Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Feb 04 - 10, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - DoubleQlik
  - CONTEC CMS8000 Patient Monitor

- **New Threat Protections - 186**

The following threats were added to Crystal Eye this week:

1. DoubleQlik

In August 2023, Qlik released patches addressing two critical vulnerabilities in Qlik Sense Enterprise: CVE-2023-41265 and CVE-2023-41266. These vulnerabilities permitted unauthenticated remote code execution through path traversal and HTTP request tunnelling. Subsequent analysis by security researchers revealed that the initial fix for CVE-2023-41265 could be bypassed. Attackers could exploit this by manipulating the Transfer-Encoding header in HTTP requests, using variations like tchunked instead of chunked, to circumvent the patch's validation mechanism. This bypass allowed for unauthenticated remote code execution even on systems that had applied the original patch. Qlik has since issued a more robust patch to address this bypass, tracked as CVE-2023-48365.

Threat Protected: 01
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Reject	Drop
Connectivity	Alert	Alert
OT	Disabled	Disabled

Class Type: Attempted Admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

2. CONTEC CMS8000 Patient Monitor

In January 2025, the U.S. Food and Drug Administration (FDA) and the Cybersecurity and Infrastructure Security Agency (CISA) issued alerts regarding potential cybersecurity vulnerabilities in CONTEC CMS8000 patient monitors. Initial concerns suggested the presence of a hidden backdoor communicating with a Chinese IP address. However, further analysis by researchers revealed that these issues stem from insecure design choices rather than malicious intent. The devices are configured to communicate with hardcoded public IP addresses (202.114.4.119 for the Central Management System and 202.114.4.120 for the HL7 server) for firmware updates and data transmission. This design exposes the monitors to potential unauthorised access and data leakage, posing significant risks to patient safety and data integrity.

Threat Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Alert	Alert
Security	Alert	Alert
WAF	Disabled	Disabled
Connectivity	Disabled	Disabled
OT	Disabled	Disabled

Class Type: Attempted-admin

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Known exploited vulnerabilities (Week 1 February 2024):

Vulnerability	CVSS	Description
CVE-2018-19410	9.8 (Critical)	Paessler PRTG Network Monitor Local File Inclusion Vulnerability
CVE-2018-9276	7.2 (High)	Paessler PRTG Network Monitor OS Command Injection Vulnerability
CVE-2024-29059	7.5 (High)	Microsoft .NET Framework Information Disclosure Vulnerability
CVE-2024-45195	9.8 (Critical)	Apache OFBiz Forced Browsing Vulnerability
CVE-2024-53104	7.8 (High)	Linux Kernel Out-of-Bounds Write Vulnerability
CVE-2020-15069	9.8 (Critical)	Sophos XG Firewall Buffer Overflow Vulnerability
CVE-2020-29574	9.8 (Critical)	CyberoamOS (CROS) SQL Injection Vulnerability
CVE-2024-21413	9.8 (Critical)	Microsoft Outlook Improper Input Validation Vulnerability
CVE-2022-23748	7.8 (High)	Dante Discovery Process Control Vulnerability
CVE-2025-0411	7.0 (High)	7-Zip Mark of the Web Bypass Vulnerability
CVE-2025-0994	8.6 (High)	Trimble Cityworks Deserialisation Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-february-2025/544

Updated Malware Signatures (Week 1 February 2024)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organizations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Group	Overall Percentage of total attack coverage
Lynx	3.82%
Killsec3	1.53%
Rhysida	1.53%
Leaked Data	4.58%
8Base	3.05%
Space Bears	2.29%
Wikileaksv2	2.29%
Arcus Media	3.82%
Lockbit3	1.53%
Abyss-data	1.53%
Handala	0.76%
Bianlian	6.11%
Fog	2.29%
Medusa	2.29%
Ransomexx	0.76%
Clop	4.58%
RansomHub	11.45%
Qilin	12.98%
Cloak	0.76%
Eraleign (APT73)	3.82%
Play	6.87%
SafePay	3.05%
RansomHouse	0.76%
Cactus	3.82%
Cicada3301	3.05%
Everest	1.53%
Kairos	1.53%
Fsociety	1.53%
3AM	0.76%
Stormous	1.53%
Akira	2.29%
Hunters	0.76%

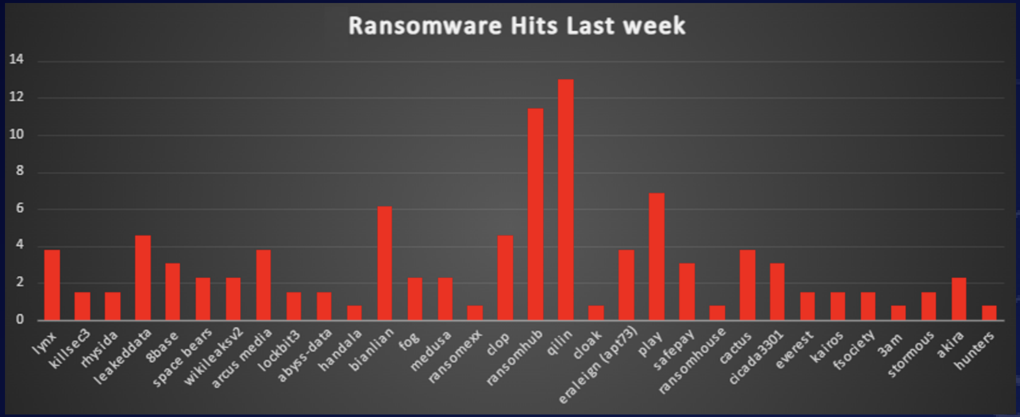


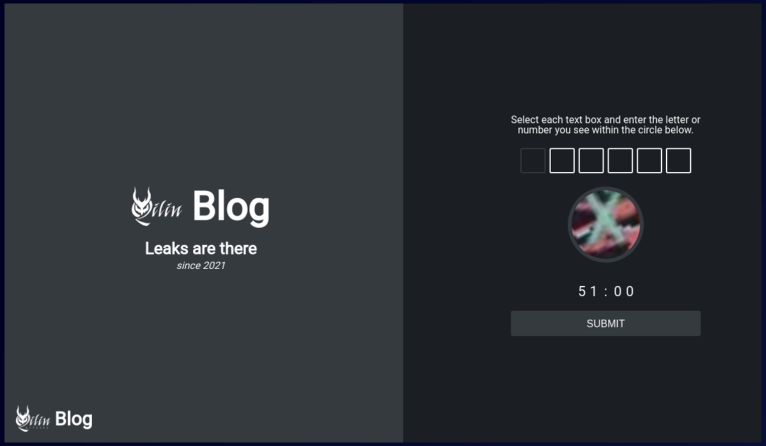
Figure 1: Ransomware Group Hits Last Week

Qilin Ransomware Group

Overview

The Red Piranha Team continuously monitors ransomware groups and underground cybercrime activity to track emerging threats. In recent investigations, we analysed a Qilin (Agenda) ransomware attack that leveraged VPN compromise, lateral movement, and advanced EDR evasion techniques to infiltrate corporate networks.

Qilin operates as a Ransomware-as-a-Service (RaaS), allowing affiliates to conduct attacks in exchange for a large percentage of ransom payments. This particular attack showcased sophisticated kernel exploitation techniques, including a Bring-Your-Own-Vulnerable-Driver (BYOVD) attack to disable endpoint detection and response (EDR) solutions at the deepest levels of the Windows operating system.



Select each text box and enter the letter or number you see within the circle below.

Attack Chain Analysis

Initial Access: VPN Compromise & Covert Network Tunnelling

An unusual VPN session was observed from 31.192.107[.]144, an IP address associated with a Russia-based cloud hosting provider.

- First session lasted over six hours; a second session occurred later for an additional hour and a half.
- Indicates compromised credentials or stolen session tokens, allowing the attacker to bypass MFA or other security controls.

Once inside the network, the attacker deployed a reverse proxy tool (main.exe), a Golang-based executable that established an SSH tunnel to 216.120.203[.]26 (Shock Hosting). This allowed the attacker to:

- Bypass firewalls and internal security controls.
- Access internal machines remotely via RDP and other remote tools.
- Exfiltrate data through encrypted tunnels, making detection harder.

Privilege Escalation & Lateral Movement

After securing a foothold, the attacker expanded access within the network using:

- Remote Desktop Protocol (RDP)
  - Logged into additional systems using compromised credentials.
  - Avoided detection by mimicking legitimate user activity.
- Built-in Windows Administration Tools
  - Used PsExec and Windows Management Instrumentation (WMI) to execute commands remotely.
  - Reduced reliance on custom malware, making the attack harder to detect.

EDR Evasion: DLL Sideloading & Kernel Exploitation

Phase 1: DLL Sideloading Attack

To avoid detection, the attacker deployed a signed Windows executable (upd.exe), a legitimate Carbon Black Cloud Sensor AV update tool.

- Normally, upd.exe loads a trusted DLL (avupdate.dll) for software updates.
- The attacker replaced this DLL with a malicious version, allowing them to execute arbitrary code.

How it worked:

- upd.exe executed avupdate.dll, which then:
- Loaded web.dat, an XOR-encoded payload containing a customised version of EDRSandblast, a known EDR-disabling tool.
- Performed anti-analysis checks to detect debuggers or virtual machines.

Phase 2: BYOVD Attack with TPwSav.sys

Instead of using a well-known vulnerable driver (which modern EDRs flag), the attacker introduced:

- TPwSav.sys – A signed but vulnerable Windows driver originally developed for Toshiba laptop power-saving features.
- Why TPwSav.sys?
  - Compiled in 2015, still holds a valid signature.
  - Allows direct kernel memory access.
  - Undetected by most security solutions, unlike older exploited drivers.

Once loaded, the attacker hijacked the Windows Beep.sys driver, modifying its BeepDeviceControl function to execute malicious shellcode.

Key techniques used in the attack:

- Overwrote kernel memory to disable EDR hooks.
- Used MmMapIoSpace to read/write arbitrary memory.
- Hijacked IofCompleteRequest for kernel function execution.

After successfully executing EDRSandblast, the attacker:

- Removed kernel callback routines, cutting off EDR visibility.
- Disabled event tracing, blocking forensic tools from recording system activity.

Tactic	Tactic	Technique	Description
Initial Access	Valid Accounts (T1078)	Compromised VPN credentials	Used stolen credentials to log in via SSL VPN
Execution	Command and Scripting Interpreter (T1059)	Remote execution via RDP and management tools	Used PsExec, WMIC for lateral movement
Persistence	DLL Sideloading (T1574.002)	Malicious DLL sideloaded via upd.exe	upd.exe loaded avupdate.dll, leading to web.dat execution
Privilege Escalation	Exploiting Vulnerable Drivers (T1068)	BYOVD attack with TPwSav.sys	Leveraged signed driver to disable EDR
Defence Evasion	Disabling Security Tools (T1562.001)	Kernel callback removal & EDRSandblast execution	Killed EDR processes, disabled event tracing
Impact	Data Encryption for Impact (T1486)	Ransomware execution	Exfiltrated data, encrypted critical files

Mitigations Against Qilin Ransomware

- Enforce Strong VPN Security – Require Multi-Factor Authentication (MFA) and geolocation-based restrictions to prevent unauthorised access.
- Monitor VPN & RDP Activity – Detect long-duration VPN sessions, logins from cloud-hosted IPs, and unusual RDP usage.
- Restrict RDP & Remote Access – Disable RDP where possible; otherwise, restrict by IP allowlists, enforce MFA, and limit admin privileges.
- Implement Network Segmentation – Prevent lateral movement by isolating critical systems and enforcing least privilege access.
- Use Endpoint Detection & Response (EDR) Policies – Deploy behaviour-based anomaly detection to identify suspicious process executions.
- Block Vulnerable Drivers (BYOVD Protection) – Enable Windows Defender Application Control (WDAC) and Hypervisor-Protected Code Integrity (HVCI) to block outdated or unsigned drivers.
- Harden Privileged Account Usage – Implement Privileged Access Management (PAM) and just-in-time (JIT) access to limit admin rights.
- Disable Unnecessary Windows Services & Tools – Block execution of PsExec, WMIC, PowerShell, and other remote admin tools where not needed.

IOCs
Hashes
TPwSav.sys: 011df46e94218cbb2f0b8da13ab3cec397246fdc63436e58b1bf597550a647f6
avupdate.dll: d3af11d6bb6382717bf7b6a3aceada24f42f49a9489811a66505e03dd76fd1af
main.exe: aeddd8240c09777a84bb24b5be98e9f5465dc7638bec41fb67bbc209c3960ae1
web.dat: 08224e4c619c7bbae1852d3a2d8dc1b7eb90d65bba9b73500ef7118af98e7e05
upd.exe: 3dfae7b23f6d1fe6e37a19de0e3b1f39249d146a1d21102dcc37861d337a0633

IP:
216.120.203[.]26
31.192.107[.]144

File servers
ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS@85.209.11.49
ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@188.119.66.189

DLS URLs
http://ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd.onion/
http://24kckepr3tdbcomkimbov5nqv2alos6vmrmlxdr76lfmkgegukubctyd.onion
http://wlh3dpptx2gt7nsxcor37a3kiyaiy6qwhdv7o6nl6iuniu5ycze5ydid.onion/blog
http://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad.onion/
http://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd.onion
https://31.41.244.100/
http://ijzn3sicrcy7quixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvad.onion
http://kbsqoiyihadmwczmxkbovk7ss2dcynitwhhfu5yw725dbogo5kthfaad.onion

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 66.41% of global incidents, highlighting its continued vulnerability to ransomware threats. Following this, Canada reported 10.69% of the attacks, emerging as another highly targeted region.

India and the United Kingdom also faced considerable exposure, reporting 3.05% and 3.82% of ransomware incidents, respectively. Italy experienced 2.29% of attacks, indicating an ongoing risk in the region. Meanwhile, Sweden recorded 1.53% of global ransomware cases.

Several other nations exhibited moderate levels of ransomware incidents, including Singapore, Brazil, Israel, Turkey, China, Mexico, Germany, Jamaica, Saudi Arabia, Switzerland, France, Australia, South Korea, Netherlands, and Japan, each reporting 0.76% of global ransomware cases.

This analysis underscores the persistent and widespread nature of ransomware attacks, with North America facing particularly high levels of risk. These findings highlight the critical need for robust cybersecurity measures, proactive defence strategies, and heightened vigilance across all sectors to counteract the increasing ransomware threat worldwide.

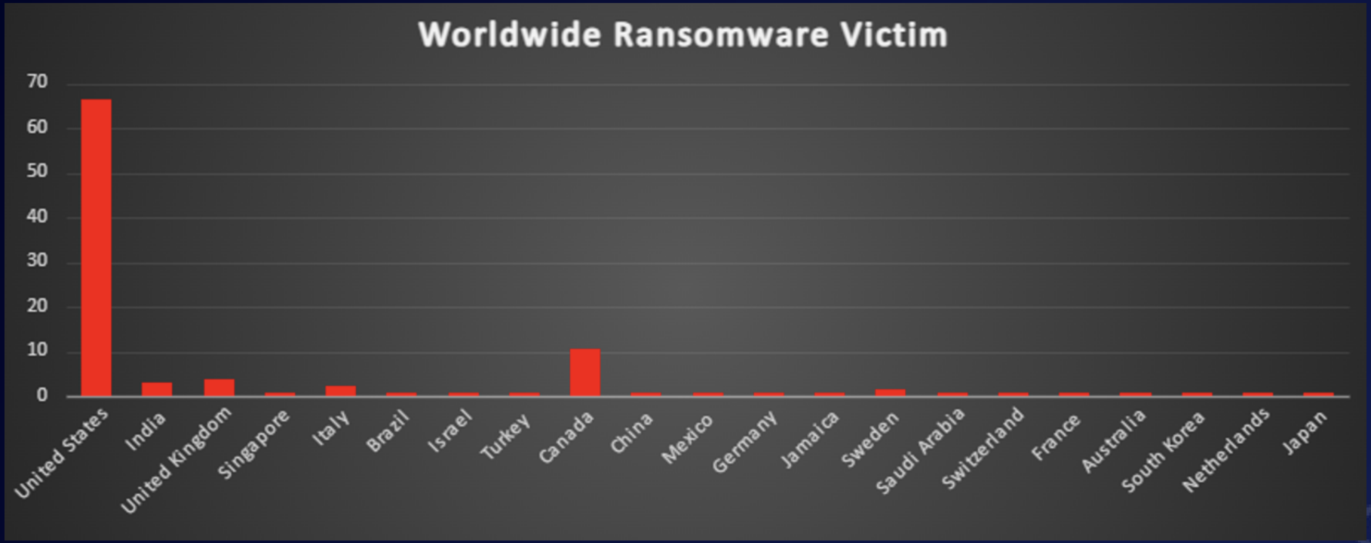


Figure 3: Ransomware Victims Worldwide

Ransomware Victims by Industry

A recent ransomware analysis highlights the Manufacturing sector as the most targeted industry, accounting for 21.37% of total reported incidents. This underscores the persistent threats faced by production processes and supply chain operations.

Following this, the Retail and Business Services sectors each reported 10.69% of attacks, emphasising the heightened risk to consumer-facing businesses and service-oriented organisations. The Hospitality industry also saw a significant impact, accounting for 8.4% of ransomware incidents.

Other heavily affected industries include Construction and IT, each reporting 6.11%, reflecting ongoing security challenges in infrastructure development and technology services. Education and Transportation both recorded 4.58% of attacks, followed closely by Law Firms at 4.58% and Healthcare at 3.82%, highlighting vulnerabilities in sectors handling sensitive data.

Meanwhile, Finance and Federal institutions each accounted for 2.29% of reported ransomware incidents. Energy also faced 2.29%, indicating cybercriminals' focus on critical infrastructure. Telecommunications, Insurance, and Media & Internet sectors each saw 1.53% of attacks, while Real Estate reported 5.34%, underscoring the diverse impact of ransomware across industries.

Lower, yet notable, shares of ransomware activity were recorded in Agriculture (0.76%) and Organisations (0.76%), showcasing the widespread reach of ransomware across sectors.

This analysis reinforces the indiscriminate nature of ransomware threats, impacting industries across critical infrastructure, public services, and commercial enterprises. The findings highlight the urgent need for sector-specific cybersecurity strategies, robust defences, and proactive risk management to mitigate the evolving ransomware landscape.

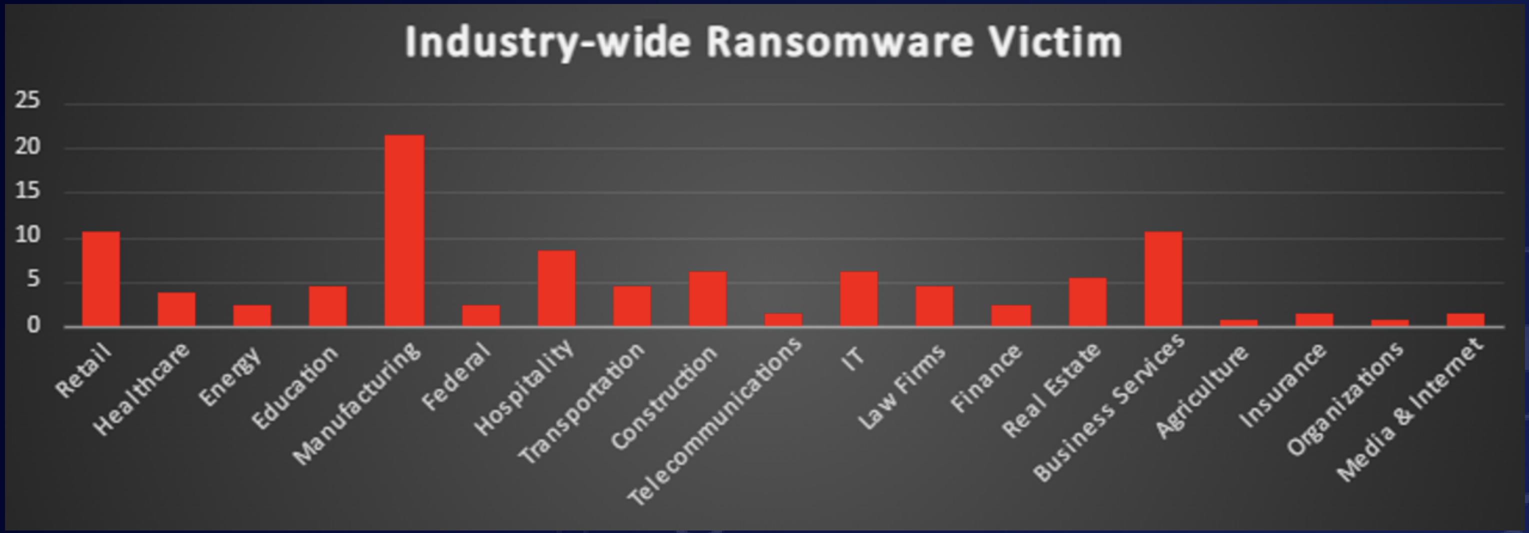


Figure 4: Industry-wide Ransomware Victims