	86	56	126	[illegible]	[illegible]	118	76	166	v	v
23	17	027	ETB (end of transmission block)	55	37	067	7	[illegible]	87	57	127	[illegible]	[illegible]	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	[illegible]	88	58	130	[illegible]	[illegible]	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	[illegible]	89	59	131	[illegible]	[illegible]	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

- **bytehist**
  - Static analysis
- Green section is histogram of byte occurrences from 0x00 to 0xFF
- It's not *compressed* or *encrypted* (which would show fully random/even distribution), but perhaps *encoded*?


suspicious cat
suspectz
ICANHASCHEEZBURGER.COM

Static Analysis

- We could continue using other static analysis tools, but likely a waste of time
- Few imported libraries?
  Few imported functions?
  Few readable strings?
  Histogram showing perfectly random or lumpy distribution?
- Could be a binary program that does *absolutely nothing useful*, or **malware is likely <u>packed</u>**

Packing

Original Executable

- Malware
- Not obfuscated
- Easy for AV programs to detect
- Easy for static analysis tools to examine

Packing program

- Compression
- Encryption
- XOR
- Standard or custom algorithms - easy to write new variants

Obfuscated Malware

- Unpacking program is wrapper
- Original executable is payload to be unpacked

Next Steps

- We *could* dive into the packer assembly code next
  - Figure out exactly how it works…
  - Write a tool to extract the malware payload…
  - Try our static analysis tools again…
- But, the payload may not be a nice PE executable with perfect header. Could be a binary blob injected into memory
- And do we really *care* how the packer works?
  - Packers are throwaway code –
    You have your malware interns write them!

Behavioral Analysis

Behavioral Analysis

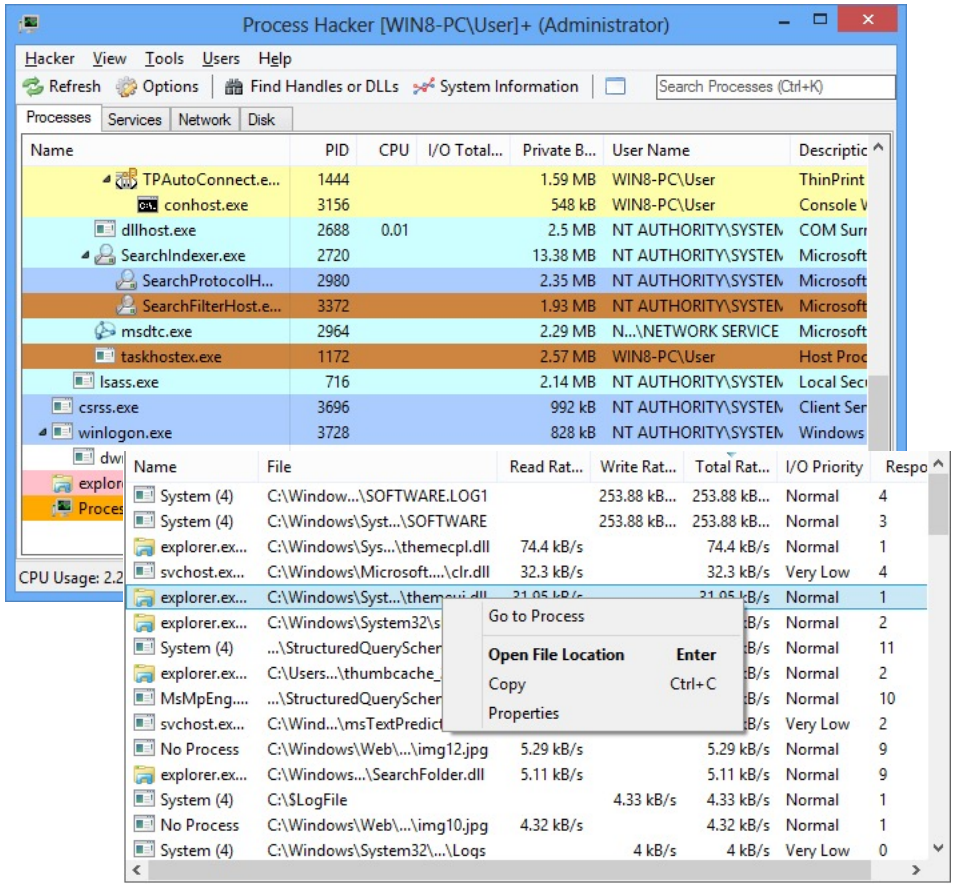
- Run the malware in its native environment and observe what happens
  - Filesystem access? (Read/Write/Create/Delete)
  - Registry access? (Read/Write/Create/Delete)
  - Network access?
  - System calls?
- Can interact with malware and change its behavior

Let’s run the malware and see what happens!

Try not to get bitten…

Or trampled…

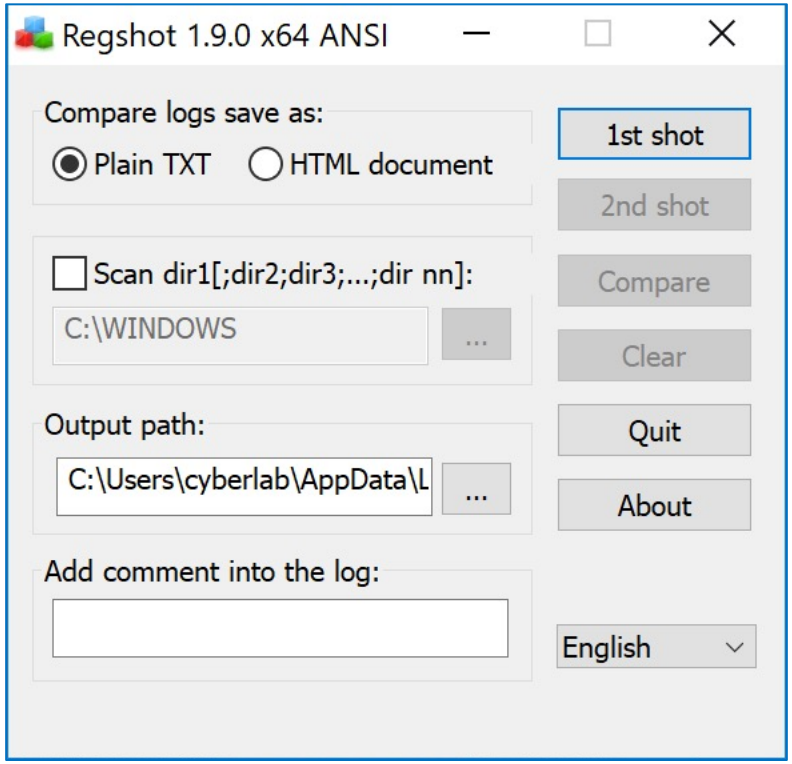
Tools – Process Hacker



- Like Task Manager on steroids
  - Processes and threads
  - Resource utilization
  - Disk utilization (open files, I/O activity)
  - Network utilization (active connections, I/O activity)
  - Handles (Mutexes, Keys, …)
  - Stack traces
  - Strings / Memory dumps
- **[Demo: Changing text in Notepad]**

http://processhacker.sourceforge.net/

Tool - Regshot



- Registry and file monitoring utility
- Snapshots
  - #1 – *Before* malware runs
  - #2 – *After* malware runs
  - Compare to see what the malware did
- Limitations: Will not report the *sequence* of events, or catch temporary changes

https://sourceforge.net/projects/regshot/

Tool – Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

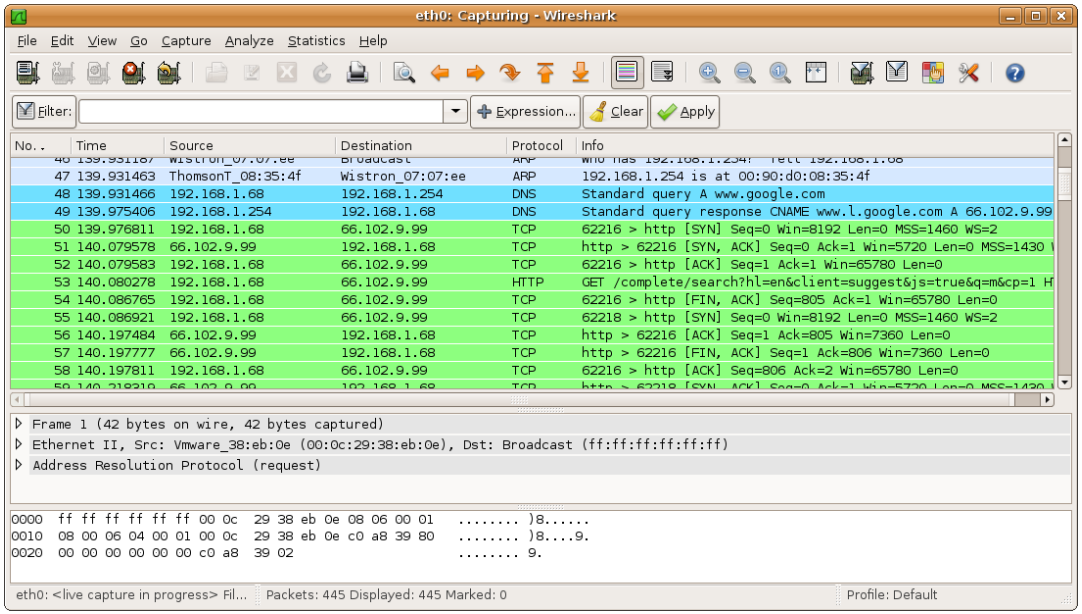
Time o...	Process Name	PID	Operation	Path	Result	Detail
9:29:41...	svchost.exe	736	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Length: 28
9:29:41...	svchost.exe	736	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows ...	NAME NOT FOUND	Length: 28
9:29:41...	svchost.exe	736	QueryNameInfo...	C:\Windows\System32\dllhost.exe	SUCCESS	Name: \Windows\System32\dllhost.exe
9:29:41...	svchost.exe	736	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: All Access
9:29:41...	svchost.exe	736	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	NAME NOT FOUND	Length: 40
9:29:41...	svchost.exe	736	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
9:29:41...	svchost.exe	736	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Cont...	REPARSE	Desired Access: Query Value
9:29:41...	svchost.exe	736	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Query Value
9:29:41...	Explorer.EXE	3524	RegCloseKey	HKCR\CLSID\{0340F119-A598-4ed9-B0...	SUCCESS	
9:29:41...	svchost.exe	736	Process Create	C:\WINDOWS\system32\DllHost.exe	SUCCESS	PID: 356, Command line: C:\WINDOW...
9:29:41...	DllHost.exe	356	Process Start		SUCCESS	Parent PID: 736, Command line: C:\WI...
9:29:41...	DllHost.exe	356	Thread Create		SUCCESS	Thread ID: 2720
9:29:41...	svchost.exe	736	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows ...	SUCCESS	
9:29:41...	svchost.exe	736	RegOpenKey	HKCU\Software\Microsoft\Windows\Cur...	SUCCESS	Desired Access: Query Value
9:29:41...	svchost.exe	736	RegQueryValue	HKCU\Software\Microsoft\Windows\Cur...	SUCCESS	Type: REG_SZ, Length: 120, Data: C:\...
9:29:41...	Explorer.EXE	3524	CloseFile	C:\Users\cyberlab\Desktop\Fiddler.lnk	SUCCESS	
9:29:41...	svchost.exe	736	RegCloseKey	HKCU\Software\Microsoft\Windows\Cur...	SUCCESS	
9:29:41...	svchost.exe	736	RegOpenKey	HKCU\Software\Microsoft\Windows NT\...	SUCCESS	Desired Access: Enumerate Sub Keys
9:29:41...	svchost.exe	736	RegOpenKey	HKCU\Software\Microsoft\Windows NT\...	NAME NOT FOUND	Desired Access: Query Value
9:29:41...	svchost.exe	736	RegCloseKey	HKCU\Software\Microsoft\Windows NT\...	SUCCESS	
9:29:41...	svchost.exe	736	QuerySecurityF...	C:\Windows\System32\dllhost.exe	SUCCESS	Information: Owner, Group, DACL, SA...
9:29:41...	Explorer.EXE	3524	CloseFile	C:\Users\cyberlab\Desktop\Fiddler.lnk	SUCCESS	
9:29:41...	Explorer.EXE	3524	RegCloseKey	HKCR\CLSID\{00021401-0000-0000-C0...	SUCCESS	
9:29:41...	svchost.exe	736	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Dispo...
9:29:41...	svchost.exe	736	QueryBasicInfo...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	CreationTime: 1/24/2018 11:54:42 AM,...
9:29:41...	svchost.exe	736	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
9:29:41...	svchost.exe	736	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Dispo...
9:29:41...	svchost.exe	736	QueryBasicInfo...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	CreationTime: 1/24/2018 11:54:42 AM,...
9:29:41...	svchost.exe	736	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
9:29:41...	svchost.exe	736	QueryBasicInfo...	C:\Windows\System32\dllhost.exe	SUCCESS	CreationTime: 9/29/2017 5:41:43 AM, ...
9:29:41...	svchost.exe	736	RegOpenKey	HKLM\Software\Microsoft\Windows\Cur...	SUCCESS	Desired Access: Read
9:29:41...	svchost.exe	736	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\...	NAME NOT FOUND	Length: 20
9:29:41...	svchost.exe	736	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\...	SUCCESS	

Showing 36,914 of 156,611 events (23%) Backed by virtual memory

- Capture real-time file system, registry, and process/thread activity
- *Will need to filter desired processes or events (or be overwhelmed with data)*

https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

Tool - Wireshark



- Packet capture and analysis
- *Will need to filter (or be overwhelmed with data)*
- Suggestion: Run this <u>outside</u> of the Windows VM to minimize interference or detection

https://www.wireshark.org/

Tool - TcpLogView

TcpLogView

File Edit View Options Help

Event Time	Event Type	Local Address	Remote Address	Remote Host Name	Local Port
2/3/2018 5:23:58...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:23:59...	Open				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:04...	Close				
2/3/2018 5:24:40...	Open	172.16.196.143	23.193.108.220	a23-193-108-220.deploy....	49763
2/3/2018 5:24:59...	Open	172.16.196.143	72.21.91.29		49764

Properties

Event Time:	2/3/2018 5:24:40 PM
Event Type:	Open
Local Address:	172.16.196.143
Remote Address:	23.193.108.220
Remote Host Name:	a23-193-108-220.deploy.static.akamaitechnologie
Local Port:	49763
Remote Port:	443
Process ID:	3124
Process Name:	svchost.exe
Process Path:	C:\Windows\System32\svchost.exe
Remote IP Country:	United States

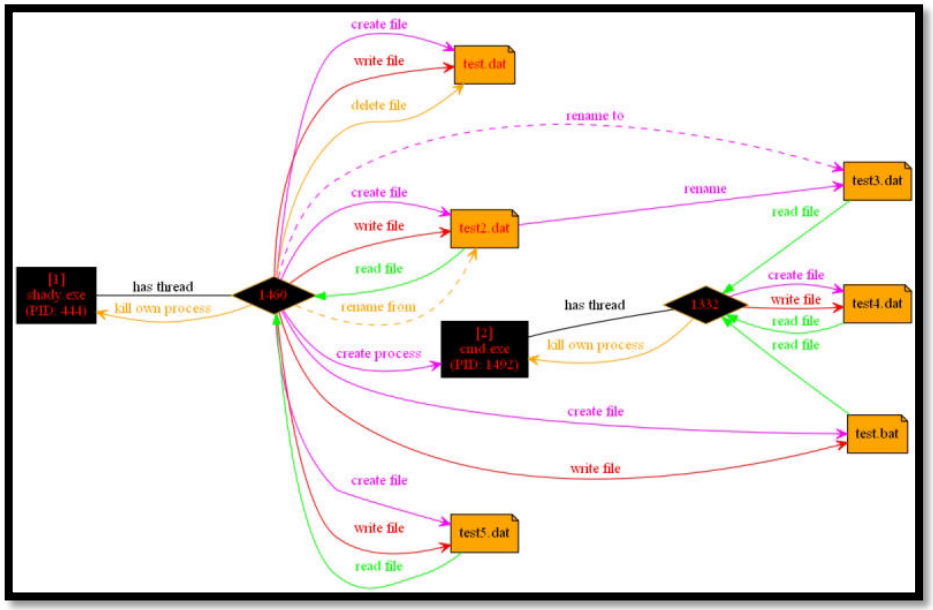
OK

20 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

- List of TCP connections (which you could get from Wireshark) *plus* the process responsible for the connection
- Very useful for *brief* network connections you might otherwise miss

https://www.nirsoft.net/utils/tcp_log_view.html

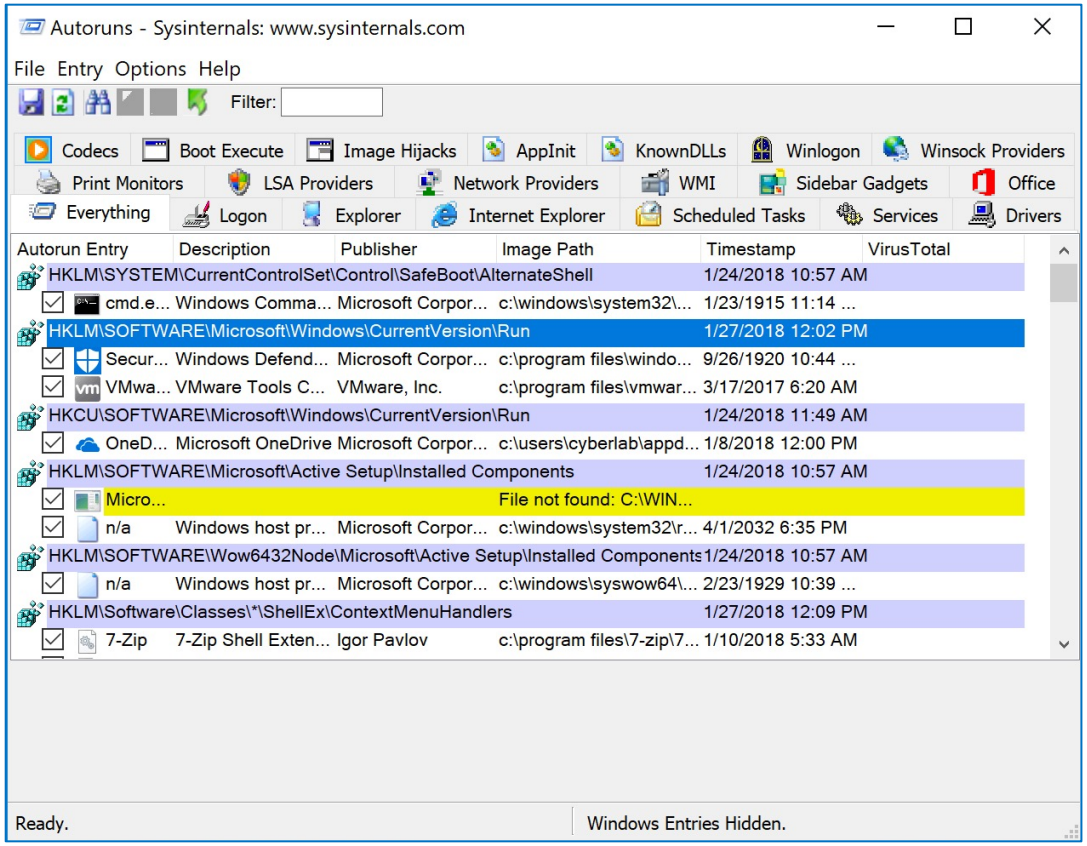
Tool - ProcDOT



- Correlation of data from Process Monitor (system calls) and Wireshark (networking)
- Interactive visual analysis
- Timeline (sequence) of events

http://www.procdot.com/

Tool - AutoRuns



- What services, processes, or drivers will start at system boot?
- At user login?
- When launching IE or Windows Media Player?

https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

MALWARE DEMO!

Upcoming Events

- Tuesday Feb 22nd
  - **Exam 1**
  - Topics: Static and behavioral analysis
  - In class
  - Open notes, open computer, open Internet
  - "Lab-like activities" *(Labs 1-3)*