KryptoKloud

SECURITY MADE SIMPLE

KryptoKloud Cyber Threat Briefing
April 2025

CyberShadows

INTELLIGENCE LED APPROACH TO CYBER RESILIENCE

CS Labs

Roundup from the KryptoKloud Cyber Intelligence Centre

April 2025 witnessed a significant escalation in cyber threat activity, marked by high-profile ransomware attacks and the growing use of AI-driven tactics. Notably, UK retailers **Marks & Spencer** and **Co-op** faced major disruptions due to cyber incidents. The attack on M&S, attributed to the "**Scattered Spider**" group, led to substantial operational challenges and financial losses, highlighting the vulnerabilities within retail IT systems. Similarly, Co-op proactively shut down parts of its IT infrastructure in response to unauthorized access attempts, underscoring the pervasive threat landscape.

“ Cyber threats are evolving - our defences must evolve faster. It's time for a new approach to cyber security. “

The RSAC Conference 2025 emphasized the urgent need for adaptive security measures to counter these evolving threats. Additionally, the aviation industry faced unprecedented challenges, with incidents involving GPS spoofing and potential sabotage, signaling a shift towards more complex, hybrid cyber-physical threats. These developments underscore the necessity for organisations to bolster their cybersecurity strategies, emphasizing proactive threat intelligence, robust incident response plans, and continuous monitoring to defend against the increasingly sophisticated threat environment.

Year to date 2025

⚠ **7748**

Global Ransomware Victims

April 2025

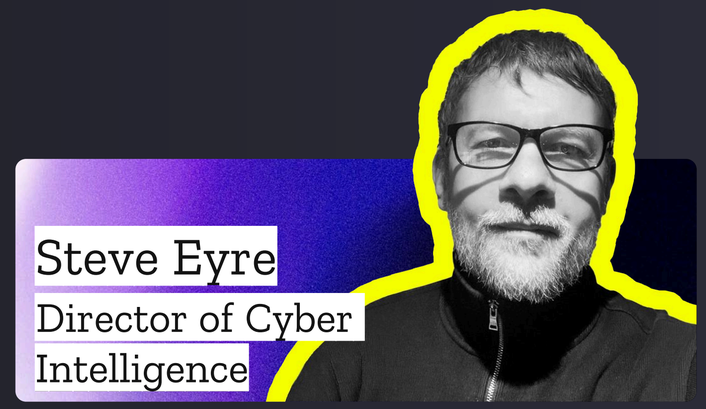
↗ **498**

Global Ransomware Victims

United Kingdom

559

UK Ransomware Attacks in 2025 so far



CS/Labs

Scattered Spider Intelligence Brief

☣ AveMaria ☣ Raccoon Stealer
☣ VIDAR Stealer ⌘ Fleetdeck.io
⌘ Level.io ⌘ Mimikatz ⌘ Ngrok
⌘ Pulseway ⌘ Screenconnect
⌘ TeamViewer ⌘ Tailscale
⌘ Splashtop ⌘ Tactical.RMM

Who are Scattered Spider?

Scattered Spider, also known by aliases such as **0ktapus** and **Octo Tempest**, is a cybercriminal group primarily composed of teenagers and young adults from the U.S. and U.K.

First identified in 2022, the group initially targeted telecommunications companies but has since expanded its focus to include technology and hospitality sectors.

Scattered Spider is notorious for high-profile cyberattacks, including the Twilio breach in August 2022 and the MGM Resorts breach in September 2023.

The group employs a variety of tactics, including SIM swapping, multi-factor authentication (MFA) fatigue attacks, and phishing campaigns via SMS and Telegram.

They utilize **infostealers** like **AveMaria**, **Raccoon Stealer**, and **VIDAR Stealer**, along with legitimate remote management tools, to gain and maintain access to compromised networks.

M&S Ransomware Incident – April 2025

On 23 April, **Marks & Spencer** fell victim to a ransomware attack by the Scattered Spider group, disrupting online orders, contactless payments, and store operations. Attackers exploited social engineering and credential theft to deploy the **Dragon Force** encryptor via compromised VMware ESXi hosts.

Key Impacts:

- Online orders cancelled and refunded
- Contactless payments and gift cards temporarily disabled
- Over 200 warehouse staff stood down
- Share price dropped by ~8%

Response:

- No evidence of customer data being compromised
- Cybersecurity firms (CrowdStrike, Microsoft, Fenix24) engaged
- Authorities notified; phased service restoration ongoing

The incident underscores the importance of swift containment, transparency, and cyber resilience in today's threat landscape.

Malware & Tooling Used By Scattered Spider

Malware:

- **AveMaria -** A remote access trojan (RAT) that enables full control of infected systems, including webcam/mic access and keylogging.
- **Raccoon Stealer -** A credential stealer that extracts passwords, cookies, and autofill data from browsers.
- **VIDAR Stealer -** Similar to Raccoon, it grabs credentials, cryptocurrency wallets, and sensitive files.
- **Mimikatz -** A well-known tool used to extract passwords and authentication tokens from memory.

Tooling:

- **Ngrok –** Tunnels internal services to the internet, often used to bypass firewalls.
- **Fleetdeck.io / Level.io / Pulseway / Tactical.RMM / Tailscale –** Legitimate IT management tools used for remote access and system control.
- **ScreenConnect / Splashtop / TeamViewer –** Remote desktop tools repurposed by attackers for stealthy access.

TTPs of Malware Used Scattered Spider

Technique (ID)	Description	AveMaria	Raccoon	Vidar
Initial Access				
Phishing (T1566.001)	Malicious email attachments (spearphishing) deliver the malware	✓		✓
Exploitation for Client Execution (T1203)	Exploits a vulnerable Office application to run shellcode	✓		
Supply Chain Compromise (T1195)	Distributed via cracked software downloads		✓	
Execution				
Command and Scripting Interpreter (T1059.003)	Uses Windows command shell (batch scripts) for execution	✓		
Windows Management Instrumentation (T1047)	Launches processes via WMI (WMIC) commands	✓		
Malicious File (T1204.002)	Executes delivered malicious binaries/files			✓
Persistence				
Registry Run Keys / Startup Folder (T1547.001)	Creates a registry Run key for auto-start on logon	✓		
Privilege Escalation				
Bypass User Account Control (T1548.002	Bypasses UAC via the SDCLT (Computer Defaults) technique	✓		
Process Injection (T1055)	Injects code into other processes (e.g. cmd.exe or explorer.exe)	✓		✓
Credential Access				
Input Capture: Keylogging (T1056.001)	Hooks keystroke APIs to log user input	✓		
Credentials from Web Browsers (T1555.003)	Harvests saved browser passwords, cookies, autocomplete data	✓	✓	✓
Credentials in Files (T1552.001)	Searches for insecurely stored credentials in files on disk			✓
Discovery				
System Information Discovery (T1082)	Gathers system details (OS version, CPU, memory, etc.)	✓	✓	
Account Discovery (T1087)	Enumerates local user accounts and privileges		✓	
File and Directory Discovery (T1083)	Identifies target files/folders for collection based on configuration		✓	✓
Exfiltration				
Automated Exfiltration (T1020)	Automatically collects and exfiltrates identified files/data		✓	
Exfiltration Over C2 Channel (T1041)	Sends stolen data out over existing C2 (HTTP) channels		✓	✓
Archive Collected Data (T1560)	Compresses or archives data prior to exfiltration		✓	
Command and Control				
Application Layer Protocol: Web (T1071.001)	C2 communication over HTTP(S) (POST requests)		✓	✓
Non-Application Layer Protocol (T1095)	Uses custom/non-HTTP protocols for C2 (RC4-encrypted TCP)	✓		

Ransomware Statistics Summation

CyberShadows
INTELLIGENCE LED APPROACH TO CYBER RESILIENCE

Year to date 2025

7748

Global Ransomware Victims

Over the year to date for 2024, there have been 7748 companies that have been affected by Ransomware attacks.

April 2025

498

Global Ransomware Victims

In April alone there has been 498 confirmed incidents of successful ransomware attacks globally, indicating a steady rise in attacks.

United Kingdom

559

UK Ransomware Attacks

559 UK Businesses have been victims of ransomware attacks in 2025 so far.

Ransomware Groups Activity (30 Days)

Akira	72 Companies Impacted
Qilin	42 Companies Impacted
Play	40 Companies Impacted

Top Targeted Industries April 2025

1	Healthcare
2	Manufacturing
3	Technology

Top Targeted Countries (Ransomware)

USA	39%
Germany	5%
Canada	4%

Latest Ransomware Events

Lynx ransomware group were responsible for 5 cyber attacks in recent days.

3 Victims | 1 Victim | 1 Victim

UK Businesses That Experienced A Cyber Incident This Year To Date

49%

Phishing

Remains Most Common Attack Vector Globally Across The First Quarter Of 2025

New **Crypto24** Ransomware Group Hits 8 Victims in April 2025

8 Victims Across Canada, Indonesia, Singapore and the US

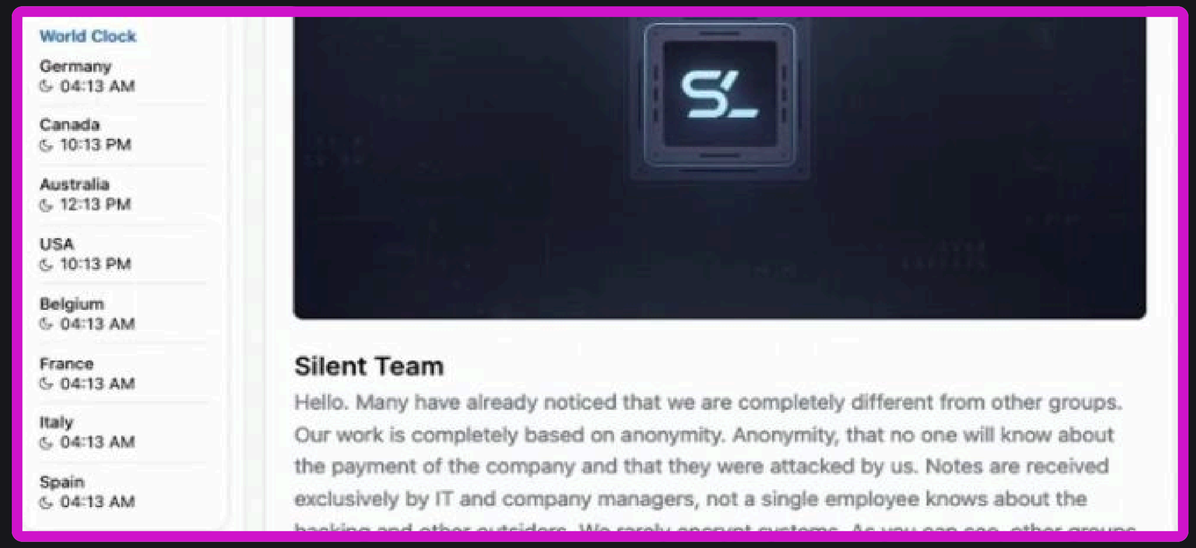
Purview of the Threat Landscape

CS Labs

Over April we have seen a record number of New Threat Groups in particular Silent and Gunra:

Who are **Silent** Threat Group?

Silent Team differentiates itself from other threat groups by openly publishing sensitive information, such as company revenue and employee counts, directly on their Data Leak Site (DLS). Recent breaches involve Advanced Simulation Technology Inc., Fleet Canada, and ESP Associates, all accompanied by scare tactics like countdown timers. Unlike traditional ransomware groups, Silent Team claims to operate discreetly without public negotiations, focusing on stealing and selling or selectively publishing confidential corporate information, although their precise tactics (TTPs) remain unknown

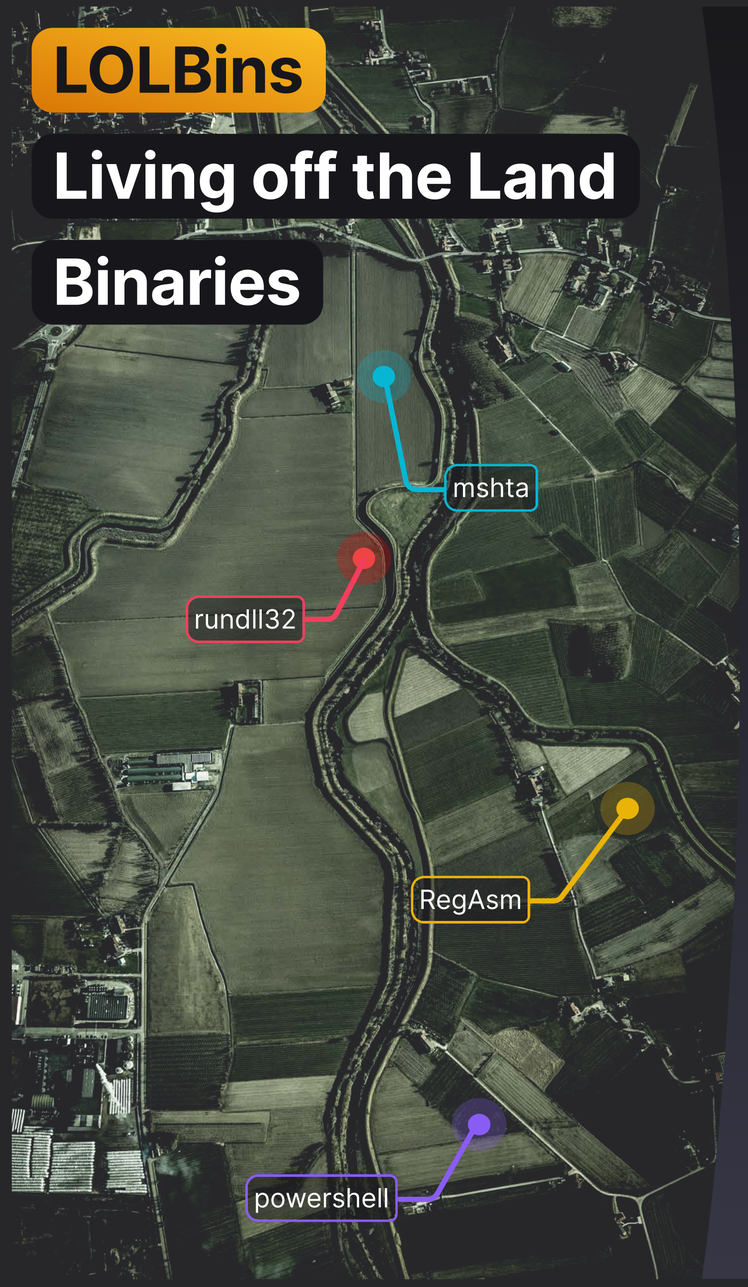


Who are **Gunra** Threat Group?

Gunra is a newer ransomware group known for using 'StealC' family infostealers to exfiltrate data, targeting both internal systems and third-party domains. Their Data Leak Site (DLS) is extremely minimalist, featuring only a 'Contact Us' button aside from breach announcements. Recent breaches of Shinko Shoji, Dar Al Teb, and Varela Hermanos have already expired. Gunra's specific motives and tactics (TTPs) are currently unclear, reflecting their secretive and emerging threat profile.

TTP Deeper Insights

CS Labs



What are LOLBins?

LOLBins (Living-off-the-Land Binaries) are legitimate system tools that attackers abuse to avoid detection. Since they're trusted Windows components, using them helps malware blend in and bypass security controls like Application Whitelisting (AWL).

AgentTesla Overview

A recent sample of the AgentTesla info-stealer revealed a multi-stage infection chain:

- Stage 1: A JavaScript file downloads a PowerShell script from a malicious IP.
- Stage 2: The script decrypts a payload and generates a new executable.
- Stage 3: The malware downloads a file containing a malicious DLL.

LOLBins Highlight: RegAsm.exe

- The malware uses **RegAsm.exe**, a legitimate .NET tool, to execute the DLL.
- This technique enables an AWL bypass, since RegAsm is trusted by Windows.

Exfiltration & Impact

- AgentTesla exfiltrates data via FTP, with open ports confirmed on Shodan.
- Stolen data was accessible on the server, dated as recently as 14 April 2025.

Key Takeaway

LOLBins like RegAsm.exe are powerful tools for attackers. Detection must focus on behavior, not just binaries.

Managing & Mitigating Threats

CS Labs

Detecting Living-off-the-Land Binaries (LOLBins)

Living-off-the-land binaries (LOLBins) are legitimate system tools such as PowerShell, WMIC, or mshta that attackers exploit to execute malicious activity while avoiding detection. Because these binaries are trusted and often whitelisted, identifying their misuse requires a more advanced, behavior-based detection approach. In modern Security Operations, detecting LOLBins involves monitoring for abnormal usage patterns, such as unusual execution contexts, command-line arguments, or the invocation of scripts from unexpected locations. Our Security team leverage endpoint detection and response (EDR) tools, threat intelligence, and behavioral analytics to flag suspicious activity that deviates from normal ‘patterns of life’. Proactive hunting and detailed logging are essential to distinguishing between benign administrative use and malicious exploitation of these native tools.

Best Practices

- Use strong, unique passwords for each account (consider a password manager).
- Enable multi-factor authentication (MFA) wherever possible.
- Keep all software and systems updated with the latest security patches.
- Regularly back up important data to secure, offline locations.
- Be cautious with links and attachments in emails and messages — verify before clicking.

Mitigate Malware

- Install reputable antivirus and anti-malware software and keep it updated.
- Download software only from official or trusted sources.
- Disable macros in Office documents received via email, unless necessary.

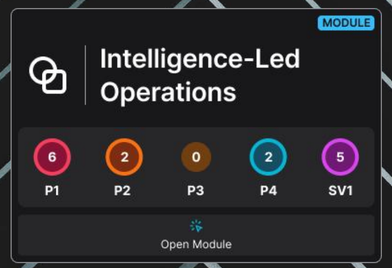
Safe Web Browsing

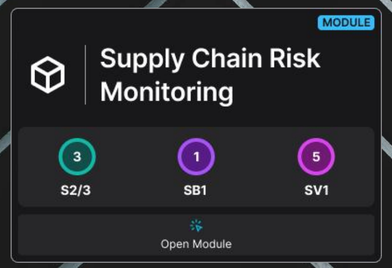
- Use HTTPS websites — check for the padlock icon in the browser address bar.
- Avoid public Wi-Fi for sensitive transactions, or use a trusted VPN service.
- Keep all software and systems updated with the latest security patches.
- Clear your browser cache and cookies regularly.

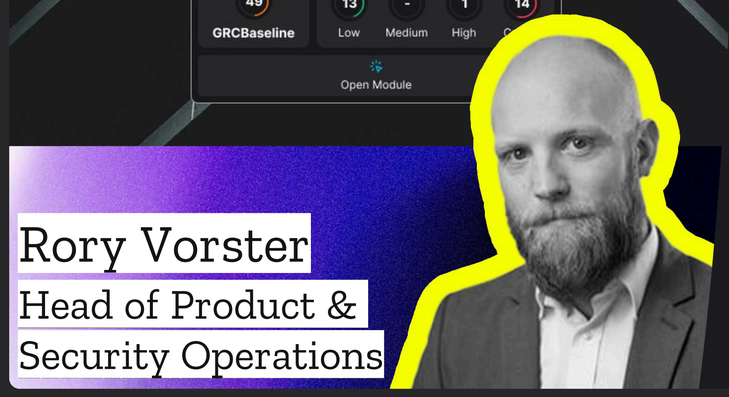
CyberShadows
INTELLIGENCE LED APPROACH TO CYBER RESILIENCE

CyberShadows Product Development Update

Version 2.0







Rory Vorster
Head of Product & Security Operations

CyberShadows Version 2.0

As V2 progresses through final testing, we are extremely excited to get the new CyberShadows experience into the hands of all our users.

With massive advancements to Forensic Data Analytics and the inclusion of our industry leading Rumour Engine - this truly is a massive step forward in providing a powerful, Intelligence-led platform to discover, detect and respond to zero-hour threats.

Enhanced Forensic Data Analytics (FDA)

Enhanced FDA now delivers a process focus in the context of a detection, affording a rich data pool to support the trigger of an alert - informing analysts with the full picture down to bit-level.

This greater depth within the 60 second pre and post Indicator of Attack interaction means that the critical timeline is already to hand within seconds. Allowing for rapid response to threats with the greatest level of confidence.

The All New Analysis Workbench

The Workbench is a growing suite of tools that will support the analysis, investigation and research into evolving threats with direct user feedback on suspicious IP addresses, showing the active ports that are serving malware in real-time.

Advancements in this space will enable incident management, analyst reporting and a deeper view into the intelligence core surrounding malicious infrastructure globally.


KryptoKloud
SECURITY MADE SIMPLE
For more information contact
sales@kryptokloud.com
CyberShadows
INTELLIGENCE LED APPROACH TO CYBER RESILIENCE
CS Labs