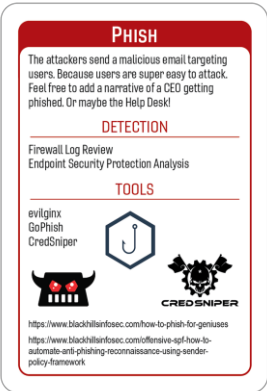


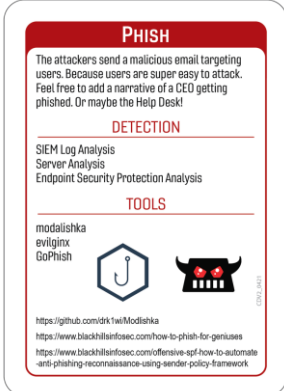


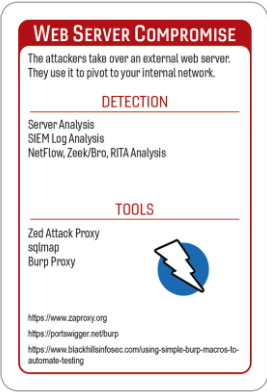

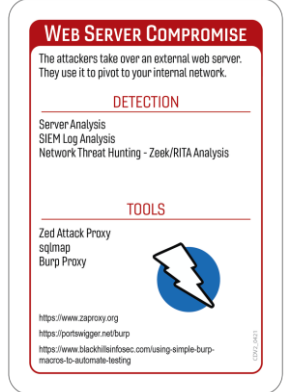

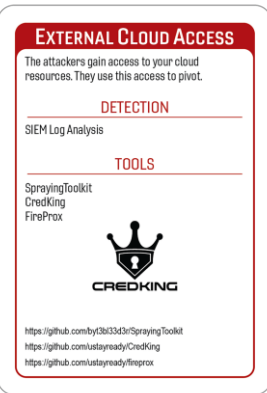

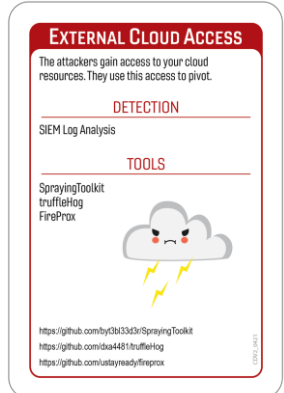

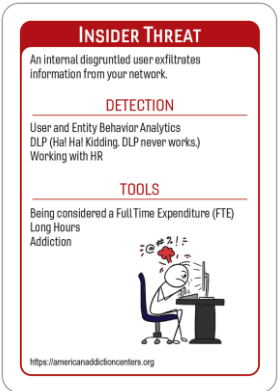

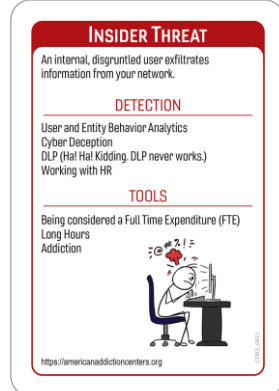


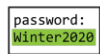
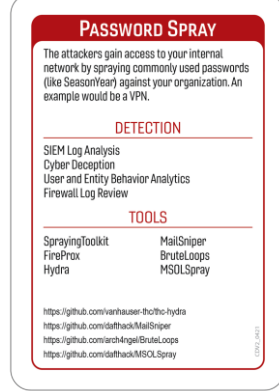
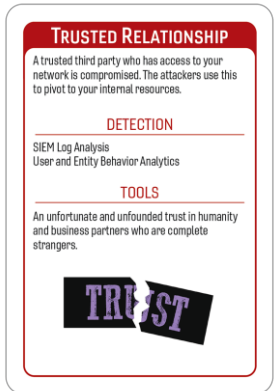

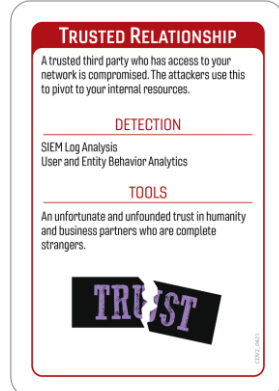

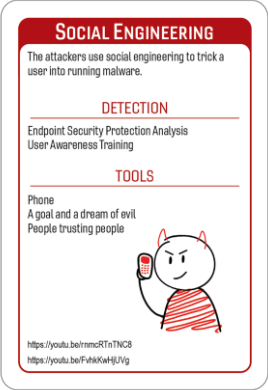


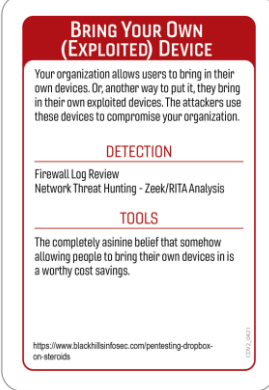

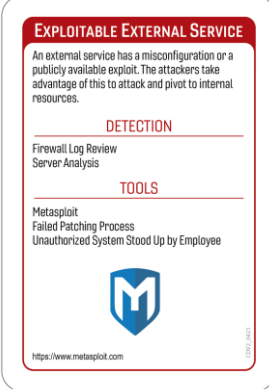

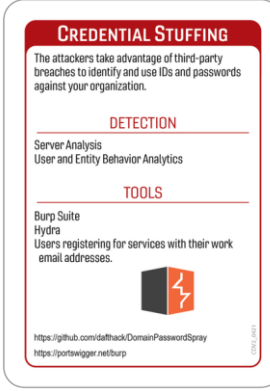

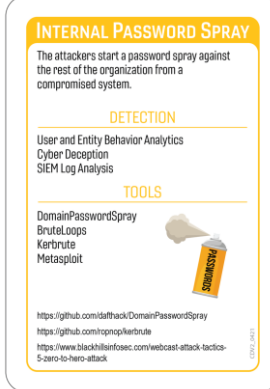

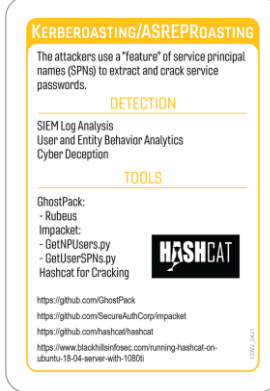


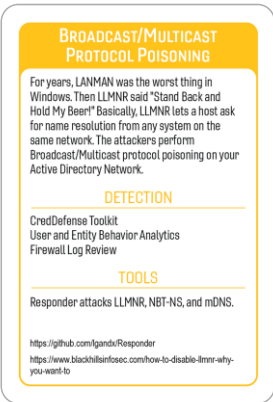
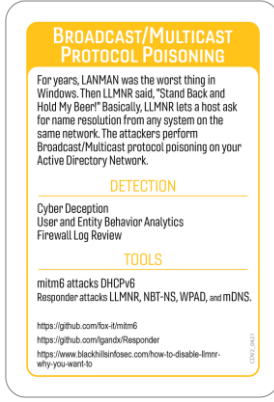
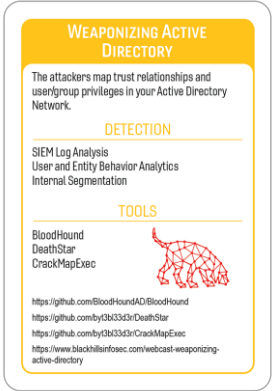
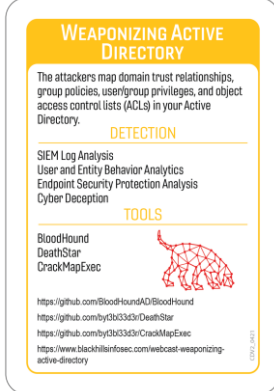
Backdoors & Breaches Change Log - 2021

Card #	Ver 1	Changes	Ver 2
1	 <p>PHISH</p> <p>The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!</p> <p>DETECTION</p> <p>Firewall Log Review Endpoint Security Protection Analysis</p> <p>TOOLS</p> <p>evilginx GoPhish CredSniper</p> <p> </p> <p>CRED SNIPER</p> <p>https://www.blackhillsinfosec.com/how-to-phish-for-geniuses https://www.blackhillsinfosec.com/offensive-spl-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Added "SIEM Log Analysis" Added "Server Analysis" Deleted "Firewall Log Review"</p> <p>Tools: Added "modalishka" Deleted "CredSniper"</p> <p>Graphics: Changed</p> <p>Links: Added https://github.com/drk1wi/Modlishka</p>	 <p>PHISH</p> <p>The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!</p> <p>DETECTION</p> <p>SIEM Log Analysis Server Analysis Endpoint Security Protection Analysis</p> <p>TOOLS</p> <p>modalishka evilginx GoPhish</p> <p> </p> <p>https://github.com/drk1wi/Modlishka https://www.blackhillsinfosec.com/how-to-phish-for-geniuses https://www.blackhillsinfosec.com/offensive-spl-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework</p>
2	 <p>WEB SERVER COMPROMISE</p> <p>The attackers take over an external web server. They use it to pivot to your internal network.</p> <p>DETECTION</p> <p>Server Analysis SIEM Log Analysis NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Zed Attack Proxy sqmap Burp Proxy</p> <p></p> <p>https://www.zaproxy.org https://portswigger.net/burp https://www.blackhillsinfosec.com/using-simple-burp-macro-to-automate-testing</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Deleted "NetFlow, Zeek/ Brow"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>WEB SERVER COMPROMISE</p> <p>The attackers take over an external web server. They use it to pivot to your internal network.</p> <p>DETECTION</p> <p>Server Analysis SIEM Log Analysis Network Threat Hunting - Zeek/RITA Analysis</p> <p>TOOLS</p> <p>Zed Attack Proxy sqmap Burp Proxy</p> <p></p> <p>https://www.zaproxy.org https://portswigger.net/burp https://www.blackhillsinfosec.com/using-simple-burp-macro-to-automate-testing</p>
3	 <p>EXTERNAL CLOUD ACCESS</p> <p>The attackers gain access to your cloud resources. They use this access to pivot.</p> <p>DETECTION</p> <p>SIEM Log Analysis</p> <p>TOOLS</p> <p>SprayingToolkit CredKing FireProx</p> <p></p> <p>CRED KING</p> <p>https://github.com/by3k33d3r/SprayingToolkit https://github.com/ustayready/CredKing https://github.com/ustayready/fireprox</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: Changed</p> <p>Links: No Changes</p>	 <p>EXTERNAL CLOUD ACCESS</p> <p>The attackers gain access to your cloud resources. They use this access to pivot.</p> <p>DETECTION</p> <p>SIEM Log Analysis</p> <p>TOOLS</p> <p>SprayingToolkit truffleHog FireProx</p> <p></p> <p>https://github.com/by3k33d3r/SprayingToolkit https://github.com/ide4481/truffleHog https://github.com/ustayready/fireprox</p>

4	 <p>INSIDER THREAT An internal disgruntled user exfiltrates information from your network.</p> <p>DETECTION User and Entity Behavior Analytics DLP (Hal Hal Kidding, DLP never works.) Working with HR</p> <p>TOOLS Being considered a Full Time Expenditure (FTE) Long Hours Addiction</p> <p></p> <p>https://americanaddictioncenters.org</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>INSIDER THREAT An internal, disgruntled user exfiltrates information from your network.</p> <p>DETECTION User and Entity Behavior Analytics Cyber Deception DLP (Hal Hal Kidding, DLP never works.) Working with HR</p> <p>TOOLS Being considered a Full Time Expenditure (FTE) Long Hours Addiction</p> <p></p> <p>https://americanaddictioncenters.org</p>
5	 <p>PASSWORD SPRAY The attackers gain access to your internal network by spraying commonly used passwords (like SeasonYear) against your organization.</p> <p>DETECTION SIEM Log Analysis User and Entity Behavior Analytics Firewall Log Review</p> <p>TOOLS SprayingToolkit FireProx Hydra DomainPasswordSpray</p> <p></p> <p>https://github.com/by3b3333r/SprayingToolkit https://github.com/usatready/fireprox https://github.com/daftack/DomainPasswordSpray</p>	<p>Title: No Changes</p> <p>Description: Added "An example would be a VPN"</p> <p>Detection: Added "Cyber Deception"</p> <p>Tools: Deleted "DomainPasswordSpray" Added "MailSniper" Added "BruteLoops" Added "MSOLSpray"</p> <p>Graphics: Removed</p> <p>Links: Added "https://github.com/vanhauser-thc/thc-hydra" Added "https://github.com/daftack/MailSniper" Added "https://github.com/arch4ngel/BruteLoops" Added "https://github.com/daftack/MSOLSpray" all previous links no longer on card</p>	 <p>PASSWORD SPRAY The attackers gain access to your internal network by spraying commonly used passwords (like SeasonYear) against your organization. An example would be a VPN.</p> <p>DETECTION SIEM Log Analysis Cyber Deception User and Entity Behavior Analytics Firewall Log Review</p> <p>TOOLS SprayingToolkit FireProx Hydra</p> <p>MailSniper BruteLoops MSOLSpray</p> <p>https://github.com/vanhauser-thc/thc-hydra https://github.com/daftack/MailSniper https://github.com/arch4ngel/BruteLoops https://github.com/daftack/MSOLSpray</p>
6	 <p>TRUSTED RELATIONSHIP A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.</p> <p>DETECTION SIEM Log Analysis User and Entity Behavior Analytics</p> <p>TOOLS An unfortunate and unfounded trust in humanity and business partners who are complete strangers.</p> <p></p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics:</p>	 <p>TRUSTED RELATIONSHIP A trusted third party who has access to your network is compromised. The attackers use this to pivot to your internal resources.</p> <p>DETECTION SIEM Log Analysis User and Entity Behavior Analytics</p> <p>TOOLS An unfortunate and unfounded trust in humanity and business partners who are complete strangers.</p> <p></p>

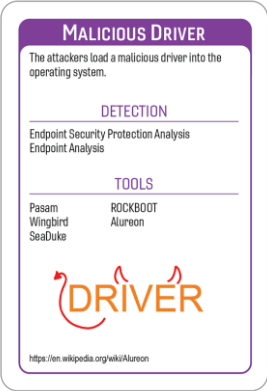

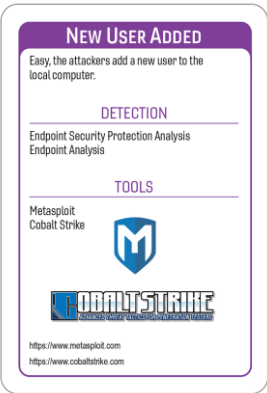
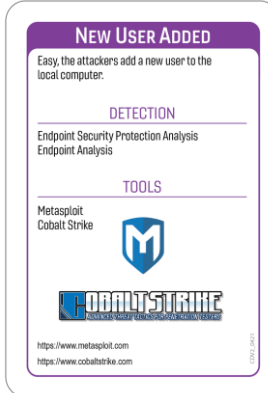

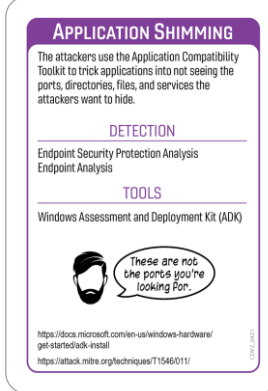
		No Changes Links: No Changes	
7		Title: No Changes Description: No Changes Detection: Added - "Network Threat Hunting - Zeek/RITA Analysis" Tools: No Changes Graphics: No Changes Links: No Changes	
8		Title: No Changes Description: No Changes Detection: Deleted "NetFlow, Zeek/ Bro" Tools: No Changes Graphics: No Changes Links: No Changes	
9		Title: No Changes Description: No Changes Detection: No Changes Tools: No Changes Graphics: No Changes Links: No Changes	

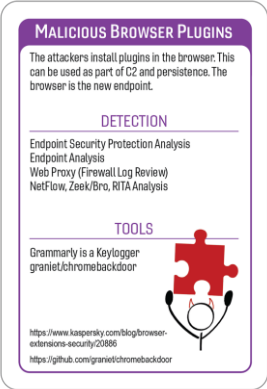
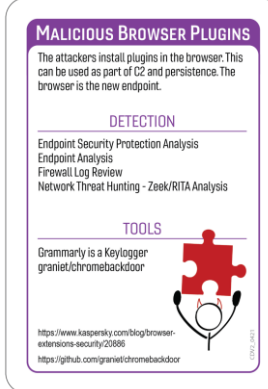
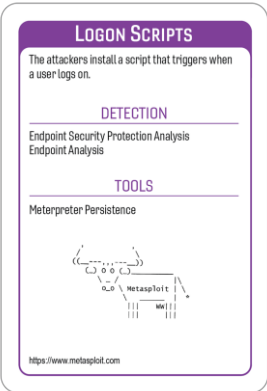
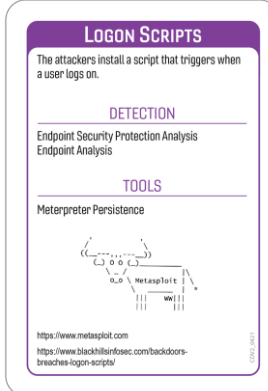
10	 <p>CREDENTIAL STUFFING</p> <p>The attackers take advantage of third-party breaches to identify and use IDs and passwords against your organization.</p> <p>DETECTION</p> <p>Server Analysis User and Entity Behavior Analytics</p> <p>TOOLS</p> <p>Burp Hydra Users registering for services with their work email addresses.</p> <p>https://github.com/vastayready/fireprox https://github.com/delfhack/DomainPasswordSpray https://github.com/byt3b33n/SprayingToolkit https://portswigger.net/burp</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: Added "Suite" to term "Burp Suite"</p> <p>Graphics: Note Changes</p> <p>Links: Deleted two links, and kept previous links</p>	 <p>CREDENTIAL STUFFING</p> <p>The attackers take advantage of third-party breaches to identify and use IDs and passwords against your organization.</p> <p>DETECTION</p> <p>Server Analysis User and Entity Behavior Analytics</p> <p>TOOLS</p> <p>Burp Suite Hydra Users registering for services with their work email addresses.</p> <p>https://github.com/delfhack/DomainPasswordSpray https://portswigger.net/burp</p>
11	 <p>INTERNAL PASSWORD SPRAY</p> <p>The attackers start a password spray against the rest of the organization from a compromised system.</p> <p>DETECTION</p> <p>User and Entity Behavior Analytics SIEM Log Analysis</p> <p>TOOLS</p> <p>Domain Password Spray</p> <p>https://github.com/delfhack/DomainPasswordSpray https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Added "Cyber Deception"</p> <p>Graphics: Note Changes</p> <p>Tools: Added "BruteLoops" Added "Kerbrute" Added "Metasploit"</p> <p>Links: Added https://github.com/ropnop/kerbrute</p>	 <p>INTERNAL PASSWORD SPRAY</p> <p>The attackers start a password spray against the rest of the organization from a compromised system.</p> <p>DETECTION</p> <p>User and Entity Behavior Analytics Cyber Deception SIEM Log Analysis</p> <p>TOOLS</p> <p>DomainPasswordSpray BruteLoops Kerbrute Metasploit</p> <p>https://github.com/delfhack/DomainPasswordSpray https://github.com/ropnop/kerbrute https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack</p>
12	 <p>KERBEROASTING</p> <p>The attackers use a "feature" of SPNs to extract and crack service passwords.</p> <p>DETECTION</p> <p>SIEM Log Analysis User and Entity Behavior Analytics Honey Services Internal Segmentation</p> <p>TOOLS</p> <p>GetUserSPNs.py from Impacket Hashcat for Cracking</p> <p>https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080s https://github.com/SecureAuthCorp/impacket/blob/master/examples/GetUserSPNs.py</p>	<p>Title: Deleted: Kerberoasting Added: Kerberoasting/ASREPRoasting</p> <p>Description: No Changes</p> <p>Detection: Added "Cyber Deception" Deleted "Honey Services" Deleted "Internal Segementation"</p> <p>Tools: Added "GhostPack: - Rubeus Impacket: - GetNPUsers.py - GetUserSPNs.py" Deleted "GetUserSPNs.py from Imacket"</p>	 <p>KERBEROASTING/ASREPROASTING</p> <p>The attackers use a "feature" of service principal names (SPNs) to extract and crack service passwords.</p> <p>DETECTION</p> <p>SIEM Log Analysis User and Entity Behavior Analytics Cyber Deception</p> <p>TOOLS</p> <p>GhostPack: - Rubeus Impacket: - GetNPUsers.py - GetUserSPNs.py Hashcat for Cracking</p> <p>https://github.com/GhostPack https://github.com/SecureAuthCorp/impacket https://github.com/blackhillsinfosec/running-hashcat-on-ubuntu-18-04-server-with-1080s</p>

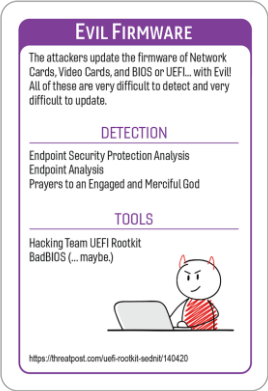
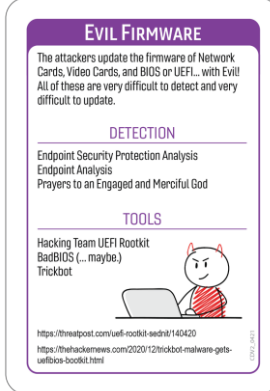

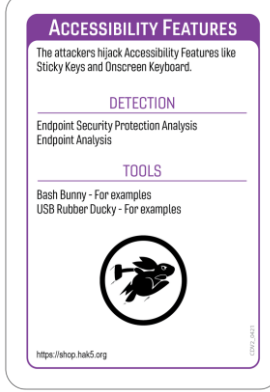
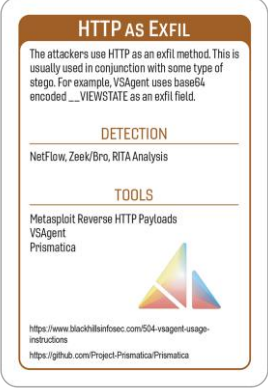
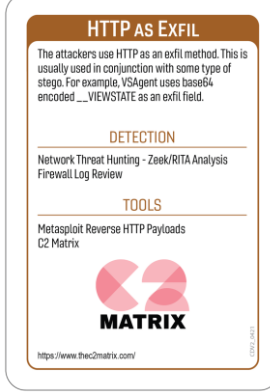
		<p>Graphics: No Changes</p> <p>Links: Added "https://github.com/GhostPack" Added "https://github.com/hashcat/hashcat"</p>	
13		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Added "Cyber Deception" Deleted "CredDefense Tookit"</p> <p>Tools: Added "mitm6 attacks DHCPv6"</p> <p>Graphics: No Changes</p> <p>Links: Added https://github.com/fox-it/mitm6</p>	
14		<p>Title: No Changes</p> <p>Description: The attackers map domain trust relationships, group policies, user/group privileges, and object access control lists (ACLs) in your Active Directory.</p> <p>Detection: Added "Endpoint Security Protection Analysis" Added "Cyber Deception" Deleted "Internal Segmentation"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	

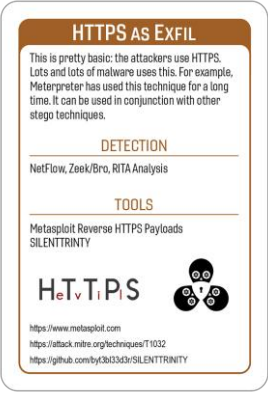
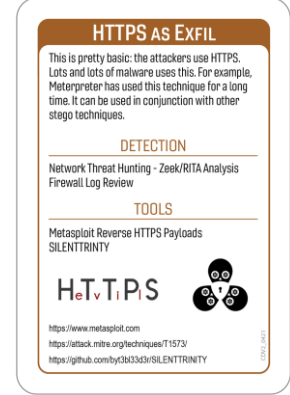
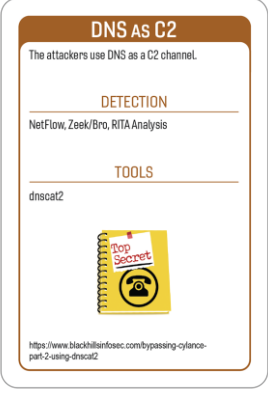
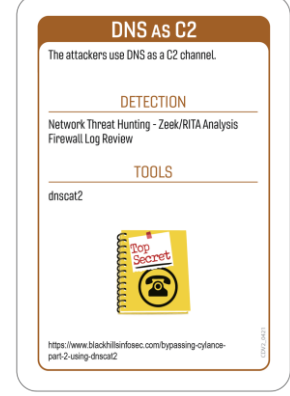
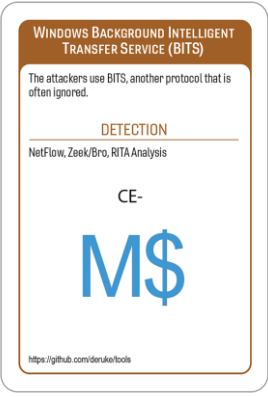
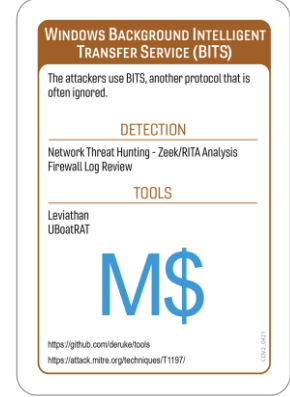
15	<div data-bbox="256 107 522 495" data-label="Image"> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Added "Cyber Deception" Deleted "Internal Segmentation"</p> <p>Tools: Added "Snaffler" Added "CrackMapExec" Added "PowerSploit:"</p> <p>Graphics: Removed</p> <p>Links: Added "https://github.com/Exploit-install/PowerSploit"</p>	<div data-bbox="1214 107 1481 495" data-label="Image"> </div>
16	<div data-bbox="256 879 522 1268" data-label="Image"> </div>	<p>Title: Deleted: New Service Creation Added: New Service Creation/Modification</p> <p>Description: New: The attackers create and load their malware using a new service or existing service modification. Old: The attackers create and load their malware using a service with SYSTEM privileges. Or, they just create a new service.</p> <p>Detection: No Changes</p> <p>Tools: Added Sysinternals PSEXEC services.msc Impacket: - psexec.py Metasploit: - psexec - getsystem Deleted "Endpoint Analysis" Deleted "Endpoint Security Protection Analysis"</p> <p>Graphics: Note Changes</p> <p>Links: Added "https://github.com/SecureAuthCorp/impacket"</p>	<div data-bbox="1214 879 1481 1268" data-label="Image"> </div>



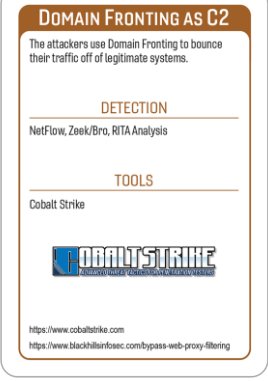
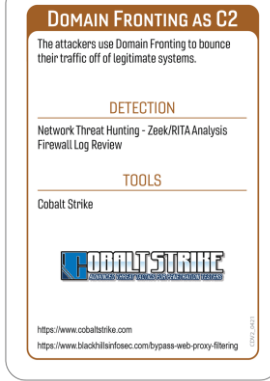
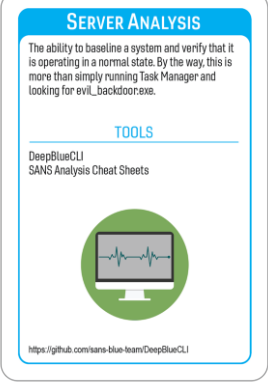
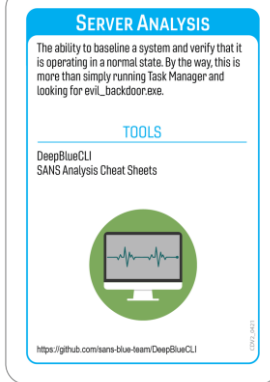
17	<div data-bbox="256 107 522 495"> <p>LOCAL PRIVILEGE ESCALATION</p> <p>The attackers use a vulnerability in local software to gain administrative access.</p> <p>DETECTION</p> <p>Endpoint Analysis Endpoint Security Protection Analysis</p> <p>TOOLS</p> <p>Powersploit's PowerUp Meterpreter Post-Exploitation Scripts</p> <p>https://www.blackhatinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av</p> </div>	<p>Title: No Changes</p> <p>Description: The attackers use a misconfiguration or vulnerability in local software to gain administrative access.</p> <p>Detection: Added "Cyber Deception"</p> <p>Tools: Added "Meterpreter Post-Exploitation Scripts DLLHijackTest PowerSploit: - PowerUp GhostPack: - SharpUp" Deleted Powersploit's PowerUp Deleted Meterpreter Post- Exploitation Scripts</p> <p>Graphics: No Changes</p> <p>Links: All new links from what was here before</p>	<div data-bbox="1214 107 1481 495"> <p>LOCAL PRIVILEGE ESCALATION</p> <p>The attackers use a misconfiguration or vulnerability in local software to gain administrative access.</p> <p>DETECTION</p> <p>Endpoint Analysis Cyber Deception Endpoint Security Protection Analysis</p> <p>TOOLS</p> <p>Meterpreter Post-Exploitation Scripts DLLHijackTest PowerSploit: - PowerUp GhostPack: - SharpUp</p> <p>https://github.com/ty4dyg/DLLHijackTest https://www.blackhatinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av</p> </div>
18	<div data-bbox="256 993 522 1373"> <p>MALICIOUS SERVICE/JUST MALWARE</p> <p>The attackers add a service that starts every time the system starts.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Metasploit Persistence autoruns.exe msconfig.exe SILENTRINITY</p> <p>https://github.com/ty4dyg/SILENTRINITY</p> </div>	<p>Title: Deleted: Malicious Service/Just Malware Added: Malicious Service</p> <p>Description: No Changes</p> <p>Detection: Added "Memory Analysis"</p> <p>Tools: Added "Sysinternals:"</p> <p>Graphics: No Changes</p> <p>Links: Added "Sysinternals:"</p>	<div data-bbox="1214 993 1481 1373"> <p>MALICIOUS SERVICE</p> <p>The attackers add a service that starts every time the system starts.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Memory Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Meterpreter Persistence Modules msconfig.exe SILENTRINITY Sysinternals: - autoruns.exe</p> <p>https://github.com/ty4dyg/SILENTRINITY https://docs.microsoft.com/en-us/sysinternals</p> </div>
19	<div data-bbox="256 1593 522 1974"> <p>DLL ATTACKS</p> <p>The attackers hijack the order in which DLLs are loaded. This is usually done through insecure directory/file permissions.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Powersploit InvisiMole</p> <p>https://www.blackhatinfosec.com/digging-deeper-vulnerable-windows-services</p> </div>	<p>Title: No Changes</p> <p>Description: The attackers hijack the order in which dynamic link libraries (DLLs) are loaded. This is usually done through insecure directory/file permissions.</p> <p>Detection: Added "Memory Analysis"</p> <p>Tools:</p>	<div data-bbox="1214 1593 1481 1974"> <p>DLL ATTACKS</p> <p>The attackers hijack the order in which dynamic link libraries (DLLs) are loaded. This is usually done through insecure directory/file permissions.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Memory Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>DLLHijackTest PowerSploit: - PowerUp</p> <p>https://github.com/ty4dyg/DLLHijackTest https://github.com/Exploit-instaal/PowerSploit https://www.blackhatinfosec.com/digging-deeper-vulnerable-windows-services</p> </div>

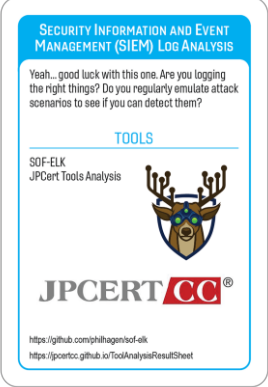

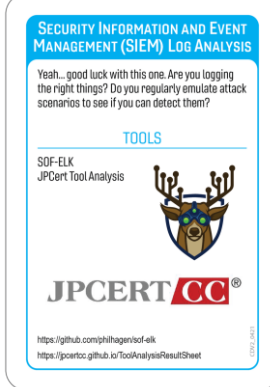



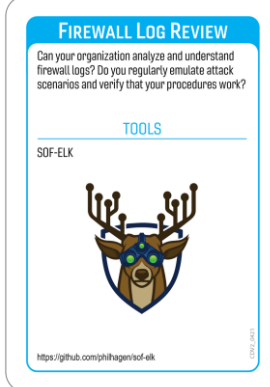







		<p>Added "DLLHijackTest" Added "- PowerUp" Deleted "Invisimole"</p> <p>Graphics: No Changes</p> <p>Links: All different links than what was there before</p>	
20	 <p>MALICIOUS DRIVER The attackers load a malicious driver into the operating system.</p> <p>DETECTION Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS Pasam ROCKBOOT Wingbird Alureon SeaDuke</p> <p>DRIVER</p> <p>https://en.wikipedia.org/wiki/Alureon</p>	<p>Title: No Changes</p> <p>Description: The attackers load a malicious driver into the operating system.</p> <p>Detection: Added "Memory Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>MALICIOUS DRIVER The attackers load a malicious driver into the operating system.</p> <p>DETECTION Endpoint Security Protection Analysis Memory Analysis Endpoint Analysis</p> <p>TOOLS Pasam ROCKBOOT Wingbird Alureon SeaDuke</p> <p>DRIVER</p> <p>https://en.wikipedia.org/wiki/Alureon</p>
21	 <p>NEW USER ADDED Easy, the attackers add a new user to the local computer.</p> <p>DETECTION Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS Metasploit Cobalt Strike</p> <p>M</p> <p>COBALT STRIKE</p> <p>https://www.metasploit.com https://www.cobaltstrike.com</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>NEW USER ADDED Easy, the attackers add a new user to the local computer.</p> <p>DETECTION Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS Metasploit Cobalt Strike</p> <p>M</p> <p>COBALT STRIKE</p> <p>https://www.metasploit.com https://www.cobaltstrike.com</p>
22	 <p>APPLICATION SHIMMING The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.</p> <p>DETECTION Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS Windows Assessment and Deployment Kit (ADK)</p> <p>These are not the ports you're looking for.</p> <p>https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install https://attack.mitro.org/techniques/T1136</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p>	 <p>APPLICATION SHIMMING The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.</p> <p>DETECTION Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS Windows Assessment and Deployment Kit (ADK)</p> <p>These are not the ports you're looking for.</p> <p>https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install https://attack.mitro.org/techniques/T1546/11/</p>








		<p>Graphics: Changed</p> <p>Links: No Changes</p>	
23	 <p>MALICIOUS BROWSER PLUGINS</p> <p>The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis Web Proxy (Firewall Log Review) NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Grammarly is a Keylogger graniel/chromebackdoor</p> <p>https://www.kaspersky.com/blog/browser-extensions-security/20886 https://github.com/graniel/chromebackdoor</p>	<p>Title: No Changes</p> <p>Description: The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.</p> <p>Detection: Deleted "Web Proxy" Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>MALICIOUS BROWSER PLUGINS</p> <p>The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis Firewall Log Review Network Threat Hunting - Zeek/RITA Analysis</p> <p>TOOLS</p> <p>Grammarly is a Keylogger graniel/chromebackdoor</p> <p>https://www.kaspersky.com/blog/browser-extensions-security/20886 https://github.com/graniel/chromebackdoor</p>
24	 <p>LOGON SCRIPTS</p> <p>The attackers install a script that triggers when a user logs on.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Meterpreter Persistence</p> <p>https://www.metasploit.com</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: Added https://www.blackhillsinfosec.com/backdoors-breaches-logon-scripts/</p>	 <p>LOGON SCRIPTS</p> <p>The attackers install a script that triggers when a user logs on.</p> <p>DETECTION</p> <p>Endpoint Security Protection Analysis Endpoint Analysis</p> <p>TOOLS</p> <p>Meterpreter Persistence</p> <p>https://www.metasploit.com https://www.blackhillsinfosec.com/backdoors-breaches-logon-scripts/</p>

25		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: Added "Trickbot"</p> <p>Graphics: No Changes</p> <p>Links: Added https://thehackernews.com/2020/12/trickbot-malware-gets-uefibios-bootkit.html</p>	
26		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	
27		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Changed - "Netflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: Added "C2 Matrix" Deleted "VSAgent" Deleted "Prismatic"</p> <p>Graphics: Changed</p> <p>Links: Completely different links than before</p>	


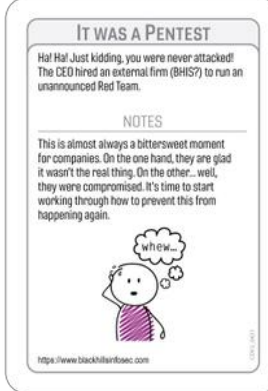
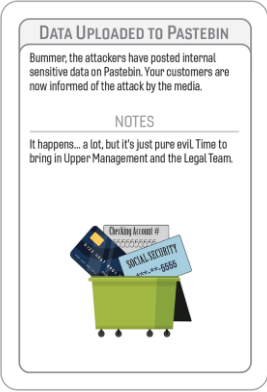
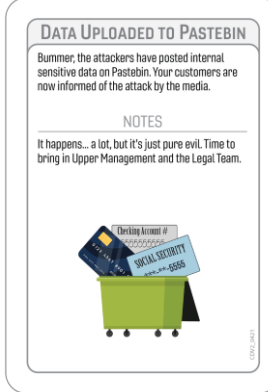
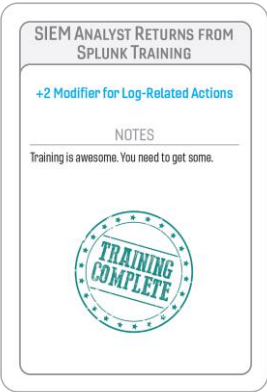
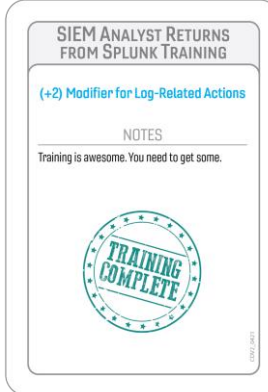
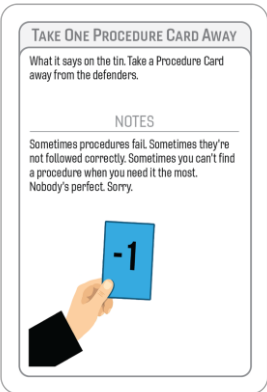
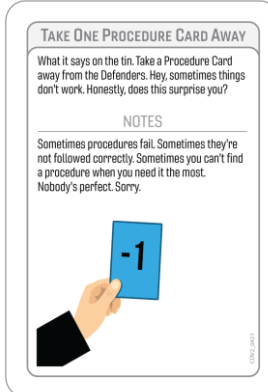
28	 <p>HTTPS AS EXFIL</p> <p>This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Metasploit Reverse HTTPS Payloads SILENTRINITY</p> <p>H.T.T.P.S</p> <p>https://www.metasploit.com https://attack.mitre.org/techniques/T1032 https://github.com/by033d3r/SILENTRINITY</p>	<p>Description: No Changes</p> <p>Detection: Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: Completely different links than before</p>	 <p>HTTPS AS EXFIL</p> <p>This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.</p> <p>DETECTION</p> <p>Network Threat Hunting - Zeek/RITA Analysis Firewall Log Review</p> <p>TOOLS</p> <p>Metasploit Reverse HTTPS Payloads SILENTRINITY</p> <p>H.T.T.P.S</p> <p>https://www.metasploit.com https://attack.mitre.org/techniques/T1032 https://github.com/by033d3r/SILENTRINITY</p>
29	 <p>DNS AS C2</p> <p>The attackers use DNS as a C2 channel.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>dnscat2</p> <p>Top Secret</p> <p>https://www.blackhlinfsec.com/bypassing-cyance-part-2-using-dnscat2</p>	<p>Title: No Changes</p> <p>Description: The attackers use DNS as a C2 channel.</p> <p>Detection: Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>DNS AS C2</p> <p>The attackers use DNS as a C2 channel.</p> <p>DETECTION</p> <p>Network Threat Hunting - Zeek/RITA Analysis Firewall Log Review</p> <p>TOOLS</p> <p>dnscat2</p> <p>Top Secret</p> <p>https://www.blackhlinfsec.com/bypassing-cyance-part-2-using-dnscat2</p>
30	 <p>WINDOWS BACKGROUND INTELLIGENT TRANSFER SERVICE (BITS)</p> <p>The attackers use BITS, another protocol that is often ignored.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>CE-</p> <p>M\$</p> <p>https://github.com/denukes/tools</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: Added "Leviathan" Added "UBoatRAT"</p> <p>Graphics: No Changes</p> <p>Links: Added https://attack.mitre.org/techniques/T1197/</p>	 <p>WINDOWS BACKGROUND INTELLIGENT TRANSFER SERVICE (BITS)</p> <p>The attackers use BITS, another protocol that is often ignored.</p> <p>DETECTION</p> <p>Network Threat Hunting - Zeek/RITA Analysis Firewall Log Review</p> <p>TOOLS</p> <p>Leviathan UBoatRAT</p> <p>M\$</p> <p>https://github.com/denukes/tools https://attack.mitre.org/techniques/T1197/</p>









31	 <p>GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2</p> <p>The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Goat Sneaky Creeper</p> <p>C2 TOOLS</p> <p>https://github.com/by3b33d3r/goat https://github.com/DakotaNelson/sneaky-creeper</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2</p> <p>The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.</p> <p>DETECTION</p> <p>Network Threat Hunting - Zeek/RITA Analysis Firewall Log Review</p> <p>TOOLS</p> <p>Goat Sneaky Creeper</p> <p>C2 TOOLS</p> <p>https://github.com/by3b33d3r/goat https://github.com/DakotaNelson/sneaky-creeper</p>
32	 <p>DOMAIN FRONTING AS C2</p> <p>The attackers use Domain Fronting to bounce their traffic off of legitimate systems.</p> <p>DETECTION</p> <p>NetFlow, Zeek/Bro, RITA Analysis</p> <p>TOOLS</p> <p>Cobalt Strike</p> <p>COBALT STRIKE</p> <p>https://www.cobaltstrike.com https://www.blackhatinfsec.com/bypass-web-proxy-filtering</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: Changed - "Nelflow, Zeek/Bro" to "Network Threat Hunting - Zeek/RITA Analysis"</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>DOMAIN FRONTING AS C2</p> <p>The attackers use Domain Fronting to bounce their traffic off of legitimate systems.</p> <p>DETECTION</p> <p>Network Threat Hunting - Zeek/RITA Analysis Firewall Log Review</p> <p>TOOLS</p> <p>Cobalt Strike</p> <p>COBALT STRIKE</p> <p>https://www.cobaltstrike.com https://www.blackhatinfsec.com/bypass-web-proxy-filtering</p>
33	 <p>SERVER ANALYSIS</p> <p>The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.</p> <p>TOOLS</p> <p>DeepBlueCLI SANS Analysis Cheat Sheets</p> <p>SANS ANALYSIS</p> <p>https://github.com/sans-blue-team/DeepBlueCLI</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Detection: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>SERVER ANALYSIS</p> <p>The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.</p> <p>TOOLS</p> <p>DeepBlueCLI SANS Analysis Cheat Sheets</p> <p>SANS ANALYSIS</p> <p>https://github.com/sans-blue-team/DeepBlueCLI</p>


34	 <p>SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) LOG ANALYSIS</p> <p>Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?</p> <p>TOOLS</p> <p>SOF-ELK JPCert Tools Analysis</p>  <p>JPCERT CC</p> <p>https://github.com/jphhagen/sof-elk https://jpcertcc.github.io/ToolAnalysis/ResultSheet</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) LOG ANALYSIS</p> <p>Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?</p> <p>TOOLS</p> <p>SOF-ELK JPCert Tool Analysis</p>  <p>JPCERT CC</p> <p>https://github.com/jphhagen/sof-elk https://jpcertcc.github.io/ToolAnalysis/ResultSheet</p>
35	 <p>FIREWALL LOG REVIEW</p> <p>Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?</p> <p>TOOLS</p> <p>SOF-ELK</p>  <p>https://github.com/jphhagen/sof-elk</p>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	 <p>FIREWALL LOG REVIEW</p> <p>Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?</p> <p>TOOLS</p> <p>SOF-ELK</p>  <p>https://github.com/jphhagen/sof-elk</p>
36	 <p>NETFLOW, ZEEK/BRO, REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS</p> <p>Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?</p> <p>TOOLS</p> <p>Real Intelligence Threat Analytics (RITA) Security Onion AI-Hunter</p>   <p>https://www.activecountermeasures.com/free-tools/rita https://securityonion.net https://www.activecountermeasures.com</p>	<p>Title: Deleted: NetFlow, Zeek/Bro, Real Intelligence Threat Analytics (RITA) Analysis Added: Network Threat Hunting – Zeek/RITA Analysis</p> <p>Description: Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/RITA/Security Onion/ELK because the cool kids are doing it?</p> <p>Tools: Added "AC-Hunter" Added "Passer" Added "espy" Deleted "AI- Hunter"</p> <p>Graphics: No Changes</p> <p>Links: Completely different links than before</p>	 <p>NETWORK THREAT HUNTING - ZEEK/RITA ANALYSIS</p> <p>Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/RITA/Security Onion/ELK because the cool kids are doing it?</p> <p>TOOLS</p> <p>Real Intelligence Threat Analytics (RITA) Security Onion AC-Hunter Passer espy</p>   <p>https://www.activecountermeasures.com/free-tools/ https://securityonionsolutions.com/</p>

37	<div> <div>INTERNAL SEGMENTATION</div> <div>Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.</div> <div>TOOLS</div> <div>netch advfirewall Windows Defender Firewall iptables</div> <div></div> </div>	** Replaced “Internal Segmentation” **	<div> <div>CYBER DECEPTION</div> <div>The attackers go after one of your deception technologies. This could be a Word Web Bug, Honey Account, or a full honeypot.</div> <div>TOOLS</div> <div>CanaryTokens HoneyBadger Active Defense Harbinger Distribution MITRE Shield</div> <div></div> <div>https://shield.mitre.org/ https://www.activecountermeasures.com/free-tools/adhd/</div> </div>
38	<div> <div>ENDPOINT SECURITY PROTECTION ANALYSIS</div> <div>We know, you have AV. Great! Do you actually get alerts and logs? Or do you simply turn it on and walk away while the network explodes like you're in a bad action movie?</div> <div>TOOLS</div> <div>Check with your vendor, they miss you and always want to chat.</div> <div></div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: Added "https://www.velocidex.com/" Added "https://www.elastic.co/downloads/elastic-agent"</p>	<div> <div>ENDPOINT SECURITY PROTECTION ANALYSIS</div> <div>We know, you have AV. Great! Do you actually get alerts and logs? Or do you simply turn it on and walk away while the network explodes like you're in a bad action movie?</div> <div>TOOLS</div> <div>Check with your vendor, they miss you and always want to chat.</div> <div></div> <div>https://www.velocidex.com/ https://www.elastic.co/downloads/elastic-agent</div> </div>
39	<div> <div>USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)</div> <div>It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, password sprays, and more!</div> <div>TOOLS</div> <div>LogonTracer</div> <div></div> <div>https://github.com/JPCERTCC/LogonTracer</div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: Added "DeepBlueCLI" Added "OpenUBA"</p> <p>Graphics: No Changes</p> <p>Links: Added "http://openuba.org/"</p>	<div> <div>USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)</div> <div>It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, password sprays, and more!</div> <div>TOOLS</div> <div>LogonTracer DeepBlueCLI OpenUBA</div> <div></div> <div>https://github.com/JPCERTCC/LogonTracer http://openuba.org/</div> </div>
40	<div> <div>ENDPOINT ANALYSIS</div> <div>This is where the defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.</div> <div>TOOLS</div> <div>DeepBlueCLI SANS IR Cheat Sheets</div> <div></div> <div>https://github.com/sans-blue-team/DeepBlueCLI</div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: Added "Velociraptor"</p> <p>Graphics: Changed</p> <p>Links: Added "https://www.velocidex.com/"</p>	<div> <div>ENDPOINT ANALYSIS</div> <div>This is where the Defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.</div> <div>TOOLS</div> <div>DeepBlueCLI Velociraptor SANS IR Cheat Sheets</div> <div></div> <div>https://github.com/sans-blue-team/DeepBlueCLI https://www.velocidex.com/</div> </div>

41	<div> <div>ISOLATION</div> <div>Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.</div> <div>TOOLS</div> <div>Switch and Router Commands</div> <div> </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	<div> <div>ISOLATION</div> <div>Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.</div> <div>TOOLS</div> <div>Switch and Router Commands</div> <div> </div> </div>
42	<div> <div>CRISIS MANAGEMENT</div> <div>Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.</div> <div>NOTES</div> <div>This counteracts the "Data Uploaded to Pastebin" Inject Card.</div> <div>TOOLS</div> <div>This almost never happens. But, a good notification strategy will really help deal with the political fallout.</div> <div> </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Tools: Deleted "The Counteracts the 'Data Uploaded to Pastebin' Inject Card"</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	<div> <div>CRISIS MANAGEMENT</div> <div>Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.</div> <div>TOOLS</div> <div>This almost never happens. But, a good notification strategy will really help deal with the political fallout.</div> <div> </div> </div>
43		**NEW CARD**	<div> <div>MEMORY ANALYSIS</div> <div>Incident Response Team pulls the memory from the suspect system and reviews it for possible malicious activity.</div> <div>TOOLS</div> <div>Volatility, to review the memory Velociraptor, to dump the memory</div> <div> </div> <div> https://www.velociraptor.com/ https://www.volatilityfoundation.org/ </div> </div>
44	<div> <div>HONEYPOTS DEPLOYED</div> <div>The defenders had honeypots on their network. The "Incident Master" has to show their Pivot and Escalate Card to the defenders.</div> <div>NOTES</div> <div>Check out the Active Defense Harbinger Distribution (ADHD), it has lots and lots of cool tools. Also, take a look at canarytokens.org.</div> <div> </div> <div> https://www.activecountermeasures.com/free-tools/adhd https://canarytokens.org/generate </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Notes: No Changes</p> <p>Graphics: No Changes</p> <p>Links:</p>	<div> <div>HONEYPOTS DEPLOYED</div> <div>The Defenders had honeypots on their network. The Incident Master must reveal the Pivot and Escalate Card to the Defenders.</div> <div>NOTES</div> <div>Check out the Active Defense Harbinger Distribution (ADHD), it has lots and lots of cool tools. Also, take a look at canarytokens.org.</div> <div> </div> <div> https://www.activecountermeasures.com/free-tools/adhd https://canarytokens.org/generate </div> </div>

		No Changes	
45		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Notes: No Changes</p> <p>Graphics: No Changes</p> <p>Links: No Changes</p>	
46		<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	
47		<p>Title: Changed: Increased font size</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	
48		<p>Title: No Changes</p> <p>Description: What it says on the tin. Take a Procedure Card away from the Defenders. Added " Hey, sometimes things don't work. Honestly, does this surprise you?"</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	

49	<div> <div> <p>GIVE THE DEFENDERS A RANDOM PROCEDURE CARD</p> <p>For whatever reason, everyone forgot they had this procedure. It must be Monday.</p> <p>NOTES</p> <p>Look, it happens all the time. We forget what we have. Different teams, different tools, different offices. It's nice when we all pull together as a team.</p>  </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	<div> <div> <p>GIVE THE DEFENDERS A RANDOM PROCEDURE CARD</p> <p>For whatever reason, everyone forgot they had this procedure. It must be Monday.</p> <p>NOTES</p> <p>Look, it happens all the time. We forget what we have. Different teams, different tools, different offices. It's nice when we all pull together as a team.</p>  </div> </div>
50	<div> <div> <p>LEAD HANDLER HAS A BABY, TAKES FMLA LEAVE</p> <p>Yeah, there's always one person who pretty much runs the whole IR process. That one essential person. Well, now it's time for the "Incident Master" to silence that person.</p> <p>NOTES</p> <p>We have to continue to be able to work effectively without the one or two most advanced people on the team. All of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p>  </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	<div> <div> <p>LEAD HANDLER HAS A BABY, TAKES FMLA LEAVE</p> <p>Yeah, there's always one person who pretty much runs the whole IR process. That one essential person. Well, now it's time for the Incident Master to silence that person.</p> <p>NOTES</p> <p>We have to continue to be able to work effectively without the one or two most advanced people on the team. All of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p>  </div> </div>
51	<div> <div> <p>BOBBY THE INTERN KILLS THE SYSTEM YOU ARE REVIEWING</p> <p>This. Happens. Far. Too. Often.</p> <p>NOTES</p> <p>No. Murder is never okay. Don't even think that.</p>  </div> </div>	<p>Title: No Changes</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	<div> <div> <p>BOBBY THE INTERN KILLS THE SYSTEM YOU ARE REVIEWING</p> <p>This. Happens. Far. Too. Often.</p> <p>NOTES</p> <p>No. Murder is never okay. Don't even think that.</p>  </div> </div>
52	<div> <div> <p>LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT</p> <p>Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."</p> <p>NOTES</p> <p>They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p>  </div> </div>	<p>Title: Changed: Increased font size</p> <p>Description: No Changes</p> <p>Graphics: No Changes</p> <p>Notes: No Changes</p>	<div> <div> <p>LEGAL TAKES YOUR MOST SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT</p> <p>Who brought a lawyer to the party? There's always one person who pretty much runs the whole IR process. That one essential person. Well, the legal team took that person away for "Very Important Reasons."</p> <p>NOTES</p> <p>They may never come back... all of the quiet people who were just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!</p>  </div> </div>

53	<div><div>MANAGEMENT HAS JUST APPROVED THE RELEASE OF A NEW PROCEDURE</div><div>Internal Network Capture and Analysis (+5 Modifier for Network Capture Analysis Tasks)</div><div>How many times has management come to the rescue? Knights in shining business suits. Every once in a great while the benevolent C-suite smiles on you.</div><div>NOTES</div><div>Get taps and monitoring in ASAP!!</div><div></div></div>	Removed “Management has Just Approved the Release of a New Procedure”	
----	---	--	--