Malware Reverse Engineering Report Practical 3

By: Gary Jones <u>Jonegn1@ufl.edu</u> CAP4136 Practical 3: Reverse Malware Engineering

Executive summary

Project overview

The goal of Practical 3 is to dissect the functionality of sample3.dll using static and dynamic analysis.

Summary of findings

Sample3.dll has proven to be a challenging piece of malware to analyze. It is packed and it uses anti-debugging techniques. This malware challenges the user at every turn. Through the use of various tools it was found that this malware bares hallmarks of the EnigmaProtector and Armadilo Packer. In addition the family of malware it is most closely related to is Emotet which means that it focuses on downloading other malware from the internet and discovering other systems on a users network. This malware was also found to target the WPAD registry. This means that it could be extracting passwords and might be compromising the system for a man in the middle attack. Adding on to this the malware was also found to contain strings that point to hooking so this is a possible operation performed by the program.

Technical report

Findings: Static Analysis

1. Identify the apparent compilation date of the program.

The compilation date of sample3.dll is 04MAR2022. This is in the past however it is incredibly recent and could be a suspicious indicator for malfeasance.

settings about			
1× 🛯 💡			
c:\users\malware\desktop\sample3.dll	property	value	
N virustotal (error)	signature	0x00004550 (PE00)	
A dos-header (64 bytes)	machine	Intel	
dos-stub (192 bytes)	sections	5	
rich-header (checksum)	compiler-stamp	0x62220B53 (Fri Mar 04 07:51:31 2022)	
file-header (time-stamp)	pointer-symbol-table	0x00000000	
optional-header (GUI)	number-of-symbols	0	
- 📆 directories (7)	size-of-optional-header	224 (bytes)	
sections (file)	processor-32bit	true	
-5 libraries (13)	relocation-stripped	false	
- imports (count)	large-address-aware	false	
- contraction (duplicated)	uniprocessor	false	
- 🖇 exceptions (n/a)	system-image	false	
o tis-callbacks (n/a)	dynamic-link-library	true	
- ŷ relocations (16502)	executable	true	
- 🔂 resources (unknown)	debug-stripped	false	
abc strings (6294)	media-run-from-swap	false	
-🏦 debug (n/a)	network-run-from-swap	false	
🗐 manifest (asInvoker)			
version (CustomMessageBox.exe)			
certificate (n/a)			
overlay (n/a)			

Figure 1: Compilation Date of Sample3.dll

2. Identify any suspicious properties of the program's Imports.

Sample3.dll has a significant amount of imports with a number of 534. Within this number there are 61 blacklisted and 2 imports without a listed group. There are 15 groups that the blacklisted functions fall within and two names that do not have a group attributed to them. These groups are as follows:

- Windowing
- System-information
- Storage
- Shell
- Resource
- Registry
- Memory
- Keyboard-and-mouse
- Hooking
- File
- Execution
- Exception-handling
- Dynamic-library
- Data-exchange
- Console

The most suspicious among these groups are as follows: keyboard-and-mouse, hooking, data-exchange, and registry.

The imports associated with keyboard-and-mouse: GetKeyNameTextA, MapVirtualKeyA, and GetKeyState

The imports associated with Hooking: CallNextHookEx, UnhookWindowsHookEx, SetWindowsHookExA

The imports associated with Data-exchange: GetAtomNameA, GlobalGetAtomNameA, GlobalFindAtomA, GlobalAddAtomA, GlobalDeleteAtom, RegisterClipboardFormatA, OleSetClipboard, OleFlushClipboard

The imports associated with Registry: RegCreateKeyA, RegDeleteValueA, RegSetValueExA, RegSetValueA, RegEnumKeyA, RegDeleteKeyA, 163 (RegisterTypeLib)

The two imports not associated with any group but are still blacklisted are DuplicateHandle and SystemParametersInfoA

EDMINISTRATING STREET,	TERO GIVE	in the second			
WritePrivateProfileStringA	registry	implicit	2	x	
RegCreateKeyA	registry	implicit	-	×	
RegDeleteValueA	registry	implicit	6	x	
RegSetValueExA	registry	implicit	5	×	
RegSetValueA	registry	implicit	2	×	
RegEnumKeyA	registry	implicit	že.	x	
RegDeleteKeyA	registry	implicit	1	×	
163 (RegisterTypeLib)	registry	implicit	х	×	
VirtualProtect	memory	implicit	-	×	
<u>GetKeyNameTextA</u>	keyboard-and-mouse	implicit	2	x	
MapVirtualKeyA	keyboard-and-mouse	implicit		×	
GetKeyState	keyboard-and-mouse	implicit	8	x	
CallNextHookEx	hooking	implicit	5	×	
<u>UnhookWindowsHookEx</u>	hooking	implicit	8	x	
SetWindowsHookExA	hooking	implicit	8	×	

Figure 2: Sample3.dll Imported Libraries Part 1

	e				
<u>GetAtomNameA</u>	data-exchange	implicit	2	×	
<u>GlobalGetAtomNameA</u>	data-exchange	implicit		×	
GlobalFindAtomA	data-exchange	implicit	*	×	
GlobalAddAtomA	data-exchange	implicit	2	×	
GlobalDeleteAtom	data-exchange	implicit	*	×	
RegisterClipboardFormatA	data-exchange	implicit	÷	x	
OleSetClipboard	data-exchange	implicit	*	x	
OleFlushClipboard	data-exchange	implicit	2	×	
<u>SetConsoleCtrlHandler</u>	console	implicit	5	x	
DuplicateHandle	×	implicit		×	
<u>SystemParametersInfoA</u>	2	implicit	2	×	

Figure 3: Sample3.dll Imported Libraries Part 2

3. Identify any suspicious or relevant strings (IP addresses, urls, process names, file names, etc.).

After looking at the strings I was not able to identify any IP addresses or URL names. However, there are 6294 strings with 73 blacklisted strings. An interesting observation is that a number of the blacklisted strings are also found in the import section and are like for like with the reported groups: keyboard-and-mouse, hooking, registry, and data-exchange.

With that said, other suspicious strings include activities with files such as MoveFile, DeleteFile, LockFile, UnlockFile, SetFileAttributes, PathRemoveFileSpec and more.

S 🖬 8							
users\malware\desktop\sample3.dll	type (2)	size (bytes)	file-offset	blacklist (73)	hint (286)	group (18)	value (6294)
indicators (51)	ascii	14	0x0007672D	×		windowing	GetMonitorInfo
virustotal (error)	ascii	19	0x0007673C	×		windowing	EnumDisplayMonitors
Jos-header (64 bytes)	ascii	16	0x00076750	×		windowing	MonitorFromPoint
los-stub (192 bytes)	ascii	15	0x00076764	×		windowing	MonitorFromRect
In-neader (checksum)	ascii	17	0x00076774	×		windowing	MonitorFromWindow
netional header (GLID)	ascii	16	0x0008DACE	x		windowing	GetDesktopWindow
rectories (7)	ascii	19	0x0008DD6E	×		windowing	SetForegroundWindow
ections (file)	ascii	19	0x0008DE76	x		windowing	GetForegroundWindow
ibraries (13)	ascii	12	0x0008DEF9	×		windowing	GetClassLong
nports (count)	ascii	10	0x0008DF08	×		windowing	GetCapture
exports (duplicated)	ascii	18	0x00076719	×		system-information	EnumDisplayDevices
exceptions (n/a)	ascii	22	0x0008D68E	x		system-information	GetTimeZoneInformation
ds-callbacks (n/a)	ascii	20	0x0008D267	×		storage	GetVolumeInformation
relocations (16502)	ascii	7	0x0008DF21	×		shell	WinHelp
esources (unknown)	ascii	21	0x0008CDD7	×		resource	EnumResourceLanguages
ngs (6294)	ascii	22	0x00077E6C	×		registry	RegisterTypeLibForUser
ug (n/a)	ascii	25	0x0008CF8D	×		registry	WritePrivateProfileString
est (asInvoker)	ascii	12	0x0008E9F1	×		registry	RegDeleteKey
ion (CustomMessageBox.exe)	ascii	10	0x0008EA01	x		registry	RegEnumKey
cate (n/a)	ascii	11	0x0008EA2F	×		registry	RegSetValue
rlay (n/a)	ascii	13	0x0008EA51	x		registry	RegSetValueEx
	ascii	14	0x0008EA63	×		registry	RegDeleteValue
	ascii	12	0x0008EA75	×		registry	RegCreateKey
	ascii	20	0x0007D398	×		memory	HeapQueryInformation
	ascii	14	0x0008D43A	x		memory	VirtualProtect
	ascii	11	0x0008D9B8	×		keyboard-and-mouse	GetKeyState
	ascii	14	0x0008E305	×		keyboard-and-mouse	GetKeyNameText
	ascii	13	0x0008E317	×		keyboard-and-mouse	MapVirtualKey
	ascii	14	0x00078AC0	×		hooking	NotifyWinEvent
	ascii	14	0x0008D7DC	×		hooking	CallNextHookEx
	ascii	19	0x0008D7EE	×		hooking	UnhookWindowsHookEx
	ascii	16	0x0008D833	×		hooking	<u>SetWindowsHookEx</u>
	ascii	8	0x0008D161	×		file	MoveFile

Figure 4: Blacklisted strings part 1

c:\users\malware\desktop\sample3.dll	type (2)	size (bytes)	file-offset	blacklist (73)	hint (286)	group (18)	value (6294)
- indicators (51)	ascii	8	0x0008D161	x	-	file	MoveFile
	ascii	10	0x0008D16D	x	-	file	DeleteFile
> dos-header (64 bytes)	ascii	8	0x0008D1EA	x		file	LockFile
dos-stub (192 bytes)	ascii	10	0x0008D1F6	×		file	UnlockFile
rich-header (checksum)	ascii	13	0x0008D255	×		file	FindFirstFile
- P file-header (time-stamp)	ascii	17	0x0008D373	x		file	SetFileAttributes
	ascii	13	0x0008EAA3	×		file	SHGetFileInfo
directories (7)	ascii	17	0x0008EAEF	×		file	PathFindExtension
libraries (12)	ascii	16	0x0008EB1D	×		file	PathEindEileName
imports (count)	ascii	18	0x0008EB53	×		file	PathRemoveFileSpec
exports (duplicated)	ascii	23	0x0007D364	×		execution	SetThreadStackGuarantee
g exceptions (n/a)	ascii	18	0x0008CCF6	×		execution	GetCurrentThreadId
	ascii	16	0x0008CE08	×		execution	GetCurrentThread
- 🏠 relocations (16502)	ascii	13	0x0008CE84	×		execution	SuspendThread
	ascii	19	0x0008CFC6	×		execution	GetCurrentProcessId
-abc strings (6294)	ascii	15	0x0008D18E	×		execution	GetThreadLocale
	ascii	16	0x0008D496	×		execution	TerminateProcess
manifest (asInvoker)	ascii	21	0x0008D58E	×		execution	GetEnvironmentStrings
version (CustomMessageBox.exe)	ascii	21	0x0008D5C1	×		execution	GetEnvironmentStrings
	ascii	22	0x0008D7B5	×		execution	SetEnvironmentVariable
overlay (n/a)	ascii	24	0x0008DB9E	×		execution	GetWindowThreadProcessId
	ascii	17	0x0008E341	×		execution	PostThreadMessage
	ascii	14	0x0008D428	×		exception-handling	RaiseException
	ascii	17	0x0008CD0D	×		dynamic-library	GetModuleFileName
	ascii	17	0x0008D021	×		dynamic-library	GetModuleFileName
	ascii	23	0x0007E80C	×		desktop	GetProcessWindowStation
	ascii	24	0x0007E825	×		desktop	GetUserObjectInformation
	ascii	16	0x0008CE1C	×		data-exchange	GlobalDeleteAtom
	ascii	13	0x0008CEA5	×		data-exchange	GlobalAddAtom
	ascii	14	0x0008CFF9	×		data-exchange	GlobalEindAtom
	ascii	17	0x0008D00B	×		data-exchange	GlobalGetAtomName
	ascii	11	0x0008D2C9	×		data-exchange	GetAtomName
	ascii	23	0x0008E2D1	×		data-exchange	RegisterClipboardFormat

Figure 5: Blacklisted strings part 2

🖃 📸 c:\users\malware\desktop\sample3.dll	type (2)	Size
- Indicators (51)	ascii	23
virustotal (error)	ascii	15
— > dos-header (64 bytes)	arcii	17
dos-stub (192 bytes)	ascii	17
> rich-header (checksum)	dscil	21
> file-header (time-stamp)	ascii	21
⊵ optional-header (GUI)	ascii	0
	ascii	13
— > sections (file)	ascii	15
libraries (13)	ascii	20
	ascii	6
	ascii	7
🖇 exceptions (n/a)	ascii	6
tis-callbacks (n/a)	unicode	4
- 🎓 relocations (16502)	unicode	64
	unicode	64
-abc strings (6294)	ascii	26
	ascii	13
	ascii	16
- te version (CustomMessageBox.exe)	arcii	16
	arcii	12
overlay (n/a)	ascii	15
	dscil	13
	ascii	13
	ascii	26
	accii	4.4

type (2)	size (bytes)	file-offset	blacklist (73)	hint (286)	group (18)	value (6294)
scii	23	0x0008E2D1	×		data-exchange	RegisterClipboardFormat
scii	15	0x0008EDD2	x		data-exchange	OleSetClipboard
scii	17	0x0008EDFC	×		data-exchange	OleFlushClipboard
scii	17	0x0007DB00	x		cryptography	SystemFunction036
scii	21	0x0008D60E	×		console	SetConsoleCtriHandler
scii	6	0x000761B4	x			system
scii	13	0x00078900	×			DIIGetVersion
icii	15	0x0008D222	x			DuplicateHandle
cii	20	0x0008DBE1	×			SystemParametersInfo
cii	6	0x000776E4		utility		Delete
icii	7	0x00077D90		utility		Control
cii	6	0x0008ED60		utility		OleRun
nicode	4	0x000BCD4F		utility		Open
nicode	64	0x000BCF31		size		An unknown error has occurred. Encountered an improper argument
nicode	64	0x000BDAAB		size		No error occurredAn unknown error occurred while accessing %1.
cii	26	0x0008F008		rtti		.?AVCCustomMessageBoxApp@@
cii	13	0x0008F02C		rtti		.?AVCWinApp@@
cii	16	0x0008F044		rtti		.?AVCWinThread@@
cii	16	0x0008F060		rtti		.?AVCCmdTarget@@
icii	13	0x0008F07C		rtti		.?AVCObject@@
cii	15	0x0008F104		rtti		.?AVCAboutDlg@@
cii	13	0x0008F11C		rtti		.?AVCDialog@@
cii	26	0x0008F148		rtti		.?AVCCustomMessageBoxDlg@@
icii	44	0x0008F170		rtti		.?AUThank you@Define the symbol ATL MIXED@@
cii	22	0x0008F23C		rtti		.?AVCCommandLineInfo@@
icii	16	0x0008F25C		rtti		.PAVCException@@
icii	12	0x0008F284		rtti		.?AVCCmdUI@@
cii	22	0x0008F29C		rtti		.PAVCMemoryException@@
cii	19	0x0008F2BC		rtti		.?AVCOleException@@
icii	16	0x0008F2D8		rtti		.?AVCException@@
scii	19	0x0008F2F4		rtti		.PAVCOIeException@@
scii	13	0x0008F310		rtti		.PAVCObject@@
scii	22	0x0008F338		rtti		.PAVCSimpleException@@

Figure 6:Blacklisted strings part 3

After the initial look at the program with pestudio the static analysis was extended to include Virus Total and Intezer Analyze. From these tools several other strings were identified to be indicative of malware. These strings include the following:

- $77$707@7L7\7h7x7$ associated with Generic Malware
- 4W5]5s5~5 associated with poison Malware
- >5>E>X>p> associated with RedLeaves Malware
- SVWjkXjef associated with Turla Malware
- Y;D\$8t associated with Emotet Malware
- 1 272E2N2 associated with RootKit, RatankbaPOS Malware
- GBBFRF associated with Emotet Malware

e Genetic Analysis		• IOCs 🕴 • Behavior	🧔 De	etect & Hunt BETA		🕸 Extended Dynamic Execution
Original File		Genetic Summary	Related	d Samples Code (539) S	trings (2,599) [©] Capabilities [©]	
					Malware Generic Malware	
ynamic Execution		Filters				
	Show all	Family types				
emory				4W5]5s5-5		
		Malware				
					Malware RedLeaves	
undli32.exe Ialicious Emorer (38 Genes)						
				SvWjkXjef		
				14 mm		
				r,usat	Maiware Emotet	
				-1000/0		
	Extract				Maiware Generic Maiware	
				€9-\u'		
		El All				
				sUnknown exception	Malware, ColoMiner DAS	
					Malware RootKit, RatankbaPOS	
				GBBFRF	Malware Generic Malware, Emotet	
		RatankbaPOS				

Figure 7: String Association with Malware

In addition to the malware family identifiers, Intezer Analyze also identified strings associated with different packers which include the following:

- 6:6>6B6F6J6N6R6V6Z6^6b6f6j6n6r6v6z6~6 associated with EnigmaProtector Packer
- :6;<;L; associated with Armadilo Packer

6:6>6B6F6J6N6R6V6Z6^6b6f6j6n6r6v6z6~6	Packer EnigmaProtector	
:6;<;L;	Packer Armadillo	Related Samples

Figure 8: String Association with Packers

4. If you find anti-disassembly techniques, report them.

Through analysis with the debugger on the Windows 7 virtual machine anti-debugging properties were identified. As shown in Figure 9 we can see eax+2. This line is identifying whether or not debugger is being used. When this results in 1 it indicates that a debugger has been detected. For further verification we can also see the anti-debugging property in Ghidra as shown in FUN_10047030 (Figure 10).



Figure 9: Anti-debugging property x32dbg



Figure 10: Ghidra anti-debugging

5. Describe the obfuscation methods you find. You will surely be impacted by them, but identifying any interesting patterns might be helpful in developing a tool to combat them.

With the use of JOESandbox Cloud the analysis of malware was analyzed and from the results some suspicious functions were identified that were identified as being related to encryption. Looking into it we find a high degree of relation to FUN_10001985 (see Figures 11 through 13) and FUN_10005367 (see Figures 14 through 16) with the latter function calling the former function numerous times – in a very suspicious manner that indicates that encryption is likely occurring.



Figure 11: FUN_0001985 Part 1

Activities	🚅 ghidra-Ghidra 🔻	\$			Apr 11 22:23	4) ()	•
				Code	Browser: sadf:/sample3.dll	-	•	×
<u>Eile Edit An</u>	alysis <u>G</u> raph <u>N</u> avigation	n <u>S</u> earch Se <u>l</u> ect <u>T</u> ools <u>W</u> indow <u>H</u> elj)					
		IDULFKVB- 🍇	a n a	18	19 🖪 📴 😋 🏯 🔿 🗷 🔶 🗐 🙀 🏤 🗣			
Program Tree	es 🗔 边 🏷 🗙 📕 Lis	ting: sampl 🗅 🍋 🔽 🛙 🐺 🥻	💩 📑 • 🗙	: G _f [Decompile: FUN_10001985 - (sample3.dll)		.	×
🔻 📷 sample	e3.dll	100019a4 Of af d5	IMUL 🔺	27	iVar8 = *(int *)(DAT_100910c4 * 0x4d8 +			
🗟 Hea	aders	100019a7 03 dd	ADD	28	((*(int *)(((((DAT_100910d4 + DAT_100910cc * -2 + DAT_100910d0) *	DAT_100910c4	+	
🖾 .tex	t	100019a9 56	PUSH	29	<pre>(1 - DAT_100910d4 * DAT_100910d0) * DAT_100910c8 + D</pre>	AT_100910d4 *	4 3	
E rda	ta	100019aa 8b 35 c4	MOV	30) - DAT_100910d0) + DAT_100910c0 * 2) * 0x140 + 0x3c	+ param_1) +		
100		100019b0 57	PUSH	31	((DAT_100910c4 * DAT_100910d0 - DAT_100910cc * DAT_100910cc * DAT	_100910c0) *		
[1007	76000, 100903ff]	100019b1 Of af de	IMUL	32	0x4d8 + 0x134a +			
		100019b4 33 ff	XOR	33	((DAT_100910d4 * DAT_100910d4 * DAT_100910c0 - DAT_100910c8) * DA	T_100910c4 +		
e .rel	DC I	100019b6 47	INC	34	DAT_100910cc + DAT_100910d0) * 0x18) * DAT_100910c8) -			
Program T	ree ×	100019b7 2b fa	SUB	35	((DAT_100910c0 + 1) * 0x4d8 + 1) * DAT_100910cc) +			-
		100019b9 8b 0d c0	MOV	36	(DAT_100910c8 + DAT_100910c4 * -0x17 + 0x19) * DAT_100910d0 +			
Symbol Tre		100019bf 8b d7	MOV	37	DAT_100910d4 * -0xea2 + DAT_100910c0 + 0x78 + param_1) +			
In Symbol Ine		100019c1 8b 3d c8	MOV	38	(((DAT_100910c8 * DAT_100910d4 + -3) * DAT_100910cc - DAT_100910d4) + DAT_1	00910c8 +		
► 😑 COM	1DLG32.DLL	100019c7 Of af d7	IMUL	39	DAT_100910c4) * 0xa0 + param_1;			
▶ 🦳 GDI	32.DLL	100019ca 03 da	ADD	40	iVarl3 = DAT_100910d0 - DAT_100910c4;			
NCD VCD	NEL 22 DU	100019cc 8b d0	MOV	41	iVar14 = ((DAT_100910c4 - DAT_100910c8 * DAT_100910d0) + 3) * DAT_100910d4 + DAT_10	0910c0 * 2 +		
NEN OLE	NEES2.DEE	100019ce 6b d2 03	IMUL	42	DAT_100910c8;			
P OLE	32.DLL	100019d1 03 da	ADD	43	iVar16 = ((DAT_100910c8 * DAT_100910c4 * DAT_100910c0 * DAT_100910c0 * 8 -			
OLE.	ACC.DLL	100019d3 2b dd	SUB	44	(DAT_100910c4 * 8 + 3) * DAT_100910d0) + DAT_100910cc * -10 + -8) * DAT_1	.00910c4;		
OLE.	AUT32.DLL	100019d5 8d 14 09	LEA	45	iVar9 = ((DAT_100910cc * DAT_100910c8 * DAT_100910c0 + 1) * DAT_100910c8 * 8 + -0x1	.d) *		
		100019d8 03 da	ADD	46	DAT_100910d0;			
Filter:		100019da 8b 15 cc	MOV	47	iVar4 = DAT_100910cc * -0x10;			
		100019e0 69 db 40	IMUL 5	48	iVar2 = *(int *)(iVar8 + Oxlc);			
Data Type	Mana 💌 🗙	100019e6 Of af d2	IMUL	49	iVar10 = (DAT_100910cc * DAT_100910c4 * 2 + -1) * DAT_100910c8;			
a outa type		100019e9 Of af d1	IMUL	50	iVar15 = (DAT 100910c8 + 6) * DAT 100910d4;			- 11
(m · m) ·	14 · N 🕅	100019ec 8b ce	MOV	51	iVar1 = DAT_100910c4 + DAT_100910d0;			
		100019ee Of af cd	IMUL Y	52	iVar3 = *(int *)(iVar8 + 0x24);			1
	100		7.0	53	local lc = 0:			۳

Figure 12: FUN_0001985 Part 2



Figure 13: FUN_0001985 Part 3

Activities	🗯 ghidra-Ghid	ra 🕶		Apr 11 22:37	●) () -
				CodeBrowser: sadf:/sample3.dll	_ 0 ×
Eile Edit Ana	alysis <u>G</u> raph <u>N</u> avig	ation <u>S</u> earch Select <u>T</u> ool	s <u>W</u> indow <u>H</u> elp		
📄 (🗭 • 🔿		JIDULFK	🗑 🖻 - 🖓 🛬 🗠 🗠	🗸 🖺 🖄 🖽 📴 🗣 🏯 🛇 🕮 🗇 🗐 🖓 📩 🔍	
Program Tree	es 🗔 🙋 🏷 🗙	🗏 Listing: sa 🗋 💼 🛛 🚱	🖳 - 🔊 🖓 👘	📴 Decompile: FUN_100053b7 - (sample3.dll)	i 💩 🗝 🗙
★ sample ★ Hea Hea Hea text Hea text Train .text .rec .rec .rec Forgram Tr Symbol Tre Somoon CoM Somoon Somoo	e3.dll A dders t t t ta aa c pc V Free × ae 20 X X NEL32.DLL ALT32.DLL ALT32.DLL X ALT32.DLL V Mana × X C N C N C N C C C C C C C C C C C C C	68 21 35 68 21 35 68 12 35 68 65 33 68 65 33 68 65 33 68 67 33 71 74 24 20 ff 74 24 20 ff 74 24 20 e8 f1 f0 83 c4 20 c3 fined4 fined4 fined4 fined4 fined4 fined4 fined2 fined2 fined2 fined2 fined2 fined2 fined2 fined2 fined2 fined2	PUSH 000 PUSH LAB PUSH LAB PUSH LAB PUSH LAB PUSH LAB PUSH LAB PUSH dwor CALL FUN ADD ESP, RET FUNCTION ndefined _fastcall AL:1 <fun EDX:4 pat Stack(0x4]:4 pat Stack(0x4]:4 pat Stack(0x4]:4 pat Stack(0x4]:2 pat Stack(-0x8):2 loc Stack(-0x8):2 loc</fun 	<pre>1 2 /* WARNING: Globals starting with '_' overlap smaller symbols at the same address */ 3 3 4 5 6 6 7 8 9 9 1 1 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>	
► 🖬 ntdd		fined2	Stack [-0x16]:210	30 undefined2 local_42;	
ntdd	dk_64	Console - Scripting		int in additional for the	🔒 🖉 🗙

Figure 14: FUN_10005367 Part 1

Activities 🦸 ghidra-Gh	idra 🔻		Apr 11 22:37	10
			CodeBrowser: sadf:/sample3.dll	_ = ×
<u>File Edit Analysis Graph Nav</u>	vigation <u>S</u> earch Se <u>l</u> ect <u>T</u> ools	s <u>W</u> indow <u>H</u> elp		
	JIDULFK'	🕷 🖪 🔹 🐐 🐐 👘 🗠 🖓	🗸 🖏 🏽 📾 😋 🏤 🔕 🗷 🧇 🗐 🖗	
Program Trees 🐻 🙋 🏷 🗙	🗉 Listing: sa 🗅 💼 🛛 🗛	🖳 🖌 🖓 🗐 • 🗙	GF Decompile: FUN_100053b7 - (sample3.dll)	🎯 🕞 🎯 🔹 🗙
Y Gample3.dll Headers Headers Headers Idata J.data J.rsrc J.src J.rsrc J.rsrc	fined2 fined3 fined3 fined3 fined3 fined4 fined4 fined4 fined4 fined5 fi	Stack [-0:18]: 2 lor Stack [-0:12]: 2 lor Stack [-0:20]: 2 lor Stack [-0:22]: 2 lor Stack [-0:24]: 2 lor	100 local_14 = local_46; 101 local_6 = local_8; 102 local_6 = local_46; 103 local_6 = local_46; 104 iVar2 = FUN_1000128/(6local_50); 105 iVar2 = FUN_1000128/(6local_61); 106 iVar4 = FUN_1000128/(6local_61); 107 DAT_10094274 = FUN_10001985/(Var4,0x2189fb61); 108 DAT_10094274 = FUN_10001985/(Var4,0x2189fb61); 109 DAT_10094274 = FUN_10001985/(Var4,0x2125301); 110 DAT_10094274 = FUN_10001985(Var4,0x22173436); 111 DAT_10094274 = FUN_10001985(Var4,0x22173436); 112 DAT_10094274 = FUN_10001985(Var4,0x2172436); 113 DAT_10094324 = FUN_10001985(Var2,0x03f49fe1); 114 DAT_10094340 = (code *FFUN_10001985(Var2,0x03f49fe1); 115 DAT_10094340 = FUN_10001985(Var2,0x03f49fe1); 116 DAT_10094340 = FUN_10001985(Var2,0x03f49fe1); 117 DAf_10094340 = FUN_10001985(Var2,0x03f49fe1); 118 DAT_10094330 = FUN_10001985(Var2,0x03f49fe1); 119 DAT_10094330 = FUN_10001985(Var2,0x03f49fe1); 120 DAT_10094328 = FUN_10001985(Var2,0x03f49fe1);	
► SuiltInTypes ► Sample3.dll	fined2 fined2 fined2	Stack[-0x4e]:2 loc Stack[-0x50]:2 loc	127 pc/ar5 = (cod *)FUN [cod)885(1/ar2, -0x2c99b3); 128 _DAT_10094310 = pc/ar5;	
ntddk_32		7.	129 DAT_1009430c = (code *)FUN_10001985(iVar2.0x3790ef3e); DAT_20004390 (code *)FUN_20004065(iVar2.0x3790ef3e);	1
ntddk_64	🖳 Console - Scripting			🔒 🌽 🗙

Figure 15: FUN_10005367 Part 2

Activities	🕬 ghidra-Ghid	ra 🔻		Apr 11 22:38	4 0)) ()	•
				CodeBrowser: sadf:/sample3.dll	-		×
<u>File Edit An</u>	alysis <u>G</u> raph <u>N</u> avig	ation <u>S</u> earch Select <u>T</u> ool	s <u>W</u> indow <u>H</u> elp				
🔒 (🗢 - 🖃		JIDULF K	W B・ 御 御 ち Ci	/ 🗸 🛐 🖄 🖻 📴 😋 🚠 🔷 🛄 🚸 🔲 🐺 🏤 🛛 🗣			
Program Tree	es 🗔 🙆 🏷 🗴	🗏 Listing: sa 🗅 💼 🛛 🚱	🖳 🖌 🕲 📑 • 🗙	C_f Decompile: FUN_100053b7 - (sample3.dll) S □ [21	8 -	- ×
🔻 💓 sample	e3.dll 🔺	fined2	Stack[-0x18]:2loc	124 DAT_1009431c = FUN_10001985(iVar2, -0x73ee4987);			
🗟 Hea	aders	fined2	Stack[-0x1a]:2lo	125 DAT_10094318 = FUN_10001985(1Var2.0x13461505);			- 1
.tex	t	tined2	Stack[-Ox1c]:2 Loc	126 DAT 10094314 = FUN 10001985 (1Var2, -0x6taee18t);			- 11
🔄 .rda	ita	fineda	Stack [0v201-2 1a	127 pcvar5 = (code *)FUN_10001985(1var2, -0x2c9903);			- 11
🗟 .dat	a	Tined2	Stack[-0x20]:2 Lot	128 DAT_10094310 = pcvar5;			- 11
S .rsr	c 🖉	fined2	Stack[-0x24]:2 100	$120 \text{DAT}_{10094302} = (code +)E[N_{10001905}(iver2, -0v1ed9e(35))]$			- 11
🛐 .relo	oc 🔹	fined2	Stack[-0x24]:2 to	$131 \qquad $			- 11
		fined2	Stack[-0x28]:2 loc	132 $uVar7 = (*DAT 1009430c)(param 3.uVar6):$			- 11
Program I	ree ×	fined2	Stack[-0x2a]:2lo	133 puVar8 = (undefined *) (*DAT 10094308) (param 3, uVar6);			- 11
	A 3 14	fined2	Stack[-0x2c]:2loc	134 if (DAT 10094340 == (code *)0x0) {			- 11
Symbol Tre	ee 🖉 🗠 🗙	fined2	Stack[-0x2e]:2lo	135 puVar9 = (ushort *)			- 11
► 😑 COM	IDLG32.DLL	fined2	Stack[-0x30]:2 loc	136 (*DAT_10094344) (0, puVar8, ((DAT_100910c4 * 2 -			- 11
► 📋 GDI3	32.DLL	fined2	Stack[-0x32]:2 lo	137 (DAT_100910cc * DAT_100910c8 + 1) * DAT_100910d4) -			- 11
► C KER	NEL32 DU	.fined2	Stack[-0x34]:2loc	DAT_100910cc) * 6 + 0x1000 +			- 11
	22 DU			[139] ((DAT_100910d0 * DAT_100910c8 * DAT_100910c0 -			- 11
OLE.	32.DLL	fined2	Stack[-0x38]:2 loc	DAT_100910d4 * DAT_100910c4) * 6 + -6) * DAT_100910d0	1		- 11
P OLE	ACC.DLL	fined2	Stack[-0x3a]:2 lot	[14] (((DAT_100910c8 * DAT_100910c8 * DAT_100910c4 + 2) *			- 11
DLE/	AUT32.DLL	Tined2	Stack[-0x3c]:2100	142 DAI 100910c8 +			- 11
mile		Tined2	Stack[-Ox3e]:2100	(DAT_10091004 + DAT_10091000) * DAT_10091000 + 04100	+		
Filter:	8	fined2	Stack [-0x40] : 2 100		£,		
		fined2	Stack[0x44] 2 100	145 ((12 - 0)(109104 + 2 + 041109104) + 0411091040) -			
Data Type	Mana 🔻 🗙	fined2	Stack[-0x44]:2 10				
dm - mb -	1: • N M	fined2	Stack[-0x48]-2 10				
		fined2	Stack[-0x4a]:2 lo	149 else f			- 11
		fined2	Stack[-0x4c]:2loc	150 vVar12 = 0;			- 11
🕨 🍯 Built	InTypes 🔺	fined2	Stack[-0x4e]:2loc	151 IVar2 = (DAT 100910c4 * 2 + -2) * DAT 100910c0 +			- 11
🕨 🧊 🖉 sam	iple3.dll 🐴	fined2	Stack[-0x50]:2 lo	152 ((0x20 - (DAT_100910c8 * DAT_100910c4 + DAT_100910cc) * DAT_100910d0) - DAT_10090	LOd4		
🕨 🧊 ntdo	dk_32		7.	153) * 2; bct			

Figure 16: FUN_10005367 Part 3

Findings: Dynamic Analysis

1. Interesting behaviors that occur after the malware has executed.

The most notable behavior exhibited by the malware is its interaction with WPAD. From experience with penetration testing the modification of this software can be used to further compromise a system by stealing listed passwords and setting the environment for a man in the middle attack. However, no other notable behaviors were observed and there were no persistence mechanisms identified.

2. Identify whether or not there is any networking behavior exhibited by the program and, if so, record it.

By utilizing fakedns the network activity being utilized by the sample3.dll was analyzed. From this activity the following network activity was identified:

- dns.msftncsi.com
- fs.microsoft.com
- 255.245.168.192.in-addr.arpa
- 133.245.168.192.in-addr.arpa
- 104.195.71.45.in-addr.arpa
- 167.106.37.54.in-addr.arpa
- 138.130.168.185.in-addr.arpa
- 177.244.44.37.in-addr.arpa
- 78.25.184.185.in-addr.arpa
- 15.168.148.185.in-addr.arpa
- 135.192.199.128.in-addr.arpa
- 141.209.59.37.in-addr.arpa
- 169.204.41.103.in-addr.arpa
- 120.58.42.103.in-addr.arpa
- 220.168.148.185.in-addr.arpa

As shown in Figures 17 and 18 there are more addresses attempting contact.

```
fakedns[INF0]: Response: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: dns.msftncsi.com -> 192.168.245.133
fakedns[INFO]: Response: dns.msftncsi.com -> 192.168.245.133
fakedns[INF0]: Response: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: fs.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: dns.msftncsi.com -> 192.168.245.133
fakedns[INFO]: Response: dns.msftncsi.com -> 192.168.245.133
fakedns[INF0]: Response: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: dns.msftncsi.com -> 192.168.245.133
fakedns[INF0]: Response: settings-win.data.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: 255.245.168.192.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Response: 133.245.168.192.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Response: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Response: 104.195.71.45.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Response: 167.106.37.54.in-addr.arpa -> 192.168.245.133
192.168.245.133
```

Figure 17: Network Activity Part 1

APELACOLE IDIADO	
fakedns[INF0]: Respon	se: 138.130.168.185.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 177.244.44.37.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 78.25.184.185.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: 15.168.148.185.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 135.192.199.128.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 141.209.59.37.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: dns.msftncsi.com -> 192.168.245.133
fakedns[INF0]: Respon	se: wpad.localdomain -> 192.168.245.133
fakedns[INF0]: Respon	se: wpad.localdomain -> 192.168.245.133
fakedns[INF0]: Respon	se: 169.204.41.103.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: 220.168.148.185.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 120.58.42.103.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 125.73.46.78.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: fs.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: tlu.dl.delivery.mp.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 250.93.183.68.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 66.233.90.190.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 177.132.56.5.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: 147.178.171.62.in-addr.arpa -> 192.168.245.133
fakedns[INF0]: Respon	se: teredo.ipv6.microsoft.com -> 192.168.245.133
fakedns[INF0]: Respon	se: 190.98.44.196.in-addr.arpa -> 192.168.245.133

Figure 18: Network Activity Part 2

3. Identify any registry keys created/modified by the malware.

In order to identify any registry keys being created or modified procmon was used. After initiating the program and letting it run the file was saved and analyzed. By filtering for the Process Name: regsvr32.exe and the Operation: RegCreateKey I was able to identify the created keys of sample3.dll as shown in Figure 19. I did not notice the modification of any registry keys. From Figure 19 we can see extensive work being performed on WPAD, connections with the internet, and Tcpip parameters. The interaction with WPAD is especially concerning as it can be exploited to glisten passwords and perform a man in the middle attack.

Process Monitor - C:\Users\malware\Desktop	final.PML			- • ×
File Edit Event Filter Tools Options	Help			
0 2 2 5 🖬 7 2 0	盎∲ ↗↗ ▓☴⊋✍д			
Time Process Name PID Operation	Path	Result	Detail	
12:16: RegSvr32.exe 3152 RegCreateK	y HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	Desired Access: R	
12.16 # regvv32.exe 12.16 # regvv32.exe 11.26 # regvv32.exe 12.26 # regvv32.exe 12.26 # regvv32.exe 12.26 # regvv32.exe 12.26 # regvv32.exe 12.27 # regvv32.exe 12.28 # regvv32.exe 12.29 # regvv32.exe 12.29 # regvv32.exe 12.20 # regvv32.exe 12.20.	HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Connections HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLM/System/CurrentControlSet/Services/Topi/Parameters HKLU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Vopad/(\$11837E1-86E3-4F85-8556-82464EB0A388)) HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Vopad/(\$11837E1-86E3-4F85-8556-82464EB0A388)/00 HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Cornections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Cornections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Cornections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Cornections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Cornections HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Vopad/(\$11837E1-86E3-4F85-8556-82464EB0A388)/00 HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Vopad/(\$11837E1-86E3-4F85-8556-82464EB0A388)/00 HKCU/Software/Microsoft/Windows/Current/Version/In	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS REPARSE SUCCESS	Desired Access: Q. Desired Access: Q. Desired Access: Q. Desired Access: Q. Desired Access: Q. Desired Access: Q. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: Q. Desired Access: Q.	
Showing 28 of 70,239 events (0.039%)	Backed by C\Users\malware\Desktop\final.PML			

Figure 19: Created Registry Keys

4. Identify any files created/modified by the malware.

In order to identify the files created and modified procmon was used. As seen below in Figure 20 a significant amount of modifications was made in association with WPAD which as described earlier is a concerning indicator for the system being compromised.

	Process Monitor - C	:\Users\malware\Desktop\fin	al.PML			- • ×
File	e Edit Event F	Filter Tools Options H	elp			
	7 🔙 🖸 🗖		Å <u>∲ </u>			
Tim	e Process Name	PID Operation	Path	Result	Detail	
12:1 12:1 12:1 12:1 12:1 12:1 12:1 12:1	6 regsvr32.exe 6 regsvr32.exe 6 regsvr32.exe 6 regsvr32.exe 6	3152 1 RegSetValue 3152 1 RegSetValue	HKCU Vsoftware VMcrosoft Windows Currert Version Vitemet Settings 'ProxyEnable HKCU Software VMcrosoft Windows Currert Version Vitemet Settings' ZoneMap' ProxyBpass HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' VitranetName HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' Untranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' VAtoDetect HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' VAtoDetect HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' VAtoDetect HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' Vitranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' Vitranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap' Vitranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet Name HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Windows Currert Version Vitemet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitemate Settings ZoneMap Vitranet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitemate Settings ZoneMap Vitranet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitemate Settings ZoneMap Vitranet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitemate Settings ZoneMap Vitranet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitemate Settings ZoneMap Vitranet Settings ZoneMap Vitranet Settings ZoneMap Vitranet HKCU Software VMcrosoft Vitranet Settings Zoftw	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Type: REG_DWO Type: REG_BINA Type: REG_DWO Type: REG_DWO Type: REG_DWO Type: REG_DWO Type: REG_DWO Type: REG_DWO Type: REG_DWO	
12:1	6 Tregsvr32 exe	3152 RegSetValue	HKCU/Software/Microsoft/Windows/Current/Version/Internet/Settings/Wpad/(911837E1-B6E3-4FB5-B556-82464EB0A38B)/Wp	SUCCESS	Type: REG_DWO	
12:1 12:1 12:1 12:1 12:1 12:1 12:1 12:1	6. • regard 22 exe 6. • regard 22 exe 6. • regard 22 exe 6. • regard 22 exe 6. • regard 22 exe 9. • regard 22 exe	112 Reg Set Value 3152 Reg Set Value	HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (911837E 1.86E3.4FB5.8556.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (911837E 1.86E3.4FB5.8556.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Reason HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Reason HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision Time HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (00.505.687.8b3c.Wipad Decision HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (01.571.1663.44FB.5856.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (11.837E 1.6663.44FB.5856.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (11.837E 1.6663.44FB.5856.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (11.837E 1.6663.44FB.5856.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (11.837E 1.6663.44FB.5856.82464EB0A38B)/Wip. HKCU Software Microsoft Windows Current Version Internet. Settings Wipad (10.505.667.7b3c.Wipad Decision Re	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Type: REG_DWO Type: REG_SZ, LE Type: REG_DWO. Type: REG_BINA. Type: REG_DWO. Type: REG_DWO. Type: REG_DWO. Type: REG_SINA. Type: REG_SZ, LE Type: REG_DWO. Type: REG_DWO. Type: REG_DWO. Type: REG_DWO. Type: REG_DWO. Type: REG_BINA.	
12:1 12:1 12:1 12:1	9: Pregsvr32.exe 9: Pregsvr32.exe 9: Pregsvr32.exe 9: Pregsvr32.exe	3152 RegSetValue 3152 RegSetValue 3152 RegSetValue 3152 RegSetValue 3152 RegSetValue	HKCU/Software Microsoft/Windows/Current/Version/Internet Settings/Wipad/00-50-56-87-86-30:Wipad/Decision/Reason HKCU/Software/Microsoft/Windows/Current/Version/Internet Settings/Wipad/00-56-587-86-30:Wipad/Decision/Reason HKCU/Software/Microsoft/Windows/Current/Version/Internet Settings/Wipad/00-50-56-87-86-30:Wipad/Decision HKCU/Software/Microsoft/Windows/Current/Version/Internet Settings/Wipad/00-50-56-87-86-30:Wipad/Decision	SUCCESS SUCCESS SUCCESS SUCCESS	Type: REG_DWO Type: REG_DWO Type: REG_BINA Type: REG_DWO	

Figure 20: Modified Files

5. Identify any processes started by the malware.

By utilizing process explorer we can observe that there were no processes started by the sample3.dll file when run.

e Options view Process i	ind User	s Help	1.12		0 10
a 🙆 🚍 🗉 🗖 🗐 😁	XA				<filter by="" name=""></filter>
ICESS	CPU	Private Bytes	Working Set	PID Description	Company Name
dwm.exe	< 0.01	80,860 K	75,512 K	1868 Desktop Window Manager	Microsoft Corporation
svchost.exe		5,376 K	11,936 K	844 Host Process for Windows S	Microsoft Corporation
svchost.exe	< 0.01	15,468 K	26,704 K	872 Host Process for Windows S	Microsoft Corporation
svchost.exe	< 0.01	8,324 K	10,128 K	1088 Host Process for Windows S	Microsoft Corporation
spoolsv.exe		4,416 K	8,916 K	1220 Spooler SubSystem App	Microsoft Corporation
svchost.exe		8,856 K	10,772 K	1248 Host Process for Windows S	Microsoft Corporation
svchost.exe		2,964 K	5,556 K	1336 Host Process for Windows S	Microsoft Corporation
svchost.exe		3,060 K	6,632 K	1364 Host Process for Windows S	Microsoft Corporation
VGAuthService.exe		1,844 K	7,484 K	1416 VMware Guest Authenticatio	VMware, Inc.
m3dservice.exe		896 K	3,252 K	1540 VMware SVGA Helper Service	VMware, Inc.
vm3dservice.exe		896 K	3,472 K	1592	
vm vmtoolsd.exe	< 0.01	8,972 K	15,680 K	1584 VMware Tools Core Service	VMware, Inc.
dlhost.exe	< 0.01	2,768 K	8,736 K	2008 COM Surrogate	Microsoft Corporation
s msdtc.exe		2,392 K	6,496 K	320 Microsoft Distributed Transa	Microsoft Corporation
sppsvc.exe		5,724 K	11,060 K	2308 Microsoft Software Protectio	Microsoft Corporation
svchost.exe		173,452 K	29,256 K	2352 Host Process for Windows S	Microsoft Corporation
SearchIndexer.exe		18,428 K	10,940 K	2440 Microsoft Windows Search I	Microsoft Corporation
taskhost.exe	< 0.01	6,856 K	10,772 K	2728 Host Process for Windows T	Microsoft Corporation
sass.exe		2,436 K	7,664 K	500 Local Security Authority Proc	Microsoft Corporation
🔝 Ism.exe		1,208 K	3,116 K	508	
💽 winlogon.exe		1,608 K	5,256 K	432	
a explorer.exe	< 0.01	26,584 K	49,056 K	2168 Windows Explorer	Microsoft Corporation
vmtoolsd.exe	< 0.01	4,644 K	8,680 K	3016 VMware Tools Core Service	VMware, Inc.
🖃 📷 cmd.exe	Constanting of	1,812 K	2,436 K	2856 Windows Command Processor	Microsoft Corporation
regsvr32.exe		2,980 K	10,160 K	3152 Microsoft(C) Register Server	Microsoft Corporation
🖃 🌉 Procmon.exe		3,704 K	6,848 K	952 Process Monitor	Sysintemals - www.sysinter
Procmon.exe	< 0.01	67,256 K	23,384 K	2740	
Drocexp.exe	< 0.01	10,164 K	18,676 K	1912 Sysintemals Process Explorer	Sysintemals - www.sysinter

Figure 21: process explorer

6. Identify any persistence mechanisms employed by the malware.

After analyzing sample3.dll there was no persistence mechanisms observed with exception of the mutants stored in the Windows and System32 folders.

7. Describe what you did to overcome the obfuscation methods the program uses.

Directly overcoming the obfuscation methods issued by this malware was beyond my ability. To help alleviate overcome this obstacle and still analyze the malware virus total, JOES and box Cloud, and Intezer Analyze were leveraged to help guide the direction taken. From there I used the tools available to the best of my ability to confirm sections of compromise.

Indicators of Compromise

There are several indicators of compromise for this malware sample including the obfuscation methods as well as anti-debugging techniques deployed. In addition there is observable interactions with WPAD, however; even more blatant is that several minutes after activation there is a significant uptick in network activity. These behaviors are the observed indicators of compromised of this malware.

To identify this malware a yara rule was created and tested for correct use. See below for the established rule:

rule creds_ru

{

meta:

description = "simple YARA rule"

strings:

condition:

(\$a and \$b)

}