

GOLD BLADE's strategic evolution – Sophos News

news.sophos.com/en-us/2025/12/05/sharpening-the-knife-gold-blades-strategic-evolution

Morgan Demboski

December 05, 2025



Between February 2024 and August 2025, Sophos analysts investigated nearly 40 intrusions related to STAC6565, a campaign the analysts assess with high [confidence](#) is associated with the [GOLD BLADE](#) threat group (also known as RedCurl, RedWolf, and Earth Kapre). This campaign reflects an unusually narrow geographic focus for the group, with almost 80% of the attacks targeting Canadian organizations. Once focused primarily on cyberespionage, GOLD BLADE has evolved its activity into a hybrid operation that blends data theft with selective ransomware deployment via a custom locker named QWCrypt.

GOLD BLADE continually refines its intrusion methods and has shifted from traditional phishing emails to abusing recruitment platforms to deliver weaponized resumes. Its operations follow a rhythm of dormancy followed by sudden bursts of activity, with each wave introducing newly developed or adapted tradecraft. The threat actors have modified the RedLoader infection chain multiple times to test different combinations of payload formats, execution mechanisms, and locations to host malicious files. They also implemented a Bring Your Own Vulnerable Driver (BYOVD) chain involving renamed Zemana drivers and modified versions of the Terminator endpoint detection and response (EDR) killer tool to evade detection.

The enigma known as GOLD BLADE

Since emerging in 2018, GOLD BLADE has been linked to attacks aimed at stealing sensitive business information, credentials, and emails. The targeted nature of its operations and the lack of a data leak site (DLS) suggest the group conducts tailored intrusions on behalf of clients under a “hack-for-hire” model. In April 2025, Sophos analysts observed the group selectively deploying QWCrypt ransomware, which was first [reported](#) by Bitdefender the previous month. Sophos analysts have continued to see GOLD BLADE deploy the ransomware against select victims, indicating the threat actors may be independently monetizing intrusions in addition to conducting espionage for clients.

GOLD BLADE’s ability to cycle through delivery methods and refine its techniques over time reflects a professionalized operation that treats intrusions as a core service requiring routine updates to maintain effectiveness. However, the group does not neatly fit into a conventional threat category. While it is financially motivated, GOLD BLADE’s discreet extortion strategy, long-running campaigns, and evolving tradecraft differentiate it from many other cybercriminal groups. At the same time, there is no evidence of the group being state-sponsored or politically motivated. There is also little known about where the threat actors are based. Though some [third-parties](#) report that GOLD BLADE is a Russian-speaking group, Sophos analysts have not found sufficient evidence to confirm or deny that assessment at this time.

Attack tempo and victimology

Sophos analysts observed notable iterations of GOLD BLADE’s RedLoader delivery chain in September 2024, March 2025, and July 2025, each of which was preceded by one to two months of inactivity (see Figure 1). For example, after the March spike in incidents and the QWCrypt attack in April, the group appeared to go on a hiatus, only to resume activity in July with novel combinations of prior techniques. Although this pattern is based solely on Sophos visibility, it likely reflects development time for new attack chains and responses to external reporting of the group’s methods. Group-IB [reported](#) a similar pattern in 2021, describing the group hibernating for seven months before conducting a wave of attacks using improved tactics.

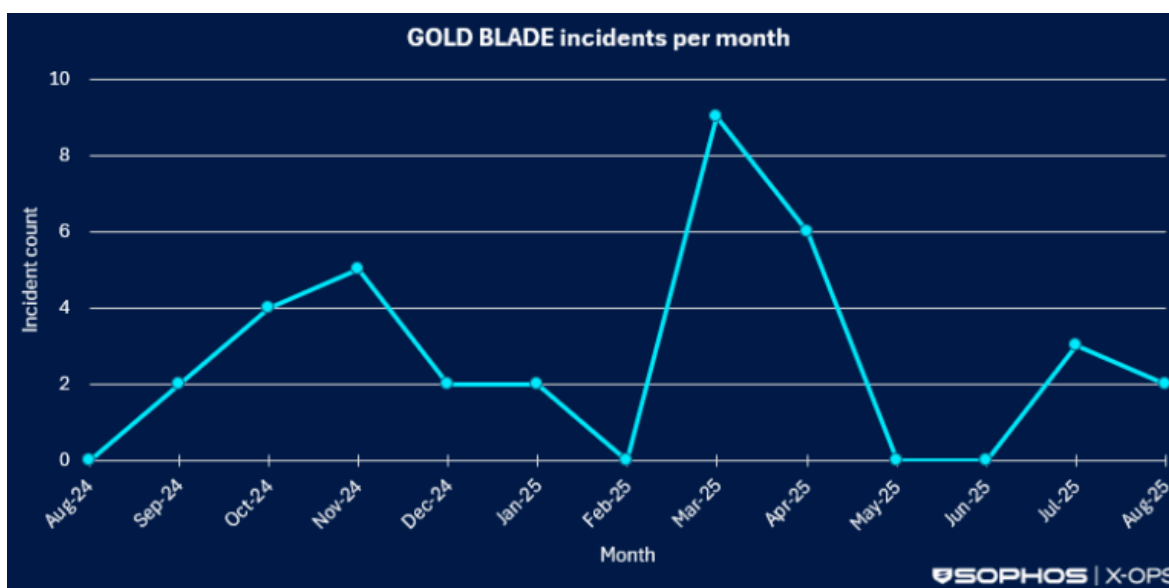


Figure 1: Observed GOLD BLADE activity from August 2024 through August 2025

Analysis of STAC6565 victimology suggests that GOLD BLADE has narrowed its targeting to focus almost exclusively on organizations based in North America. Nearly 80% of GOLD BLADE attacks linked to the STAC6565 campaign targeted Canada-based organizations. The U.S. ranked second with 14% (see Figure 2).

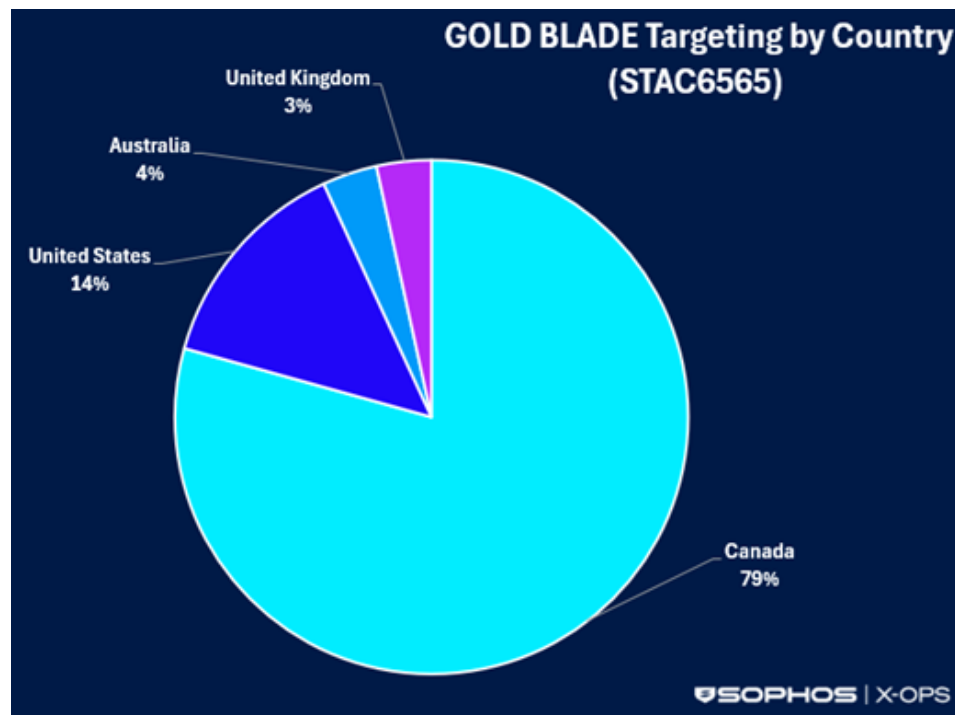


Figure 2: GOLD BLADE targeting by country from February 2024 through August 2025

Industry-specific targeting was much less concentrated and spanned over a dozen sectors. Services organizations were targeted in 21% of the incidents, followed by manufacturing, retail, and technology (see Figure 3).

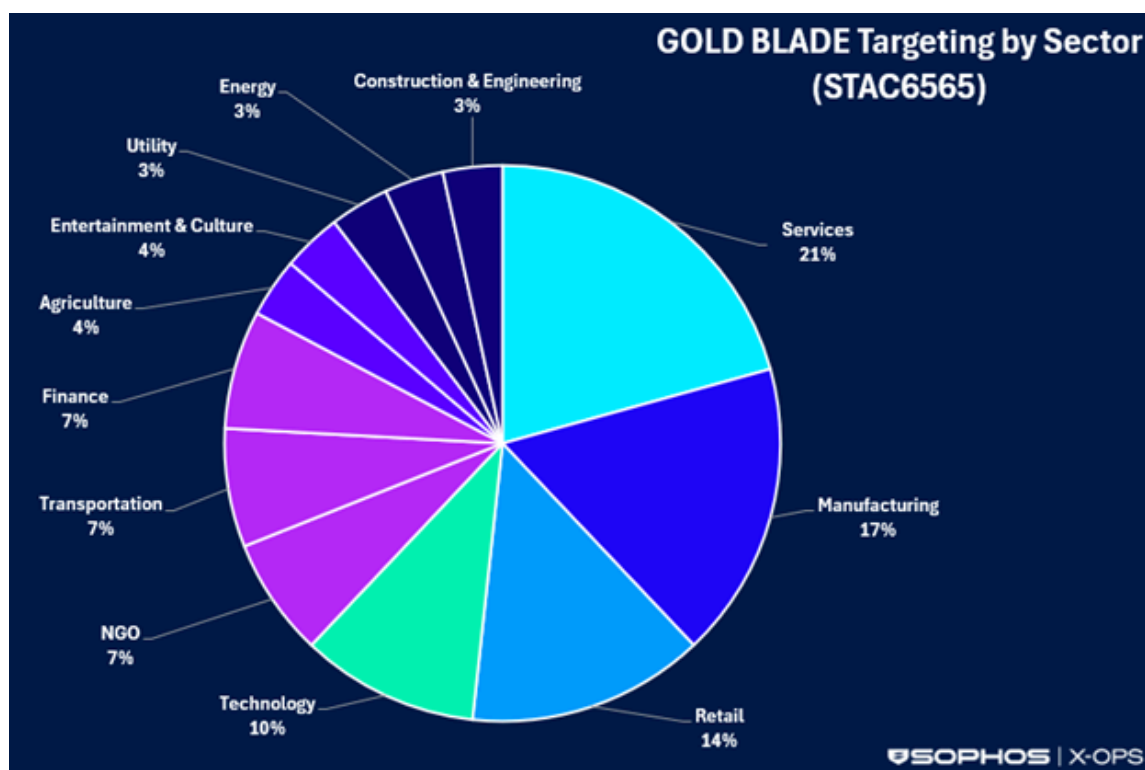


Figure 3: GOLD BLADE targeting by sector from February 2024 through August 2025

GOLD BLADE's activity appears to be targeted rather than opportunistic. Based on the tailored resume filenames used in their phishing lures and repeated attempts to compromise the same organizations over weeks or months, the threat actors likely conduct passive open-source intelligence (OSINT) to identify desirable targets or to collect information on organizations specified by their clients.

Initial access

GOLD BLADE historically targeted human resources (HR) personnel by sending well-crafted spearphishing emails containing malicious documents disguised as resumes, curricula vitae (CVs), or cover letters from purported job applicants. Since at least September 2024, the threat actors have made a tactical shift from phishing emails to abusing third-party recruitment platforms such as Indeed, JazzHR, and ADP WorkforceNow to distribute their malicious payloads.

This approach of submitting weaponized resumes through recruitment platforms may represent a notable evolution in HR-themed social engineering. Many threat groups have delivered malware via job-application lures by communicating with HR staff via email, LinkedIn, or Indeed to drive them to external phishing sites. However, GOLD BLADE skips this interaction step and relies on recruiters' trust in the applicant-tracking system. As recruitment platforms enable HR staff to review all incoming resumes, hosting payloads on these platforms and delivering them via disposable email domains not only increases likelihood that the documents will be opened but also evades detection by email-based protections.

The initial lure used in the STAC6565 campaign is often a resume submitted as a PDF to the target's external recruitment portal (see Figure 4). These PDFs are either weaponized directly or link to externally hosted content.

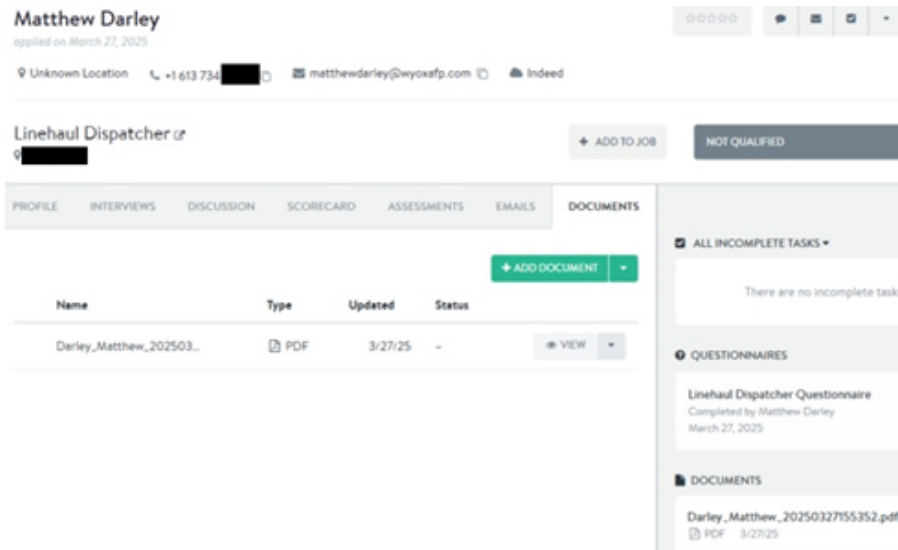
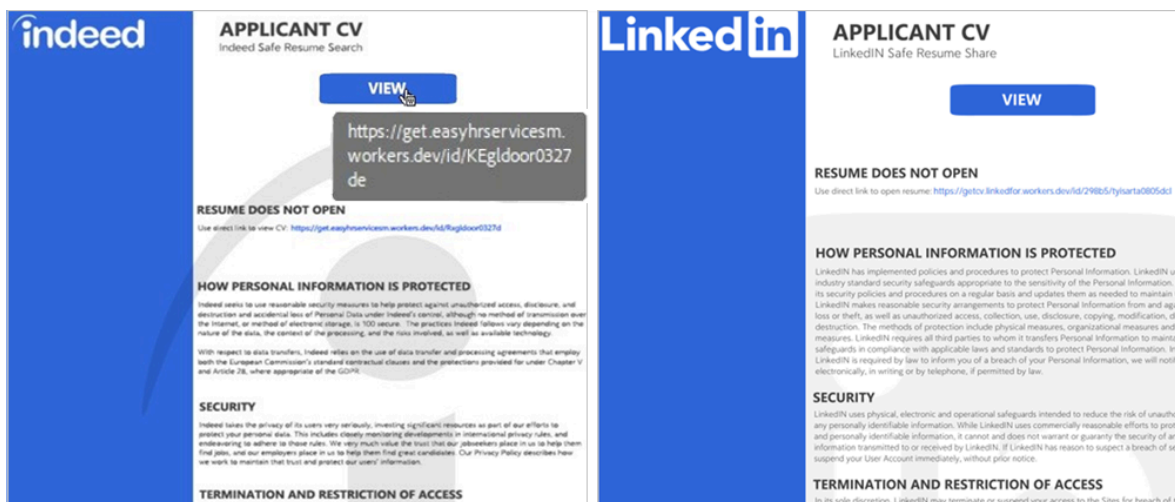


Figure 4: Fake resume uploaded to the JazzHR external recruitment platform

In the April QWCrypt incident, an HR employee’s attempt to view the PDF resulted in a fake Indeed Safe Resume Share Service page displaying a “Resume does not open” message. Hovering the cursor over the “View” button revealed the lure domain. When clicked, the link redirected the employee to a fake HR services site to view the resume (see Figure 5). In August 2025, Sophos observed the threat actors reusing this Safe Resume Share Service template for a LinkedIn-themed lure.



RedLoader delivery chain

When downloaded, the weaponized resume launches a multi-stage infection chain that delivers GOLD BLADE’s custom RedLoader malware. Sophos analysts track the RedLoader delivery chain in three distinct stages: initial execution, secondary payload deployment, and full malware installation.

Sophos first observed RedLoader being deployed in February 2024 in an attack chain that overlapped with Trend Micro observations [reported](#) the following month. However, a RedLoader infection in September 2024 introduced an alternative delivery chain that continued to evolve over the following year. By July 2025, Sophos analysts [observed](#) GOLD BLADE combining prior methods into a novel, unreported delivery chain (see Figure 6).

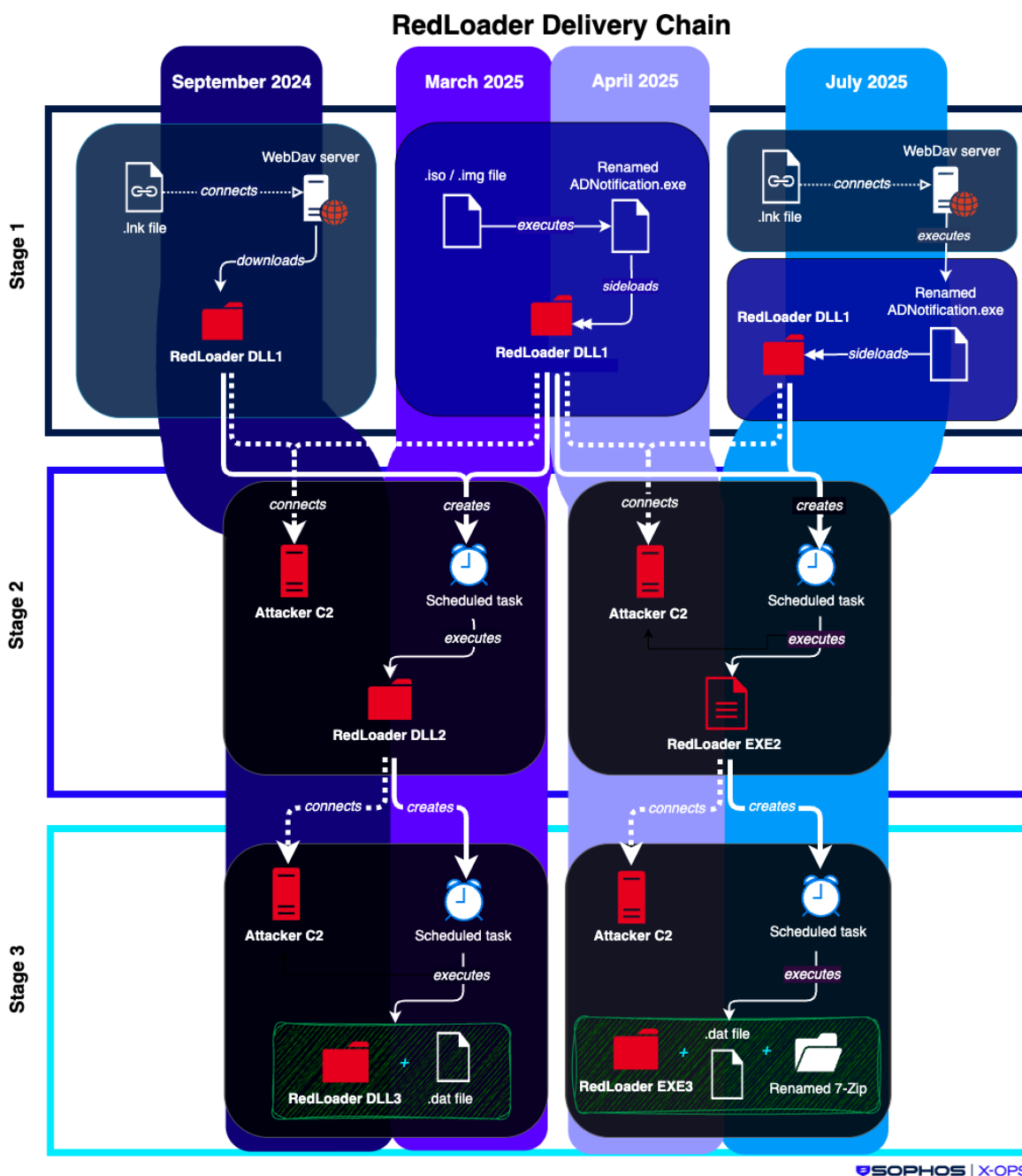


Figure 6: Progressive iterations of the RedLoader delivery chain from September 2024 to July 2025

Stage 1: Initial execution

The first stage of the delivery chain begins with the weaponized resume PDF dropping a .zip file, followed by one of three methods to deliver the initial RedLoader payload as a DLL:

- Method 1 (September 2024): The fake resume drops a ZIP archive containing a .lnk file disguised as a PDF. The .lnk file uses rundll32.exe to retrieve the initial RedLoader DLL from a WebDAV server hosted behind a Cloudflare Workers domain. The DLL is executed in memory via a “rundll32.exe <GUID>.dll,CplApplet” command. By fetching payloads over WebDAV from a domain hosted under Cloudflare Workers, the threat actors limit disk artifacts while also hiding the origin of the payload.

- Method 2 (March 2025, April 2025): The fake resume drops a ZIP archive containing an .iso or .img file. When clicked, the .iso or .img file is auto mounted as a virtual drive that contains a renamed copy of the legitimate ADNotificationManager.exe file (e.g., CV Applicant <GUID>.exe, CV Applicant ID <GUID>.scr). Execution of the legitimate file [sideloads](#) the initial RedLoader DLL (srvcli.dll or netutils.dll).
- Method 3 (July 2025): This method combines methods 1 and 2. The fake resume drops a ZIP archive containing a .lnk file disguised as a PDF. The .lnk file uses rundll32.exe to retrieve a renamed copy of ADNotificationManager.exe (CV-APP-<GUID>.exe) from a WebDAV server hosted behind a Cloudflare Workers domain. Execution of the legitimate file remotely sideloads the initial RedLoader DLL (srvcli.dll or netutils.dll) from the same WebDAV path. While GOLD BLADE previously assigned a unique subdomain for each victim, multiple July 2025 incidents reused the same workers[.]dev domain (e.g., automatinghrservices[.]workers[.]dev).

When executed, the initial RedLoader DLL opens a decoy Indeed login page using a distinctive User-Agent string previously attributed to GOLD BLADE (Mozilla/5.0 (Windows NT; Windows NT 10.0;) WindowsPowerShell/5.1.20134.790).

Stage 2: Secondary payload deployment

The first-stage DLL connects to an external C2 server before creating a scheduled task to download and execute the second-stage payload, which is staged in the C:\Users\<username>\AppData\Roaming\ directory. The scheduled task and filename of the second-stage malware often use a browser-themed naming pattern (e.g., BrowserEngineUpdate, BrowserSMP, BrowserQE) followed by a Base64-encoded computer name.

While GOLD BLADE's use of the Program Compatibility Assistant (pcalua.exe) living-off-the-land binary ([LOLBin](#)) for payload execution has remained the same, the format of both the second- and third-stage payloads shifted in April 2025 from DLLs to standalone executables.

- September 2024 and March 2025: The scheduled task launches pcalua.exe, which invokes rundll32.exe to deliver the second-stage payload as a DLL.
- April 2025 and July 2025: The scheduled task launches pcalua.exe and a conhost.exe –headless argument to deliver the second-stage payload as a standalone executable. While the executable name is victim-specific, all July 2025 samples observed by Sophos analysts share the same SHA256 hash (f5203c7ac07087fd5029d83141982f0a5e78f169cdc4ab9fc097cc0e2981d926).

Stage 3: Full malware installation

Following deployment of the secondary payload, the attackers appear to selectively choose which compromised systems receive the final RedLoader payload. In a July incident, Sophos analysts observed the second-stage payload beacon to the C2 infrastructure without proceeding to stage three, while other victims compromised during the same timeframe received the third-stage payload.

After connecting to a different external C2 server than the initial RedLoader DLL, the second-stage malware creates a new scheduled task to download and execute the final RedLoader payload, which is also typically staged in the C:/Users/<username>/AppData/Roaming directory. The scheduled task name format is a string of words (e.g., HybridDriveCacheRebalance, RegisterDevicePolicyChange, LicenseAcquisition,

FODCleanupTask) followed by a pseudo-random alphanumeric substring from the final payload filename. As in other files, the strings used in both the third-stage malware filename and scheduled task name vary across victims, suggesting GOLD BLADE may be using victim or build-specific IDs to track deployments.

- September 2024 and March 2025: The third-stage payload is delivered as a DLL alongside a malicious .dat file. The scheduled task executes the payload by running a “rundll32.exe <GUID>.dll,CPIApplet” command or by launching pcalua.exe, which invokes rundll32.exe to load the DLL.
- April 2025 and July 2025: The third-stage payload is delivered as a standalone executable alongside a malicious .dat file and a renamed 7-Zip file. The scheduled task executes the payload by launching pcalua.exe.

The payload parses the malicious .dat file and checks internet connectivity. It then connects to another attacker-controlled C2 server to create and run a .bat script that automates system discovery. The script unpacks Sysinternals AD Explorer and runs commands to gather details such as host information, disks, processes, and installed antivirus (AV) products. The script compresses the results into encrypted, password-protected archives via 7-Zip and transfers the data to an attacker-controlled WebDAV server.

Command and control (C2)

In the STAC6565 campaign, Sophos analysts observed GOLD BLADE deploying RPivot for C2 communications. RPivot is an open-source reverse proxy that tunnels traffic into internal networks via SOCKS4. The threat actors download the SOCKS proxy as a Python script named sra.py or osr.py. A .bat file then executes the script to establish a connection to remote IP address 109[.]206[.]236[.]209, with the ports differing across incidents.

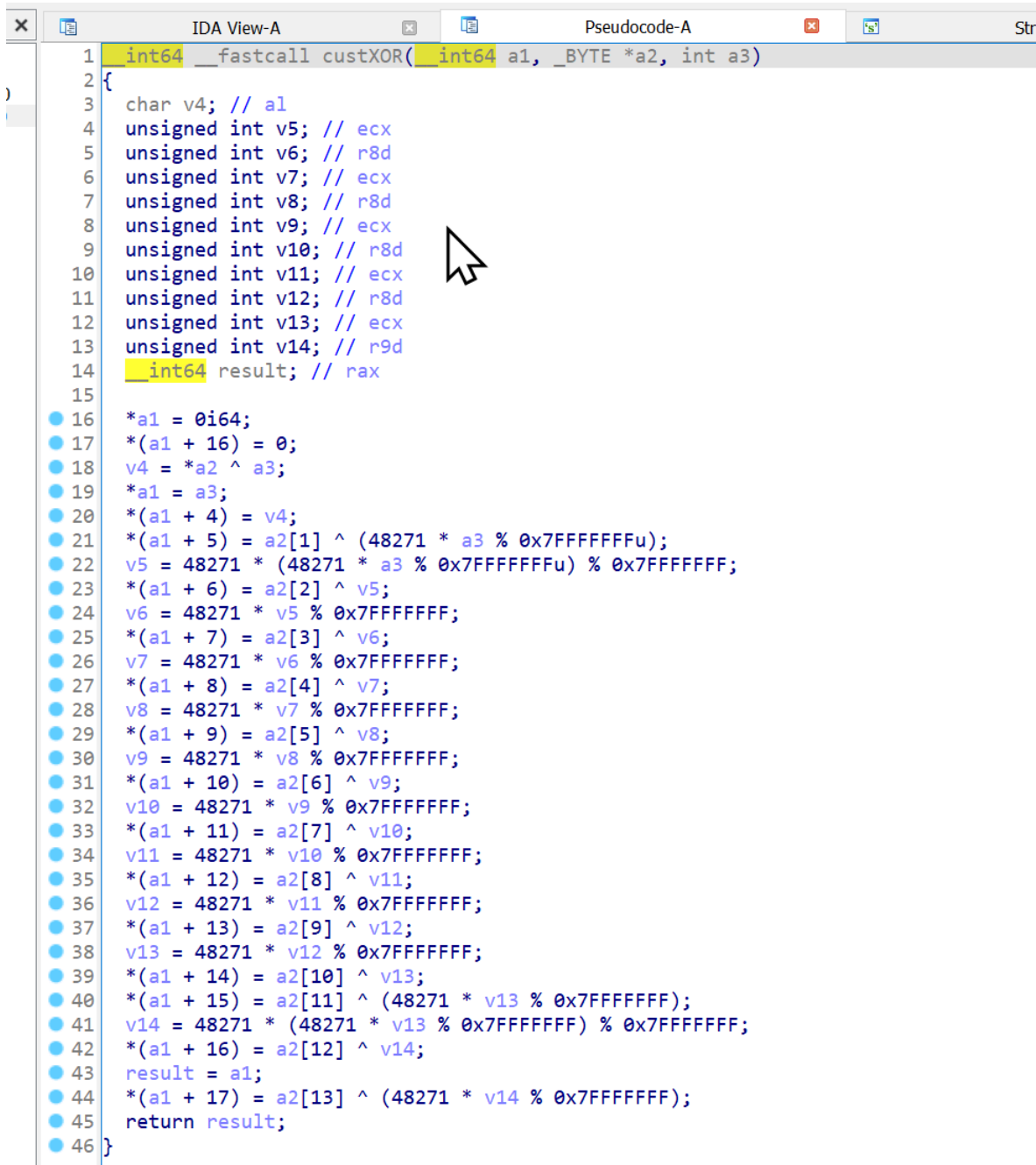
In one QWCrypt incident, the attackers also used the Chisel SOCKS5 tunneling tool. Leveraging the open-source Non-Sucking Service Manager (NSSM) utility that enables executables to run as system services, the threat actors created two distinct Windows service entries pointing to the same Chisel binary (MSAProfileNotificationHandler.exe). Each service was configured as a SOCKS client to attacker-controlled servers (e.g., stars[.]medbury[.]com:18810, 194[.]113[.]245[.]238:8810). In a likely effort to rotate C2 infrastructure or create redundant execution paths, the attackers copied the Chisel binary to a new binary name (SensorPerformanceEvents.exe) several days later and started it to provision a SOCKS tunnel to a different C2 server (162[.]33[.]178[.]61:18810).

Defense evasion

In several STAC6565 incidents, Sophos analysts observed the threat actors using a customized Terminator sample and a signed Zemana AntiMalware driver to attempt to disable extended detection and response (XDR) solutions. [Terminator](#) is an endpoint detection and response (EDR) killer tool that uses a Bring Your Own Vulnerable Driver (BYOVD) approach and loads a legitimately signed but vulnerable Zemana driver to kill protected processes, unload drivers, and modify kernel memory.

Sophos analysis indicates the threat actors repurposed code from an open-source version of [Spyboy's Terminator](#) posted to [GitHub](#) and modified it to obfuscate all the strings using a custom XOR routine (see Figure 7). This XOR implementation has been used in RedLoader samples to decode and resolve the

bcrypt functions that use AES to decrypt other API calls. Third parties such as [eSentire](#) and [Huntress](#) reported similar observations. However, Sophos analysis revealed there were no AES-encrypted strings in the Terminator samples.



```

1  int64 __fastcall custXOR(int64 a1, _BYTE *a2, int a3)
2  {
3      char v4; // a1
4      unsigned int v5; // ecx
5      unsigned int v6; // r8d
6      unsigned int v7; // ecx
7      unsigned int v8; // r8d
8      unsigned int v9; // ecx
9      unsigned int v10; // r8d
10     unsigned int v11; // ecx
11     unsigned int v12; // r8d
12     unsigned int v13; // ecx
13     unsigned int v14; // r9d
14     int64 result; // rax
15
16     *a1 = 0i64;
17     *(a1 + 16) = 0;
18     v4 = *a2 ^ a3;
19     *a1 = a3;
20     *(a1 + 4) = v4;
21     *(a1 + 5) = a2[1] ^ (48271 * a3 % 0x7FFFFFFFu);
22     v5 = 48271 * (48271 * a3 % 0x7FFFFFFFu) % 0x7FFFFFFF;
23     *(a1 + 6) = a2[2] ^ v5;
24     v6 = 48271 * v5 % 0x7FFFFFFF;
25     *(a1 + 7) = a2[3] ^ v6;
26     v7 = 48271 * v6 % 0x7FFFFFFF;
27     *(a1 + 8) = a2[4] ^ v7;
28     v8 = 48271 * v7 % 0x7FFFFFFF;
29     *(a1 + 9) = a2[5] ^ v8;
30     v9 = 48271 * v8 % 0x7FFFFFFF;
31     *(a1 + 10) = a2[6] ^ v9;
32     v10 = 48271 * v9 % 0x7FFFFFFF;
33     *(a1 + 11) = a2[7] ^ v10;
34     v11 = 48271 * v10 % 0x7FFFFFFF;
35     *(a1 + 12) = a2[8] ^ v11;
36     v12 = 48271 * v11 % 0x7FFFFFFF;
37     *(a1 + 13) = a2[9] ^ v12;
38     v13 = 48271 * v12 % 0x7FFFFFFF;
39     *(a1 + 14) = a2[10] ^ v13;
40     *(a1 + 15) = a2[11] ^ (48271 * v13 % 0x7FFFFFFF);
41     v14 = 48271 * (48271 * v13 % 0x7FFFFFFF) % 0x7FFFFFFF;
42     *(a1 + 16) = a2[12] ^ v14;
43     result = a1;
44     *(a1 + 17) = a2[13] ^ (48271 * v14 % 0x7FFFFFFF);
45     return result;
46 }

```

Figure 7: Custom XOR algorithm in a Terminator sample

One unusual discovery was a full Program Database (PDB) path found in GOLD BLADE's Terminator samples:

```
E:\SpecOp\js!\LOCKERS!\TOOLS\13_KILLAV\DISTRIB\WIN 2012 - WIN 2022 (Win10 - Win11)\Terminator_v1.1
(WITHOUT INSTALL)\x64\Release\Terminator.pdb
```

Cautious threat actors typically redact these paths before deployment to avoid leaking metadata that aids attribution or reverse engineering. While the PDB path could be a deliberate false flag, its presence more likely reflects a lapse in GOLD BLADE's operational security. Analyzing the path provides a glimpse into GOLD BLADE's development practices and reveals a structured offensive toolkit oriented around ransomware operations. The path also suggests that the group maintains multiple builds that contain different packages (e.g., with versus without installer) and are tailored to specific operating system versions.

In some STAC6565 incidents, Sophos analysts observed the threat actors drop the Terminator (term.exe) and driver (term.sys) files into C:\ProgramData. When the Terminator file is executed, it writes and installs the vulnerable driver (term.sys), which is then loaded via a kernel-mode driver service (TRM or SfTerm). The threat actors then delete the service and files, likely to evade detections that monitor persistent services (see Figure 8). In one July QWCrypt incident, the attackers deployed multiple Terminator binaries under this default naming schema (term*.exe, trm*.exe) to try to bypass Sophos detections. The binary hashes were unique for each variant, suggesting repacking or obfuscation.

```

357     goto LABEL_254;
358 }
359 *&v122 = 0x1B58538F88A5A2FBi64;
360 DWORD2(v122) = 0x656235C5;
361 BYTE12(v122) = 74;
362 *(&v122 + 13) = 0;
363 HIBYTE(v122) = 0;
364 v122 = *decodeXOR(v121, (&v122 + 4), 0x88A5A2FB); // term.sys
365 lpLibFileName[0] = 0i64;
366 v119.m128i_i64[0] = 0i64;
367 v119.m128i_i64[1] = 15i64;
368 v50 = -1i64;
369 do
370     ++v50;
371 while ( *(&v122 + v50 + 4) );
372 ValidateStr(lpLibFileName, &v122 + 4, v50);
373 TermSys_Str = lpLibFileName;
374 if ( v119.m128i_i64[1] >= 0x10ui64 )
375     TermSys_Str = lpLibFileName[0];
376 v52 = FindFirstFileA(TermSys_Str, &findFileData);
377 if ( v119.m128i_i64[1] >= 0x10ui64 )
378 {
379     v53 = lpLibFileName[0];
380     if ( (v119.m128i_i64[1] + 1) >= 0x1000 )
381     {
382         v53 = *(lpLibFileName[0] - 1);
383         if ( (lpLibFileName[0] - v53 - 8) > 0x1F )
384             invalid_parameter_noinfo_noreturn();
385     }
386     j_j_free(v53);
387 }
388 if ( v52 == -1 )
389 {
390     *v121 = 0x88A5A2F8;
391     *&v121[4] = _mm_load_si128(&xmmword_140034B70);
392     *&v121[20] = 0x1167CAC5;
393     v121[24] = 21;
394     *&v121[25] = 0;
395     v121[27] = 0;
396     v95 = sub_14000AA90(&v122, &v121[4], 0x88A5A2F8i64); // b'driver not found !!\n'
397     *v121 = *v95;

```

Figure 8: Terminator executable code includes a search for a vulnerable driver named term.sys

The threat actors went a step further in the April QWCrypt incident and renamed the loader and driver to lmhost.exe and lmhost.sys before distributing them via SMB shares to all servers in the environment. The attackers then modified the registry to disable two core Windows security mechanisms: the vulnerable

driver blocklist, which prevents loading of known-bad drivers, and Hypervisor-Enforced Code Integrity, which defends against kernel-level tampering. The following are the modified registry keys:

- HKLM\SYSTEM\CurrentControlSet\Control\CI\Config /v VulnerableDriverBlocklistEnable /t REG_DWORD /d 0x0 /f
- HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity /v Enabled /t REG_DWORD /d 0x0 /f

After making those changes, the threat actors copied the driver to the system directory and installed it as a kernel-mode service (LMHost) set to start automatically at boot. They repeated the same method to deploy the driver (renamed wmlib.sys) and Terminator tool (renamed wmlib.exe) across all available endpoints.

QWCrypt ransomware deployment

In most observed STAC6565 incidents, Sophos detections and response teams alerted on and mitigated the attacks before ransomware deployment. However, Sophos analysts observed QWCrypt ransomware deployed once in April and twice in July. In the April incident, the threat actors manually browsed and collected sensitive files, then paused activity for over five days before deploying the locker. This delay may suggest the attackers turned to ransomware after trying to monetize the data or failing to secure a buyer.

The QWCrypt ransomware launcher and deployment scripts are tailored to the target environment, with the script names containing a victim-specific ID. In the April incident, the ransomware and associated scripts were delivered in an encrypted 7-Zip archive (<victim ID>.tmp) and staged on endpoints across the environment via automated SMB transfers. After staging, the threat actors used local admin accounts and Impacket remote execution to run the launcher script (<victim ID>.bat) that began the ransomware deployment chain.

The launcher script ensured the Terminator service (WMLib) was active before extracting the ransomware payload (qwc_<victim ID>.exe) and associated files from the encrypted 7-Zip archive. It then started the main script (qwc_<victim ID>_1.bat) responsible for executing the ransomware. Like the launcher script, the main script confirmed the Terminator service was running, likely to reduce the risk of active protections causing the script to fail. It created a mutex file to prevent concurrent runs and wrote extensive discovery logs (tasklist, WMIC) to a temp directory that was exfiltrated via curl.exe to the attacker's C2 server (local.chronotypelabs . workers . dev).

The qwc_<victim ID>_1.bat script then disabled recovery via the 'bcdedit /set {default} recoveryenabled no' command and extracted the ransomware payload (qwc_<victim ID>.exe) from the archive. The script attempted to execute the ransomware on endpoint devices across the network via the 'qwc_537aab1c.exe -v -key <key> -nosd' command. However, [Sophos CryptoGuard](#) blocked the attack on protected systems, resulting in only a few impacted hosts that were not managed by Sophos. The attempted encryption of endpoints differs from previous reporting of the threat group targeting only hypervisors for encryption. The attackers then tried to manually execute the binary on the organization's hypervisors, using an option (-hv) to specifically target the locally running virtual machines. While only a few flags were used in the incident, QWCrypt windows cryptor offers numerous usage options (see Figure 9). Finally, the script runs a cleanup .bat script (qwc_<victim ID>_3.bat), which deletes existing shadow copies and every PowerShell console history file (ConsoleHost_history.txt) to hinder forensic recovery.

```

qwCrypt windows cryptor

Usage:
  qwc [flags]

Flags:
  --block-size string    AES Block size (default "1M")
  --chacha               Use ChaCha20 algorithm
  --dryrun              Do not modify anything
  --excludeVM string     Exclude VMs (csv list)
  --folder stringArray   Folders to serch files (default [all])
  --full-enc-less string Full encrypt files less than (default "50M")
  -h, --help            help for qwc
  --hv                 Encrypt HyperV VMs
  -i, --info           Print system info
  -k, --key string      Vars key
  --kill              Kill VM process
  --log string         Log file
  --maxsize string     Vars key (default "0")
  --minsize string     Vars key (default "0")
  --nosd              Do not self delete
  --noshadowdelete     Do not delete shadow copies
  --skip-count int     Skip blocks count (default 5)
  --threads int        Cryptor thread count (default 10)
  --turnoff            TurnOff HyperV VMs (default true)
  -v, --verbose        Use verbose output format

```

Figure 9: QWCrypt windows cryptor usage flags

The binary appends encrypted files with a .qwCrypt extension and drops a ransom note (!!!how_to_unlock_qwCrypt_files.txt) in every encrypted folder (see Figure 10). The ransom note observed by Sophos analysts in the April incident appears to be a condensed version of the note shown in the appendix of the [Bitdefender](#) analysis. While it contains the core double-extortion elements, it omits longer persuasive blocks like the detailed insurance-negotiation text reminiscent of HardBit ransom notes. Linguistically, several phrases in both QWCrypt notes are near-verbatim matches to well-known LockBit templates (e.g., “your data is stolen and encrypted,” “do not delete files,” “a paid training lesson for your admins”). This overlap does not necessarily indicate a connection between GOLD BLADE and LockBit threat actors. It is more likely that GOLD BLADE is reusing language from an established ransomware family to pressure victims.

PERSONAL_ID: [REDACTED]

Dear valued customer,

We regret to inform you that your company's data has been stolen and encrypted by our ransomware group. We understand this situation can be distressing, but rest assured there is a solution.

If you do not pay the ransom, your data will be published on our TOR darknet sites. Once your data appears on these leak sites, it could be bought by competitors at any moment. To avoid such complications, we advise you to act promptly and pay the ransom.

Leaking your company's data carries numerous dangers: hefty fines from governing bodies like GDPR, potential lawsuits from customers for leaking confidential information, and the misuse of stolen data by hackers worldwide.

By paying the ransom, you can ensure the safety of your business. Our group will provide decryption software upon receiving payment. This situation serves as a valuable lesson for your system administrators, reminding them to prioritize proper network configuration to prevent future attacks.

We kindly ask that you do not delete or modify any encrypted files, as this could lead to issues with decrypting your data.

If you choose not to pay the ransom, we will be forced to attack your company again in the future.

Contact our Support Team by email at qwcrypt_01ae4c@proton.me (please include your PERSONAL_ID in the subject field) for assistance in resolving this matter.

Thank you for your understanding and cooperation in this unfortunate situation.

Sincerely, qwCrypt Team.

Figure 10: QWCrypt ransomware note

Recommendations

GOLD BLADE's abuse of recruitment platforms, cycles of dormancy and bursts, and continual refinement of delivery methods demonstrate a level of operational maturity not typically associated with financially motivated actors. In addition to leveraging various LOLBins, the group maintains a comprehensive and well-organized attack toolkit, including modified versions of open-source tooling and custom binaries to facilitate a multi-stage malware delivery chain. GOLD BLADE's introduction of a custom locker for encryption and ability to pivot between espionage and ransomware further points to the group's continual evolution and the need for organizations to bolster their defenses.

Many attacks can be prevented by training employees to recognize phishing attempts and potentially malicious resumes, and advising them to never bypass errors by downloading resumes from external links. It is also good practice to maintain backups of critical business data offline or in an isolated environment to limit the impact of an attack and facilitate recovery. Additionally, the following technical approaches can be effective against known GOLD BLADE tactics:

Harden recruitment workflows – Consider routing attachments from recruitment platforms through email and security gateways for inspection before HR review, or automatically quarantining resumes containing embedded links, macros, or redirects. Organizations can also use secure document viewers that open resumes in a sandboxed browser or PDF-only viewer.

- **Prioritize endpoint coverage and monitoring** – Ensure that every endpoint (server or workstation) is centrally managed and kept up to date with protections. Comprehensive logging should be a baseline requirement for modern environments to provide visibility of impacted data, which is important not only for remediation but also for responding to regulatory and legal obligations.

- **Implement a managed detection and response (MDR) solution** – While having detection and blocking tools in place is critical, detection without action is less effective. Skilled analysts must be actively monitoring, investigating, and responding to alerts to ensure full coverage.

Detections

SophosLabs has developed the detections in Table 1 to detect activity associated with this threat.

Name	Description
Troj/Agent-BKZE	RedLoader detection
Troj/Agent-BLEI	RedLoader detection
ATK/Rpivot-B	RPivot detection
ATK/Rpivot-D	RPivot detection
Troj/Agent-BLED	RedLoader detection
Troj/Agent-BLEE	RedLoader detection
Troj/Agent-BLEM	RedLoader detection
Troj/Drop-DLF	RedLoader detection
Troj/Drop-DLG	RedLoader detection
Troj/Ransom-HHH	QWCrypt ransomware detection
Troj/Agent-BLGG	RedLoader detection
CXmal/KillAV-ZA	Detection for a vulnerable signed Zemana AntiMalware driver

Table 1: Sophos detections associated with this threat

Threat indicators

The threat indicators in Table 2 can be used to detect activity related to this threat. Note that IP addresses can be reallocated. The domains, URLs, and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
hxxps://get[.]easyhrservicesm[.]workers[.]dev/id/KEgldoor0327de	URL	Initial RedLoader download link used by GOLD BLADE (April 2025)

Indicator	Type	Context
netutils.dll	Filename	First-stage RedLoader payload used by GOLD BLADE (July 2025)
srvcli.dll	Filename	First-stage RedLoader payload used by GOLD BLADE (March, April 2025)
d302836c7df9ce8ac68a06b53263e2c685971781a48ce56b3b5a579c5bba10cc	SHA256 hash	First-stage RedLoader payload used by GOLD BLADE (July 2025)
45777688e870e806aa3123a566f8728e2a0f5620	SHA1 hash	First-stage RedLoader payload used by GOLD BLADE (April 2025)
af912641a80f0c8a79f77ffe359bb5f6	MD5 hash	First-stage RedLoader payload used by GOLD BLADE (April 2025)
567f8647be25cd2943a014d525923e9fa17a129cf48b0a9802f0180b13ed130c	SHA256 hash	First-stage RedLoader payload used by GOLD BLADE (April 2025)

Indicator	Type	Context
798f7c7c61c09a3f3e3c75c09b1464a6efc936dd	SHA1 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
8beaf5bc60bcf735808485ac12457468	MD5 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
a22676c6897da69c5f2c62b31ad5b0e26af706cbcb052bed60cd784e6b56d70f	SHA256 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
0705efc42ab20fda36ea55b6583370b60e087288	SHA1 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
64eed490f2ebd040b8822c47622c47a0e592e3d8	SHA1 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
264be41070c4270adf337e1119842d9f	MD5 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)

Indicator	Type	Context
ab4695e5d5472af124ea69e0c1abb4c9726980b4c99c5da10ae2ba85f55bf1e4	SHA256 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
6b53e25bbf07ce657347164026f6bc50680319f5	SHA1 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
3debde1aeae4255e0d40ad410421f175	MD5 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
dcc85cc6b984961187ae364be8ee11541dee4f7a46bea3960c0218465fbc6b96	SHA256 hash	First-stage RedLoader payload used by GOLD BLADE (March 2025)
369acb06aac9492df4d174dbd31ebfb1e6e0c5f3	SHA1 hash	Second-stage RedLoader payload used by GOLD BLADE (July 2025)
5f75d4e51b35f37274340db905209f15	MD5 hash	Second-stage RedLoader payload used by GOLD BLADE (July 2025)

Indicator	Type	Context
f5203c7ac07087fd5029d83141982f0a5e78f169cdc4ab9fc097cc0e2981d926	SHA256 hash	Second-stage RedLoader payload used by GOLD BLADE (July 2025)
9bdefba7d577b6c6dbc579624efb8166b8877182	SHA1 hash	Second-stage RedLoader payload used by GOLD BLADE (April 2025)
0972894a5d3bfe100d22b6a640c2d772	MD5 hash	Second-stage RedLoader payload used by GOLD BLADE (April 2025)
d46244bafae8cb2e38eaf22dd650250b2cb35cd9907d3952a28d6ed9c3b83e05	SHA256 hash	Second-stage RedLoader payload used by GOLD BLADE (April 2025)
0f1fa903a1b80c645b6e9fd2297fcb8da96fba6d	SHA1 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)

Indicator	Type	Context
8d665f24b9c9b90ae9adebed1a94c379	MD5 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
a6c68b0d059d6db29d2c35740b77cd5dedee156ec7da4b2d61c863951b78b5b0	SHA256 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
71d0e43c49bf3c869ed1cb9f11ab85cbb375718d	SHA1 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
43978cd8feea45000bab3d715c87c014	MD5 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
601157a51973814f9f60f269f5537451861029371615115dbf851d9e32d79096	SHA256 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)

Indicator	Type	Context
417d1fd1c1230771dd48de84e78a7071d6f8ece1	SHA1 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
85c4605c22601156105fc2e98982e5da	MD5 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
40506a308bfbb71e1f7d6a6473f4cc3eafa8d594232f0f23208494ec3649b69a	SHA256 hash	Second-stage RedLoader payload used by GOLD BLADE (March 2025)
082464ee1ea8569c60f311b6c870005221f54c31	SHA1 hash	Third-stage RedLoader payload used by GOLD BLADE (July 2025)
ae26db422bdc97439c4606e514ae79a8	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (July 2025)
0b514f6bdf501d600db057a44b652a28889a28ee844ed2c9419f9b45273ad2cc	SHA256 hash	Third-stage RedLoader payload used by GOLD BLADE (July 2025)

Indicator	Type	Context
3e73debf95ec6fc3fee8507f9d4e764dd9ee2700	SHA1 hash	Third-stage RedLoader payload used by GOLD BLADE (April 2025)
16357720fd9b8fee705c4aa13fb03faa	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (April 2025)
b47447e55fc832b3b25150a9143a6bbd9f504559edb6dd1eb1a9890a221cda5f	SHA256 hash	Third-stage RedLoader payload used by GOLD BLADE (April 2025)
f6c1985418c8cc35e80e525cdb2b7aae416d2fd3	SHA1 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)
8b2028dc135d6e06c0a1617ddf04ec29	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)
ef9a9a48b800e9fc9b10c652d00218ea1a068f000b935d49588898f048510e1e	SHA256 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)

Indicator	Type	Context
e908aa98b8e53fa555fb0a0d81138ee4755ee077	SHA1 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)
4af2096912f8a6dc08b5f71090b4339d	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)
62a42954a162e8fe43a976a2b7a43643d3ecf559e64b9d174f50698106783dff	SHA256 hash	Third-stage RedLoader payload used by GOLD BLADE (March 2025)
84e79b115ebe278dc9e36a1c2b51b5cdbb7f900b	SHA1 hash	Third-stage RedLoader payload used by GOLD BLADE (November 2024)
2ef6b29c7443ff759343368bbf56ae92	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (November 2024)
ac57fdf8297ec48e506f686c7f9ec90c1ccd7f828193eeb37f86483a43519617	MD5 hash	Third-stage RedLoader payload used by GOLD BLADE (November 2024)

Indicator	Type	Context
live[.]airemoteplant[.]workers[.]dev	Domain name	GOLD BLADE C2 server (July 2025)
quiet[.]msftlivecloudsrv[.]workers[.]dev	Domain name	GOLD BLADE C2 server (July 2025)
automatinghrservices[.]workers[.]dev	Domain name	GOLD BLADE C2 server (July 2025)
local[.]chronotypelabs[.]workers[.]dev	Domain name	Cloudflare Workers site used by GOLD BLADE for exfiltration (April 2025)
soft[.]rippleserveruns[.]workers[.]dev	Domain name	GOLD BLADE C2 server (April 2025)
cv[.]optimalconfluenceservices[.]workers[.]dev	Domain name	GOLD BLADE C2 server (March 2025)
23[.]254[.]224[.]79	IP address	GOLD BLADE C2 server (November 2024)
!!!how_to_unlock_qwCrypt_files.txt	Filename	QWCrypt note used by GOLD BLADE (April, July 2025)
ef740910242d80800c3409991f51f563ea11af9d	SHA1 hash	QWCrypt binary used by GOLD BLADE (July 2025)

Indicator	Type	Context
0f5744007f5bbdc4ebae8a79e1d3e399	MD5 hash	QWCCrypt binary used by GOLD BLADE (July 2025)
568352411deff640ba781ae55d98d657da02191d97e0466e6883b966dd1e77db	SHA256 hash	QWCCrypt binary used by GOLD BLADE (July 2025)
e51eb7ab20848cc68dcb6c65fc181f9a	MD5 hash	QWCCrypt binary used by GOLD BLADE (April 2025)
3db407d3e1b2d72ee37232ea520f567b733c5f26	SHA1 hash	QWCCrypt binary used by GOLD BLADE (April 2025)
6755db8d62c605cb15cc7eca9d857601e0911dd839562027e3cb03f12d25ef4c	SHA256 hash	QWCCrypt binary used by GOLD BLADE (April 2025)
a5cfcd25bfa23b700f5284a59dd9390b542881c5	SHA1 hash	Modified Terminator binary used by GOLD BLADE (July 2025)
c4d7582502b42a3224ede295bbac1fc9	MD5 hash	Modified Terminator binary used by GOLD BLADE (July 2025)
7b9673bb17ec56662d15ab78f49a13c78c89f8bc88085d4f3dbb8dd9d9d68f43	SHA256 hash	Modified Terminator binary used by GOLD BLADE (July 2025)

Indicator	Type	Context
de5ab1711b338bd7a4cc7f20478a6be892c46a5a	SHA1 hash	Zemana AntiMalware driver used by GOLD BLADE (July 2025)
70aba3937c6b26b5ead7c773cb411661	MD5 hash	Zemana AntiMalware driver used by GOLD BLADE (July 2025)
c330c918051e07c50f023e9bd5099dc34f81778c6d0d1a8ad245687b701f5278	SHA256 hash	Zemana AntiMalware driver used by GOLD BLADE (July 2025)
31a167bf48da4dc31de17e16e5b4da9c56e7d7db	SHA1 hash	Modified Zemana AntiMalware driver used by GOLD BLADE (July 2025)
02b029e93f1859eb8b05216263db868b	MD5 hash	Modified Zemana AntiMalware driver used by GOLD BLADE (July 2025)
712f3f8d43b57099d374bd35558da1b6fc48835efa4a55180377a2b22fd95cff	SHA256 hash	Modified Zemana AntiMalware driver used by GOLD BLADE (July 2025)

Indicator	Type	Context
6b53e25bbf07ce657347164026f6bc50680319f5	SHA1 hash	Modified Terminator binary used by GOLD BLADE (April 2025)
3debde1aeae4255e0d40ad410421f175	MD5 hash	Modified Terminator binary used by GOLD BLADE (April 2025)
dcc85cc6b984961187ae364be8ee11541dee4f7a46bea3960c0218465fbc6b96	SHA256 hash	Modified Terminator binary used by GOLD BLADE (April 2025)
261f78c7fe8162b36a55ad3848dbe4a203e3ea9493feb46988704ea5a01e356c	SHA256 hash	Modified Terminator binary used by GOLD BLADE (March 2025)
5dd82e082edcc6f005997a27a701301663b8e6a7	SHA1 hash	RPivot binary used by GOLD BLADE (March, April 2025)
dd81deba7c0066ed848a030efdef3526	MD5 hash	RPivot binary used by GOLD BLADE (March, April 2025)
88177fe4a455312cd94ae2ccbf274181dff1feea85a7288cb91683c788a10462	SHA256 hash	RPivot binary used by GOLD BLADE (March, April 2025)

Indicator	Type	Context
7c6636711618ef6c539dc6d4868c1c4e7090129e5b544b8e799088f11619c727	SHA256 hash	Chisel binary used by GOLD BLADE (April 2025)
109[.]206[.]236[.]209	IP address	RPivot C2 server used by GOLD BLADE (April 2025)
hxxp://194[.]1113[.]245[.]238:8810	URL	Chisel C2 server used by GOLD BLADE (April 2025)
hxxp://stars[.]medbury[.]com:18810	URL	Chisel C2 server used by GOLD BLADE (April 2025)
hxxp://162[.]33[.]178[.]61:18810	URL	Chisel C2 server used by GOLD BLADE (April 2025)
9fda15cdac5f73c0f56497b0b32706180871f3be	SHA1 hash	RPivot binary used by GOLD BLADE (March 2025)
bbe856330766da83686750b4eb6767bd	MD5 hash	RPivot binary used by GOLD BLADE (March 2025)
9ce8c43d7d8ddab18fde6ca3c0f23efb5491d460bffc8c0ea5fc2f61a6e7b8e4	SHA256 hash	RPivot binary used by GOLD BLADE (March 2025)

Indicator	Type	Context
109[.]206[.]236[.]209	IP address	RPivot C2 server used by GOLD BLADE (March 2025)

Table 2: Indicators for this threat



About the Author

Morgan is a Threat Intelligence Analyst for the Sophos Managed Detection and Response (MDR) team, where her focuses include tactical cyber intelligence, data enrichment, and monitoring emerging threats. With a Masters in Intelligence and Security Studies, her areas of interest span beyond the cyber realm to include geopolitics and international security. In past roles, Morgan worked in the Network Detection and Response (NDR) space, where she focused on tracking attack patterns, analyzing command-and-control infrastructure, and threat research reporting.

Read Similar Articles

May 24, 2021

[What to expect when you've been hit with Avaddon ransomware](#)

May 19, 2021

[What's New in Sophos EDR 4.0](#)

May 19, 2021

[Sophos XDR: Driven by data](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Subscribe to get the latest updates in your inbox.

Which categories are you interested in?

- Products and Services
- Threat Research
- Security Operations
- AI Research
- #SophosLife