Moving Left of the Ransomware Boom

accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom

To foster better collaboration and cyber ground truth, VMware and Accenture's Cyber Defense group teamed up to deliver relevant security research. Our goal is to expose criminals' tactics, techniques, and procedures (TTPs) and thereby help security teams better focus their prevention, detection and response programs.

Ransomware isn't new—in fact, it's over 30 years old. Attacks date back as far as 1989 and have been the most pervasive cyber threat since 2005, with a dramatic spike in recent years that continues to increase. In fact, Cybersecurity Ventures predicts that the damage caused by ransomware could cost up to $265 billion by 2031, making it ever more important for companies to prepare their defenses and understand ways to stop the attackers prior to ransomware deployment.

<<< Start >>>

Time-to-Ransom (TTR)

Time-to-Ransom refers to the amount of time from when the threat actor gains initial access into a network to the time the threat actor deploys the ransomware. This time can range from hours to days, or even months.

<<< End >>>

The old quote “defenders have to be right 100% of the time” proves to be untrue. The reality is that in most cases there are several opportunities for teams to disrupt the criminal's behavior prior to the ransomware executing. This blog will examine the common tactics that cybercriminals use to infiltrate and move around a company network prior to ransomware deployment, paying close attention to the time-to-ransom (TTR). Each stage of the attacker lifecycle offers unique opportunities to detect and remove them from the network prior to significant and costly damage. It only takes one mitigation to break the criminals’ kill chain.

Cyber Extortion at scale is big business and business is good for criminals

As ransomware-as-a-service (RaaS) explodes in popularity on the crimeware forums, cybercriminals are finding new and unique ways to deploy ransomware across organizations. Ransomware groups may be recruiting insiders or affiliates specializing in a specific part of the attack chain to increase the stealth of their attack while employing multiple extortion tactics by first stealing company data before locking it up. According to Accenture incident responders, data extortion was confirmed in about 30% of 10 cases they analyzed between June 2020 and June 2021.

As ransomware groups become increasingly capable, TTR can decrease. In contrast, however, if the actor combines data extortion with data destruction, the on-network requirements to steal sensitive data require greater TTR and additional on-host activities, providing opportunities for detection. According to Accenture incident response investigators, in analyzed cases over the past year, the TTR has been as low as 2.5 hours and as high as six months, with Carbon Black estimating that the TTR is on average between two and four days. The longer the TTR, the more opportunity there is for an organization to detect and respond to an attack prior to data destruction.

Methodology

Accenture Cyber Defense utilized data from over 10 recent cyber investigations, forensics and response (CIFR) ransomware incident response investigations, combined with Accenture’s Cyber Threat Intelligence’s (ACTI) dark web monitoring to identify popular pre-ransomware deployment network activities. Additionally, VMware Carbon Black leveraged data from the Carbon Black Cloud where the product suite can successfully prevent the execution of ransomware, as well as the pre-execution TTPs that were observed prior to ransomware payload execution.

Our threat research uses MITRE ATT&CK® – a comprehensive framework to document adversary TTPs - to focus on TTPs relevant to the initial stages of infection that precede a ransomware attack. We will also be focused on the TTR to help teams better create playbooks and responses when an infection occurs.

MITRE ATT&CK Stages

Initial Access

Accenture and Carbon Black have identified remote desktop protocol (RDP) vulnerabilities as a primary initial access method for ransomware actors. RDP is exploited in roughly half of the documented attacks that are escalated to VMware's Threat Analysis Unit (TAU). In many of these attacks there is a 48-to-92-hour period between the initial observed RDP access and the ransomware portion of the attack. Similarly, Accenture has found RDP vulnerabilities to be a preferred method for several ransomware groups. For example, the ransomware group Avaddon appears to prefer exploiting RDP vulnerabilities as a breach methodology. This group has advertised specific interest in acquiring specialists who can develop network access through compromised RDP sessions or virtual private network (VPN) connections.

The second-greatest portion of the remaining cases studied by TAU initially start with a social engineering element like phishing emails. These emails will typically contain an initial dropper which is either an office document or an executable concealed in an archive format, like a zip file. The initial dropper will either download a first-stage payload like IcedID, SdBot, Trickbot, or Emotet or leverage PowerShell to execute a Cobalt Strike cradle. These tools help the threat actor gain unauthorized access to the remote systems and can perform a variety of functions including, downloading and executing additional files, credential harvesting, and lateral movement operations.

The remainder are known vulnerabilities being exploited combined with lateral movement.

Execution

Accenture Security and VMware TAU continue to observe ransomware actors leverage living-off-the-land techniques in conjunction with off-the-shelf tools like Cobalt Strike, Koadic, PowerShell Empire, and Metasploit. Because of the effectiveness of tools like Cobalt Strike, as well as the anonymity that their popularity provides, many actors have adopted them into their overall attacker portfolios.

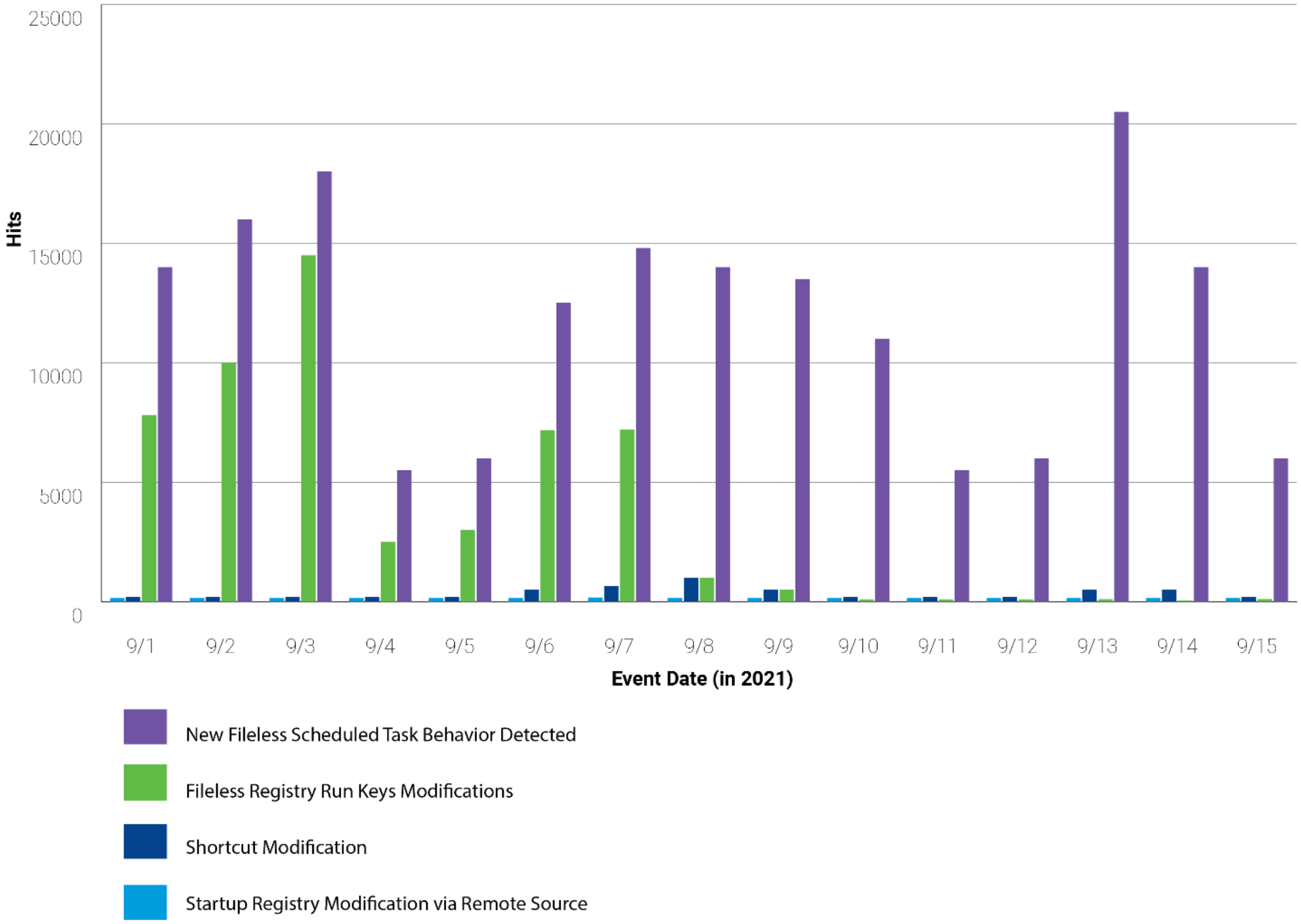
Prior to bans on ransomware advertisements by many forums, dark web findings indicated that at least Ragnar Locker and REvil operators had actively recruited hackers experienced with commodity tools including the Cobalt Strike platform; additionally, actors regularly sell or release cracked versions of Cobalt Strike, lowering the barrier to entry for this versatile tool. Cobalt Strike Beacon, a penetration testing product, provides vast functionality against the host, including privilege escalation, file transfer, command execution, port scanning and lateral movement, which is why it is an increasingly popular tool for ransomware operations.

Persistence

VMware TAU and the Carbon Black Cloud identified attackers using PowerShell to modify windows registry and startup files as the predominate method of gaining persistence on endpoints observed in the bar graph below. This finding is consistent with observations by Accenture's CIFR team. For easiest viewing, the graph below represents a two-week period, however, the trends have been consistent over time. Based on Windows Antimalware Scan

Interface (AMSI) data that Carbon Black monitors, the two largest spikes are specifically from PowerShell modifying the startup folders, in purple, and PowerShell modifying different registry run keys, in green.

<<< Start >>>

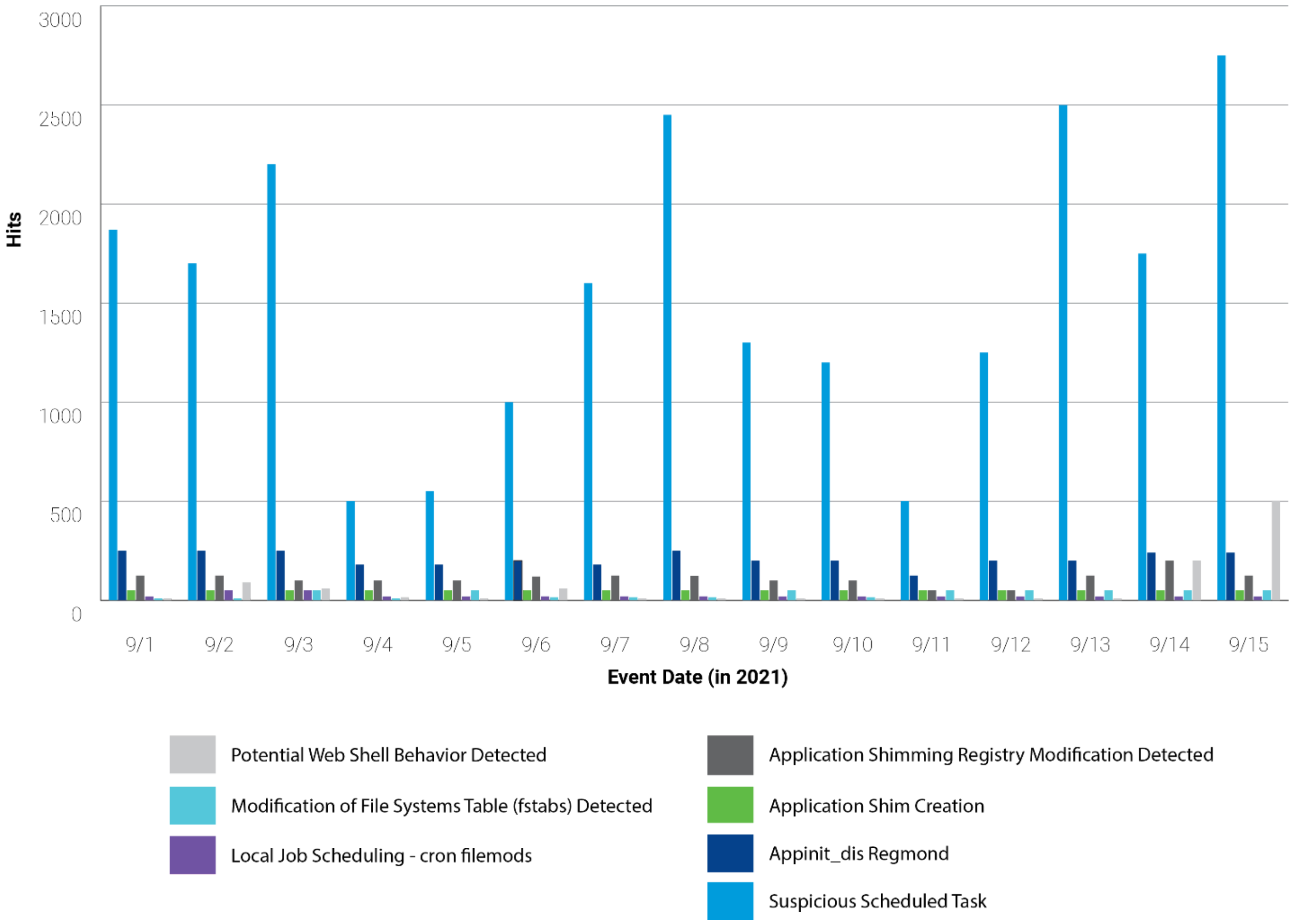


Source: Carbon Black AMSI data

<<< End >>>

When looking at non-AMSI data, the single largest persistence method is scheduled tasks; in blue in the graph below.

<<< Start >>>



Source: Carbon Black AMSI data

<<< End >>>

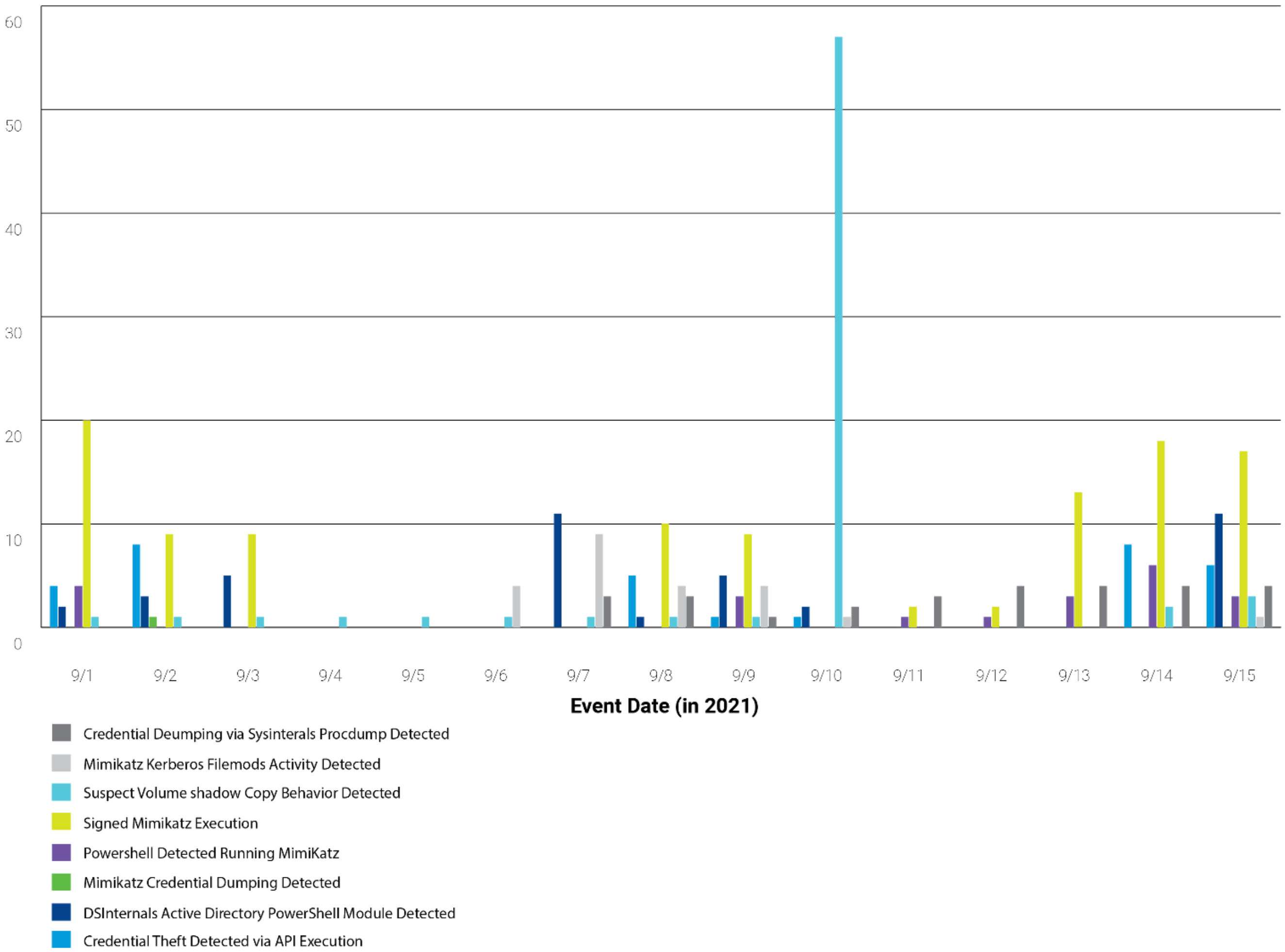
The commodity trojans prevalent in ransomware operations, like Trickbot, IcedID, and Emotet, have the capability to create scheduled tasks for persistence.

Privilege Escalation / Credential Access

Privilege Escalation / Credential AccessPrivilege escalation and credential access are priorities for ransomware operators, as these tactics often enable additional actions against the network, such as lateral movement or disabling endpoint monitoring software. Credential harvesting is one of the tactics used to ensure secondary extortion methods have higher efficacy. This allows attackers to gain access to business communication channels like email, Slack and Microsoft teams, which can make real-time response communications a challenge during an outbreak.

Attackers are using Mimikatz predominately to harvest credentials. The execution of signed Mimikatz binaries remains the highest detection related to credential harvesting that VMWare has historically observed. This is followed by PowerShell running Mimikatz and credential theft using NTDSutil. Commodity tools, such as Meterpreter, have built-in techniques to try to obtain system-level administration privileges.

<<< Start >>>



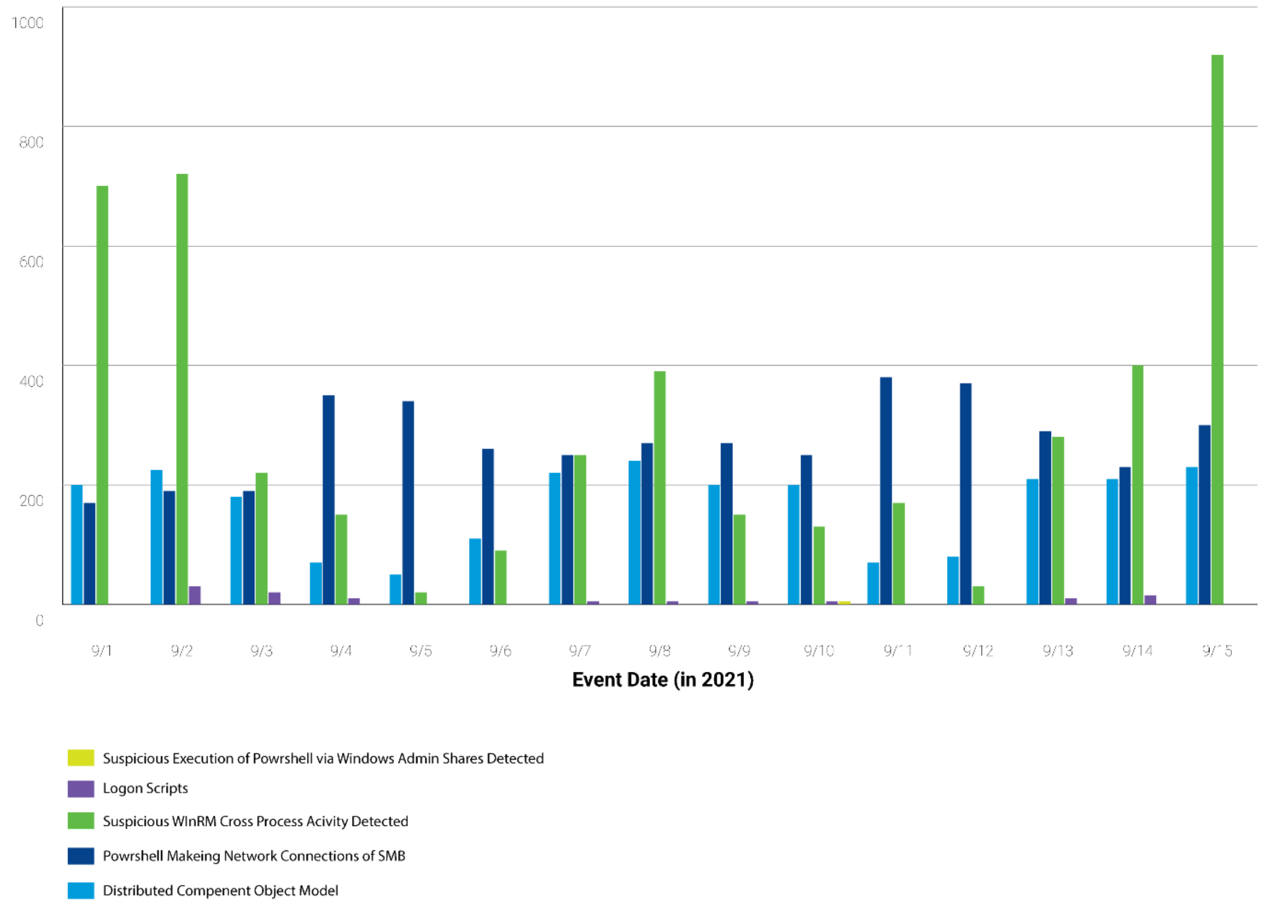
Source: Carbon Black AMSI data

<<< End >>>

Lateral Movement

Lateral movement is a key component of an effective attack and ransomware groups can use port scans and the lateral movement capabilities embedded in commodity malware and tools. As the use of Cobalt Strike increases among ransomware operators, Accenture Security and Carbon Black have, in turn, observed attackers use Cobalt Strike Beacon capabilities, such as named pipes over Server Message Block (SMB) and WinRM to move laterally in targeted networks.

<<< Start >>>



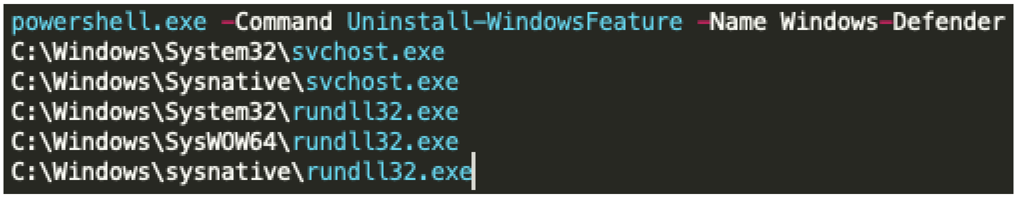
Source: Carbon Black AMSI data

<<< End >>>

Defense Evasion

Ransomware threat actors are keenly aware of being exposed through antivirus or other endpoint defense detections and would proactively try to nullify these tools with antivirus blocking tools or by uninstalling antivirus from a privileged account.

<<< Start >>>



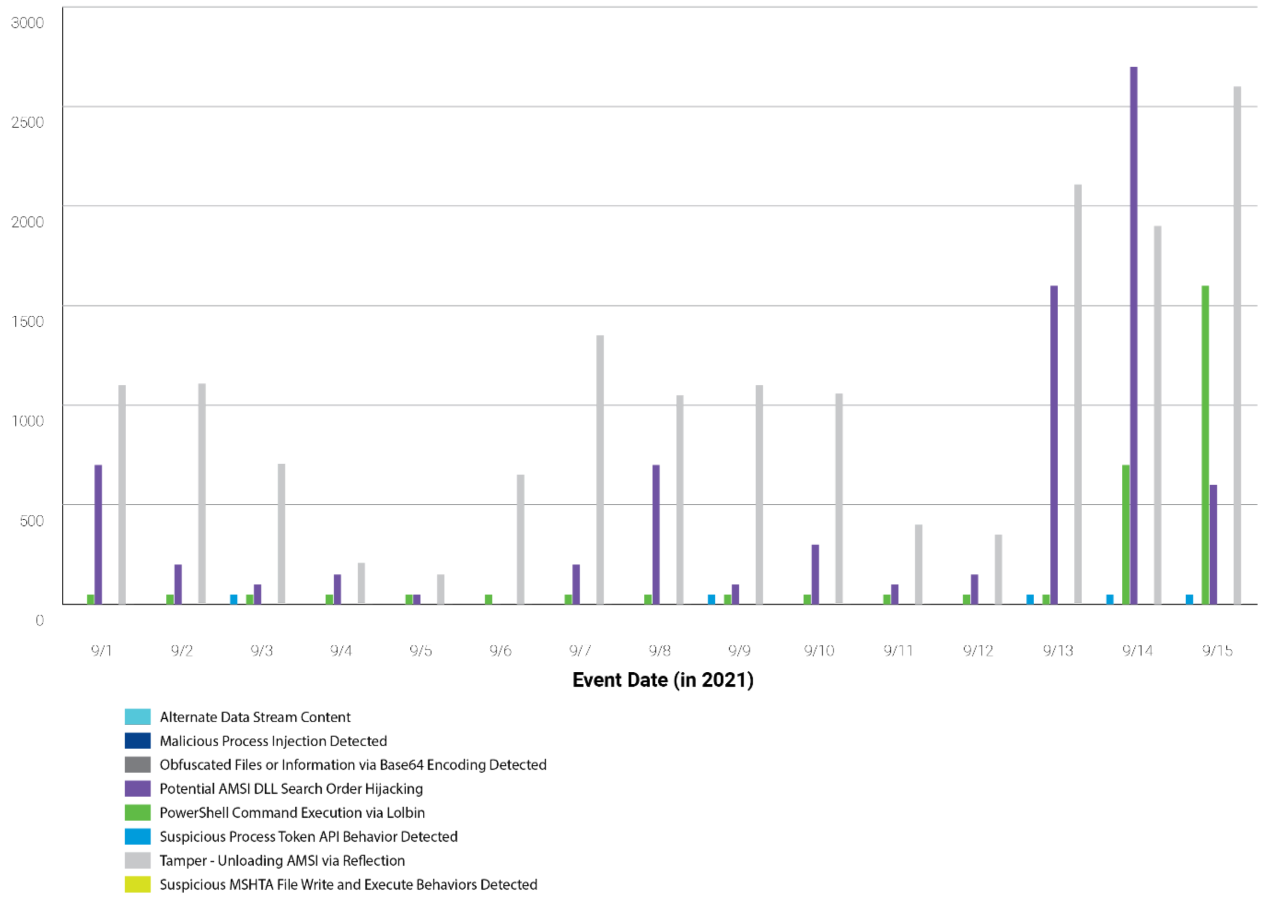
```
powershell.exe -Command Uninstall-WindowsFeature -Name Windows-Defender
C:\Windows\System32\svchost.exe
C:\Windows\Sysnative\svchost.exe
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\sysnative\rundll32.exe
```

Example of an Actor using PowerShell to try and uninstall Windows Defender

<<< End >>>

Carbon Black monitors numerous techniques that fall into the defense evasion category. The graph below is data solely from AMSI-based detections; historically attempting to unload AMSI via reflection is the most popular PowerShell defense evasion technique observed.

<<< Start >>>



Source: Carbon Black AMSI data

<<< End >>>

In other cases, ransomware operators will try to work around endpoint defenses. For example, in one ransomware attack at a health and public services company, the threat actors executed a Cobalt Strike payload. However, the execution sequence was detected by Windows Defender and quarantined accordingly. After about two days of triggering Windows Defender detections, the threat actor pivoted to the use of another open-source tool called Koadic. This tool is also a Windows Post-Exploitation rootkit that utilizes Windows Script Host; however, it creates small payloads executed in memory which can be less noise-generating. Throughout the engagement, the threat actor continued to monitor the endpoint detections and would pivot to new tools or tactics in an attempt to avoid them.

Command and control

Often ransomware actors achieve command and control in one of two ways. First, the actor will leverage compromised credentials in combination with exposed RDP. Second, the attackers once again leverage the capabilities within Cobalt Strike to communicate externally. In one CIFR investigation, the ransomware actors used domain fronting to disguise the destination of their command and control.

Exfiltration

Ransomware groups have widely adopted double extortion as a core tactic to ensure profitability. In fact, nearly 40% of security professionals said double-extortion ransomware was the most observed new ransomware attack technique in 2020. By taking time to quietly exfiltrate sensitive information from the organization, cybercriminals gain incrementally significant leverage on their victim organizations, forcing organizations to not only pay to decrypt their content but also prevent potentially harmful data from being sold or otherwise publicly disclosed.

Ransomware groups will use a variety of methods to exfiltrate data, and this additional process will likely mean more TTR, leaving artifacts that can trigger detection and remediation efforts.

In one investigation, Accenture identified a ransomware gang use RClone to exfiltrate 2TB of data prior to executing Maze and Mountlocker ransomware. RClone is an open-source command line tool that allows the actors to sync files from the local disk to a cloud storage provider. During another investigation the ransomware actors downloaded and utilized curl.exe to maximize download capabilities and exfiltrate .bat files and a tmp.vbs file used to calculate disk space on the staging server.

Opportunities for Defenders

The above pre-ransomware tactics leave evidence that provides organizations with possible detection opportunities prior to exfiltration of data and deployment of destructive malware. VMware and ACTI recommend implementing a managed detection and response (MDR) service like Accenture’s, which is a true multi-tenant, cloud-based service that provides extended threat detection and response via network monitoring, endpoint management and remediation; security incident analysis; and escalation via a dedicated team of security experts. The Accenture MDR service helps secure the client’s endpoints, while leveraging their existing investments, with a managed endpoint detection and response service that provides additional investigation of identified suspicious endpoint-based activities, and enhanced context, threat hunting and proactive responses.

<<< Start >>>

Accenture MDR Key Features:

- **Data Analysis:** processing and analysis of log data from security controls, network infrastructure, and endpoints to identify events of interest.
- **24/7 Alert Monitoring:** 24x7 alert monitoring, analysis, identification, and escalation of incidents through industry specific threat intelligence.
- **Highly Qualified Analyst Teams:** client aligned specialists, including GIAC-certified Security Analysts, Service Delivery Leads, On-Boarding Engineers, and Senior Analysts
- **Customizable Service:** customizable set of processes, including client specific security incident escalation and individualized incident severity tuning.
- **Anomaly Detection:** anomalous traffic detection, data mining, and statistical analysis to identify known and previously unknown malicious activity.
- **Single Pane-of-Glass Customer Portal:** a comprehensive view of all security incidents, devices, assets, and reporting through a self-service portal.
- **Threat Intelligence:** visibility into threats impacting client specific industries and geographies, including specific attacker tools, tactics and procedures.
- **Rapid Proactive Response:** active remediation based on pre-authorized actions for rapid response with access to incident response.

<<< End >>>

Additionally, Accenture and VMware advise optimizing for the detection opportunities below:

Additionally, Accenture and VMware advise optimizing for the detection opportunities below:

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Detection Opportunity
Initial Access	T1189: Drive-by Compromise T1566: Phishing T1133: External Remote Services T1078: Valid Accounts	Monitor antivirus and Intrusion Detection/Prevention detections. Scrutinize PowerShell logs for obfuscated commands and command-line arguments. Prevent installation of legacy PowerShell versions as well as the execution of Base64-encoded commands. Monitor for anomalous log-in activity such as multiple log-in attempts, log-in outside of business hours, etc.

Execution	T1059: Command and Scripting Interpreter T1569.002: Service Execution T1047: Windows Management Instrumentation T1559: Inter-Process Communication	Monitor for potentially suspicious command-line activity including parameters for security tool service modifications, anomalous process executions, or encoded commands. Monitor Windows event logs for service creation and modification, registry changes, and command-line parameters of files and processes. Monitor for host browser process anomalies including suspicious file writes and process injections. Review PowerShell logs to search for loading or execution of artifacts. Monitor network traffic for Windows Management Instrumentation (WMI) connections and investigate any suspicious connections. Review command-line arguments for use of “wmic” or other indicators of remote behavior. Track any unauthorized or unusual loading of DLL files.

Persistence	T1078: Valid Accounts T1543: Create or Modify System Process T1543.003: Windows Services T1053: Scheduled Task T1547: Boot or Logon Autostart Execution T1547.001: Registry Run Keys / Startup Folders T1133: External Remote Services T1037: Boot or Logon Initialization Scripts • T1037.003: Network Logon Script • T1037.005: Startup Items	Investigate parental processes to determine the process tree and identify binaries for subsequent analysis. Audit system settings for potential unknown autostart execution configurations. Monitor systems for abnormal process behavior and processes loading malicious DLLs. Monitor logon scripts for unusual access to accounts outside of regular or expected time periods. Monitor for unexpected new system processes or changes that are unrelated to scheduled activity such as patches and software updates. Monitor for suspicious activity relating to user accounts, such as the sharing of accounts or access outside of usual business hours.

Privilege Escalation	T1055: Process Injection • T1055.001: Dynamic-link Library Injection • T1055.012: Process Hollowing T1548: Abuse Elevation Control Mechanism T1548.002: Bypass UAC T1078: Valid Accounts T1543: Create or Modify System Process T1543.003: Windows Service	Monitor events of files commonly used in process injection, such as DLLs and PEs, that are not recognized or normally loaded into processes. Monitor for malicious PowerShell modules like PowerSploit (Invoke-Mimikatz). Monitor Active Directory for unusual changes or requests. Regularly check for system process modification using commands or executables in service file names, anomalous service creations, and unsigned binaries in image paths. Monitor for use of unsigned applications or those not from trusted repositories. Monitor for suspicious activity relating to user accounts, such as the sharing of accounts or access outside of usual business hours.

Defense Evasion	T1562: Impair Defenses T1562.001: Disable or Modify Tools T1550: Use Alternate Authentication Material T1550.002: Pass the Hash T1036: Masquerading T1112: Modify Registry T1553: Subvert Trust Controls T1553.002: Code Signing T1027: Obfuscated Files or Information • T1027.003: Steganography • T1027.005: Indicator Removal from Tools T1140: Deobfuscate/Decode Files or Information T1218: Signed Binary Proxy Execution • T1218.011: Rundll32 • T1218.005: Mshta • T1218.010: Regsvr32	Monitor activity of processes and command-line arguments that may relate to disabling or terminating security tools and logging services, scripts, and system utilities used to deobfuscate/decode files and information, or activity indicating proxy execution of malicious files. Regularly audit and monitor account activity that may indicate unauthorized access or account sharing Monitor files by their hashes to identify any suspicious changes to filenames that may indicate. masquerading. Monitor the registry for unfamiliar changes such as newly added startup processes and modified binary paths. Analyze signing certificates of software to identify unusual certificates that may indicate malicious activity. Use and configure antivirus and antimalware solutions to identify and analyze commands that may relate to obfuscating files or information. Investigate and analyze security events relating to file obfuscation for any malicious activity that may have gone undetected. Implement host and network rules to detect commonly used deobfuscation/decoding techniques.

Credential Access	T1558: Steal or Forge Kerberos Tickets • T1558.001: Golden Ticket • T1558.002: Silver Ticket • T1558.003: Kerberoasting T1003: OS Credential Dumping • T1003.001: LSASS Memory • T1003.002: Security Account Manager • T1003.003: NTDS • T1003.006: DCSync T1552: Unsecured Credentials T1552.001: Credentials in Files	Monitor for suspicious activity on networks that may indicate the stealing or forging of Kerberos tickets. Monitor for suspicious LSASS.exe executions or unusual processes interacting with LSASS, SAM. Monitor for malicious PowerShell modules like PowerSploit (Invoke-Mimikatz). Monitor command line activity for indications of password searches (for example, searching for keywords “password, pwd, login, credentials”).

Lateral Movement	T1550: Use Alternate Authentication Material - T1550.002: Pass the Hash - T1550.003: Pass the Ticket T1570: Lateral Tool Transfer T1072: Software Deployment Tools T1210: Exploitation of Remote Services T1021: Remote Services - T1021.001: Remote Desktop Protocol - T1021.002: SMB/Windows Admin Shares - T1021.006: Windows Remote Management	Look for anomalous activity from non-privileged accounts, particularly monitoring for the use of LoLbins. Monitor remote logins, access patterns, and activity. Investigate “impossible logins” – user logins from geographically dispersed IP addresses (although VPN use could cause false positives). Scrutinize command-line arguments associated with network share mounting and remote access tools.

Command and Control	T1102: Web Services T1573: Encrypted Channel T1132: Data Encoding T1090: Proxy T1090.004: Domain Fronting T1219: Remote Access Software T1105: Ingress Tool Transfer T1071: Application Layer Protocol • T1071.001: Web Protocols • T1072.004: DNS	Monitor for uncommon data flows. Watch for processes that do not normally have network access. Monitor the SNI field of TLS headers and the host field in HTTP headers, check domains against a block/allow list, and identify beaconing activity. Use network intrusion detection and prevention systems that use network signatures to identify traffic. Monitor the use and activity of utilities such as FTP that are not typical in the network environment. Filter network traffic to prevent the accessing of anonymity networks and inspect traffic for indications of potential domain fronting.
Exfiltration	T1029: Scheduled Transfer T1048: Exfiltration Over Alternate Protocol T1041: Exfiltration Over C2 Channel T1567: Exfiltration Over Web Service T1567.002 Exfiltration to Cloud Storage	Identify anomalies in network activity associated with known binaries, analyze uncommon data flows and packet inspection for misuse of protocol to port behaviors. Monitor environment and network activity for suspicious or unknown processes and scripts that appear to be traversing file systems or sending network traffic. Monitor for unusual network activity and analyze packet contents that do not use standard ports or expected protocol behavior. Analyze unknown network connections to the same destination that occur regularly at the same time of day.

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this article is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.