blackpoint

THREAT PROFILE:

# World Leaks Ransomware

ADVERSARY
BLACKPOINT CYBER
APG
PURSUIT GROUP

# TABLE OF CONTENTS

# Executive Summary

**First Identified:**

2025

**Operation style:**

Extortion-as-a-Service platform

**Extortion method:**

Data Extortion - World Leaks is reported to have shifted away from encryption after rebranding from Hunters International Ransomware.

**Most frequently targeted industry:**

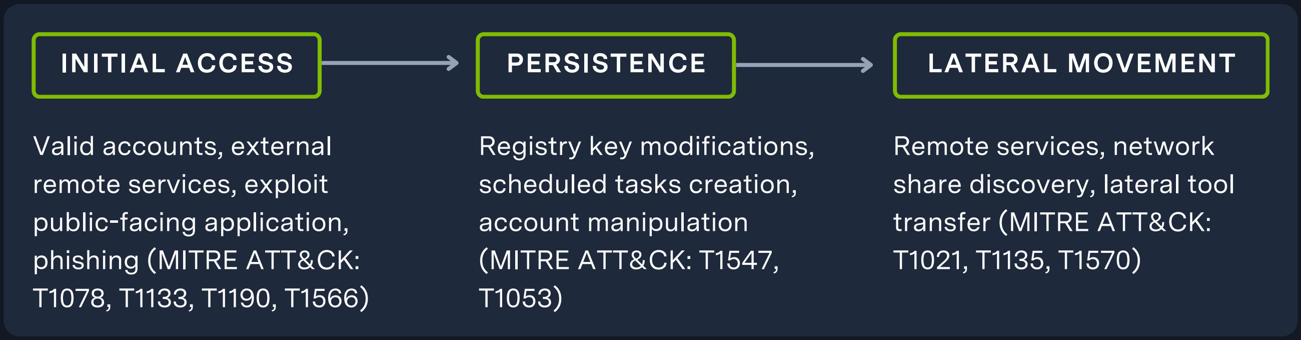
- Industrials (Manufacturing)

**Most frequently targeted victim HQ region:**

- North America

**Known Associations:**

- Hunters International Ransomware
- Hive Ransomware
- Secp0 Ransomware
- UNC6148



INITIAL ACCESS

Valid accounts, external remote services, exploit public-facing application, phishing (MITRE ATT&CK: T1078, T1133, T1190, T1566)

PERSISTENCE

Registry key modifications, scheduled tasks creation, account manipulation (MITRE ATT&CK: T1547, T1053)

LATERAL MOVEMENT

Remote services, network share discovery, lateral tool transfer (MITRE ATT&CK: T1021, T1135, T1570)

# Description

World Leaks emerged in early 2025 as the successor to Hunters International, a ransomware group known for encrypting victim data and demanding payment for decryption keys. Unlike Hunters International, World Leaks claims to have abandoned encryption; however, some incidents have reported encryption despite group claims.

This change reflects a broader trend in cybercriminal activity where threat actors prioritize data theft and public exposure over traditional ransomware encryption, reducing operational complexity and increasing pressure on victims through reputational damage. This approach is growing in popularity because when encryption-based attacks are avoided, they are harder to detect and remediate.

Their attack pattern focuses on stealing sensitive data from targeted organizations rather than encrypting files. They typically gain initial access through phishing campaigns, compromised credentials, or exploitation of exposed services.

Once inside, they perform data discovery and exfiltration, prioritizing confidential corporate or personal information. After successfully exfiltrating data, World Leaks initiates the extortion phase, threatening to publish the stolen information on their leak site if the victim does not pay. This approach eliminates the need for encryption, allowing the group to remain stealthier and execute attacks faster while maintaining strong leverage over victims

World Leaks primarily targets large enterprises, technology firms, and organizations with valuable intellectual property, as noted by Unit42 and Trend Micro. They focus on companies with Internet facing infrastructure and weak authentication controls, such as VPNs without MFA. Their victim profile includes high-value sectors where data exposure can cause severe reputational and regulatory damage.

> "The emergence of World Leaks underscores a growing trend among cybercriminals: prioritizing data theft and leak-based extortion over encryption, reducing operational complexity and increasing pressure on victims."
> — Recorded Future Threat Intelligence

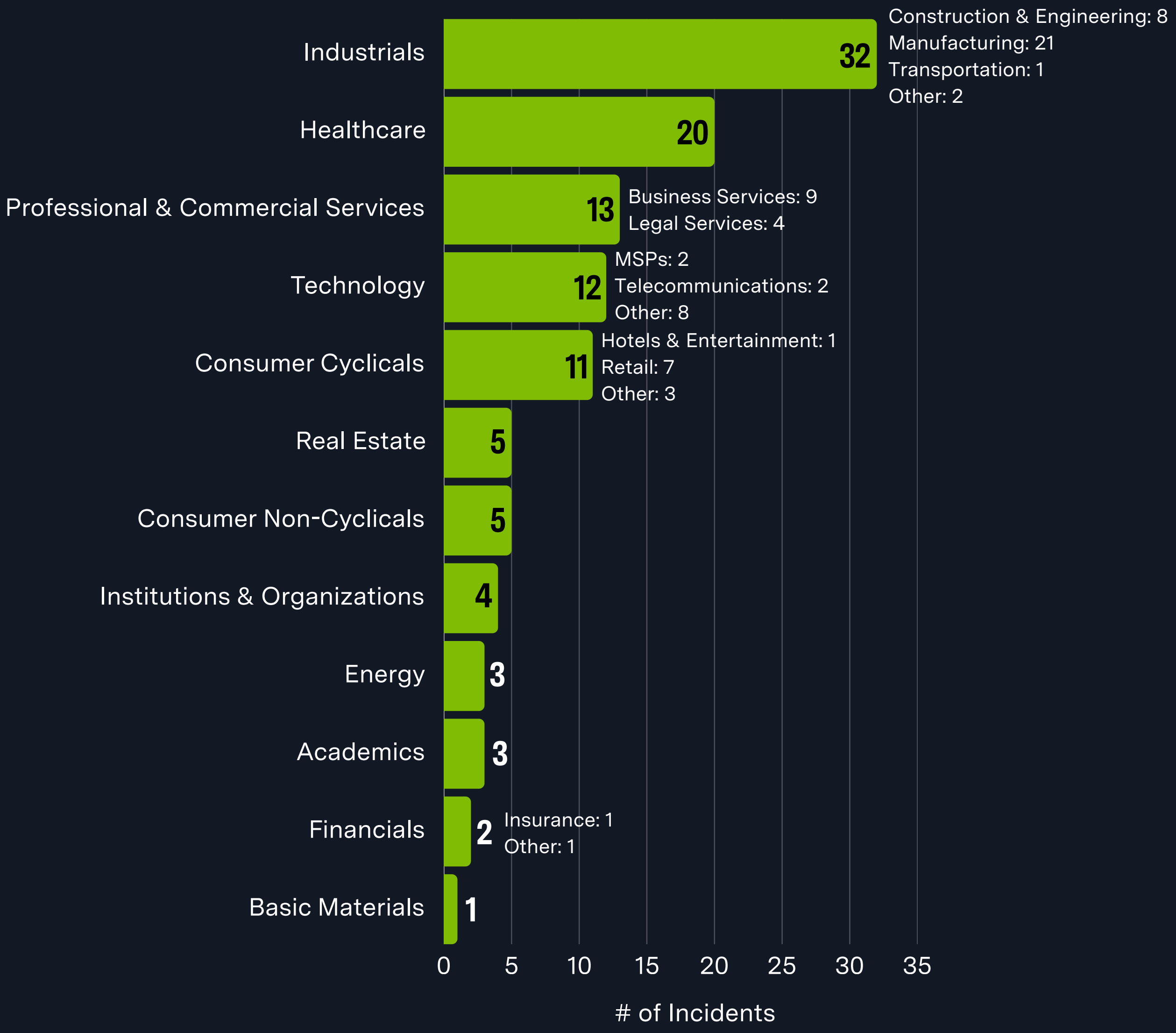
One of the most significant incidents attributed to World Leaks was the Dell breach, where the group claimed to have stolen 1.3 TB of sensitive data, including infrastructure and customer information. Dell confirmed a compromise of its test lab platform, though it disputed the scale of the breach. This attack underscores World Leaks' ability to infiltrate major tech companies and exfiltrate massive datasets without deploying ransomware encryption.

World Leaks has demonstrated a clear evolution in tactics and targeting that reflects broader shifts in the ransomware ecosystem. The group leverages techniques such as SOCKSv5 proxies and TOR for secure communications and ransom negotiations, making attribution and tracking difficult.

They also maintain an active leak site to publish stolen data, which serves both as a pressure tactic and a reputation-building mechanism within the criminal underground. Intelligence reports indicate that World Leaks is highly selective in its targeting, focusing on organizations with significant intellectual property and weak authentication practices, such as VPNs lacking multifactor authentication. This strategic approach, combined with their pure extortion model, positions World Leaks as a leading example of the growing trend toward hack and leak operations that prioritize stealth, speed, and reputational damage over traditional encryption based ransomware attacks.

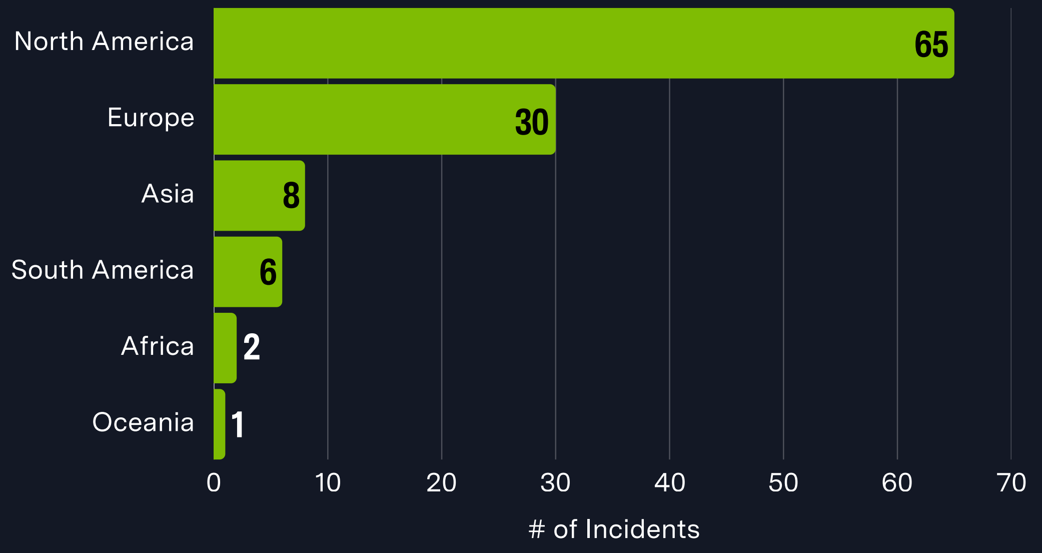
# Previous Targets

## Previous Industry Targets from 01 Jan 2025 to 15 Dec 2025

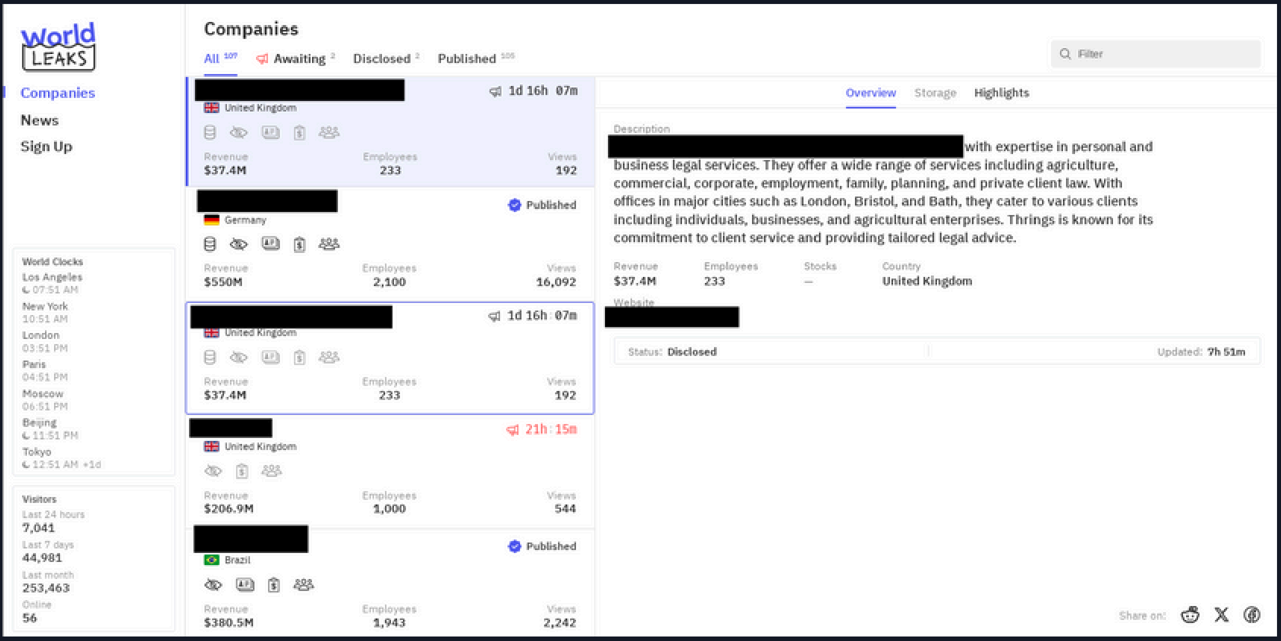


# Previous Targets

## Previous Victim HQ Regions from 01 Jan 2025 to 15 Dec 2025



# Data Leak Site



World LEAKS

Companies

News

Sign Up

World Clocks
Los Angeles
07:51 AM
New York
10:51 AM
London
03:51 PM
Paris
04:51 PM
Moscow
06:51 PM
Beijing
11:51 PM
Tokyo
12:51 AM +1d

Visitors
Last 24 hours
7,041
Last 7 days
44,981
Last month
253,463
Online
56

## Companies

All 107 · Awaiting 2 · Disclosed 2 · Published 105

Filter

[redacted] — 1d 16h 07m
United Kingdom
Revenue $37.4M · Employees 233 · Views 192

[redacted] — Published
Germany
Revenue $550M · Employees 2,100 · Views 16,092

[redacted] — 1d 16h 07m
United Kingdom
Revenue $37.4M · Employees 233 · Views 192

[redacted] — 21h 15m
United Kingdom
Revenue $206.9M · Employees 1,000 · Views 544

[redacted] — Published
Brazil
Revenue $380.5M · Employees 1,943 · Views 2,242

Overview · Storage · Highlights

Description

[redacted] with expertise in personal and business legal services. They offer a wide range of services including agriculture, commercial, corporate, employment, family, planning, and private client law. With offices in major cities such as London, Bristol, and Bath, they cater to various clients including individuals, businesses, and agricultural enterprises. Thrings is known for its commitment to client service and providing tailored legal advice.

| Revenue | Employees | Stocks | Country |
|---|---|---|---|
| $37.4M | 233 | — | United Kingdom |

Website
[redacted]

Status: Disclosed · Updated: 7h 51m

Share on:

hxxps[:]//worldleaksartrjm3c6vasllvgacbi5u3mgzkluehrzhk2jz4taufuid[.]onion/

The platform prominently displays a victim list with countdown timers to pressure organizations into payment before public disclosure. Its design includes a file explorer that enables browsing individual files rather than downloading entire archives, amplifying psychological impact and accessibility. Additional features such as a news section, social sharing buttons, and a recently introduced journalist sign-up for early access via the Insider platform demonstrate a strategic effort to maximize visibility and influence.

Integrated with a victim panel, the site offers tabs for overview, storage, disclosure, payment, and live chat, allowing victims to monitor exfiltrated data and interact with attackers under a strict Bitcoin only, “no negotiation” policy. Despite its ambitions, the platform has faced operational challenges, including missed disclosure deadlines and inconsistent leak sizes, which undermine its credibility. These issues, combined with its evolving partnerships and shift toward an extortion only model, indicate that World Leaks is actively refining its tactics to maintain relevance in the cyber extortion ecosystem.

# Known Exploited Vulnerabilities

| Vulnerability | Description | Product Affected | CVSS |
|---|---|---|---|
| CVE-2021-20035 | OS Command Injection Vulnerability | SonicWall SMA100 Appliances | 6.5 |
| CVE-2021-20038 | Stack-based Buffer Overflow Vulnerability | SonicWallSMA100Appliance | 9.8 |
| CVE-2021-20039 | OS Command Injection Vulnerability | SonicWall SMA100 Appliances | 8.8 |
| CVE-2024-38475 | Improper Escaping of Output Vulnerability | Apache HTTP Server | 9.1 |
| CVE-2025-32819 | Authentication Bypass Vulnerability | SonicWall SMA100 Appliances | 8.8 |

# Associations

## Hunters International Ransomware

World Leaks is a direct rebrand of the Hunters International ransomware group. Hunters International shut down its ransomware operations in mid 2025 due to law enforcement pressure and declining profitability, pivoting to World Leaks' extortion-only model. This transition preserved much of the infrastructure and affiliate network from Hunters International, making World Leaks a strategic evolution rather than a new entity.

## Hive Ransomware

Hunters International, and by extension World Leaks, inherited tactics and some infrastructure from Hive, which was dismantled by law enforcement in early 2023. This lineage indicates a continuity of expertise and operational methods across these groups.

## Secp0 Ransomware

World Leaks has a confirmed collaboration with Secp0, sharing leak site infrastructure and possibly resources for extortion campaigns. This partnership suggests World Leaks is positioning itself as an Extortion-as-a-Service platform attractive to other threat actors seeking to leverage its tools and infrastructure.

## UNC6148

A financially motivated threat group known for targeting SonicWall Secure Mobile Access (SMA) 100 series appliances for initial access. The group has impacted at least one victim that has been named on the World Leaks data leak site. The extent of the relationship between the two groups remain unknown at the time of writing.

# Known Tools

| | |
|---|---|
| **7-zip** | A tool that is used to compress files into an archive. Used by threat actors to compress data before exfiltration. |
| **AdFind** | A free command-line query tool that can be used for gathering information from Active Directory. |
| **bcdedit** | A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options. |
| **LSASS** | A Windows component that manages user authentication and security policies. |
| **MEGA** | A cloud storage and file hosting service that has been abused by threat actors to host stolen data. |
| **NirSoft** | A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more. |
| **OVERSTEP** | A rootkit and persistent backdoor specifcally designed to target SonicWall Secure Mobile Access (SMA) 100 series appliances. |
| **PC Hunter** | A toolkit for Windows with various powerful features for kernel structure viewing and manipulating. |
| **PowerShell** | A task automation and configuration management program that includes a command-line shell and the associated scripting language. |
| **Process Hacker** | An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process. |
| **PsExec** | A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute. |
| **Rclone** | A command line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA. |

# Known Tools

| | |
|---|---|
| **RDP** | A protocol that provides a user with a graphical interface to connect to another computer over a network connection. |
| **SMB** | A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network. |
| **Storage Software** | A proprietary exfiltration utility developed after rebranding from Hunters International. The tool automates large-scale data theft and is central to their extortion-only model. |
| **wbadmin** | A command line utility that is used to backup and restore OS, drive volumes, files, folders, and applications from a command line interface. |
| **WMIC** | A utility that provides a command-line interface for Windows Management Instrumentation. |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| **Initial Access** | |
| T1078: Valid Accounts | |
| T1190: Exploit Public - Facing Application | |
| T1555: Extraction of Stored Credentials from Browsers and Applications | |
| T1566: Phishing | .001: Spearphishing Attachment |
| **Execution** | |
| T1059: Command line | .001 Powershell |
| **Persistence** | |
| T1053: Scheduled Task/Job | .005: Scheduled Task |
| T1098: Account Manipulation | |
| T1547: Boot or Logon Autostart Execution | .001 Registry Run Keys / Startup Folder |
| **Defense Evasion** | |
| T1027: Obfuscated Files or Information | |
| T1070: Inicator Removal | |
| T1562: Impair Defense | |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| Credential Access | |
| T1003: OS Credential Dumping | |
| T1555: Credentials from password stores | |
| Discovery | |
| T1069: Permissions Groups Discovery | .002 Domain Groups |
| T1082: System Information Discovery | |
| T1083: Fie and Directory Discovery | |
| T1087: Account Discovery | .002 Domain Account |
| T1135: Network Share Discovery | |
| T148: Domain Trust Discovery | |
| Lateral Movement | |
| T1021: Exploitation of Remote Services | .001: Remote Desktop Protocol<br>.002: SMB/Windows Admin Shares |
| T1570: Lateral Tool Transfer | |
| Collection | |
| T1005: Data from Local System | |
| T1560: Archive Collected Data | |

# MITRE ATT&CK® Mappings

| | |
|---|---|
| Command and Control | |
| T1090: Proxy | |
| T1071: Application Layer Protocol | |
| T1219: Remote Access Tools | .002: Remote Desktop Software |
| T1573: Encrypted Channel | |
| Exfiltration | |
| T1041: Exfiltration Over C2 Channel | |
| T1048: Exfiltration Over Alternative Protocol | |
| T1567: Exfiltration Over Web Server | .002: Exfiltration to Cloud Storage |
| Impact | |
| T1490: Inhibit System Recovery | |
| T1491: Defacement | .001: Internal Defacement |
| T1657: Financial Theft | |

# References

- Halcyon (n.d.) “World Leaks Threat Actor.” https://www.halcyon.ai/threat-group/worldleaks
- Ransom Live (n.d.) “World Leaks.” https://www.ransomware.live/group/worldleaks
- SOSRansomware (2025, August 20) “World leaks: between pure extortion and traditional ransomware, what’s the difference?” https://sosransomware.com/en/ransomware-groups/worldleaks-between-pure-extortion-and-traditional-ransomware-whats-the-difference/
- CPO Magazine (2025, July 28) “IT giant Dell Technologies has confirmed a security breach after a threat actor leaked extensive infrastructure data.” https://www.cpomagazine.com/cyber-security/dell-confirms-security-breach-after-world-leaks-gang-releases-1-3-tb-of-data-company-disputes-claims/
- Bleeping Computer (2025, July 21) “Dell confirms breach of test lab platform by World Leaks extortion group.” https://www.bleepingcomputer.com/news/security/dell-confirms-breach-of-test-lab-platform-by-world-leaks-extortion-group/”
- Bleeping Computer (2025, April 3) “Hunters International shifts from ransomware to pure data extortion.” https://www.bleepingcomputer.com/news/security/hunters-international-rebrands-as-world-leaks-in-shift-to-data-extortion/
- Hack Read (2025, July 21) “World Leaks Claims Dell Data Breach, Leaks 1.3 TB of Files.” https://hackread.com/world-leaks-dell-data-breach-leaks-1-3-tb-of-files/
- Lexfo (2025, May 20) “World Leaks: An Extortion Platform.” https://blog.lexfo.fr/world-leaks-an-extortion-platform.html
- Secureworks (2025, August 15) “World Leaks: GOLD CRESCENT’s Shift to Hack-and-Leak Extortion.” https://www.secureworks.com/blog/world-leaks-gold-crescent-hack-and-leak
- Secureworks (2025, June 10) “Hunters International Evolves into World Leaks.” https://www.secureworks.com/blog/hunters-international-evolution

Adversary Pursuit Group

blackpoint