You need a PROcess to check your running processes and modules. The bad guys, and red teams are coming after them! RUNDLI **NCCOIOUD** Michael Gough – Principal NCC Group Founder MalwareArchaeology.com & IMFSecurity.com Malwar MalwareArchaeology.com

	or_proc *	W_Proce*	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	1/2 $M/ho am I$
2T13:26:58:02	n/a	n/a	C:\Windows\system3\\cvid.ext_/:\User\BCB\.pplata\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	Blue To	eam [efender Ninia. Malware Archaeologist. Logoholic and
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""1
2T13:26:58:34	rincip	bal Ind	Ident Response Engineer for Acc group
2T13:26:58:751	n/a	n/a	
2T13:26:59:391	love .	'prop	erly" configured logs – they tell us Who, What, Where,
2T13:26:59:391	N/hon	and h	opofully How
2T13:27:01:902	viien	anui	operativitiow
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a Creator of
2T13:27:17:922	n/a	n/a	n/a (N/indexus Leasing Cheet Cheet"
2T13:27:17:922	n/a	n/a	n/a "Windows Logging Cheat Sheet"

"Windows File Auditing Cheat Sheet"

"Windows Registry Auditing Cheat Sheet"

"Windows Splunk Logging Cheat Sheet"

"Malware Management Framework" C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO

Co-Creator of "Log-MD" – Log Malicious Discovery Tool 🕇 LOG-MD And co-host of "THE Incident Response Podcast"

n/a

n/a

n/a

n/a

2T13:27:23:87Discover it

n/a

MalwareArchaeology.com



Archaeology

	or_Proc *	w_Proce*	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L205N7882P.doc"
2T13:26:51:263	s n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	t n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	2 n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	l n/a	n/a	n/a
2T13:26:59:391	. n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 - n 4
2T13:27:01:902	t n/a	n/a	n/a
2T13:27:01:902	2 n/a	n/a	n/a
2T13:27:04:804	l n/a	n/a	n/a
2T13:27:17:922	2 n/a	n/a	n/a
2T13:27:17:922	2 n/a	n	
2T13:27:17:922	2 n/a	n/	
2T13:27:17:922	2 n/a	n/a	Consert BODIA; Mata\Loug Tempe 9. kt
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\Ap_Data\Local\Temp\"9.exe
2T13:27:19:201	. n/a	n/a	n/a
2T13:27:19:934	l n/a	n/a	n/a
2T13:27:20:137	7 n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:137	7 Oxaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:200) n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200) 0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:246	5 n/a	n/a	n/a
2T13:27:20:246	5 n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	5 0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0 0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	
2713	JG+N		MalwareArchaeology.com
2T13:27:23:87	Discover it	n/a	n/a Archaeology

	or_Proc * w	Proce	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L20SN7882P.doc"
2T13:26:51:263	s n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	Filo		s in memory only malware
2T13:26:58:02	nfa		Swiddlwl\syltdml2Chdlele1CCulerS808Cpbala[LS9ai\TImb\L4CL1aVVCIIC
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	2 n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	To ac	Idre	ess this expanding threat that is
2713:26:58:751	10 40	i ui t	255 this expanding threat that is
2113:26:59:391	hace	mir	m mara and mara common too
2113:20:39:391	peco	reger	ig more and more common, too
2T13-27-01-902		n/a	0/3
2713:27:04:804	comr	nor	
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	2 n/a	n/a	n/a
2T13:27:17:922	2 n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	Com	20	dity malwara Rod Taam angagamanta
2T13:27:19:201	COIIII	110	uity maiware, neu ream engagements,
2T13:27:19:934	l n/a	n/a	
2T13:27:20:137	and	DT C	OURSE API I STATTACKERS USE IT Local GCEXN54 XBe6RSIM.exe C: Users \BC
2T13:27:20:137	7 Oxaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200) n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2713:27:20:200	0 0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2113:27:20:246	n/a	n/a	
2113:27:20:240	Thic	$\infty \circ$	thad can avoid many cocurity tools
2112:27:20:240	111121	ne	thou can avoid many security tools
2T13:27:20:30:	0x6b0	0xa30	ping 1.3.1.2 - n.1
2T13:27:20:34) n/a	n/a	n/a
2113	DG-M	D/a	Malware Malware
2T13:27:23:87	Discover it	n/a	Archaeology

	• or_Proc •	w_Proce*	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L205N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	. n/a	/a	n/a
2T13:26:59:391	n/a	/a	DT'C KOTNINK OK
2T13:26:59:391	0x6b0	d74	ping 2 L1.1 - nd
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	
2T13:27:17:922	n/a	n/a	
2T13:27:17:922	n/a	n/a	
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	- • 1	n/a
2T13:27:20:137	n/a	r Ba	Condensioner sympleyers.cete:\m\BBB\preat/LongCondinie6RSIM.exe C:\Users\B0
2T13:27:20:137	0xaa4	0> 00	<pre>unvindersesystems.systems.systems/systems/sest/users/BBB_structure/LocalSC_EKNe+txbe6RSIM.exe C:\Users\B0</pre>
2T13:27:20:200	n/a	nya.	C:\windows\systemsz\sysprep\sysprep.exe C:\bsers\B0B\AppData\Local\GCczKN54\xbe6RSIM.exe C:\Users\B0
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:246	i n/a	n/a	n/a
2T13:27:20:246	i n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:305	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	
2713	JG-N	D/a	MalwareArchaeology.com
2T13:27:23:87	iscover it	n/a	n/a Archaeology

or Proc v w Proci v Process Command Line/CommandLine **Rethinking Fileless Malware** C:\Users\BOB\Desktop\LZ0SN7882P.doc" • Fileless Malware that can only be found in the memory of a running system (Malware + Memory = *Memware*) No files can be found if you scan the disk while the system is running Or are very short lived, just long enough to load (bypasses FIM) Typical infection vectors are: - "Injection^{C:\Users\BOB\AppData\Local\Temp\"9.exe} Dll side-loading/Hijacking - nProcess Hollowingem32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO Download source code and compile on the fly, .NET, JSC -Ox User double-click, etc. "Fileless" malware, the file lives somewhere, so lets do a better job guiding people where to look for signs of it MalwareArchaeology.com

Discover it

v or Proc v w Proci v Process Command Line/CommandLine Other Fileless Malware types C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs" n/a Regware – Malware payload is stored in the registry with an autorun/ASEP that calls and loads it into memory (Malware + Payload in Registry = RegWare) ping 2.2.1.1 -n 4 • WMIware - Malware payload is stored in the WMI database with an autorun/ASEP 2113-27-01-902 that calls and loads it into memory (Malware + Payload in WMI database = 2T13:27:04:804 WMIWare)/a n/a • PowerShellware - Malware payload is in the form of PowerShell scripts, downloaded or stored somewhere on the fly with an autorun/ASEP that calls and 2T13:27:17:922 loads it into memory (Malware + Payload in PowerShell = PowerShellWare) Compileware – Malware payload is not yet compiled, stored anywhere with an accused anywhere with any accused any accused anywhere with any accused anywhere with any accused any a 2713:27:20:133 autorun/ASEP that calls and loads it into memory (Malware + Payload compiled on users) and lo the fly = CompileWare)\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC 0xc38 C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO n/a Downloadware – Autorun/ASEP calls out to the Internet to download malware 2T13:27:20:246 payload or source code that is then compiled and loads it into memory (Malware + ^{2T13:27:20:309} Payload downloaded each time = DownloadWare) maybe LOLBASWare ;-) MalwareArchaeology.com 2T13:27:23:87Discover it

	* or_Proc *	w_Proce	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	Autorung/ASED
2T13:26:58:02	n/a	n/a	C:\Windows\\yUmC:\UdextY.dextY.d\usSidowA, Sathusaal\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	2 n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34 2T13:26:58:751	Keep) în	cscript.exe_'C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:59:391	. n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	$-\infty Nc$	of al	I malware will have an autorun/ASEP
2T13:27:01:902	n/a	n/a	
2T13:27:01:902	n/a	Late	st TrickBat on Domain Controllers
2T13:27:04:804	n/a	Late	
2113:27:17:922	n/a	Ecn	cially the Red Team deern't like to leave IOCs
2113:27:17:322	n/a •	LShe	e lang the red learn, doesn't like to leave locs
2T13-27-17-922	n (C)	inja .	Chilsen BOB ano Dati Ni ocali Tempi 19 erel
2T13:27:17:922	– Or	, τηε	e autorun is created on shutdown, then
2T13:27:19:201	n/a	n/a	
2T13:27:19:934	ae	lete	d on startup once the maiware loads
2T13:27:20:137	/ n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\E
2T13:27:20:137	0xaa4●	Not	hing found when doing live triage/analysis (Dridex)
2T13:27:20:200) n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\E
2T13:27:20:200		wh	at is in memory may he all that we can see
2T13:27:20:246	n/a C	V N/3 1	at is in memory may be an ende we can see
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246) 0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
21131271201309		n/a	ping 1.3.1.2 - n 1
2113:27:20:309	0000	uxasu a /a	ping 1.5.1.2-11
211212/1201340	G_N		Malware
2T12-27-22-87	Discover it	n la	MalwareArchaeology.com Archaeology
and deal of a field of a stand of the field	1.1		

v or_Proc v w_Proc v Process_Command_Line/CommandLine

2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	Istact TrickRat
2T13:26:58:02	n/a	n/a	C:\WindowL, Genus Cn Set /c Clubert \Cal, p. 21, VacU, Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2712-26-50-24	mila	min	manine and Proliticard BOBI Amportal Local Tampa PRADON WILLER

TrickBot Caused By Nworm: Not Persistent

2T13:2 When nworm infects a vulnerable DC, the malware is run from memory. No artifacts are found on the infected DC 2T13:2 and TrickBot on the DC doesn't survive a reboot.

T13:27:01:902	n/a	n/a	Initial TrickBot binary	saved to disk (usually a	an EXE, sometimes a DLL)	
T13:27:04:804	n/a	n/a			bis bipany loads the	
T13:27:17:922	n/a	n/a			rickBot modules	
T13:27:17:922	n/a	n/a			nekbot modules	
T13:27:17:922	n/a	n/a			Δ	
T13:27:17:922	n/a	n/a		00		
T13:27:17:922	0x6b0	0xc10	\sim		\sim	
T13:27:19:201	n/a	n/a				
T13:27:19:934	n/a	n/a	WEN	KJV	W W	
T13:27:20:137	n/a	n/a	DLL			GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:137	0xaa4	0x600		[]		GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:200	n/a	n/a	· · · · · · · · · · · · · · · · · · ·	ЧПППТ		GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:200	0xaa4	0xc38	TrickBot module	TrickBot module	TrickBot module	GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:246	n/a	n/a	run from memory	run from memory	run from memory	
T13:27:20:246	n/a	n/a	C. (users (oup)-pppara (cocarlaceswino+typeon	aimiexe ci (users (pop (A)	pData\Local\Temp\9.exe 3
T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\	Local\GCEzKN54\xBe6R	SIM.exe C:\Users\BOB\A;	opData\Local\Temp\9.exe 3
PaloAlt	o Unit 42 -	https://	/unit42 paloaltonetworks	com/goodbye-mworm	-hello-nworm-trickbot-ur	odates-propagation-module/
T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1			
T13:27:20:340	n/a	n/a	n/a			
T13 22 20	G-N	D/a	n/a	MalwareArchaeology.c	com	Malware
T13:27:23:87Dis	cover it	n/a	n/a	- 67		Archaeology

	or_Proc *	w_Proce*	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	. n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/	n/a
2T13:27:01:902	n/a	n/s	
2T13:27:04:804	n/a	n/a	
2T13:27:17:922	t n/a	n/a	n/a
2T13:27:17:922	2. n/a	n/a	n/a
2T13:27:17:922	2 n/a	n/a	n/a
2T13:27:17:922	2. n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	0x6b0	0×0	C:\Lisers\BOR\ ppDateLlow \Templ*9.eve
2T13:27:19:201	n/a	n	
2T13:27:19:934	l n/a	n	
2T13:27:20:137	r n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:200) n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:200) 0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B0
2T13:27:20:246	i n/a	n/a	n/a
2T13:27:20:246	i n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	
2713	JG-N		MalwareArchaeology.com
2T13:27:23:87)iscover it	n/a	n/a Archaeology

	• or_Proc •	N_Proci *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	s n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	l n/a	n/a	\wedge N/ITREATE/CK
2T13:26:58:02	n/a	n/a	C:\Windows\Vystein3L\chote/cC\Usert\BCB\
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	2 n/a	n/a	n/a
2713:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2113:26:5 2T13:26:58:751	First	-n/L	erything you do should be mapped to
2T13:26:59:391			TTP.CK https://attack.mitro.org/
2T13:26:59:391	ТУффьр Г		a lack - https://attack.httle.org/
2T13:27:01:902	2 n/a	n/a	n/a
2T13:27:0=902 2T13:27:04:804	Som	e of	the techniques used
2T13:27:17:922 2T13:27:17:922	$\frac{n/a}{-n/1}$	500	- Compile After Delivery
2T13:27:17:922	2 n/a	n/a	n/a
2T13:27:17:922	2n/T1	127	- Trusted Developer Utilities
2T13:27:17:922	2 0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"5.exe
2T13:27:19:201 2T13:27:19:934	<u> </u>	055	 Process Injection
2T13:27:20:137	r n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\I
2T13:27:20:137	7 <u>0</u> xa14	196	-VControl Panel Itemsers\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\i
2T13:27:20:200) n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\I
2113:27:20:200 2T13:27:20:266	– eta	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCE2KN54\xBebRSIM.exe C:\Users\I n/a
2T13:27:20:246	5 n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe_C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:29.246	Sub-	teck	niques are coming.electusers\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:20:	ps://www.jaimi	nton.com/r	nitreatt&ck
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340		n/a	
2713		/a	MalwareArchaeology.com

MalwareArchaeology.com

n/a

n/a

2T13:27:23:87Discover it



or Proc v w Proci v Process Command Line/CommandLine We need a PROcess cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs" We need to create a PROcess to start looking for this condition Tools are just not preventing this technique We need to build this PROcess into our hourly/daily/weekly/monthly routines to detect and alert for this technique We need to build this PROcess into our daily/weekly/monthly/yearly routines to Threat Hunt for this technique

b0 0xa30 ping 1.3.1.

MalwareArchaeology.com



	<pre>v or_Proc v </pre>	v_Proce*	Process_Command_Line/CommandLine	
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L205N7882P	v.doc"
2T13:26:51:263	s n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P	v.doc"
2T13:26:57:924	l n/a	n/a	Finding Memware	
2T13:26:58:02	n/a	n/a	C:\\Indlub\IyMnl2lcri De/ICVULeC318IAIpVaV\MilTeC\14323.bat	
2113:26:58:02	0x160	0x660	C:\Windows\system32\cmd.exe /cC:\Users\BOB\AppData\Local\Temp\14323.bat	
(113:20:36:114)T12:36:58:24	n/a	n/a n/a	nya cscript eye "C\Users\BOB\AnnData\Local\Temp\""14323"" v""hs"	
2713:26:50:34	Tradit	iona	al forensics has us dumning a memory image	
2T13:26:58:751	/i	n/a	interesting a sub-	
2T13:26:59:391	and r	unni	ing tools like volatility against it	
2T13:26:59:391		0xd74	contain a lot of dotails that can alort you to	
2T13:27:01:902	LUgs		contain a lot of details that can alert you to	
T13:27:01:90/	this b	eha	vior, IF you collect THEN detect OR hunt	
T13:27:17:922			a proposed line is KEV to establing these attacks	
2T13:27:17:922		cess	s command line is KEY to catching these attacks	
2713:27:17:922	Check	king	running processes and their modules on a live	
(113:27:17:92) (T13:27:17:92)	cvctor	n ic	aGREAT ontion	
2T13:27:19:201	Syster	n/a	a GREAT OPTION	
2713:27:19:934	– Bet	tter y	yet look for signs of injection !!	Line and Di
2T13:27:20:137	look	fort	he other artifacts autorun/ASEP registry keys	Users\B(
2T13:27:20:200	n/a	n/a	(Windows)system/2)system)system exect (User ARD) / Cotal (GCE X 154) xBedRSIM, exe C	Users\B0
2T13:27:20:200	storin	ig sc	ripts and/or payloads, wivil databases storing	Users\B(
2T13:27:20:246	script	s an	d/or payloads, and odd PowerShell, large	
2113:27:20:240	block			
T13:27:20:240	DIOCK	s, or	Ding 1.3.1.2 - n.1	
T13:27:20:30	0x6b0	0xa30	ping 1.3.1.2 -n 1	
T13:27:20:340	n/a	n/a	n/a	
2113	JG-N	D/a	n/a MalwareArchaeology.com	1 # 6



n/a

n/a

2T13:27:23:87Discover it



v or Proc v w Proci v Process Command Line/CommandLine

2T13:26:51:248	0xaa4	Oxf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L205N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	Frances
2T13:26:58:02	n/a	n/a	C:\Windows\system
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\1432s.bat

Kovter injects into SvcHost 32bit

			n ocan i e		0				,	1.
Process_Name	Executable	Module_Name	- V -	Log-MD	Valuation	b9 💌	Injection	Τ.	Catalog 🔽	k
IAStorIcon.exe	C:\Program Files\Intel\Intel(R) R	apid S [.] C:\Program Files\Intel\Intel(R) Rapi	d Storage h	Suspect		in digest (trusted)	Hook 1 Det 3 In	np 4	FALSE	h
IAStorDataMgrSv	C:\Program Files\Intel\Intel(R) R	apid S [·] C:\Program Files\Intel\Intel(R) Rapi	d Storage h	Suspect		in digest (trusted)	Hook 1 Det 7 In	np 18	FALSE	h
SupportAssistAg	C:\Program Files\Dell\SupportA	sistA <mark>gCt\Program Files\Doll\SupportAccic</mark>	t≜gent\bi h	Suspect		in digest (trusted)	Hook 1 Dot 2		FALSE	s
svchost.exe	C:\Windows\SysWOW64\svchos	t.exe C:\Windows\SysWOW64\svchost.e>	e h	Suspect		in digest (trusted)	Hook 3 Imp 2		TRUE	Ν
svchost.exe	C:\Windows\SysWOW64\svchos	t.exe C:\Windows\SysWOW64\svchost.e>	e h	Suspect		in digest (trusted)	Hook 3 Imp 2		TRUE	٨
								· · · · · · · · · · · · · · · · · · ·		

Qakbot

n/a

	U	E	F	G	Н		J	K
Process_Name	Executable	Module_Name	VT 🔹	Log-MD_Valuation	r b9 🔽	Injection 🗾	Catalog 💌	Issuer_Name
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\WINDOWS\Explorer.EXE		Suspect	in digest (trusted)	Imp 3	TRUE	Microsoft Win
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\WINDOWS\system32\explorerframe.d	II	Suspect	in digest (trusted)	Parent Injection Indi	TRUE	Unsigned
explorer.exe	C:\WINDOWS\Explorer.EXE	C:\Windows\System32\Windows.UI.FileE	xplorer.d	II Suspect	in digest (trusted)	Parent Injection Indi	TRUE	Unsigned
explorer.exe	C:\WINDOWS\Explorer.EXE	c.\www.bows\systems2\wetworkExplore	- dll	Suspect	in digest (trusted)	Parent Injection Ind	TRUE	Unsigned
explorer.exe	C:\WINDOWS\SysWOW64\explorer.exe	C:\WINDOWS\SysWOW64\explorer.exe		Suspect	in digest (trusted)	Hook 1 Imp 2	TRUE	Microsoft Win
13:27:19:934	n/a n/a n/a							
13:27:20:131)ridex _{/a} c:\win	dows\system32\sysprep\syspr	ep.exe	C:\Users\BOB\A	ppData\Local\0	CEzKN54\xBe6R	SIM.ex	e C:\Users\)

stem22) sysprep, exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC

2	_					Log-MD								1	\B
1	Process_Name	IM	odule_Name		VI	Valuation	69	Injection	Catalog	Issuer_Na	a Subject_N	Process_I	Parent	ŀ	1
2	svchost.exe	(Pr	ocess likely termi	nated during c	apture.							10356	6	88	\B(
2	rundll32.exe	(C:\	\Windows\SysWC	0W64\rundII32	.exe h	Suspect	in digest (trusted)	Rep 1	TRUE	Unsigned	Unsigned	6356	124	<mark>92 7</mark>	
	rundll32.exe	(C:\	\Windows\SYSTE	VI32\ntdll.dll	h	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Microsoft	Microsoft	6356	124	92 k	
2	rundll32.exe	10.	Windows\Cyster	-22\imagehip	h h	Suspect	in digest (trusted)	Parent Injection Indicator	TRUE	Minnef	1.1: ft	6356	124	92 c	
2	rundll32.exe	(c:\	Users\Hackme\D	esktop\Dridex	.dll h	Malicious	Suspicious	Parent Injection Indicator	FALSE	Unsigned	Unsigned	6356	C:\Windows\System32\rundll32.exe 12492	<mark>2)</mark> 5	
y.	F13:27:20:3	09	n/a	n/a	ning	1.3.1.20	- 1- 171 - N	 A set of the set of				6051		00 f	
	a she at a size of a size of a soft		riy w	11/14		dell'a della de	-								
2	T13:27:20:3I	09	0x6b0	0xa30	ping	1.3.1.2 -n	1								
ż	T13:27:20:3-	40	n/a	_n/a	n/a									11	
x	T1: 01 2		DG-N	Dia	nla								Malware		
	a deal of the state of the stat	-			1.4.0		Ma	wareArchaeology.c	om				A DIT A	e cr	
Z	F13:27:23:8	Di	scover it	n/a	n/a								Archaeolog	19	2

		+				
	v or_Proc v	v_Proci *	Process_Command_Lin	e/CommandLine		
2T13:26:51:24	3 Oxaa4	0xf60	C:\Program Files (x86)\I	Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L	Z05N7882P.do	c"
2T13:26:51:26	3 n/a	n/a	C:\Program Files (x86)\/	Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L	Z0SN7882P.do	C
2T13:26:57 92	vtra	oto	nd Eila	CINC MD 8. Valatil	i+\/	
2T13:26:58	Χισ		C Moores stele C2	SLUG-IVID & VUIALII	ιιγ	
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\	cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat		
2T13:26:58:11	2 n/a	n/a	n/a			
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\B	OB\AppData\Local\Temp\""14323"".v""bs"		
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\B	OB\AppData\Local\Temp\""14323"".v""bs"		
2T13:26:08:75	NakB	ot	n/a			
2T13:26:59:39	QUND	n/a	ping 2.2.1.1 -n 4			
2T13:26:59:39	Z Ox6ba	0xd74	ping 2.2.1.1 -n 4			
2T13:27:01:90	κοντε	2 n/a	n/a			
2T13:27:01:90	2 n/a.	n/a	n/a			
2T13:27:04:80	Dride	Yn/a	n/a			
2T13:27:17:92		n/a	n/a			
2T13:27:17:92	2 n/a	n/a	n/a			
2T13:27:17:92	z n/a	n/a	n/a			
2T13:2 File Na	me 🔽 Origin	al Filoname	v Internal Filename	Result of DDR Dath	Certificates 🔻	
2T13 Qakbot	1.exe			suspicious C:\Users\parkhyunseo\source\repos\Project28\Debug\Project28.pdb	None found.	
Faxprint	.dll			malware	None found.	
Kovter_	1.exe diffuse	eGravity.exe	e diffuseGravityP	malware	None found.	
2113	z.exe rjrwer	.exe	Java(TM) Control Panel	malware	None found.	rs\F
OakBot	3 exe nio.dll		D		None found.	rs\F
Dridex.o			Process Fire	suspicious c:\stop\Soft\duck\liquid\build\wide\DivideDictionary.pdb	None found.	rs\F
2T13:2 rofce.dl	2.2.2			suspicious		10015
2712-27-20-24	5	nla	nla		1	in the

C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3 n/a

0xc38

ated with LOG-MD B9 module Evalu

n/a

G-MD

2T13:27:23:87Discover.it

MalwareArchaeology.com



	• or_Proc •	w_Proce *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	n/a	n/a	Fyamnlas
2T13:26:58:02	n/a	n/a	C:\Windows\systemte\c.in.Cl. /c Cl\Us (EDN+), Data\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:5334 2T13:26:58:751	They	/ ca	n call out to the Internet to download
2T13:26:59:391 2T13:26:59:391	the d	code	e to compile, or fetch the malware so
2T13:27:01:902	it do		at live on dick. Some examples:
2113:27:01:902	n uo	621	iot live offusk. Some examples.
2113:27:04:804	n/a	n/a	n/a _/_
2113:27:17:322	n/a	n/a n/a	n/a
2T13:27:17-922	n/a	n/a	n/a
2T13:27:17:922	– (c	halt	Strike and Sythe custom malware nackages
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n ja 👝	I Din	/ al Pac Dundll22 Pageur22 Pagacon ata
2T13:27:19:934	—,LO	LDII	S/LOLDAS – RUHUHSZ, REGSVISZ, REGASHI, ELC.
2T13:27:20:137	n/a	http	ci//github.com/IOIPAC Droject/IOIPAC
2T13:27:20:137	0xaa4	nup	S.//github.com/LOLDAS-Project/LOLDAS:kns4\xBe6RSIM.exe C:\Users\B
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:200	CC	mpi	iers - Csc.exe, Misbulla.exe, JSC.exe, etc.
2T13:27:20:246	n/a	n/a	n/a
2113:27:20:246	-M	ay w	rite to disk on shutdown, delete on startup
2113:27:20:240	0xC38	ala.	c:\users\bublecalbublecal\bublecalbubleca
2113-27-20-309	ny a Oyébû	0ya20	ping 1312-01
2T13:27:20:309	n/a	n/a	n/a
2713 2126)G-N		Malware Archaeology com
2T13:27:23:87D	iscover it	n/a	Archaeology

	• or_Proc •	w_Proce *	Process_Command_Line/Comman	dLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft (ffice\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft (flice\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	l n/a	n/a		avamnla
2T13:26:58:02	n/a	n/a	C:\WinCJC.CAC	C:\CAGAppDataCd\Cnp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /	: C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a	
2T13 2T13 2T13 2T13 2T13 2T13 2T13 2T13 2T13 2T13 2T13	Procmon.exe (285 Procmon64.ex cmd.exe (6732) conhost.exe (5 powershell.exe csc.exe (3 cvtres.exe)	56) e (2140) 5064) e (1756) 84) exe (1884)	Process Monitor C:\Users\testuser Process Monitor C:\Users\TESTU Windows Comma C:\WINDOWS\sy Console Window C:\WINDOWS\sy Windows PowerS C:\WINDOWS\S Visual C# Comma C:\Windows\Micr Microsoft® Resou C:\Windows\Micr	Sysintemals - ww DES Sysintemals - ww DES Microsoft Corporat DES Microsoft Corporat DES Microsoft Corporat DES Microsoft Corporat DES Microsoft Corporat DES
2T13 <		>	<	C:\WINDOWS\system32\cmd.exe
2T13 Description: 2T13 Company: Path: Command: 2T13 User: 2T13 PID: 2T13 Go To Even 2T13 Go To Even	Visual C# Com Microsoft Corp C:\Windows\M "C:\Windows\ DESKTOP-Q4N 384 S E nt Include P	mand Line Co oration licrosoft.NET dicrosoft.NET DIRQ\testus Started: 10, Exited: 10, rocess	ompiler \Framework64\v4.0.30319\csc.exe F\Framework64\v4.0.30319\csc.exe" /noconfig er 1 /14/2019 9:16:36 PM /14/2019 9:16:38 PM Include Subtree	C:\Users\testuser1\AppData\Local\Temp>dir Volume in drive C has no label. Volume Serial Number is CAED-FF5D /fullpaths @"C Directory of C:\Users\testuser1\AppData\Local\Temp 10/14/2019 09:20 PM <dir> 10/14/2019 09:20 PM <0IR> 10/14/2019 09:20 PM 0 arla-debug-5148.log 10/14/2019 09:20 PM 36 oj52lfcy.0.cs 10/14/2019 09:20 PM 359 oj52lfcy.cmdline 10/14/2019 09:20 PM 0 oj52lfcy.err 10/14/2019 09:20 PM 0 oj52lfcy.err 10/14/2019 09:20 PM 0 oj52lfcy.out</dir>
2T13:27:20:200 2T13:27:20:200 2T13:27:20:246 2T13:27:20:246 2T13:27:20:246 2T13:27:20:246	<random <random Csc.exe /</random </random 	n.cs> n.cmdli 'nocon	C:\Windows\system32\sysprep\sy C:\Windows\system32\sysprep\sy n/a ine>ers\BOB\AppData\Local\GCE ofig /fullpaths @\Local\GCE	Sprep.exe C: 10/14/2019 09:20 PM 0 oj52lfcy.tmp 10/14/2019 09:15 PM Vmware-testuser1 10/14/2019 09:15 PM Vmware-testuser1 10/14/2019 09:206 AM 35,077,976 wct5500.tmp Vmware-testuser1 10/11/2019 09:50 PM 20,668 wctABEA.tmp 9 File(s) 35,099,039 bytes 2KN54\xBe6R 3 Dir(s) 47,555,522,560 bytes free 2KN54\xBe6R
2T13:27:20:305	https://k	log didieret	tevens com/2019/10/15/nowershell-add-	vne-csc-eve/
2T13:27:20:340	n/a	n/a	n/a	
2T13.27:23:87	DG-N Discover it	ND/a n/a	n/a Malware/	Archaeology.com Archaeology

	or_Proc *	w_Proce	Process_Command_Line/CommandLine		
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EX	E /n "C:\User	s\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EX	E /n "C:\User	s\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	Control Panel Ann	loto	
2T13:26:58:02	n/a	n/a	сопцогтанстдрр	12-163	bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local	l\Temp\1432	3.bat
2T13:26:58:112	n/a	n/a	n/a		
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""b	5"	
2T13:26:58:34 2T13:26:58:751	.CPL	files	s are all those Control Pane	el apj	plets
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4		Devices and Drinters
2T13:26:59:391	— Ru	Indli	32 C:\ <whateverdir>\Fakejava</whateverdir>	.cpl	
2T13:27:01:902	n/a	n/a	n/a	•	Flash Player (32-bit)
2T13:27:01:902	n/a	n/a	n/a		🛓 Java (32-bit)
2T13:27:04:804	n/a	n/a	n/a		🛂 Network and Sharing Center
2713:27:17:922	n/a	n/a			
2T13:27:10922 2T13:27:17:922	Laun	cne	s a bad Dil into memory -	LOLB	IIN
2T13:27:17:922 2T13:27:19922	colf	Files	load all the time so it's no	nisv	
2T13:27:19:201	.cpr-i	n/a		515 y	
2T13:27:19:934 2T13:27:20:137	3 rd p	artv	applets are not well signe		CEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\App	Data\Local\G	CEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:200	Man	v ÉC	Rs do not alert on this me	ethod	CE2KN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:200 2T13:27:20:246	n/a	n/a	n/a		CERNIO4 (ADEORDINITEXE C. (OSEIS (D
2T13:27:22:246	Tho	Rod	Team IOV/ES this method	Coh	altStriko
2T13:27:20:246	0xc58	IVE G	Team LOVES this method	s BOB (Apple	ansume
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1		
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1		
2T13:27:20:340	n/a	n/a	n/a		
2113. 21 2			n/a MalwareArchaeology.com		
2T13:27:23:87	scover it	n/a	n/a		Archaeology

	or_Proc *	w_Proci *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L20SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	n/a		
2T13:26:59:391	n/a	12	// nitoring tor
2T13:26:59:391	0x6b0	0 17-	
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Lo
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppDat_\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:137	0xaa4	0>	<pre>indexs) endings and systep.ele a\U arsi222\Landaab\LardaCC ===================================</pre>
2T13:27:20:200	n/a	r B	:\\Uniows () stem = i spisyspep.e e \Unirs BOL Ap Dai \L.tal' C = 54\xBe6RSIM.exe C:\Users\B
2T13:27:20:200	0xaa4	0,438	C:\\Windows\bytemsetaysprep\sysprep.exe C:\osers\dOb\AppData\Local\dC are 4\xBe6RSIM.exe C:\Users\B
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	
2713	JG-N	D/a	MalwareArchaeology.com
2T13:27:23:87D	iscover it	n/a	n/a Archaeology

or Proc v w Proci v Process Command Line/CommandLine **Monitor for & Threat Hunting** WORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc" We need to develop a PROcess to monitor/detect for and/or Threat Hunt for signs of these techniques Step 1 Enable the data Configure logs per the Windows Logging Cheat Sheet(s) Enable to collect 'Process Command Line' GCE2KN54\xBeGRSIM.exe C:\Users\BC C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO 2713-27 • 20 Step 2 / 4 Create detections for many of these techniques - Process command line is KEY.. It's in the parameters G-MD awar MalwareArchaeology.com 2T13:27:23:8 Discover it

	v or Proc v	W_Proce *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L20SN7882P.doc"
2T13:26:57:924	- A/	lor	hitor tor & Threat Hunting
2T13:26:58:02	n/a		
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2713:26:5	on 2	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2713:26:5271	ch's	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	Com	e li	n with a PROcess to scan Running
2113:27:01:902	COM	Cn/M	
2113.27.01.902	Droc	000	as and thair loaded Medules
2T13:27:04:804	FIUC	6220	es and then loaded modules
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	$-D\epsilon$	etect	these memory only infections
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	0x000	ic ch	ould be both for regular detection and for
2T13:27:19:201	n/a	13,31	iould be both for regular detection and for
2T13:27:19:934	Th	rost	Hunting
2T13:27:20:137	n/a	reat	d\IMId.CU/ISn32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:200	$-\mathbf{W}$	atch	for indications of injection
2113:27:20:200	Uxaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCE2KN54\xBe6KSIM.exe C:\Users\
2113:27:20:246	n/a	n/a	
2113:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
21131271200240	UXC38	Desxo	c: (users (bub (AppData (Local (GCEZKNO4 (XBeoKSIM.exe C: (Users (BUB (AppData (Local (Temp (9.exe 3
2113:27:20:309	n/a ovcho	01/8	bing 1515 bit
2112:27:20:303	0x000	n/a	build TOTTC-ILT
2712 201201340	G_N		Malware
al e al la compañía de la compañía d			MalwareArchaeology.com

2T13:27:23:87Discover it

n/a

n/a

Archaeology

	* or_Proc *	Proce -	Process_Co	command_Line/CommandLine	
2T13:26:51:248	0xaa4	0xf60	C:\Program	m Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\l	Jsers\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program	m Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\l	Jsers\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	i nV/	or	nito	r tor & Threat Hu	nting
2T13:26:58:02	n/aV			Is syste Orland, Oke C: Isels bits C; Oa Local, The	liung
2T13:26:58:02	0xf60	0x6b0	C:\Window	ws\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\J	14323.bat
2T13:26:58:112	2 n/a	n/a	n/a		
2T13:26:58:34	n/a	n/a	cscript.exe	e "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"	
2T13:26:52:04	IIgS0x6b0	0x340	cscript.exe	e "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"	
2T13:26:56:751	Maybe a	PRO	cess to so	scan strings for API calls such as;	
2T13:26:59:391	– Oper	Proces	SS 2.2.1.	1-n4	
2113:26:59:391	– Virtu	alAlloc	ping 2.2.1.	.1-04	
2113:27:01:902	– Virtu	alAlloc	:Ex		
2113-27-04-804	– Writ	Proce	ssMemory	'V	
2T13:27:17:972		Library	n/a	7	
2T13:27:17:922	Load	Library	۸n/a		
2T13:27:17:922	- Luau	LIDIALY	A Alternation	-	
2T13:27:17:922	– Crea	teremo	oteinread	BOB\AppData\Local\Temp\"9.exe	
2T13:27:17:922	– Resu	melhr	ead Users\B	BOB\AppData\Local\Temp*9.exe	
2T13:27:19:201	– Refle	ectiveLo	oader()		
2T13:27:19:934	– Oper	Proces	SSn/a		
2T13:27:20:137	– GetP	rocAdd	dress	ws\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Loc	al\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:137	– Crea	teProce	ess \Window	ws\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Loc	al\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:200	– ZwU	nMapV	/iewOfSect	ws\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Loc ction	al\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:200	– NtUr	imanVi	iewOfSect	ws\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Loc tion	al\GCEzKN54\xBe6RSIM.exe C:\Users\
2T13:27:20:246	- GotT	broad	Context		
2T13:27:20:246		anaadC	ontout	BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\Ap	pData\Local\Temp\9.exe 3
2713:27:20:246		TreadC	ontext	BOB\AppData\Local\GCEzKN54\xBebR5IM.exe C:\Users\BOB\Ap	pData\Local\Temp\9.exe 3
21131271201305	– Kesu	meinr	eads		
21131271201305	00000	uxas0	ping 1.3.1.		
21131271201340	DG_N		nya n/a		Malware
alia di akain na 🔤 na dia d			1.11.00	MalwareArchaeology.com	

MalwareArchaeology.com

Archaeology

2T13:27:23:87Discover it

n/a

		-		
	or_Proc = w	Proce *	Process_Command_Line/CommandLine	
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop	LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop	LZ0SN7882P.doc"
2T13:26:57:924	(n)	3IN	JS/I OI BAS that can download	
2T13:26:58:02		nya		4
2113:26:58:02	0x160	0x6b0	C:\Windows\system32\cmd.exe /cC:\Users\BOB\AppData\Local\Temp\14323.bat	
2112-20-30-112	n/a	n/a	recript eve "C\Users\BOB\AppDet+\Local\Temp\""14323"" v""hc"	
2T13:26:58:34	powersł	nell.ex	exe Short list per Cisco Tal	OS
2T13:26:58:751	, hitsodm	in ov		
2T13:26:59:391	Ditsaum	n/a	ping 2.2.1.1 -n4	
2T13:26:59:391	certutil.	exe	ping 2.2.1.1-n.4 INSILLA.EXE	
2T13:27:01:902	psexec.	exe	n/a	
2113:27:01:902		n/a	certutil exe	
2T13:27:04:004	willic.ex	n/a		
2T13:27:17:922	mshta.e	xe	n/a	
2T13:27:1-:922	mofcom	p.exe	e bitsadmin.exe	
2T13:27:17:922	cmstn o	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe	
2T13:27:17:922	chistp.e	AC c10	C:\Users\BOB\AppData\Local\Temp*9.exe	
2113:27:18:201	windbg.	exe		
2T13:27:20:137	cdb.exe	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOII\AppII_da\Local\GCEzKN54\xBe6F	SIM.exe C:\Users\B
2T13:27:20:137	mchuild	OVO	C:\Windows\system32\sysprep\\$ysprep\DOWERShell.exe_zkN54\xBe66	SIM.exe C:\Users\B
2T13:27:20:200	n/a		C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6F	(SIM.exe C:\Users\B
2T13:27:20:200	csc.exe	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6F	ISIM.exe C:\Users\B
2T13:27:20:246	regsvr32	2.exe	n/a Process Command Line is KEY	
2713:27:20:246	Evente	o LLL	Man to MITRE ATT&CK	\9.exe 3
2113:27:20:240	Excerto	0 111	ping 1 3 1 2 - p 1	(5.exe 5
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 - n1 https://blog.tologistellisence.com/2010/11/husting.for.lellise.html	
2T13:27:20:340	n/a	n/a	n/a	
2713	DG-M	D/a	n/a MalwareArchaeology.com	Malware
2T13:27:23:87)iscover it	n/a	n/a	Archaeology

	* or_Proc *	w_Proce *	Process_Command_Line/CommandLine	
2T13:26:51:24	8 Oxaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc	2
2T13:26:51:26	3 n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc	2 ⁸⁸)
2T13:26:57:92	Be	29C	ontions for PR()cess tools	
2T13:26:58:02			op croins non service of 5	
2113:26:58:02	0x150	0x650	C:\Windows\system32\cmd.exe /cC:\Users\BOB\AppData\Local\Temp\14323.bat	
2113:20:38:11.	z nya	n/a	n/a corrint ava "C\Urar BOB\AppData\Local\Tamp\""14222"" v""bc"	
2T13:26:52:34		Man	agament is your DEST friend here	
2T13:26:58:75	LUg	Iviali	agement is your best menu here	
2T13:26:59:39	1 n/ar		any and can afford to put agonts on all your	
2T13:26:59:39	1 0x6b0	you i	lave, and can anord to put agents on an your	
2T13:27:01:90	er	ndpoi	ints and collect the needed data	
2113:27:01:90	2 n/ a 4 n/a			
2T13:27:17:92	• n/a 2 n/a	n/a	n/a	
2T13:27:17:92	2 n/a	n/a	n/a	
2T13:27:17:92	If no	t th	on you will need a PROcess to manually	
2T13:27:17:92	211 1,40	, ¹	en you will need a ritoless to manually	
2T13:27:17:92	chec	k rii	nning process their modules and signs of	
2T13:27:19:20	CIICC		Thing process, then modules and signs of	
2113:27:19:93 2T13:27:20:13	inied	ction	nya C\Windows\system33\system33\system33\systeman.exe C\Usars\BOB\AnnData\Local\GCE2KN54\xBe6RSIM.exe C\Usar	e\R/
2T13:27:20:13	7 0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\User	s\B(
2T13:27:20 20	106	-MD	-Premium Systeinternals Sysmon ID 8 &	s\B(
2T13:27:20:20	0 0xaa4	0xc38	C:\Windows\system32\Gysprev.sysprep.exe C:\Users\BOB\AppDataYocal\GCEXKN54\xBe6RSIM.exe C:\User	s\B(
2T13:27:20:24	⁵10/ªι	ising	WinRM and ARTHIR. Memory dump	
2T13:27:20:24	6 nya	n/a C	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6K5IM.2xeC:\Users\BOB\AppData\Local\Temp\9.exe 3	
2113:27:20:24	with	Vol	atility are possible options	
2T13:27:20:30	9 0x6b0	0xa30	ping 1.3.1.2 - n 1	
2T13:27:20:34	0n/a	n/a	n/a	
2713	DG-/	ND.	MalwareArchaeology.com	
2T13:27:23:87	Discover it	n/a	n/a Archaeology	E

	v or_Proc v	w_Proce*	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\L20SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 - n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 - n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BI
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	
2713	JG-N	D/a	MalwareArchaeology.com
2T13:27:23:87D	iscover it	n/a	n/a

	• or_Proc •	w_Proce *	Process_Command_Line/CommandLine
2113:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a Conclusion
2T13:26:58:02	n/a	n/a	C:\Windows\system2, indicate, C\Unit 2CB, pData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34 2T13:26:58:751	Crea	ite a	PROcess to look at running processes
(T13:26:59:391 (T13:26:59:391	and	thei	rmodules
T13:27:01:902 T13:27:01:902	n/a n/a	n/a n/a	n/a n/a
2T13:27:0●804 2T13:27:17:922	Look	< for	signs of injection
2T13:27:17:922 2T13:27:1●922	Log	the	process command line execution
T13:27:17:922	0x6b0	n/a 0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:10201	Mor	nitor	for the executions discussed in this
2113:27:20:137	pres	enta	Chivindows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB
T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
T13:27:20:340	n/a	n/a	n/a
2113	JG-A	AD/a	MalwareArchaeology.com
T13:27:23:87D	iscover it	n/a	n/a Archaeology

		-	
	* or_Proc *	w_Proce *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:57:924	l n/a	n/a	ome tools to consider
2T13:26:58:02	n/a	n/s	
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a moder	n/a
2T13:26:5P1P	aselet	пе кі	IOW OIX drig Others AppData Local Temp 14323".v" bs
2113:26:58:34	0x660	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2113:20:58:751 2T13:26:50:391	IOG-M	D-Pro	mium 1.1-0.4
2T13:26:59:391	0x6b0	0xd74	
2T13:27:01:902	– Run	ining F	rocess and Modules, Injection, and B9 static file analysis
2T13:27:01:902	Volatili	ty n/a	n/a
2T13:27:04:804	- httr	s://w	ww.volatilityfoundation.org/
2T13:27:17:922		lowEin	d Dlugin (M(in 10 compatible?)
2T13:27:17:922		IOWFII	
2713:27:17:922	2 n/a •	https:/	/github.com/monnappa22/HollowFind
2113:27:17:92	PESieve	e (Ope	ensource)
2T13:27:19:201	– httr	s://gi	thub.com/hasherezade/ne-sieve
2T13:27:19:934	i n/a	n/a	
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:131	Get-Inj	ected	Thread.ps:1em32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\B
2T13:27:20:200	– http	s://gist	.github.com/jaredcatkinson/23905d34537ce4b5b1818c3e6405c1d2
2T13:27:20:200	PSRofle		C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Locai\GCE2KN54\xBe6RSIM.exe C:\Users\B
2113:27:20:240	IJICHE		
2113:27:20:240	– http	os://gi	thub.com/mattifestation/PSReflect
2T13:27:20:20	n/a	n/a	ning 1.3.1.2 - n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a_	n/a	n/a
2713	DG-N	D/a	MalwareArchaeology.com
2T13:27:23:87	iscover it	n/a	n/a Archaeology

	v or Proc v	Proce *	Process_Command_Line/CommandLine
T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
113:26:57:924	n/a	n/a	ama table to consider
113:26:58:02	n/a	n/a	
T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
T13:26:58:112	n/a	n/a	n/a
T13:26:5P3	ease le	et m	e know of any others have been a second
113:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
113:26:58:751	n/a	n/a	nya
T13:20:39:391		nya 0vd74	ping 2.2.1.1-114
T13-20-3-521	GKK	n/a	p/ig 2.2.1.1-114
T13:27:01:902	nb++	ncill	aithub com/google/grr
T13:27:04:804		<u>ps.//</u>	<u>gittiub.com/google/git</u>
T13:27:1 - 922	Rekal	n/a	n/a
T13:27:17:922	n/a	n/a	n/a
113:27:17:922	- htt	p://v	www.rekall-forensic.com/home
T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\' 9.exe
113:27:16:922	InVte	ro ^{c10}	C:\Users\BOB\AppData\Local\Temp\"9.exe
(113:27:19:201	n/a	n/a	nya (-ithe she serve (Chan a sk2 (inc) (the sec se a t
(113)27(15)534 (T15)37(30)157	<u>– ntt</u>	ps://	<u>github.com/Shanek2/Invtero.net</u>
T13:27:20:137	htt	nc·//	github) com/seancomeau/in/teroanet.ccextn54\vBe6RSIM.exe.clusers\
T13:27:20:200	n/a	<u> </u>	C:\Windows\system32\system22\system22\system22\system22\system22\system22\system32\s
T13:27:20:200	Mem	Hun	ter (Old: requires NET 3.5) AppData\Local\GCE2KN54\xBe6RSIM.exe C:\Users\
T13:27:20:246	n/a	n/a	n/a
113:27:20:246	<u> </u>	ps://	github.com/marcosd4h/memhunterpData\Local\Temp\9.exe 3
T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
113:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
113:27:20:340		n/a	
113-1-21-2		/8	MalwareArchaeology.com

MalwareArchaeology.com

2T13:27:23:87Discover.it

n/a

n/a

Archaeology

	• or Proc •	w_Proci *	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ05N7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	
2T13:26:58:02	n/a	n/a	C:\Windows\system 32,twi
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	Red C	anar	ysePresentationppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751 2T13:26:59:391	— AT	Г&СК	Deep Dive: Process Injection
2T13:26:59:391 2T13:27:01:902	Article	e on	MITRE ATT&CK Sub-Techniques (coming soon)
2T13:27:01:902	– htt	ps://r	medium.com/mitre-attack/attack-sub-techniques-
2T13:27:04:804	pre	eview	-b79ff0ba669a
2T13:27:17:922 2T13:27:17:922	Deepl	nstir	nct - Process Injection and Manipulation
2T13:27:17:922	– htt	ps://\	www.deepinstinct.com/2019/09/15/malware-evasion-
2T13:27:19:201	tec	hniqu	ues-part-1-process-injection-and-manipulation/
2T13:27:19:934 2T13:27:20:137	EndGa	ame	
2T13:27:20:137	- htt	ps://v	www.slideshare.net/JoeDesimone4/taking-hunting-to-
2T13:27:20:200	oxthe	e-next	-level-hunting-in-memory Users BOB AppData Local GCEzKN54 & Bef SIM.exe C: Users BOB
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	i n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2713	JG-N	D/a	Malware *
2T13:27:23:87D	iscover it	n/a	n/a Archaeology

Kesources Websites - Log-MD.com The tool **ARTHIR.com** Free on GitHub The "Windows Logging Cheat Sheet(s)" MalwareArchaeology.com This presentation and others on SlideShare Search for MalwareArchaeology or LOG-MD ЛD Malwar

Questions? You can find us at: Log-MD.com **@HackerHurricane** MalwareArchaeology.com OG-MD Malware LOG-MD.COM Archaeology **Discover it**