BlackByte blends tried-and-true tradecraft with newly disclosed vulnerabilities to support ongoing attacks

blog.talosintelligence.com/blackbyte-blends-tried-and-true-tradecraft-with-newly-disclosed-vulnerabilities-to-support-ongoing-attacks/

James Nutland August 28, 2024

By James Nutland, Craig Jackson, Terryn Valikodath, Brennan Evans

Wednesday, August 28, 2024 06:00

- The BlackByte ransomware group continues to leverage tactics, techniques and procedures (TTPs) that have formed the foundation of its tradecraft since its inception, continuously iterating its use of vulnerable drivers to bypass security protections and deploying a self-propagating, wormable ransomware encryptor.
- In recent investigations, Talos IR has also observed BlackByte using techniques that depart from their established tradecraft, such as exploiting CVE-2024-37085 – an authentication bypass vulnerability in VMware ESXi – shortly after it was disclosed and using a victim's authorized remote access mechanism rather than deploying a commercial remote administration tool like AnyDesk.

- Talos IR observed a new iteration of the BlackByte encryptor that appends the file extension “blackbytent_h” to encrypted files, drops four vulnerable driver files compared to the previously observed three, and uses victim Active Directory credentials to self-propagate.
- Talos also assesses that the BlackByte group is more active than its data leak site may imply, where only 20 to 30 percent of successful attacks result in an extortion post.

BlackByte is a ransomware-as-a-service (RaaS) group believed to be an offshoot of the infamous Conti ransomware group. First observed in mid- to late-2021, their tradecraft includes the use of vulnerable drivers to bypass security controls, deployment of self-propagating ransomware with worm-like capabilities, and the use of known-good system binaries (LoLBins) and other legitimate commercial tools as part of their attack chain.

BlackByte has reengineered its ransomware binary over time, with versions written in Go, .NET, C++, or a combination of these languages. The group’s apparent efforts to continuously improve its tooling, operations and even its data leak site is well-documented.

During investigation of a recent BlackByte attack, Cisco Talos Incident Response (Talos IR) and Talos threat intelligence personnel noted close similarities between indicators of compromise (IOCs) discovered during the investigation and other events flagged in Talos’ global telemetry. Further investigation of these similarities provided additional insights into BlackByte’s current tradecraft and revealed that the group has been significantly more active than would appear from the number of victims published on its data leak site.

Technical details

Initial access

During Talos IR’s investigation into a recent BlackByte ransomware attack, the threat actor gained initial access using valid credentials to access the victim organization’s VPN. Limits in telemetry and loss of evidence following the ransomware encryption event prevented Talos IR from determining whether the credentials were obtained through brute-forcing of the VPN interface or had already been known by the adversary prior to the attack. However, Talos IR has moderate confidence that brute-force authentication facilitated via internet scanning was the initial access vector based on the following observations:

- The initial account compromised by the adversary had a basic naming convention and, reportedly, a weak password.
- The VPN interface may have allowed a domain account to authenticate without multi-factor authentication (MFA) if the target account had a specific Active Directory configuration.

- BlackByte has a history of scanning for and exploiting public-facing vulnerabilities, such as the ProxyShell vulnerability in Microsoft Exchange server.

Given BlackByte's history of exploiting public-facing vulnerabilities for initial access, the use of VPN for remote access may represent a slight shift in technique or could represent opportunism. The use of the victim's VPN for remote access also affords the adversary other advantages, including reduced visibility from the organization's EDR.

Reconnaissance and enumeration

After gaining initial access to the environment, the adversary managed to escalate privileges by compromising two Domain Admin-level accounts. One of these accounts was used to access the organization's VMware vCenter server and, shortly after, create Active Directory domain objects for individual VMware ESXi hypervisors, effectively joining those hosts to the domain. The same account was then used to create and add several other accounts to an Active Directory group called "ESX Admins." Talos IR assesses that this user group was created to exploit CVE-2024-37085, an authentication bypass vulnerability in VMware ESXi known to be used by multiple ransomware groups. Successful exploitation of this vulnerability grants members of a specific Active Directory group elevated privileges on an ESXi host, allowing for control over virtual machines (VMs), the ability to modify the host server's configuration, and access to system logs, diagnostics and performance monitoring tools.

Talos IR observed the threat actor leveraging this vulnerability, which initially received limited attention from the security community, within days of its publication. This highlights the speed with which ransomware groups like BlackByte can adapt their TTPs to incorporate newly disclosed vulnerabilities, and the level of time and effort put into identifying potential avenues for advancing an attack.

The threat actor accessed other systems, directories and files within each victim environment using protocols such as Server Message Block (SMB) and Remote Desktop Protocol (RDP). Analysis of system event and authentication logs revealed a consistent pattern where the threat actor primarily leveraged NT LAN Manager (NTLM) for authentication, while organizational users primarily used Kerberos. This early NTLM activity could reflect authentication attacks such as pass the hash for lateral movement. Dynamic analysis of the ransomware binary later revealed consistent use of NTLM for authentication by that file, as well.

Talos IR also observed the execution of a file called "atieclxx.exe" from the "C:\temp\sys\" directory on one of the file servers. The legitimate version of "atieclxx.exe" can normally be found in the "C:\Windows\System32" directory, where it supports system processes associated with AMD graphics cards. However, during the investigation of one BlackByte attack, "atieclxx.exe" was executed from the "C:\temp\sys" directory with the command

`atieclxx.exe P@$$w0rd123!!!`. Since BlackByte actors are known to favor the string "P@$$w0rd" when setting account passwords and as input parameters for custom tooling, this syntax may indicate efforts to disguise malware – such as their custom data exfiltration tool, ExByte – as a known or legitimate file. Talos IR could not obtain a copy of the file for analysis.

Finally, the threat actor was observed tampering with security tool configurations via system registry modifications, manually uninstalling EDR from multiple key systems, and, in one investigation, changing the root password for the organization's ESXi hosts. Immediately prior to the first sign of file encryption, increased volumes of NTLM authentication and SMB connection attempts were observed between dozens of systems in the environment. This activity was later understood to be characteristic of the ransomware's self-propagating mechanism.

Data exfiltration

Limitations in available telemetry, the effect of the ransomware encryption process, and the adversary's off-network staging location during Talos IR's investigation prevented a high-confidence assessment of data exfiltration methods, and whether exfiltration took place at all. As noted in previous sections, the possible use of BlackByte's custom data exfiltration tool, ExByte, was observed, but could not be confirmed.

Ransomware execution

Similarities to prior reports

In recent cases, the BlackByte ransomware binary, "host.exe," was executed from the same directory – "C:\Windows" – across all victims investigated by Talos IR. The command syntax used by the adversary during each attack – `C:\Windows\host.exe -s [8-digit numeric string] svc` – and the behavior of the ransomware binary is consistent with previous analysis of the BlackByteNT binary by Microsoft, DuskRise, Acronis and others. Observed commonalities included:

- The ransomware binary will not execute without the correct eight-digit numeric string passed to the "-s" parameter. This eight-digit string was the only part of the command syntax that differed between victims. In one attack, the adversary used two different encryptors sequentially, each with its own "-s" parameter value, though it was not clear why multiple encryptors were employed.
- The "svc" parameter causes the ransomware to install itself as a service, which appeared to convert an infected system into an additional spreader as part of the ransomware's wormable behavior. Subsequent SMB and NTLM authentications were observed against reachable hosts after the ransomware service was created, resulting in multiple waves of encryption hours after the initial event.

- The ransomware binary creates and operates primarily out of the “C:\SystemData” directory. Several common files are created in this directory across all BlackByte victims, including a text file called “MsExchangeLog1.log”, which appears to be a process tracking log where execution milestones are recorded as comma-separated “q”, “w”, and “b” values as shown in the following screenshot.

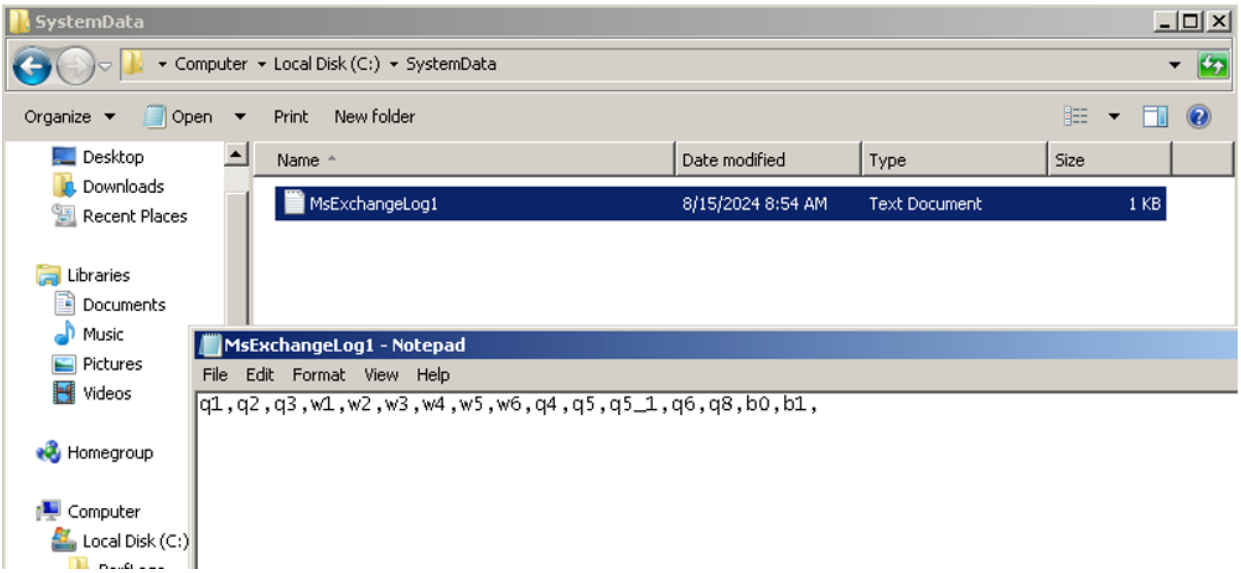

Figure 1: MsExchangeLog1.log contents mid-execution

Upon successful execution, the ransomware binary executed the command `/c ping 1.1.1[.]1 -n 10 > Nul & fsutil file setZeroData offset=0 length=503808 c:\windows\host.exe & Del c:\windows\host.exe /F /Q` which, after a delay, zeroes the contents of the file and deletes itself. This general command structure has been observed across various BlackByte tools since 2022.

Novel observations

Talos observed some differences in the recent BlackByte attacks. Most notably, encrypted files across all victims were rewritten with the file extension “blackbytent_h”, which has not yet appeared in public reporting.

This newer version of the encryptor also drops four vulnerable drivers as part of BlackByte’s usual Bring Your Own Vulnerable Driver (BYOVD) technique, which is an increase from the two or three drivers described in previous reports. The four drivers were dropped by the encryptor binary in all BlackByte attacks investigated by Talos IR, each with a similar naming convention – eight random alphanumeric characters followed by an underscore and an iterating number value. Using “AM35W2PH” as a fictitious example, the vulnerable drivers would appear in the same order as:

- “AM35W2PH” – RtCore64.sys, a driver originally used by MSI Afterburner a system overclocking utility.

- “AM35W2PH_1” – DBUtil_2_3.sys, a driver that is part of the Dell Client firmware update utility.
- “AM35W2PH_2” – zamguard64.sys, a driver that is part of the Zemana Anti-Malware (ZAM) application.
- “AM35W2PH_3” – gdrv.sys, a driver that is part of the GIGABYTE Tools software package for GIGABYTE motherboards.

The inclusion of the “zamguard64.sys” file, which is also known as “Terminator,” is particularly interesting because of recentreporting from other security researchers about its prevalence and also because the ransomware binary created two service-related registry keys associated with that file during execution, then deleted them later in the execution process. Using the same fictitious string above, those registry keys would be:

· HKLM\SYSTEM\CONTROLSET001\SERVICES\AM35W2PH_2

· HKLM\SYSTEM\CONTROLSET001\SERVICES\AM35W2PH_2\SECURITY

During dynamic analysis of multiple BlackByte ransomware binaries, Talos found that the file attempted network share enumeration via the ‘SRVSVC’ named pipe’s NetShareEnumAll function using specific user accounts associated with the victim. Since this analysis was conducted in a controlled, sandboxed environment, these accounts could only appear in network traffic if they were built into the ransomware binary itself. This finding gives Talos high confidence that BlackByte’s per-victim customization of the ransomware encryptor includes packing some form of stolen credential into the binary to support its worm capability.

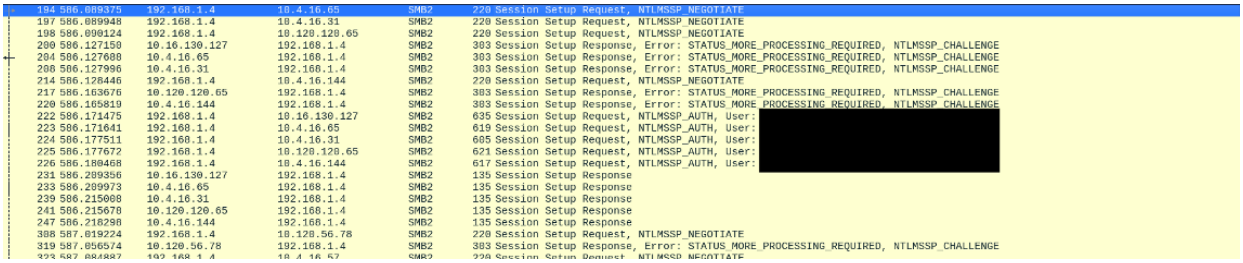

Figure 2: Victim credentials observed during ransomware execution in an isolated sandbox environment

Other behaviors of interest observed during dynamic analysis of this version of the ransomware binary included:

- Communication with msdl.microsoft[.]com via IP address 204.79.197[.]219 early in the execution process. This site is associated with the Microsoft Public Symbol Server. BlackByte tools have long been observed downloading and saving debugging symbols directly from Microsoft.

- Disabling antivirus and anti-spyware protections via the HKLM\SOFTWARE\MICROSOFT\WINDOWS DEFENDER registry key and adding the value "*.exe" to the HKLM\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\EXTENSIONS registry key.
- Deletion of system binaries from the "C:\Windows\System32" directory, including "taskmgr.exe", "perfmon.exe", "shutdown.exe", and "resmon.exe".

A broad view of BYOVD use and BlackByte victimology

Talos pivoted on the vulnerable drivers identified during this analysis, extrapolating findings from endpoint telemetry to establish a strategic picture of BYOVD exposure across various industry verticals. Our findings highlight that the professional, scientific, and technical services sectors have the greatest exposure to the observed vulnerable drivers, accounting for 15 percent of the total (see Figure 1). Analysis of the exposure reveals that certain industries are at more risk than others, such as those that are more likely to store and/or process critical or sensitive data.

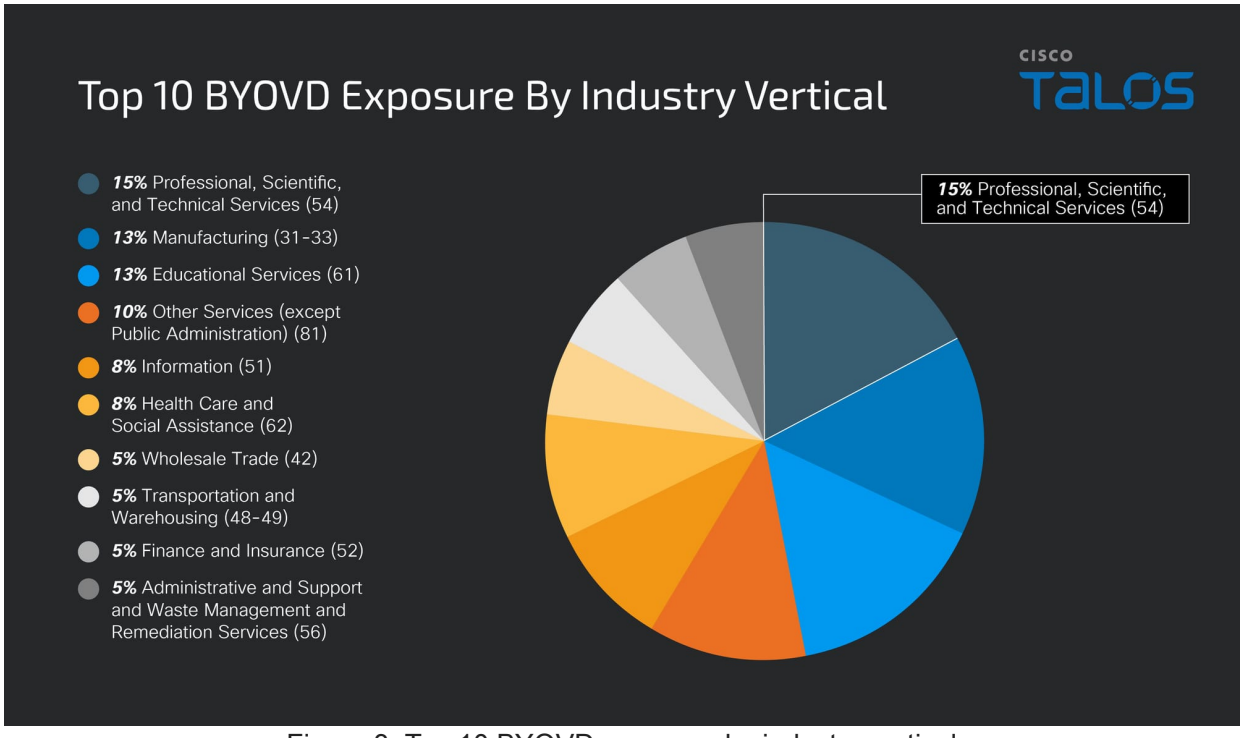

Figure 3: Top 10 BYOVD exposure by industry vertical

BlackByte's victimology aligns with this assessment, with over 32 percent of known victims falling into the manufacturing industry vertically.

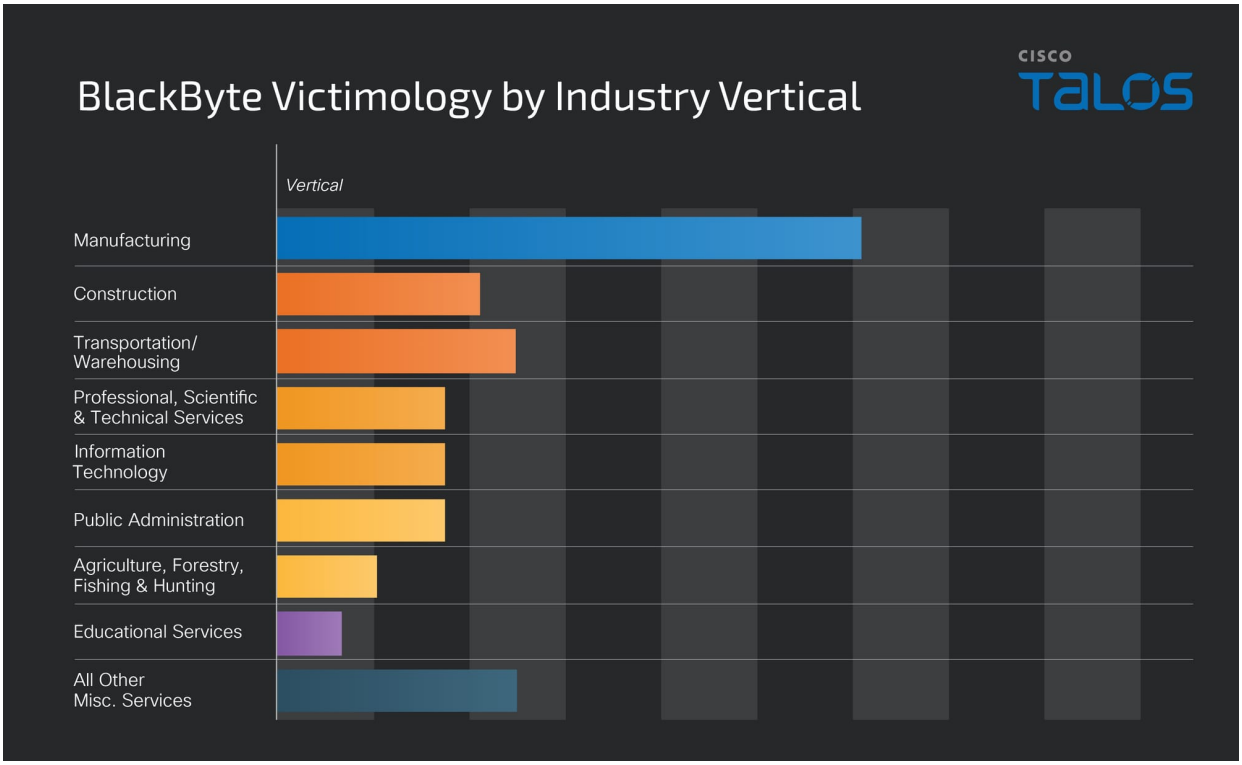

Figure 4: BlackByte victimology by industry vertical

These are likely conservative figures given the disparity between the number of victims published on BlackByte's data leak site over the past six to nine months and the number of victims found in telemetry and disclosed in public reporting. It is not clear why only a limited subset – an estimated 20 to 30 percent – of BlackByte's victims are eventually posted.

Implications for defenders

BlackByte's progression in programming languages from C# to Go and subsequently to C/C++ in the latest version of its encryptor – BlackByteNT – represents a deliberate effort to increase the malware's resilience against detection and analysis. Complex languages like C/C++ allow for the incorporation of advanced anti-analysis and anti-debugging techniques, which have been observed across the BlackByte tooling during detailed analysis by other security researchers.

The self-propagating nature of the BlackByte encryptor creates additional challenges for defenders. The use of the BYOVD technique compounds these challenges since it may limit the effectiveness of security controls during containment and eradication efforts. However, since this current version of the encryptor appears to rely on built-in credentials stolen from the victim environment, an enterprise-wide user credential and Kerberos ticket reset should be highly effective for containment. Review of SMB traffic originating from the encryptor during execution will also reveal the specific accounts used to spread the infection across the network.

Taking a wider view of ransomware tradecraft shows that the inherent flexibility of the overarching RaaS model allows threat actors to quickly counter new defensive strategies developed by cybersecurity experts by iterating and updating its tooling. This creates an ongoing arms race between cybercriminals and defenders. As BlackByte and other ransomware groups continue to evolve, organizations will need to invest in adaptive, resilient security controls and build out measures that can keep pace with a dynamic, diverse threat landscape.

Recommendations for defenders

- **Implement MFA for all remote access and cloud connections**. Prioritize “verified push” as the MFA method over less secure options such as SMS or phone call.
- **Audit VPN Configuration.** Confirm that legacy VPN policies are removed, and that authentication attempts not matching a current VPN policy are denied by default. Restrict VPN access to only necessary network segments and services, limiting exposure of critical assets like Domain Controllers.
- **Set up alerts for any changes in privileged groups**, such as the creation of new user groups or addition of accounts to domain administrators. Ensure that administrative privileges are granted only when necessary and routinely audited thereafter. A Privileged Access Management (PAM) solution may be used to streamline control and monitoring of privileged accounts.
- **Limit or disable the use of NTLM** where possible and enforce more secure authentication methods like Kerberos instead. Limit the rate of authentication attempts and failures on public-facing and internal interfaces to prevent automated authentication scanning.
- **Disable SMBv1 and enforce SMB signing** and encryption to protect against lateral movement and malware propagation.
- **Deploy EDR clients to all systems throughout the environment**. Configure an administrator password on EDR clients to prevent unauthorized tampering or removal of the client.
- **Disable vendor accounts and remote access capabilities** when not actively in use.
- **Create detections for unauthorized configuration changes** that may be made on various systems in the environment, including changes to Windows Defender policies, unauthorized changes to Group Policy Objects, and creation of unusual scheduled tasks and installed services.
- **Develop and document procedures for enterprise password reset** to ensure that all user credentials can be reset quickly and completely. Include procedures for rolling critical Kerberos tickets in this documentation.
- **Harden and patch ESX hosts** to reduce the attack surface of these critical servers to the extent possible and ensure that newly discovered vulnerabilities are corrected as quickly as possible.

MITRE ATT&CK Mapping of New TTPs

Tactic:	Technique ID:	Tactic, Technique, Sub-Technique Description:
Initial Access	T1078.002	Initial Access: Valid Accounts: Domain Accounts
	T1078.003	Valid Accounts: Local Accounts
Discovery	T1018	Discovery: Remote System Discovery
	T1083	Discovery: File and Directory Discovery
Persistence	T1136.002	Persistence: Create Account: Domain Account
Execution	T1204	Execution: User Execution
	T1569.002	Execution: System Services: Service Execution
Privilege Escalation	T1543	Privilege Escalation: Create or Modify System Process
	T1484.001	Privilege Escalation: Domain Policy Modification
	T1484	Privilege Escalation: Domain Modification
	T1098	Privilege Escalation: Account Manipulation
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares
	T1021.001	Remote Services: Remote Desktop Protocol
	T1210	Exploitation of Remote Services
Resource Development	T1608	Resource Development: Stage Capabilities

Defense Evasion	T1562.001	Defense Evasion: Impair Defenses: Disable or Modify Tools
	T1112	Defense Evasion: Modify Registry
	T1070.004	Defense Evasion: Indicator Removal: File Deletion
	T1211	Defense Evasion: Exploitation for Defense Evasion
Impact	T1529	Impact: System Shutdown/Reboot
	T1486	Impact: Data Encrypted for Impact

IOCs

NOTE: Certain IOCs have been withheld to prevent potential victim identification.

RtCore64.sys – 01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd

DBUtil_2_3.sys – 0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5

zamguard64.sys – 543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

gdrv.sys – 31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427