Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Query Registry *Discovery* (T1012)	12.E.1.7	Empire: WinEnum module included enumeration of system information via a Registry query	None	0	None	0	Telemetry	10	None	0	None	0	None	0	None	0
	13.C.1	Empire: 'reg query' via PowerShell to enumerate a specific Registry key	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed-Tainted General Behavior-Delayed	70	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	2.H.1	Cobalt Strike: 'reg query' via cmd to enumerate a specific Registry key	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	17.A.1	Empire: 'reg query' via PowerShell to enumerate a specific Registry key	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	6.A.1	Cobalt Strike: 'reg query' via cmd to remotely enumerate a specific Registry key on Conficker (10.0.0.5)	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed-Tainted	45	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
	2.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.A.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.D.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.D.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.E.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0

	2.E.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
Command-Line Interface *Execution* (T1059)	16.F.1	Empire: Built-in runas module executed to launch malicious VBScript (autoupdate.vbs) as user Kmitnick	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted	15	Enrichment-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	50	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	2.F.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.F.3		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.C.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.G.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.G.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.F.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	7.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	8.A.1		None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	8.A.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.H.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	4.A.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	6.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	4.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	4.B.1		None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	4.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
	12.D.1	Empire: 'net start' via PowerShell	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	17.A.1	Empire: 'reg query' via PowerShell to enumerate a specific Registry key associated with terminal services	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	16.J.1	Empire: 'sc qc' via PowerShell to remotely enumerate a specific service on Creeper (10.0.0.4)	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

System Service Discovery *Discovery* (T1007)	2.D.2	Cobalt Strike: 'net start' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	2.D.1	Cobalt Strike: 'sc query' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	12.E.1.8	Empire: WinEnum module included enumeration of services	None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	16.H.1	Empire: 'sc query' via PowerShell to remotely enumerate services on Creeper (10.0.0.4)	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
File Permissions Modification *Defense Evasion* (T1222)	17.B.1	Empire: 'takeown' via PowerShell to obtain ownership of magnify.exe	Telemetry Enrichment-Configuration Change	20	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Enrichment-Tainted	20
	17.B.2	Empire: 'icacls' via PowerShell to modify the DACL for magnify.exe	Telemetry Enrichment-Configuration Change	20	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
	19.A.1	Empire: File dropped to disk is a renamed copy of the WinRAR binary	Telemetry	10	None	0	Telemetry	10	None	0	Telemetry	10	None	0	Telemetry-Tainted	15
	16.I.1	Empire: 'sc description' via PowerShell to remotely disguise a service on Creeper (10.0.0.4)	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

Masquerading *Defense Evasion* (T1036)	19.B.1	Empire: Executed binary (recycler.exe) is a renamed copy of the WinRAR binary	Telemetry Specific Behavior	70	Enrichment-Tainted-Configuration Change Telemetry-Tainted	30	Specific Behavior-Tainted Telemetry Specific Behavior-Delayed	130	Specific Behavior-Tainted Telemetry-Tainted	80	Telemetry-Tainted	15	Telemetry	10	Enrichment-Tainted	20
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Service Execution *Execution* (T1035)	16.L.1	Empire: 'sc start' via PowerShell to remotely launch a specific service on Creeper (10.0.0.4)	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry-Tainted Enrichment-Delayed-Tainted Specific Behavior	90	Telemetry-Tainted Specific Behavior	75	Telemetry	10	Telemetry-Tainted General Behavior	45
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
System Owner/User Discovery *Discovery* (T1033)	2.B.1	Cobalt Strike: 'echo' via cmd to enumerate specific environment variables	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	20.B.1	Executed 'whoami' via cmd persistence mechanism through RDP connection made to Creeper (10.0.0.4)	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted	15	Telemetry	10	Enrichment	15
	12.B.1	Empire: 'whoami /all /fo list' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	General Behavior-Delayed-Tainted Telemetry General Behavior-Delayed	65	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

	12.E.1.1	Empire: WinEnum module included enumeration of user information	None	0	None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne		
Standard Cryptographic Protocol *Command and Control* (T1032)	11.B.1	Empire: Encrypted C2 channel established using HTTPS	Telemetry	10	None	0	None	0	Telemetry-Tainted	15	Telemetry-Tainted	15	None	0	None	0	
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne		
Password Policy Discovery *Discovery* (T1201)	12.E.1.3	Empire: WinEnum module included enumeration of password policy information	None	0	None	0	None	0	None	0	None	0	None	0	None	0	
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne		
	12.A.2	Empire: 'ipconfig /all' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15	
	4.B.1	Cobalt Strike: 'netsh advfirewall show allprofiles' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	General Behavior-Delayed Telemetry General Behavior-Delayed	60	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15	
	12.A.1	Empire: 'route print' via PowerShell	Telemetry	10	Enrichment-Tainted	20	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15	
System Network Configuration Discovery																	

Discovery (T1016)	2.A.2	Cobalt Strike: 'arp -a' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	2.A.1	Cobalt Strike: 'ipconfig /all' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	General Behavior-Tainted Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	75	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	12.E.1.11	Empire: WinEnum module included enumeration of network adapters	None	0	None	0	None	0	None	0	Telemetry	10	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
User Execution *Execution* (T1204)	1.A.1	Legitimate user Debbie clicked and executed malicious self-extracting archive (Resume Viewer.exe) on 10.0.1.6 (Nimda)	Telemetry General Behavior	40	Telemetry-Tainted	15	General Behavior Telemetry	40	General Behavior Telemetry-Tainted	45	Telemetry	10	Telemetry	10	Telemetry General Behavior	40
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Data from Network Shared Drive *collection* (T1039)	18.B.1	Empire: 'copy' via PowerShell collected a file (Shockwave_network.vsdx) from a network shared drive (Wormshare) on Conficker (10.0.0.5)	None	0	Telemetry-Tainted	15	None	0	None	0	None	0	None	0	Telemetry-Tainted	15
	9.B.1	Cobalt Strike: Built-in download capability executed to a collect file (Shockwave_rackb_diagram.vsdx) from a network shared drive (Wormshare) on Conficker (10.0.0.5)	None	0	None	0	None	0	None	0	None	0	None	0	Telemetry	10
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	

Process Injection *Defense Evasion, Privilege Escalation* ([T1055](T1055))	3.C.1	Cobalt Strike: Built-in process injection capability executed to inject callback into cmd.exe	Telemetry Specific Behavior	70	Specific Behavior-Tainted	65	Specific Behavior-Tainted Telemetry General Behavior-Delayed-Tainted	105	Specific Behavior	60	Enrichment-Tainted Specific Behavior-Delayed	75	Telemetry	10	Telemetry-Tainted	15
	8.D.1	Cobalt Strike: Screen capture capability involved process injection into explorer.exe	Telemetry	10	Telemetry	10	Telemetry	10	Specific Behavior-Tainted	65	Enrichment	15	None	0	Telemetry-Tainted	15
	5.A.1	Cobalt Strike: Credential dump capability involved process injection into lsass	Telemetry	10	General Behavior	30	Enrichment	15	Telemetry	10	Telemetry-Tainted Specific Behavior-Delayed	70	None	0	None	0
	5.A.2	Cobalt Strike: Hash dump capability involved process injection into lsass.exe	Telemetry Specific Behavior	70	Specific Behavior-Tainted General Behavior	95	Enrichment	15	Telemetry-Tainted Specific Behavior	75	Telemetry-Tainted Specific Behavior-Delayed	70	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Remote System	13.A.1	Empire: 'net group "Domain Computers" /domain' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted Enrichment-Tainted General Behavior-Delayed	60	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15

Discovery *Discovery* (T1018)	4.A.1	Cobalt Strike: 'net group "Domain Controllers" /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Enrichment Telemetry General Behavior-Delayed General Behavior-Delayed	75	Telemetry Enrichment-Delayed	20	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	4.A.2	Cobalt Strike: 'net group "Domain Computers" /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Enrichment Telemetry General Behavior-Delayed General Behavior-Delayed	75	Telemetry Enrichment-Delayed	20	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Standard Application Layer Protocol *Command and Control* (T1071)	6.B.1	Cobalt Strike: C2 channel modified to use HTTP traffic to freegoogleadsenseinfo.com	Telemetry	10	Telemetry	10	None	0	None	0	None	0	None	0	None	0
	1.C.1	Cobalt Strike: C2 channel established using DNS traffic to freegoogleadsenseinfo.com	None	0	Telemetry	10	Specific Behavior General Behavior-Delayed Telemetry Specific Behavior-Delayed	150	Telemetry-Tainted	15	Telemetry-Configuration Change	5	None	0	Telemetry-Tainted	15
	14.A.1	Empire: UAC bypass module downloaded a new Empire stager (wdbypass) over HTTP	None	0	Telemetry-Tainted	15	None	0	Telemetry	10	Telemetry-Tainted	15	None	0	None	0

	11.B.1	Empire: C2 channel established using HTTPS traffic to freegoogleadsenseinfo.com	Telemetry	10	None	0	None	0	Telemetry-Tainted	15	Telemetry-Tainted Indicator of Compromise-Configuration Change	30	Telemetry	10	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Network Share Discovery *Discovery* (T1135)	12.E.1.9.2	Empire: WinEnum module included enumeration of mapped network drives	None	0	None	0	None	0	None	0	None	0	None	0	Telemetry-Tainted	15
	12.E.1.9.1	Empire: WinEnum module included enumeration of available shares	None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Data Encoding *Command and Control* (T1132)	1.C.1	Cobalt Strike: C2 channel established using both NetBIOS and base64 encoding	None	0	None	0	Telemetry-Tainted	15	None	0	None	0	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Remote Desktop Protocol *Lateral Movement* (T1076)	20.A.1	RDP connection made to Creeper (10.0.0.4) as part of execution of persistence mechanism	None	0	Telemetry	10	Telemetry	10	Telemetry	10	Telemetry	10	None	0	None	0
	6.C.1	Cobalt Strike: C2 channel modified to proxy RDP connection to Conficker (10.0.0.5)	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change Telemetry	25	Telemetry General Behavior-Delayed	35	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry-Tainted	15
	10.B.1	RDP connection made to Conficker (10.0.0.5) as part of execution of persistence mechanism	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry	10	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Scheduled Task	10.A.2	Scheduled task executed when user Debbie logs on to Nimda (10.0.1.6), launching a DLL payload (updater.dll) using Rundll32	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry	10

Execution, Persistence, Privilege Escalation (T1053)	7.C.1	Cobalt Strike: 'schtasks' via cmd to create scheduled task that executes a DLL payload (updater.dll)	Telemetry Specific Behavior	70	Specific Behavior Telemetry	70	Telemetry General Behavior-Delayed-Tainted Specific Behavior-Delayed	95	Enrichment Telemetry-Tainted Enrichment-Delayed-Tainted Specific Behavior-Tainted	110	Telemetry Specific Behavior-Delayed	65	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Data Staged *collection* (T1074)	18.B.1	Empire: 'copy' via PowerShell staged a file (Shockwave_network.vsdx) from a network shared drive (Wormshare) on Conficker (10.0.0.5) in the Recycle Bin (C:\$Recycle.Bin) on CodeRed (10.0.1.5)	Telemetry Specific Behavior	70	Telemetry-Tainted	15	Telemetry Specific Behavior-Delayed	65	Telemetry-Tainted	15	None	0	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Application Window Discovery *Discovery* (T1010)	8.C.1	Cobalt Strike: Keylogging capability included residual enumeration of application windows	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	15.A.1	Empire: Built-in keylogging module included residual enumeration of application windows	None	0	None	0	Telemetry	10	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Valid Accounts *Defense Evasion, Persistence, Privilege Escalation, Initial Access* (T1078)	16.B.1	Empire: 'net use' via PowerShell to successfully authenticate to Conficker (10.0.0.5) using credentials of user Kmitnick	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed-Tainted	45	Enrichment-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	50	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	10.B.1	RDP connection to Conficker (10.0.0.5) authenticated using previously added user Jesse	Telemetry Enrichment	25	Telemetry	10	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry	10

	16.D.1	Empire: 'net use' via PowerShell to successfully authenticate to Creeper (10.0.0.4) using credentials of user Kmitnick	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Enrichment-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	50	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Brute Force *Credential Access* (T1110)	16.B.1	Empire: Successful authentication to Conficker (10.0.0.5) using credentials of user Kmitnick as a result of the brute force password spraying	Telemetry Enrichment-Configuration Change	20	Enrichment-Tainted Telemetry-Tainted	35	Telemetry-Tainted General Behavior-Delayed-Tainted General Behavior-Delayed	70	Enrichment-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	50	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry	10	Telemetry-Tainted	15
	16.A.1	Empire: 'net use' via PowerShell to brute force password spraying authentication attempts to Morris (10.0.1.4) and Nimda (10.0.1.6) targeting credentials of users Kmitnick, Bob, and Frieda	Telemetry Enrichment-Configuration Change	20	Enrichment-Tainted	20	Telemetry General Behavior-Delayed-Tainted General Behavior-Delayed	65	Enrichment-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	50	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Screen Capture *Collection* (T1113)	8.D.1	Cobalt Strike: Built-in screen capture capability executed to capture screenshot of current window of user Debbie	None	0	None	0	None	0	None	0	Enrichment-Configuration Change	10	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Create Account *Persistence* (T1136)	7.A.1	Added user Jesse to Conficker (10.0.0.5) through RDP connection	Telemetry Enrichment-Configuration Change	20	Specific Behavior-Configuration Change	55	Telemetry	10	None	0	Telemetry-Configuration Change	5	None	0	Telemetry	10
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	

System Information Discovery *Discovery* (T1082)	2.E.2	Cobalt Strike: 'net config workstation' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	2.E.1	Cobalt Strike: 'systeminfo' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed General Behavior-Delayed	65	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	12.E.1.6.1	Empire: WinEnum module included enumeration of system information	None	0	None	0	Telemetry	10	None	0	Telemetry	10	None	0	Telemetry-Tainted	15
	12.E.1.6.2	Empire: WinEnum module included enumeration of Windows update information	None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
File and Directory Discovery *Discovery* (T1083)	18.A.1	Empire: 'Get-ChildItem' via PowerShell to enumerate a network shared drive (Wormshare) on Conficker (10.0.0.5)	None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	8.A.1	Cobalt Strike: 'dir /s /b "\\conficker\wormshare"' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	8.A.2	Cobalt Strike: 'tree "C:\Users\debbie"' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed-Tainted General Behavior-Delayed	70	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

	12.E.1.4.2	Empire: WinEnum module included enumeration of interesting files	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.E.1.4.1	Empire: WinEnum module included enumeration of recently opened files	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	9.A.1	Cobalt Strike: 'ls' (List) via Win32 APIs to enumerate a network shared drive (Wormshare) on Conficker (10.0.0.5)	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	16.K.1	Empire: 'type' via PowerShell to remotely enumerate a specific file (update.vbs) on Creeper (10.0.0.4)	None	0	None	0	None	0	None	0	None	0	None	0	Telemetry	10
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Credentials in Files *Credential Access* (T1081)	15.B.1	Empire: 'get-content' via PowerShell to collect sensitive file (it_tasks.txt) from a network shared drive (Wormshare) on Conficker (10.0.0.5)	None	0	None	0	Telemetry Specific Behavior-Delayed	65	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
PowerShell *Execution* (T1086)	13.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.F.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	17.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	17.B.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.F.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	17.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.G.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.G.2		None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	12.D.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	18.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.E.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	18.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	17.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	16.K.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	11.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	16.H.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.A.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	19.D.1		None	0	None	0	None	0	None	0	Telemetry	10	None	0	None	0
	19.D.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0

	16.I.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	16.J.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	15.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	13.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	13.B.2		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	13.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	16.L.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Account Discovery *Discovery* (T1087)	2.G.2	Cobalt Strike: 'net user george /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	12.G.1	Empire: 'net user' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted	20	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	12.G.2	Empire: 'net user /domain' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted	20	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted General Behavior-Delayed Specific Behavior-Delayed	95	Telemetry	10	Telemetry-Tainted	15
	7.A.1	Microsoft Management Console (Local Users and Groups snap-in) GUI utility displayed user account information	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry	10	None	0	None	0

	2.G.1	Cobalt Strike: 'net user /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted	20	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15

Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Rundll32 *Defense Evasion, Execution* (T1085)	1.A.1	Previously executed batch file (pdfhelper.cmd) launched a DLL payload (update.dat) using Rundll32	Telemetry Enrichment	25	Telemetry-Tainted	15	Specific Behavior General Behavior-Delayed Telemetry	95	Telemetry-Tainted Specific Behavior-Tainted	80	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15

Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
System Network Connections Discovery *Discovery* (T1049)	12.E.1.12	Empire: WinEnum module included enumeration of established network connections	Telemetry Enrichment	25	None	0	Telemetry-Tainted	15	Telemetry-Tainted Enrichment-Tainted-Delayed	30	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	13.B.1	Empire: 'net use' via PowerShell	Enrichment Telemetry	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	13.B.2	Empire: 'netstat -ano' via PowerShell	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Delayed-Tainted	30	Telemetry-Tainted General Behavior-Delayed	40	None	0	Telemetry-Tainted	15

	4.C.1	Cobalt Strike: 'netstat -ano' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	General Behavior-Delayed Telemetry General Behavior-Delayed	60	Telemetry Enrichment-Delayed	20	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Bypass User Account Control *Defense Evasion, Privilege Escalation* (T1088)	3.A.1	Cobalt Strike: Built-in UAC bypass token duplication capability executed to elevate process integrity level	None	0	None	0	Telemetry	10	Telemetry	10	Telemetry-Tainted	15	None	0	Telemetry	10
	14.A.1	Empire: Built-in UAC bypass token duplication module executed to launch new callback with elevated process integrity level	None	0	None	0	Telemetry Specific Behavior-Delayed	65	Telemetry	10	Telemetry-Tainted	15	None	0	Telemetry-Tainted	15

Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Process Discovery *Discovery* (T1057)	2.C.1	Cobalt Strike: 'ps' (Process status) via Win32 APIs	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.C.2	Cobalt Strike: 'tasklist /v' via cmd	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted General Behavior-Configuration Change-Delayed-Tainted	40	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	3.B.1	Cobalt Strike: 'ps' (Process status) via Win32 APIs	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	8.B.1	Cobalt Strike: 'ps' (Process status) via Win32 APIs	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.C.1	Empire: 'qprocess *' via PowerShell	Telemetry Enrichment	25	Telemetry-Tainted	15	General Behavior-Delayed-Tainted Telemetry General Behavior-Delayed	65	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15

Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Data Encrypted *Exfiltration* (T1022)	19.B.1	Empire: Executed binary (recycler.exe) created encrypted archive (old.rar) of previously collected file	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change Telemetry-Tainted	30	Specific Behavior-Tainted Telemetry Specific Behavior-Delayed	130	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Input Capture *collection, Credential Access* (T1056)	8.C.1	Cobalt Strike: Built-in keylogging capability executed to capture keystrokes of user Debbie	None	0	None	0	None	0	None	0	Telemetry-Configuration Change Specific Behavior-Delayed	60	None	0	Telemetry-Tainted	15
	15.A.1	Empire: Built-in keylogging module executed to capture keystrokes of user Bob	Telemetry Enrichment	25	None	0	Telemetry General Behavior-Delayed	35	None	0	Telemetry-Tainted Specific Behavior-Delayed	70	None	0	Enrichment-Tainted	20
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Multiband Communication *Command and Control* (T1026)	6.B.1	Cobalt Strike: C2 channel modified to split communications between both HTTP and DNS	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
	16.B.1	Empire: Successful authentication targeted Windows admin share on Conficker (10.0.0.5)	Telemetry Specific Behavior	70	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed-Tainted General Behavior-Delayed	70	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry	10	Telemetry-Tainted	15

Windows Admin Shares *Lateral Movement* (T1077)	16.D.1	Empire: Successful authentication targeted Windows admin shares on Conficker (10.0.0.5)	Telemetry Specific Behavior	70	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	16.A.1	Empire: Brute force password spraying attempts targeted Windows admin shares on Morris (10.0.1.4) and Nimda (10.0.1.6)	Telemetry Specific Behavior	70	Enrichment-Tainted	20	Telemetry General Behavior-Delayed-Tainted General Behavior-Delayed	65	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted Specific Behavior-Delayed	70	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Clipboard Data *collection* (T1115)	12.E.1.5	Empire: WinEnum module included enumeration of clipboard contents	None	0	None	0	None	0	Telemetry-Tainted	15	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
New Service *Persistence, Privilege Escalation* (T1050)	16.I.1	Empire: 'sc create' via PowerShell to remotely create a service on Creeper (10.0.0.4)	Telemetry Specific Behavior	70	Telemetry-Tainted Specific Behavior-Configuration Change	70	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Delayed-Tainted Specific Behavior	90	Telemetry-Tainted Specific Behavior	75	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
	12.E.1.2	Empire: WinEnum module included enumeration of AD group memberships	None	0	None	0	None	0	None	0	None	0	None	0	None	0

Permission Groups Discovery *Discovery* (T1069)	12.F.1	Empire: 'net group "Domain Admins" /domain' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted Enrichment-Tainted General Behavior-Delayed	60	Telemetry-Tainted Enrichment-Tainted-Delayed Enrichment-Tainted	50	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	12.F.2	Empire: 'net localgroup administrators' via PowerShell	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Tainted-Delayed Enrichment-Tainted	50	Telemetry-Tainted General Behavior-Delayed	40	Telemetry	10	Telemetry-Tainted	15
	2.F.1	Cobalt Strike: 'net localgroup administrators' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed General Behavior-Delayed	65	Telemetry-Tainted Enrichment-Tainted General Behavior-Configuration Change-Delayed-Tainted	60	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
	2.F.3	Cobalt Strike: 'net group "Domain Admins" /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Enrichment-Tainted Telemetry-Tainted General Behavior-Delayed	60	Telemetry-Tainted Enrichment-Tainted General Behavior-Configuration Change-Delayed-Tainted	60	Telemetry General Behavior-Delayed	35	Telemetry Enrichment	25	Telemetry-Tainted	15

	2.F.2	Cobalt Strike: 'net localgroup administrators /domain' via cmd	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted Enrichment-Tainted General Behavior-Configuration Change-Delayed-Tainted	60	Telemetry General Behavior-Delayed	35	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
File Deletion *Defense Evasion* (T1107)	19.D.1	Empire: 'del C:\"$"Recycle.bin\old.rar'	Telemetry	10	Telemetry-Tainted	15	Telemetry Specific Behavior-Delayed	65	None	0	None	0	None	0	Telemetry-Tainted	15
	19.D.2	Empire: 'del recycler.exe'	Telemetry	10	Telemetry-Tainted	15	Telemetry Specific Behavior-Delayed	65	Telemetry	10	None	0	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Execution through API *Execution* (T1106)	8.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	3.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	8.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	9.B.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	8.D.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	9.A.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	2.C.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.E.1		None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Remote File Copy	19.A.1	Empire: Built-in upload module executed to write binary (recycler.exe) to disk on CodeRed (10.0.1.5)	Telemetry	10	General Behavior-Configuration Change Telemetry-Tainted	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	7.B.1	Cobalt Strike: Built-in upload capability executed to write a DLL payload (updater.dll) to disk on Nimda (10.0.1.6)	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry-Tainted	15

Command and Control, Lateral Movement (T1105)	16.E.1	Empire: Built-in upload module executed to write malicious VBScript (autoupdate.vbs) to disk on CodeRed (10.0.1.5)	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	14.A.1	Empire: UAC bypass module downloaded and wrote a new Empire stager (wdbypass) to disk	Telemetry	10	Telemetry-Tainted	15	Specific Behavior-Delayed	55	Telemetry	10	Telemetry-Tainted	15	None	0	None	0
	16.G.1	Empire: Built-in move capability executed to write malicious VBScript (update.vbs) to disk on Creeper (10.0.0.4)	Telemetry	10	Enrichment-Tainted-Configuration Change	15	Telemetry	10	Telemetry	10	Telemetry-Tainted	15	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Access Token Manipulation *Defense Evasion, Privilege Escalation* (T1134)	3.A.1	Cobalt Strike: Built-in UAC bypass token duplication capability executed to modify current process token	Telemetry	10	None	0	None	0	Telemetry	10	Telemetry-Tainted	15	None	0	None	0
	5.B.1	Cobalt Strike: Built-in token theft capability executed to change user context to George	Telemetry	10	None	0	Telemetry	10	Specific Behavior Telemetry-Tainted	75	Telemetry-Tainted	15	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Scripting *Defense Evasion, Execution* (T1064)	1.A.1	Previously executed self-extracting archive (Resume Viewer.exe) launched an embedded batch file (pdfhelper.cmd)	Telemetry Enrichment	25	Telemetry-Tainted	15	General Behavior-Delayed Telemetry	35	Telemetry-Tainted	15	Telemetry	10	None	0	Telemetry-Tainted	15
	11.A.1	Legitimate user Bob clicked and executed malicious VBScript (autoupdate.vbs) on 10.0.1.5 (CodeRed)	Enrichment Telemetry Specific Behavior Specific Behavior	145	Telemetry-Tainted	15	Specific Behavior General Behavior-Delayed Telemetry Specific Behavior-Delayed	150	Specific Behavior Telemetry-Tainted Specific Behavior	135	Telemetry Specific Behavior Specific Behavior-Delayed Specific Behavior	185	Telemetry	10	Telemetry General Behavior	40

	12.E.1	Empire: Built-in WinEnum module executed to programmatically execute a series of enumeration techniques	Telemetry	10	Telemetry	10	Telemetry Specific Behavior-Delayed Specific Behavior-Delayed	120	Specific Behavior-Tainted Telemetry-Tainted	80	Telemetry-Tainted Specific Behavior	75	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Credential Dumping *Credential Access* (T1003)	5.A.1	Cobalt Strike: Built-in Mimikatz credential dump capability executed	Telemetry Specific Behavior	70	None	0	Specific Behavior-Tainted Telemetry General Behavior-Delayed-Tainted	105	Specific Behavior	60	Enrichment-Tainted Specific Behavior-Delayed	75	None	0	None	0
	5.A.2	Cobalt Strike: Built-in hash dump capability executed	Telemetry	10	Telemetry-Tainted	15	Specific Behavior-Tainted Specific Behavior-Tainted Telemetry General Behavior-Delayed-Tainted	170	Specific Behavior	60	Enrichment-Tainted	20	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Exfiltration Over Command and Control Channel *Exfiltration* (T1041)	9.B.1	Cobalt Strike: Download capability exfiltrated data through existing C2 channel	None	0	None	0	None	0	None	0	None	0	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	

Registry Run Keys / Startup Folder *Persistence* (T1060)	10.A.1	Batch file (autoupdate.bat) previously written to Startup folder executed when user Debbie logs on to Nimda (10.0.1.6), launching a DLL payload (update.dat) using Rundll32	Telemetry	10	Telemetry	10	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry	10
	1.B.1	Previously executed batch file (pdfhelper.cmd) moved a separate batch file (autoupdate.bat) to the Startup folder	Telemetry Enrichment	25	Telemetry	10	Telemetry	10	Telemetry-Tainted Specific Behavior-Tainted	80	Telemetry	10	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Graphical User Interface *Execution* (T1061)	7.A.1	Microsoft Management Console (Local Users and Groups snap-in) GUI utility used to add new user through RDP connection	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	Telemetry	10	Telemetry	10	None	0	None	0
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Exfiltration Over Alternative Protocol *Exfiltration* (T1048)	19.C.1	Empire: Sequence of 'echo' commands via PowerShell to populate commands in text file (ftp.txt), which is then executed by FTP to exfil data through network connection separate of existing C2 channel	Telemetry Enrichment	25	Telemetry-Tainted	15	General Behavior-Delayed-Tainted Telemetry Specific Behavior-Delayed	95	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Security Software Discovery *Discovery* (T1063)	12.E.1.10.2	Empire: WinEnum module included enumeration of firewall rules	None	0	None	0	None	0	None	0	None	0	None	0	None	0
	12.E.1.10.1	Empire: WinEnum module included enumeration of AV solutions	None	0	None	0	None	0	None	0	None	0	None	0	Enrichment-Tainted Telemetry-Tainted	35
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	

Data Compressed *Exfiltration* (T1002)	19.B.1	Empire: Executed binary (recycler.exe) created compressed archive (old.rar) of previously collected file	Telemetry Enrichment	25	Enrichment-Tainted-Configuration Change Telemetry-Tainted	30	Specific Behavior-Tainted Telemetry Specific Behavior-Delayed	130	Specific Behavior-Tainted Telemetry-Tainted Enrichment-Delayed-Tainted	95	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Network Share Connection Removal *Defense Evasion* (T1126)	16.C.1	Empire: 'net use /delete' via PowerShell	Telemetry Specific Behavior	70	Telemetry-Tainted	15	Telemetry-Tainted General Behavior-Delayed	40	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Commonly Used Port *Command and Control* (T1043)	6.B.1	Cobalt Strike: C2 channel modified to use port 80	Telemetry Enrichment	25	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	1.C.1	Cobalt Strike: C2 channel established using port 53	Telemetry	10	None	0	None	0	None	0	None	0	None	0	None	0
	14.A.1	Empire: UAC bypass module downloaded a new Empire stager (wdbypass) over port 8080	Telemetry	10	Telemetry-Tainted	15	Telemetry	10	General Behavior Telemetry	40	Telemetry-Tainted	15	Telemetry	10	Telemetry-Tainted	15
	11.B.1	Empire: C2 channel established using port 443	Enrichment Telemetry	25	Telemetry	10	Telemetry-Tainted	15	Telemetry-Tainted Specific Behavior-Tainted	80	Telemetry-Tainted	15	None	0	Telemetry-Tainted	15
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
Accessibility Features *Persistence,*	17.C.1	Empire: 'copy' via PowerShell to overwrite magnify.exe with cmd.exe	Telemetry Specific Behavior	70	Enrichment-Tainted-Configuration Change Telemetry-Tainted	30	Telemetry-Tainted	15	Specific Behavior Telemetry-Tainted Enrichment-Delayed-Tainted	90	Telemetry Specific Behavior	70	Telemetry	10	Telemetry-Tainted	15

Privilege Escalation (T1015)	20.A.1	magnifer.exe previously overwritten by cmd.exe launched through RDP connection made to Creeper (10.0.0.4)	Telemetry Specific Behavior General Behavior General Behavior	130	Telemetry-Tainted	15	Specific Behavior Telemetry General Behavior-Delayed	95	Specific Behavior Telemetry-Tainted Enrichment-Delayed-Tainted	90	Telemetry Specific Behavior	70	Telemetry	10	Telemetry	10
Technique	Step	Procedures	CarbonBlack		CounterTack		CrowdStrike		Endgame		Microsoft		RSA		SentinelOne	
TOTAL SCORE			**2800**		**1835**		**4925**		**4045**		**3125**		**775**		**1590**	