DEV-0569 finds new ways to deliver Royal ransomware, various payloads

microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

November 17, 2022

Recent activity from the threat actor that Microsoft tracks as DEV-0569, known to distribute various payloads, has led to the deployment of the Royal ransomware, which first emerged in September 2022 and is being distributed by multiple threat actors. Observed DEV-0569 attacks show a pattern of continuous innovation, with regular incorporation of new discovery techniques, defense evasion, and various post-compromise payloads, alongside increasing ransomware facilitation.

DEV-0569 notably relies on malvertising, phishing links that point to a malware downloader posing as software installers or updates embedded in spam emails, fake forum pages, and blog comments. In the past few months, Microsoft security researchers observed the following tweaks in the group's delivery methods:

- Use of contact forms on targeted organizations' websites to deliver phishing links
- Hosting fake installer files on legitimate-looking software download sites and legitimate repositories to make malicious downloads look authentic to targets, and
- Expansion of their malvertising technique by using Google Ads in one of their campaigns, effectively blending in with normal ad traffic

These methods allow the group to potentially reach more targets and ultimately achieve their goal of deploying various post-compromise payloads. DEV-0569 activity uses signed binaries and delivers encrypted malware payloads. The group, also known to rely heavily on defense evasion techniques, has continued to use the open-source tool *Nsudo* to attempt disabling antivirus solutions in recent campaigns.

In this blog we share details of DEV-0569's tactics, techniques, and procedures (TTPs) and observed behavior in recent campaigns, which show that DEV-0569 will likely continue leveraging malvertising and phishing for initial access. We also share preventive measures that organizations can adopt to thwart DEV-0569's delivery methods involving malicious links and phishing emails using solutions like Microsoft Defender SmartScreen and Microsoft Defender for Office 365, and to reduce the impact of the group's follow-on activities. Microsoft Defender for Endpoint detects the DEV-0569 behavior discussed in this blog, including the code signing certificates in use and the attempts to disable Microsoft Defender Antivirus.

Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or developing cluster of threat activity, allowing Microsoft to track it as a unique set of information until we can reach high confidence about the origin or identity of the actor behind the activity. Once it meets defined criteria, a DEV group is converted to a named actor.

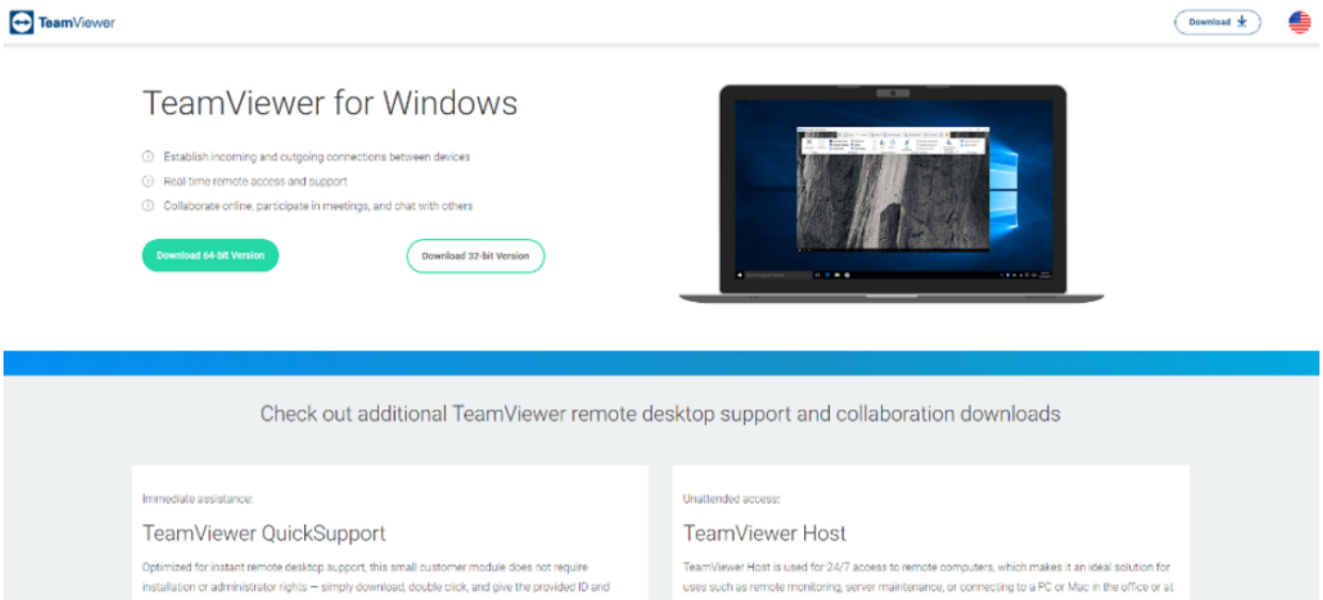
DEV-0569 attack chain: Delivery tactics tweaked

DEV-0569 has multiple methods for delivery of their initial payload. In some cases, DEV-0569 payloads are delivered via phishing campaigns run by other malicious actors that offer delivery of malware payloads as a service.

Historical observation of typical DEV-0569 attack begins with malicious links delivered to targets via malicious ads, fake forum pages, blog comments, or through phishing emails. These links lead to malicious files signed by the attacker using a legitimate certificate. The malicious files, which are malware downloaders known as BATLOADER, pose as installers or updates for legitimate applications like Microsoft Teams or Zoom. When launched, BATLOADER uses MSI Custom Actions to launch malicious PowerShell activity or run batch scripts to aid in disabling security solutions and lead to the delivery of various encrypted malware payloads that is decrypted and launched with PowerShell commands.

Posing as legitimate software download sites

From August to October 2022, Microsoft observed DEV-0569 activity where BATLOADER, delivered via malicious links in phishing emails, posed as legitimate installers for numerous applications like TeamViewer, Adobe Flash Player, Zoom, and AnyDesk. BATLOADER was hosted on attacker-created domains posing as legitimate software download sites (*anydeskos[.]com,* for example) and on legitimate repositories like GitHub and OneDrive. Microsoft takes down verified malicious content from these repositories as they are found or reported.



TeamViewer for Windows

- Establish incoming and outgoing connections between devices
- Real-time remote access and support
- Collaborate online, participate in meetings, and chat with others

Check out additional TeamViewer remote desktop support and collaboration downloads

Immediate assistance:

TeamViewer QuickSupport

Optimized for instant remote desktop support, this small customer module does not require installation or administrator rights — simply download, double click, and give the provided ID and

Unattended access:

TeamViewer Host

TeamViewer Host is used for 24/7 access to remote computers, which makes it an ideal solution for uses such as remote monitoring, server maintenance, or connecting to a PC or Mac in the office or at

Figure 1. DEV-0569 activity seen in September 2022, where the landing site hosted BATLOADER posing as a TeamViewer installer

Use of VHD file formats

Aside from using installer files, Microsoft has also observed the use of file formats like Virtual Hard Disk (VHD) impersonating legitimate software for first-stage payloads. These VHDs also contain malicious scripts that lead to the download of DEV-0569's malware payloads.

PowerShell and batch scripts for downloading

DEV-0569 has used varied infection chains using PowerShell and batch scripts that ultimately led to the download of malware payloads like information stealers or a legitimate remote management tool used for persistence on the network. The management tool can also be an access point for the staging and spread of ransomware.

NSudo to disable antivirus solutions

DEV-0569 also continues to tamper with antivirus products. In September and October 2022, Microsoft saw activity where DEV-0569 used the open-source NSudo tool to attempt disabling antivirus solutions.

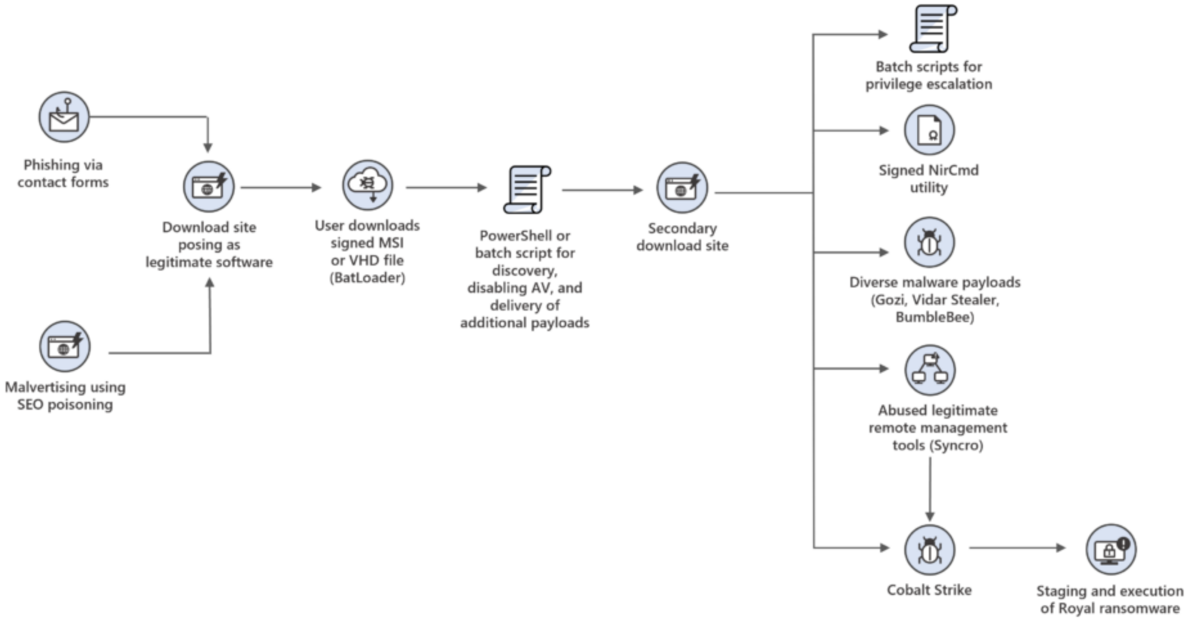

Phishing via contact forms
Malvertising using SEO poisoning
Download site posing as legitimate software
User downloads signed MSI or VHD file (BatLoader)
PowerShell or batch script for discovery, disabling AV, and delivery of additional payloads
Secondary download site
Batch scripts for privilege escalation
Signed NirCmd utility
Diverse malware payloads (Gozi, Vidar Stealer, BumbleBee)
Abused legitimate remote management tools (Syncro)
Cobalt Strike
Staging and execution of Royal ransomware

Figure 2. High-level view of observed DEV-0569 infection chains between August to October 2022

September 2022: Adopting contact forms to gain access to targets and deliver information stealers

In September 2022, Microsoft observed a campaign using contact forms to deliver DEV-0569 payloads. Using contact forms on public websites to distribute malware has been seen in other campaigns, including IcedID malware. Attackers use this technique as a defense evasion method since contact forms can bypass email protections and appear trustworthy to the recipient.

In this campaign, DEV-0569 sent a message to targets using the contact form on these targets' websites, posing as a national financial authority. When a contacted target responds via email, DEV-0569 replied with a message that contained a link to BATLOADER. Microsoft Defender for Office 365 detects the spoofing behavior as well as the malicious links in these emails.

The malicious links in the contact forms led to BATLOADER malware hosted on abused web services like GitHub and OneDrive. The installers launched a PowerShell script that issued multiple commands, including downloading a *NirCmd* command-line utility provided by freeware developer NirSoft:

```
nircmd elevatecmd exec hide "requestadmin.bat"
```

If successful, the command allows the attacker to elevate from local admin to SYSTEM rights, similar to executing a scheduled task as SYSTEM.

The PowerShell script also delivered additional executables from a remote website (e.g., *updateea1[.]com*), including an AES-encrypted Gozi banking trojan and the information stealer known as Vidar Stealer, which used Telegram to receive command and control (C2) information. DEV-0569 frequently diversifies their payloads and has shifted from delivering ZLoader at the beginning of 2022, possibly in response to disruption efforts against Zloader in April 2022.

September 2022: Deploying Royal ransomware

Microsoft identified instances involving DEV-0569 infection chains that ultimately facilitated human-operated ransomware attacks distributing Royal ransomware. Based on tactics observed by Microsoft, ransomware attackers likely gained access to compromised networks via a BATLOADER-delivered Cobalt Strike Beacon implant.

DEV-0569's widespread infection base and diverse payloads likely make the group an attractive access broker for ransomware operators.

October 2022: Leveraging Google Ads to deliver BATLOADER selectively

In late October 2022, Microsoft researchers identified a DEV-0569 malvertising campaign leveraging Google Ads that point to the legitimate traffic distribution system (TDS) Keitaro, which provides capabilities to customize advertising campaigns via tracking ad traffic and user- or device-based filtering. Microsoft observed that the TDS redirects the user to a legitimate download site, or under certain conditions, to the malicious BATLOADER download site. Microsoft reported this abuse to Google for awareness and consideration for action.

Using Keitaro, DEV-0569 can use traffic filtering provided by Keitaro to deliver their payloads to specified IP ranges and targets. This traffic filtering can also aid DEV-0569 in avoiding IP ranges of known security sandboxing solutions.

Defending against DEV-0569

DEV-0569 will likely continue to rely on malvertising and phishing to deliver malware payloads. Solutions such as network protection and Microsoft Defender SmartScreen can help thwart malicious link access. Microsoft Defender for Office 365 helps guard against phishing by inspecting the email body and URL for known patterns. Since DEV-0569's phishing scheme abuses legitimate services, organizations can also leverage mail flow rules to capture suspicious keywords or review broad exceptions, such as those related to IP ranges and domain-level allow lists. Enabling Safe Links for emails, Microsoft Teams, and Office Apps can also help address this threat.

Defenders can also apply the following mitigations to reduce the impact of this threat:

- Encourage users to use Microsoft Edge and other web browsers that support SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware. Turn on network protection to block connections to malicious domains and IP addresses.
- Build organizational resilience against email threats by educating users about identifying social engineering attacks and preventing malware infection. Use Attack simulation training in Microsoft Defender for Office 365 to run attack scenarios, increase user awareness, and empower employees to recognize and report these attacks.
- Practice the principle of least-privilege and maintain credential hygiene. Avoid the use of domain-wide, admin-level service accounts. Restricting local administrative privileges can help limit installation of RATs and other unwanted applications.
- Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Turn on tamper protection features to prevent attackers from stopping security services.

Microsoft Defender customers can turn on attack surface reduction rules to prevent common attack techniques used in ransomware attacks:

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

NSudo activity is detected by the tamper protection capability as:

- Nsudo file drop
- Nsudo runtime
- Nsudo AV tampering commandline

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

> Ransomware-linked DEV-0569 activity group

While the following alerts might indicate activity associated with this threat, they could also be triggered by unrelated threat activity:

- Ransomware-linked DEV-0858 activity group
- Cobalt Strike activity detected
- Cobalt Strike activity observed
- Cobalt Strike artifact observed
- Cobalt Strike attack tool
- Cobalt strike named pipes
- ‘Vidar’ credential theft malware was detected
- ‘VidarStealer’ malware was detected
- ‘Gozi’ malware was detected
- An active ‘Nsudo’ hacktool in a command line was detected while executing
- An active ‘NSudo’ hacktool process was detected while executing