

# 脅威アクター動向ダイジェスト（2026-09-24）

対象：直近7日間に収集した情報（09/17 16:33～09/24 16:33 JST）

注：アクターへの帰属（アトリビューション）はベンダー・当局の見解であり確定事実ではありません。リークサイト掲載は犯行グループ側の主張であり、被害の事実確認は別途必要です。

## 情報源（発信元）の内訳

| 発信国    | 記事数 |
|--------|-----|
| 日本     | 150 |
| 中国     | 141 |
| 米国     | 122 |
| 韓国     | 18  |
| ロシア    | 11  |
| スロバキア  | 10  |
| イスラエル  | 10  |
| シンガポール | 1   |
| ベトナム   | 1   |
| 国籍非公表  | 1   |

発信元の国の立場や利害が、記事の内容・帰属の主張に影響している可能性があります。

## 誰が、誰について語っているか（発信国 × 対象区分）

| 発信国<br>＼ 対象 | ランサム<br>ウェア | 米国・ファ<br>イブアイズ<br>系 | 北朝鮮系 | 中国系 | ロシア系 | イラン系 | 金銭目的犯<br>罪（ランサ<br>ム関連含<br>む） | 識別率    |
|-------------|-------------|---------------------|------|-----|------|------|------------------------------|--------|
| 米国          | 30          | ・                   | 1    | 2   | 3    | 1    | 1                            | 33/122 |
| 中国          | 13          | 2                   | 4    | 3   | 3    | 4    | 2                            | 19/141 |
| ロシア         | 9           | 1                   | ・    | ・   | ・    | ・    | 1                            | 9/11   |
| 韓国          | 5           | ・                   | ・    | ・   | 2    | ・    | ・                            | 6/18   |
| イスラエ<br>ル   | 5           | ・                   | ・    | 1   | ・    | ・    | ・                            | 5/10   |
| 日本          | 1           | ・                   | ・    | ・   | ・    | ・    | ・                            | 1/150  |
| スロバキ<br>ア   | ・           | ・                   | ・    | 1   | ・    | ・    | ・                            | 1/10   |
| シンガ<br>ポール  | ・           | ・                   | ・    | ・   | ・    | ・    | ・                            | 0/1    |

| 発信国<br>＼ 対象 | ランサム<br>ウェア | 米国・ファ<br>イブアイズ<br>系 | 北朝鮮系 | 中国系 | ロシア系 | イラン系 | 金銭目的犯<br>罪（ランサ<br>ム関連含<br>む） | 識別率 |
|-------------|-------------|---------------------|------|-----|------|------|------------------------------|-----|
| ベトナム        | .           | .                   | .    | .   | .    | .    | .                            | 0/1 |
| 国籍非公<br>表   | .           | .                   | .    | .   | .    | .    | .                            | 0/1 |

数字はグループ名が識別された記事の数（1記事が複数区分に数えられる場合あり）。識別率＝グループ名が識別された記事数／その国の記事総数。

## 1. 日本関連

リークサイト新規掲載（日本）：11 件

出典：ransomware.live（各ランサムウェアグループのリークサイトを集約する個人運営サイト）。掲載内容は犯行グループ側の主張。

| グループ            | 掲載組織                              | 業種                              | 攻撃日(主張)    | 検知日        |
|-----------------|-----------------------------------|---------------------------------|------------|------------|
| auditteam       | ki***jp                           | Not Found                       | 2026-09-09 | 2026-09-10 |
| auditteam       | kit-e.jp                          | Technology                      | 2026-09-09 | 2026-09-18 |
| vexy ransomware | Hashimoto Jimuki                  | Manufacturing                   | 2026-09-15 | 2026-09-15 |
| metaencryptor   | Astemo, Ltd.                      | Manufacturing                   | 2026-09-21 | 2026-09-21 |
| metaencryptor   | Nippon Steel Corporation          | Manufacturing                   | 2026-09-15 | 2026-09-15 |
| Qilin           | IKEGAMI TSUSHINKI COMPANY LIMITED | Manufacturing                   | 2026-09-21 | 2026-09-21 |
| Qilin           | Mitsuwa Trading Co., Ltd          | Retail & E-Commerce             | 2026-09-09 | 2026-09-09 |
| RansomHouse     | REXT Holdings Co., Ltd.           | Other                           | 2026-09-01 | 2026-09-01 |
| SafePay         | ryomo.co.jp                       | Not Found                       | 2026-09-15 | 2026-09-15 |
| The Gentlemen   | Tentac                            | Technology                      | 2026-09-14 | 2026-09-15 |
| The Gentlemen   | Wada Farms                        | Agriculture and Food Production | 2026-09-14 | 2026-09-15 |

日本関連記事：30 件

- ・ [美容医療プラットフォーム「Unni（カンナムオンニ）」への不正アクセスについてまとめたみた](#)  
piyolog・2026-09-24 / 発信元：日本・個人ブログ
- ・ [旭化成の元従業員による営業秘密の持ち出しについてまとめたみた](#)  
piyolog・2026-09-24 / 発信元：日本・個人ブログ
- ・ [Ransom & Dark Web Issues Week 4, September 2026](#)  
AhnLab ASEC・2026-09-23 / 発信元：韓国・民間企業 / 関連：ShinyHunters, metaencryptor

- [关于2026年人工智能大模型安全众测活动典型漏洞风险的通报](#)  
CNCERT・2026-09-22 / 発信元：中国・政府系機関（CNCERT・WeChat中継）
- [21st September - Threat Intelligence Report](#)  
Check Point Research・2026-09-22 / 発信元：イスラエル・民間企業
- [理工学部教職員がフィッシング被害、不審メールが送信 - 日大](#)  
Security NEXT・2026-09-18 / 発信元：日本・報道
- [TSUBAME Report Overflow \(Apr-Jun 2026\)](#)  
JPCERT/CC Eyes (英)・2026-09-18 / 発信元：日本・公的機関
- [xxx.soumu.go.jp などのサブドメインも拒否に ～ 総務省を装うフィッシングメール対策強化](#)  
ScanNetSecurity・2026-09-18 / 発信元：日本・報道
- [Should you care about an “AI slowdown?”](#)  
Cisco Talos・2026-09-18 / 発信元：米国・民間企業 / 関連：Qilin, The Gentlemen
- [The Odyssey and Trojans again: MovieReaper attacks users in multiple countries through compromised torrents](#)  
Securelist・2026-09-17 / 発信元：ロシア・民間企業（Kaspersky） / 関連：payload
- [Mitsubishi Electric GX Works3 and Motion Control Settings](#)  
CISA Advisories・2026-09-17 / 発信元：米国・政府機関
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’ s infrastructure and evidence of Qilin’ s AI use](#)  
Cisco Talos・2026-09-17 / 発信元：米国・民間企業 / 関連：AiLock, LockBit, Qilin, SafePay, The Gentlemen, netrunner, nightspire, payload, ransomexx, stormous
- [NTTドコモによるAmazonへの顧客情報の無断提供についてまとめた](#)  
piyolog・2026-09-17 / 発信元：日本・個人ブログ
- [2026年人工智能大模型安全众测结果发布](#)  
CNCERT・2026-09-17 / 発信元：中国・政府系機関（CNCERT・WeChat中継）
- [Ransom & Dark Web Issues Week 3, September 2026](#)  
AhnLab ASEC・2026-09-17 / 発信元：韓国・民間企業
- [Weekly Report: 警察庁が「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」を公開](#)  
JPCERT/CC 注意喚起等・2026-09-16 / 発信元：日本・公的機関
- [Weekly Report: 独立行政法人情報処理推進機構（IPA）が「ランサムウェア被害から学ぶ教訓集 経営者のためのランサムウェア対策ハンドブック」を公開](#)  
JPCERT/CC 注意喚起等・2026-09-16 / 発信元：日本・公的機関
- [4件目も見つかったAnthropicの評価中AIモデルによる不正アクセス事案についてまとめた](#)  
piyolog・2026-09-15 / 発信元：日本・個人ブログ
- [沖縄県知事選挙をめぐる偽情報や誹謗中傷の拡散についてまとめた](#)  
piyolog・2026-09-15 / 発信元：日本・個人ブログ
- [日本大学理工学部教職員のアカウントに対し巧妙に偽装されたフィッシングメール、多数の不審メールを送信](#)  
ScanNetSecurity・2026-09-15 / 発信元：日本・報道
- [MAMAMOO JAPAN OFFICIAL FANCLUB 「MOOMOO JAPAN」 に不正アクセス](#)  
ScanNetSecurity・2026-09-15 / 発信元：日本・報道

- ・ [日本企業はセキュリティの「意思決定」を外部委託 ～ MM総研調査](#)  
ScanNetSecurity・2026-09-15 / 発信元：日本・報道
- ・ [デジタル庁のガバメントソリューションサービス\(GSS\)への不正アクセスについてまとめた](#)  
piyolog・2026-09-11 / 発信元：日本・個人ブログ
- ・ [AI 生成图片的溯源真相：C2PA 内容凭证在传播链中的存活实测](#)  
先知社区・2026-09-08 / 発信元：中国・技術コミュニティ（アリババ系）
- ・ [Project Glasswingと日本国内の状況についてまとめた](#)  
piyolog・2026-09-08 / 発信元：日本・個人ブログ
- ・ [BinaryAI-Bench：面向实战业务的二进制安全分析任务评测集](#)  
腾讯安全威胁情报中心・2026-09-03 / 発信元：中国・民間企業（Tencent・WeChat中継） / 関連：payload
- ・ [ランサムウェアグループによるCursorの悪用についてまとめた](#)  
piyolog・2026-09-02 / 発信元：日本・個人ブログ
- ・ [“银狐” 木马专项——恶意域名及恶意IP（一）](#)  
CNCERT・2026-08-28 / 発信元：中国・政府系機関（CNCERT・WeChat中継）
- ・ [中国—东盟网络安全应急响应能力建设研讨会在北京举办](#)  
CNCERT・2026-08-27 / 発信元：中国・政府系機関（CNCERT・WeChat中継）
- ・ [Ransom & Dark Web Issues Week 4, August 2026](#)  
AhnLab ASEC・2026-08-27 / 発信元：韓国・民間企業 / 関連：NoName057(16), SafePay

## 2. ランサムウェア：リークサイト掲載状況

新規掲載 合計 619 件（74 グループ）

出典：ransomware.live（各ランサムウェアグループのリークサイトを集約する個人運営サイト）。掲載内容は犯行グループ側の主張。

| グループ            | 件数 | うち日本 |
|-----------------|----|------|
| The Gentlemen   | 60 | 2    |
| Qilin           | 59 | 2    |
| Akira           | 32 | 0    |
| Krybit          | 31 | 0    |
| auditteam       | 29 | 2    |
| storm           | 23 | 0    |
| settra          | 22 | 0    |
| INC Ransom      | 20 | 0    |
| SafePay         | 20 | 1    |
| direwolf        | 17 | 0    |
| emperador       | 16 | 0    |
| panzer          | 15 | 0    |
| Luna Moth       | 15 | 0    |
| vexy ransomware | 15 | 1    |
| metaencryptor   | 15 | 2    |

| グループ         | 件数 | うち日本 |
|--------------|----|------|
| LockBit      | 14 | 0    |
| n0n          | 13 | 0    |
| medusalocker | 9  | 0    |
| Play         | 9  | 0    |
| Rhysida      | 9  | 0    |

### 3. ランサムウェア：関連記事

#### payload

- [The Closed Quorum: Inside the first reported autonomous AI C2 implant](#)  
Cisco Talos・2026-09-22 / 発信元：米国・民間企業 / 検出表記：payload
- [Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO](#)  
Securelist・2026-09-21 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：PAYLOAD
- [Don't Call Us, We'll Call Your APIs | TraderTraitor Backdoors Resurface on Victim With No Crypto Ties](#)  
SentinelLabs・2026-09-19 / 発信元：米国・民間企業 / 検出表記：payload
- [The Odyssey and Trojans again: MovieReaper attacks users in multiple countries through compromised torrents](#)  
Securelist・2026-09-17 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：payload
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen's infrastructure and evidence of Qilin's AI use](#)  
Cisco Talos・2026-09-17 / 発信元：米国・民間企業 / 検出表記：payload
- [Agents at Large | Tracing Illicit OpenAI Agent Activity on Hugging Face](#)  
SentinelLabs・2026-09-16 / 発信元：米国・民間企業 / 検出表記：payload
- [NightEagle targets Russian companies](#)  
Securelist・2026-09-16 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：payload
- [浏览器的”信任”被伪造：KREMLIN 攻破 Chrome 完整性校验，1500+ 巴西网银主机沦陷](#)  
奇安信威胁情报中心・2026-09-16 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：payload
- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心・2026-09-11 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Payload
- [We've got one word for it, and it's usually the wrong one](#)  
Cisco Talos・2026-09-11 / 発信元：米国・民間企業 / 検出表記：payload
- [Detect and disrupt AI-themed attacks with Microsoft Defender](#)  
Microsoft Security・2026-09-11 / 発信元：米国・民間企業 / 検出表記：payload
- [PuzzleMask: Abusing Plain Prose as a Covert AI Attack Vector](#)  
Check Point Research・2026-09-10 / 発信元：イスラエル・民間企業 / 検出表記：payload

- [APT-C-55 \(Kimsuky\) 组织利用伪装安装包植入远控木马的攻击链分析](#)  
360威胁情报中心 · 2026-09-10 / 発信元：中国 · 民間企業 (Qihoo 360 · WeChat中継) / 検出表記：payload
- [Threat matrix: Mapping threats across cloud web applications](#)  
Microsoft Security · 2026-09-10 / 発信元：米国 · 民間企業 / 検出表記：payload
- [面向即时通讯工具的输入伪装与检测绕过：银狐类生态中 Hook 组件的技术迭代](#)  
腾讯安全威胁情报中心 · 2026-09-09 / 発信元：中国 · 民間企業 (Tencent · WeChat中継) / 検出表記：payload
- [Untracked Nightmares: The Threats Hiding Behind Commodity Infrastructure](#)  
Unit 42 · 2026-09-09 / 発信元：米国 · 民間企業 / 検出表記：payload
- [ClearFake WebDAV infection chain delivers Amatera stealer, ZigCryptoStealer, and NetSupport Manager](#)  
Cisco Talos · 2026-09-08 / 発信元：米国 · 民間企業 / 検出表記：payload
- [MetInfo CMS v7.6 前台 search 参数 SQL 注入漏洞分析与利用](#)  
先知社区 · 2026-09-05 / 発信元：中国 · 技術コミュニティ (アリババ系) / 検出表記：payload
- [每周高级威胁情报解读\(2026.08.28~09.03\)](#)  
奇安信威胁情报中心 · 2026-09-04 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：payload
- [BinaryAI-Bench：面向实战业务的二进制安全分析任务评测集](#)  
腾讯安全威胁情报中心 · 2026-09-03 / 発信元：中国 · 民間企業 (Tencent · WeChat中継) / 検出表記：payload
- [H1 2026 Malware Vulnerability Trends](#)  
Recorded Future · 2026-09-03 / 発信元：米国 · 民間企業 / 検出表記：payload
- [Gaming the system: how a Chinese-speaking actor turned Brazilian government sites into an SEO weapon](#)  
Check Point Research · 2026-09-02 / 発信元：イスラエル · 民間企業 / 検出表記：payload
- [Mirage Kitten targeting aviation and FinTech sectors across the Middle East and Africa with a new malware set](#)  
Securelist · 2026-09-01 / 発信元：ロシア · 民間企業 (Kaspersky) / 検出表記：payload
- [Breaking the Seal: Static Deobfuscation of JSDeal's Compiled V8 Bytecode](#)  
Check Point Research · 2026-08-31 / 発信元：イスラエル · 民間企業 / 検出表記：payload
- [ValleyRAT masquerading as adware](#)  
Securelist · 2026-08-31 / 発信元：ロシア · 民間企業 (Kaspersky) / 検出表記：payload
- [JavaScript obfuscation: From party trick to phishing kit](#)  
Cisco Talos · 2026-08-27 / 発信元：米国 · 民間企業 / 検出表記：payload
- [BlueDelta Targets Defense and Diplomacy with HOOKEDGE](#)  
Recorded Future · 2026-08-27 / 発信元：米国 · 民間企業 / 検出表記：payload

## ShinyHunters — G1057

- [FBI investigating alleged ShinyHunters breach of its jobs site](#)  
The Record · 2026-09-23 / 発信元：米国 · 報道 / 検出表記：ShinyHunters

- [Hackers claim to have stolen data on ‘almost all FBI agents’](#)  
RT・2026-09-23 / 発信元：ロシア・国営メディア / 検出表記：ShinyHunters
- [ShinyHunters claims FBI hack, data theft in PeopleSoft zero-day breach](#)  
BleepingComputer・2026-09-23 / 発信元：米国・報道 / 検出表記：ShinyHunters
- [Ransom & Dark Web Issues Week 4, September 2026](#)  
AhnLab ASEC・2026-09-23 / 発信元：韓国・民間企業 / 検出表記：ShinyHunters
- [August 2026 Dark Web Breach Incident Trend Report](#)  
AhnLab ASEC・2026-09-14 / 発信元：韓国・民間企業 / 検出表記：ShinyHunters
- [Passkey-themed social engineering leads to identity and cloud compromise](#)  
Microsoft Security・2026-09-10 / 発信元：米国・民間企業 / 検出表記：ShinyHunters
- [每周高级威胁情报解读\(2026.08.28~09.03\)](#)  
奇安信威胁情报中心・2026-09-04 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：ShinyHunters
- [The story behind the intelligence](#)  
Cisco Talos・2026-09-04 / 発信元：米国・民間企業 / 検出表記：ShinyHunters
- [実在するセキュリティ担当者を装った電話がかかってくる攻撃についてまとめてみた](#)  
piyolog・2026-08-26 / 発信元：日本・個人ブログ / 検出表記：ShinyHunters

## LockBit (ロックビット)

- [Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO](#)  
Securelist・2026-09-21 / 発信元：ロシア・民間企業 (Kaspersky) / 検出表記：LockBit
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’ s infrastructure and evidence of Qilin’ s AI use](#)  
Cisco Talos・2026-09-17 / 発信元：米国・民間企業 / 検出表記：LockBit 5.0
- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心・2026-09-11 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：LockBit
- [26秒攻陥11家机构：一场由数百个AI智能体编排的PaperCut全球攻击行动](#)  
奇安信威胁情报中心・2026-09-10 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：LockBit
- [Angry Birds: Toy Ghoul’s new toys](#)  
Securelist・2026-09-04 / 発信元：ロシア・民間企業 (Kaspersky) / 検出表記：LockBit
- [Mexico’ s Cybersecurity Plan 2025-2030: Turning Ambition Into Defense](#)  
Recorded Future・2026-08-25 / 発信元：米国・民間企業 / 検出表記：LockBit

## global

- [The New Rules of Machine Speed Defense](#)  
Recorded Future・2026-09-17 / 発信元：米国・民間企業 / 検出表記：global
- [Tajin Group: Guarantee Marketplace Vendor Involved in Phishing and Chinese Money Laundering Group](#)  
Recorded Future・2026-09-15 / 発信元：米国・民間企業 / 検出表記：global

- [GTIG AI Threat Tracker: From Prompting to Autonomy - The Evolution of Adversarial AI](#)  
Google Threat Intel · 2026-09-08 / 発信元：米国・民間企業 / 検出表記：global
- [7th September - Threat Intelligence Report](#)  
Check Point Research · 2026-09-07 / 発信元：イスラエル・民間企業 / 検出表記：global
- [一场“面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件](#)  
奇安信威胁情报中心 · 2026-09-03 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：global
- [Threat landscape for industrial automation systems. Q2 2026](#)  
Securelist · 2026-08-27 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：global

## bluesky

- [Unmasking EvilTokens: Getting to the root of device code phishing](#)  
Microsoft Security · 2026-09-23 / 発信元：米国・民間企業 / 検出表記：Bluesky
- [Protecting organizations from AI-assisted executive impersonation and invoice fraud](#)  
Microsoft Security · 2026-09-11 / 発信元：米国・民間企業 / 検出表記：Bluesky
- [Threat matrix: Mapping threats across cloud web applications](#)  
Microsoft Security · 2026-09-10 / 発信元：米国・民間企業 / 検出表記：Bluesky
- [ASCII smuggling crosses over from AI prompt injection to phishing evasion](#)  
Microsoft Security · 2026-09-04 / 発信元：米国・民間企業 / 検出表記：Bluesky

## eclipse

- [New Windows Defender zero-day blocks Microsoft antivirus updates](#)  
BleepingComputer · 2026-09-22 / 発信元：米国・報道 / 検出表記：Eclipse
- [We’ ve got one word for it, and it’ s usually the wrong one](#)  
Cisco Talos · 2026-09-11 / 発信元：米国・民間企業 / 検出表記：Eclipse
- [The Agentic SOC - From AI Theater to Real Defense](#)  
Recorded Future · 2026-09-01 / 発信元：米国・民間企業 / 検出表記：eclipse
- [Exploits and vulnerabilities in Q2 2026](#)  
Securelist · 2026-08-26 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：Eclipse

## Qilin (麒麟)

- [Should you care about an “AI slowdown?”](#)  
Cisco Talos · 2026-09-18 / 発信元：米国・民間企業 / 検出表記：Qilin
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’ s infrastructure and evidence of Qilin’ s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：Qilin
- [Active exploitation of Cisco Secure Firewall Management Center vulnerabilities](#)  
Cisco Talos · 2026-09-10 / 発信元：米国・民間企業 / 検出表記：Qilin
- [Mexico’ s Cybersecurity Plan 2025-2030: Turning Ambition Into Defense](#)  
Recorded Future · 2026-08-25 / 発信元：米国・民間企業 / 検出表記：Qilin

## cyclops

- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心・2026-09-18 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Cyclops
- [Cyclops Blink 卷土重来：沉寂四年后再升级, Sandworm 模块化植入体现身 Cisco 防火墙管理中心](#)  
奇安信威胁情报中心・2026-09-15 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Cyclops
- [Active exploitation of Cisco Secure Firewall Management Center vulnerabilities](#)  
Cisco Talos・2026-09-10 / 発信元：米国・民間企業 / 検出表記：Cyclops

## The Gentlemen

- [Should you care about an “AI slowdown?”](#)  
Cisco Talos・2026-09-18 / 発信元：米国・民間企業 / 検出表記：The Gentlemen
- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’ s infrastructure and evidence of Qilin’ s AI use](#)  
Cisco Talos・2026-09-17 / 発信元：米国・民間企業 / 検出表記：The Gentlemen
- [Ransom & Dark Web Issues Week 2, September 2026](#)  
AhnLab ASEC・2026-09-10 / 発信元：韓国・民間企業 / 検出表記：The Gentlemen

## ALPHV (ブラックキャット)

- [Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO](#)  
Securelist・2026-09-21 / 発信元：ロシア・民間企業 (Kaspersky) / 検出表記：BlackCat
- [Mexico’ s Cybersecurity Plan 2025-2030: Turning Ambition Into Defense](#)  
Recorded Future・2026-08-25 / 発信元：米国・民間企業 / 検出表記：BlackCat

## underground

- [AI Threat Landscape Digest: July-August 2026](#)  
Check Point Research・2026-09-17 / 発信元：イスラエル・民間企業 / 検出表記：underground
- [Our View on What It Takes To Be Named an Industry-Recognized Threat Intelligence Leader](#)  
Recorded Future・2026-09-17 / 発信元：米国・民間企業 / 検出表記：Underground

## SafePay

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen’ s infrastructure and evidence of Qilin’ s AI use](#)  
Cisco Talos・2026-09-17 / 発信元：米国・民間企業 / 検出表記：SafePay
- [Ransom & Dark Web Issues Week 4, August 2026](#)  
AhnLab ASEC・2026-08-27 / 発信元：韓国・民間企業 / 検出表記：SAFEPAY

## silent

- [ClearFake WebDAV infection chain delivers Amatera stealer, ZigCryptoStealer, and NetSupport Manager](#)  
Cisco Talos · 2026-09-08 / 発信元：米国・民間企業 / 検出表記：silent
- [ASCII smuggling crosses over from AI prompt injection to phishing evasion](#)  
Microsoft Security · 2026-09-04 / 発信元：米国・民間企業 / 検出表記：silent

## metaencryptor

- [Ransom & Dark Web Issues Week 4, September 2026](#)  
AhnLab ASEC · 2026-09-23 / 発信元：韓国・民間企業 / 検出表記：Metaencryptor

## Void Manticore — G1055

- [当 Telegram 变成 C2：拆解监控后门 HEAVYGRAM 与 Handala Hack 的”马甲”游戏](#)  
奇安信威胁情报中心 · 2026-09-21 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Handala Hack

## moneymessage

- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心 · 2026-09-18 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：ThreatLabz

## AiLock

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen' s infrastructure and evidence of Qilin' s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：AiLock

## netrunner

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen' s infrastructure and evidence of Qilin' s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：NetRunner

## nightspire

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen' s infrastructure and evidence of Qilin' s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：NightSpire

## ransomexx

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen' s infrastructure and evidence of Qilin' s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：RansomEXX

## stormous

- [Ransomware incidents in Japan in the first half of 2026: Investigation of The Gentlemen' s infrastructure and evidence of Qilin' s AI use](#)  
Cisco Talos · 2026-09-17 / 発信元：米国・民間企業 / 検出表記：Stormous

## wannacry

- [Securing the unpatchable in an age of AI-driven vulnerabilities](#)  
Cisco Talos · 2026-09-16 / 発信元：米国・民間企業 / 検出表記：WannaCry

## entropy

- [Siemens Reyrolle 7SR5](#)  
CISA Advisories · 2026-09-15 / 発信元：米国・政府機関 / 検出表記：Entropy

## notpetya

- [Cyclops Blink 卷土重来：沉寂四年后再升级，Sandworm 模块化植入体现身 Cisco 防火墙管理中心](#)  
奇安信威胁情报中心 · 2026-09-15 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：NotPetya

## insomnia

- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心 · 2026-09-11 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Insomnia

## LAPSUS — G1004

- [Ransom & Dark Web Issues Week 2, September 2026](#)  
AhnLab ASEC · 2026-09-10 / 発信元：韓国・民間企業 / 検出表記：LAPSUS\$

## cyberleek

- [每周高级威胁情报解读\(2026.08.28~09.03\)](#)  
奇安信威胁情报中心 · 2026-09-04 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：CyberLeek

## black x

- [Ransom & Dark Web Issues Week 1, September 2026](#)  
AhnLab ASEC · 2026-09-03 / 発信元：韓国・民間企業 / 検出表記：Black X

## aware

- [Mirage Kitten targeting aviation and FinTech sectors across the Middle East and Africa with a new malware set](#)  
Securelist · 2026-09-01 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：aware

## aurora

- ・ [黑客服务器裸奔泄露内幕：Aurora 勒索团伙用 Cursor AI 做攻击规划，完整还原从入侵到洗钱全链路](#)  
奇安信威胁情报中心・2026-09-01 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：aurora

## Cl0p（クロップ）

- ・ [Mexico' s Cybersecurity Plan 2025-2030: Turning Ambition Into Defense](#)  
Recorded Future・2026-08-25 / 発信元：米国・民間企業 / 検出表記：Cl0p

## Kazu

- ・ [Mexico' s Cybersecurity Plan 2025-2030: Turning Ambition Into Defense](#)  
Recorded Future・2026-08-25 / 発信元：米国・民間企業 / 検出表記：Kazu

## 4. 米国・ファイブアイズ系：関連記事

### NightEagle

- ・ [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心・2026-09-18 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：NightEagle
- ・ [夜鷹转向：APT-Q-95组织被曝攻击俄罗斯企业，Exchange后门GhostContainer再度现身](#)  
奇安信威胁情报中心・2026-09-17 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：APT-Q-95
- ・ [NightEagle targets Russian companies](#)  
Securelist・2026-09-16 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：NightEagle

## 5. 北朝鮮系：関連記事

### Kimsuky（キムスキー） — G0094

- ・ [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心・2026-09-18 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Kimsuky
- ・ [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心・2026-09-11 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Kimsuky
- ・ [APT-C-55（Kimsuky）组织利用伪装安装包植入远控木马的攻击链分析](#)  
360威胁情报中心・2026-09-10 / 発信元：中国・民間企業（Qihoo 360・WeChat中継） / 検出表記：Kimsuky
- ・ [每周高级威胁情报解读\(2026.08.28~09.03\)](#)  
奇安信威胁情报中心・2026-09-04 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Kimsuky

## Lazarus Group (ラザルス) — G0032

- [Don't Call Us, We'll Call Your APIs | TraderTraitor Backdoors Resurface on Victim With No Crypto Ties](#)  
SentinelLabs · 2026-09-19 / 発信元：米国・民間企業 / 検出表記：Lazarus
- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心 · 2026-09-18 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Lazarus
- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心 · 2026-09-11 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Lazarus

## APT37 — G0067

- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心 · 2026-09-18 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：APT37
- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心 · 2026-09-11 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Group123

## TraderTraitor (トレーダートレイター) — 上位: Lazarus Group

- [Don't Call Us, We'll Call Your APIs | TraderTraitor Backdoors Resurface on Victim With No Crypto Ties](#)  
SentinelLabs · 2026-09-19 / 発信元：米国・民間企業 / 検出表記：TraderTraitor

## Famous Chollima (北朝鮮IT労働者)

- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心 · 2026-09-18 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Famous Chollima

## TEMP.Hermit

- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心 · 2026-09-11 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：TEMP.Hermit

## UNC1069

- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)  
奇安信威胁情报中心 · 2026-09-11 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：CryptoCore

- [每周高级威胁情报解读\(2026.09.04~09.10\)](#)

奇安信威胁情报中心・2026-09-11 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Citrine Sleet △名寄せ曖昧

## 6. 中国系：関連記事

### Earth Lusca — G1006

- [浏览器的”信任”被伪造：KREMLIN 攻破 Chrome 完整性校验, 1500+ 巴西网银主机沦陷](#)

奇安信威胁情报中心・2026-09-16 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Chromium

- [已复现 | 搜狗输入法 1-click RCE](#)

微步在线・2026-09-14 / 発信元：中国・民間企業（ThreatBook・WeChat中継） / 検出表記：chromium

- [每周高级威胁情报解读\(2026.08.28~09.03\)](#)

奇安信威胁情报中心・2026-09-04 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：Chromium

### Salt Typhoon — G1045

- [Beware the SparroWock: The backdoor that bites, the commands that catch](#)

ESET WeLiveSecurity・2026-09-17 / 発信元：スロバキア・民間企業 / 検出表記：FamousSparrow

### UNC3569

- [已复现 | 搜狗输入法 1-click RCE](#)

微步在线・2026-09-14 / 発信元：中国・民間企業（ThreatBook・WeChat中継） / 検出表記：UNC3569

### Storm-1175

- [H1 2026 Malware Vulnerability Trends](#)

Recorded Future・2026-09-03 / 発信元：米国・民間企業 / 検出表記：Storm-1175

### Earth Berberoka

- [Gaming the system: how a Chinese-speaking actor turned Brazilian government sites into an SEO weapon](#)

Check Point Research・2026-09-02 / 発信元：イスラエル・民間企業 / 検出表記：Earth Berberoka

### TOXIC PANDA

- [“Sorry, I can’ t help with that” : How your guardrails might become the attacker’ s best friend](#)

Cisco Talos・2026-08-28 / 発信元：米国・民間企業 / 検出表記：ToxicPanda

## 7. ロシア系：関連記事

### Sandworm — G0034

- [每周高级威胁情报解读\(2026.09.11~09.17\)](#)  
奇安信威胁情报中心・2026-09-18 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：IRON VIKING
- [Cyclops Blink 卷土重来：沉寂四年后再升级，Sandworm 模块化植入体现身 Cisco 防火墙管理中心](#)  
奇安信威胁情报中心・2026-09-15 / 発信元：中国・民間企業 (QiAnXin・WeChat中継) / 検出表記：Sandworm
- [Active exploitation of Cisco Secure Firewall Management Center vulnerabilities](#)  
Cisco Talos・2026-09-10 / 発信元：米国・民間企業 / 検出表記：Sandworm
- [UAC-0099利用新型多阶段恶意软件链开展攻击活动](#)  
360威胁情报中心・2026-08-26 / 発信元：中国・民間企業 (Qihoo 360・WeChat中継) / 検出表記：Sandworm

### NoName057(16)

- [August 2026 Dark Web Threat Actor Trend Report](#)  
AhnLab ASEC・2026-09-14 / 発信元：韓国・民間企業 / 検出表記：NoName057(16)
- [Ransom & Dark Web Issues Week 4, August 2026](#)  
AhnLab ASEC・2026-08-27 / 発信元：韓国・民間企業 / 検出表記：NoName057(16)

### APT29 — G0016

- [From guidance to action: Security fundamentals that materially reduce risk](#)  
Microsoft Security・2026-09-18 / 発信元：米国・民間企業 / 検出表記：Midnight Blizzard △名寄せ曖昧

### UNC2452

- [From guidance to action: Security fundamentals that materially reduce risk](#)  
Microsoft Security・2026-09-18 / 発信元：米国・民間企業 / 検出表記：Midnight Blizzard △名寄せ曖昧

### APT28 — G0007

- [BlueDelta Targets Defense and Diplomacy with HOOKEDGE](#)  
Recorded Future・2026-08-27 / 発信元：米国・民間企業 / 検出表記：BlueDelta

## 8. イラン系：関連記事

### Cleaver — G0003

- [August 2026 CVE Landscape](#)  
Recorded Future・2026-09-08 / 発信元：米国・民間企業 / 検出表記：Alibaba

- [尽快修复！Nacos权限绕过漏洞](#)

微步在线 · 2026-08-28 / 発信元：中国 · 民間企業 (ThreatBook · WeChat中継) / 検出表記：alibaba

## BANISHED KITTEN

- [当 Telegram 变成 C2：拆解监控后门 HEAVYGRAM 与 Handala Hack 的”马甲”游戏](#)

奇安信威胁情报中心 · 2026-09-21 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Storm-0842

## Handala

- [当 Telegram 变成 C2：拆解监控后门 HEAVYGRAM 与 Handala Hack 的”马甲”游戏](#)

奇安信威胁情报中心 · 2026-09-21 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Handala

## HomeLand Justice

- [当 Telegram 变成 C2：拆解监控后门 HEAVYGRAM 与 Handala Hack 的”马甲”游戏](#)

奇安信威胁情报中心 · 2026-09-21 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Homeland Justice △名寄せ曖昧

## MuddyWater — G0069

- [浏览器的”信任”被伪造：KREMLIN 攻破 Chrome 完整性校验，1500+ 巴西网银主机沦陷](#)

奇安信威胁情报中心 · 2026-09-16 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Seedworm

## Bohrium

- [一场”面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件](#)

奇安信威胁情报中心 · 2026-09-03 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Smoke Sandstorm △名寄せ曖昧

## Tortoiseshell — G1012

- [一场”面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件](#)

奇安信威胁情报中心 · 2026-09-03 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：Smoke Sandstorm △名寄せ曖昧

## UNC1549

- [一场”面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件](#)

奇安信威胁情报中心 · 2026-09-03 / 発信元：中国 · 民間企業 (QiAnXin · WeChat中継) / 検出表記：UNC1549

## 9. 金銭目的犯罪（ランサム関連含む）：関連記事

### TeamPCP — G1056

- [GTIG AI Threat Tracker: From Prompting to Autonomy - The Evolution of Adversarial AI](#)  
Google Threat Intel · 2026-09-08 / 発信元：米国・民間企業 / 検出表記：UNC6780
- [一句「npm publish」评论，撬开一条可信发布流水线：openapi-react-query-codegen 供应链投毒事件深度复盘](#)  
奇安信威胁情报中心 · 2026-08-31 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：TeamPCP

### Silence group — G0091

- [Group Policy hijacked: PAYLOAD ransomware weaponizes Active Directory GPO](#)  
Securelist · 2026-09-21 / 発信元：ロシア・民間企業（Kaspersky） / 検出表記：silence

### SALTY SPIDER

- [运行 23 年的 P2P 僵尸网络 Sality 遭协同瓦解：没有中心节点也能被干掉？](#)  
奇安信威胁情报中心 · 2026-09-02 / 発信元：中国・民間企業（QiAnXin・WeChat中継） / 検出表記：SALTY SPIDER

## 関連記事がなかった区分

台湾系、韓国系、東南アジア系、イスラエル系

## 付録：名寄せが曖昧だった検出（同じ名前が複数アクターに対応）

- 「Homeland Justice」→ HomeLand Justice：当 Telegram 变成 C2：拆解监控后门 HEAVYGRAM 与 Handala Hack 的”马甲”游戏
- 「Midnight Blizzard」→ APT29：From guidance to action: Security fundamentals that materially reduce risk
- 「Midnight Blizzard」→ UNC2452：From guidance to action: Security fundamentals that materially reduce risk
- 「Citrine Sleet」→ UNC4736：每周高级威胁情报解读(2026.09.04~09.10)
- 「Smoke Sandstorm」→ Bohrium：一场“面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件
- 「Smoke Sandstorm」→ Tortoiseshell：一场“面试笔试”背后的入侵：Mirage Kitten 转向 Node.js/JavaScript 恶意软件