Know the threat.
Build your defense.

RANSOMWARE THREAT INTELLIGENCE FIELD GUIDE



One playbook for MSPs and their clients.

Understand the adversaries. Review the tactics. Build your next defensive move.

10	07	2026
RANSOMWARE GROUPS	DEFENSIVE PRIORITIES	FIELD GUIDE EDITION

Threat details are based on linked Blackpoint APG profiles. Illustrations are symbolic. Defensive guidance connects observed behaviors with general controls and Blackpoint capabilities.

Your ransomware ThreatDex.

Read the card. Scan the profile. Review your defense.

01 **Qilin** PAGE 03
OPEN APG PROFILE

02 **The Gentlemen** PAGE 04
OPEN APG PROFILE

03 **Akira** PAGE 05
OPEN APG PROFILE

04 **INC Ransom** PAGE 06
OPEN APG PROFILE

05 **DragonForce** PAGE 07
OPEN APG PROFILE

06 **Play** PAGE 08
OPEN APG PROFILE

07 **Clop** PAGE 09
OPEN APG PROFILE

08 **SafePay** PAGE 10
OPEN APG PROFILE

09 **Sinobi** PAGE 11
OPEN APG PROFILE

10 **Medusa** PAGE 12
OPEN APG PROFILE

7 defensive priorities

Authentication • patching • remote access • privileged credentials • lateral movement • detection • recovery

Review the defensive priorities on page 13 and the client conversation prompts on page 14.

Qilin Ransomware

FIRST IDENTIFIED 2022 / DOUBLE EXTORTION

QILIN



PRIMARY TARGETS

Manufacturing · Construction & engineering · Retail

INITIAL ACCESS

Valid accounts · Remote services · Vulnerability exploitation

T1078 / T1133 / T1190

QILIN RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Protect access. Investigate tampering.

Qilin combines stolen data and encryption to pressure victims. Its documented access methods include valid accounts, remote services, exploitation, and phishing.

YOUR DEFENSIVE MOVES

- Review exposed applications and remote services.
- Investigate changes to security tools.
- Review unusual account activity and lateral movement.

SOURCE: BLACKPOINT APG PROFILE

The Gentlemen Ransomware

FIRST IDENTIFIED 2025 / DOUBLE EXTORTION

THE GENTLEMEN



PRIMARY TARGETS

Manufacturing · Retail · Healthcare

INITIAL ACCESS

Valid accounts · Remote services · Exploitation · Phishing

T1078 / T1133 / T1190 / T1566

THE GENTLEMEN RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Treat exposed infrastructure as a priority.

The Gentlemen operates as ransomware-as-a-service and uses both encryption and data theft. Blackpoint documents access through edge infrastructure and remote services, with persistence through scripts, tasks, and accounts.

YOUR DEFENSIVE MOVES

- Prioritize exposed edge-device vulnerabilities.
- Review remote access and newly created accounts.
- Investigate security-tool tampering and unusual data transfers.

SOURCE: BLACKPOINT APG PROFILE

Akira Ransomware

FIRST IDENTIFIED 2023 / DOUBLE EXTORTION

AKIRA



PRIMARY TARGETS

Manufacturing · Construction & engineering · Retail

INITIAL ACCESS

Compromised credentials · VPN access · Exploitation

T1078 / T1133 / T1190

AKIRA RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Close the door on remote access abuse.

Akira commonly enters through compromised credentials and externally accessible remote services. Its double-extortion attacks can affect Windows and Linux environments.

YOUR DEFENSIVE MOVES

- Review VPN patching, MFA, and active sessions.
- Restrict remote administration.
- Investigate unexpected remote activity and outbound transfers.

SOURCE: BLACKPOINT APG PROFILE

INC Ransom Ransomware

FIRST IDENTIFIED 2023 / DOUBLE EXTORTION

INC RANSOM



PRIMARY TARGETS

Manufacturing

INITIAL ACCESS

Valid accounts · Exploitation · Supply chain · Phishing

T1078 / T1190 / T1195 / T1566

INC RANSOM RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Look beyond the first compromised account.

INC Ransom combines encryption with stolen-data extortion. Its documented techniques include valid accounts, exploitation, supply-chain compromise, and social engineering, followed by persistence through scheduled tasks and account changes.

YOUR DEFENSIVE MOVES

- Review privileged access and account creation.
- Investigate scheduled tasks and unexpected system processes.
- Protect backups and test restoration.

SOURCE: BLACKPOINT APG PROFILE

DragonForce Ransomware

FIRST IDENTIFIED 2023 / DOUBLE EXTORTION

DRAGONFORCE



PRIMARY TARGETS

Manufacturing

INITIAL ACCESS

Valid accounts · Remote services · Exploitation · Phishing

T1078 / T1133 / T1190 / T1566

DRAGONFORCE RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Disrupt the affiliate’s path through the network.

DragonForce uses double extortion and has been reported to operate a white-label cartel model. Blackpoint documents remote-service abuse, scheduled tasks, and lateral movement, alongside attempts to interfere with defenses.

YOUR DEFENSIVE MOVES

- Restrict exposed remote desktop access.
- Investigate new scheduled tasks and startup changes.
- Review remote-service permissions and security-tool tampering.

SOURCE: BLACKPOINT APG PROFILE

Play Ransomware

FIRST IDENTIFIED 2022 / DOUBLE EXTORTION

PLAY



PRIMARY TARGETS

Manufacturing

INITIAL ACCESS

Valid accounts · Remote services · Exploitation · Phishing

T1078 / T1133 / T1190 / T1566

PLAY RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Secure the entry points your business relies on.

Play combines data theft with encryption. Its operating model is disputed: public reporting describes ransomware-as-a-service, while the group claims it is private. Blackpoint maps access to valid accounts, remote services, vulnerabilities, and phishing.

YOUR DEFENSIVE MOVES

- Review MFA and remote-service exposure.
- Prioritize vulnerabilities affecting external systems.
- Investigate unexpected logins and remote activity.

SOURCE: BLACKPOINT APG PROFILE

Clop Ransomware

FIRST IDENTIFIED 2019 / DATA EXTORTION FOCUS

CLOP



PRIMARY TARGETS

Manufacturing · Transportation · Retail

INITIAL ACCESS

Valid accounts · Remote services · Exploitation · Supply chain

T1078 / T1133 / T1190 / T1195

CLOP RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Protect data before it leaves the environment.

Clop originally used double extortion, but Blackpoint describes a later focus on data extortion through large-scale supply-chain attacks. Encryption is not required for stolen information to become leverage.

YOUR DEFENSIVE MOVES

- Prioritize exposed file-transfer and partner-facing systems.
- Review third-party access and data-sharing dependencies.
- Investigate unusual data staging and outbound transfers.

SOURCE: BLACKPOINT APG PROFILE

SafePay Ransomware

FIRST IDENTIFIED 2024 / DOUBLE EXTORTION

SAFEPAY



PRIMARY TARGETS

Manufacturing · Construction & engineering · Healthcare

INITIAL ACCESS

Valid accounts · Exploitation · Social engineering

T1078 / T1190 / T1566

SAFEPAY RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Challenge activity that looks legitimate.

SafePay is assessed by Blackpoint as likely a private operation. It combines data theft with encryption and has documented initial-access techniques involving valid accounts, vulnerabilities, and social engineering.

YOUR DEFENSIVE MOVES

- Review account access and MFA coverage.
- Patch exposed systems.
- Investigate unusual account behavior and remote activity.

SOURCE: BLACKPOINT APG PROFILE

Sinobi Ransomware

FIRST IDENTIFIED 2025 / DOUBLE EXTORTION

SINOBI



PRIMARY TARGETS

Manufacturing

INITIAL ACCESS

Valid accounts · Remote services · Public-facing applications

T1078 / T1133 / T1190

SINOBI RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Keep privileged access from becoming a foothold.

Sinobi operates a semi-private affiliate model and uses double extortion. Blackpoint documents compromised accounts, edge-device exploitation, account changes, remote-service movement, and attempts to impede recovery.

YOUR DEFENSIVE MOVES

- Limit administrative access and review new accounts.
- Review edge-device vulnerabilities.
- Protect backups and investigate security-tool changes.

SOURCE: BLACKPOINT APG PROFILE

Medusa Ransomware

FIRST IDENTIFIED 2022 / DOUBLE EXTORTION

MEDUSA



PRIMARY TARGETS

Construction & engineering

INITIAL ACCESS

Valid accounts · Remote services · Exploitation · Phishing

T1078 / T1133 / T1190 / T1566

MEDUSA RANSOMWARE

Scan for tactics, targets, and the full Blackpoint APG profile.

HOW BLACKPOINT SUPPORTS YOUR DEFENSE

Blackpoint MDR brings contextual detection and 24/7 human-led investigation and containment to monitored environments. Pair it with disciplined access, patching, and recovery practices. ITDR extends monitoring and containment to supported cloud identities.

READ THE FULL PROFILE

Reduce both disruption and data exposure.

Medusa uses ransomware-as-a-service and double extortion. Blackpoint documents exploitation and social engineering, persistence through tasks and accounts, and lateral movement through remote services and deployment tools.

YOUR DEFENSIVE MOVES

- Review externally accessible services and vulnerabilities.
- Investigate account creation and deployment-tool activity.
- Protect sensitive data and rehearse recovery.

SOURCE: BLACKPOINT APG PROFILE

Review your defensive priorities.

Use these prompts to guide a conversation with your team and clients.

01 **Strengthen authentication**

Review MFA, remote access, and privileged accounts.

02 **Patch exposed systems**

Prioritize VPNs, edge devices, and public-facing applications.

03 **Control remote access**

Review approved tools, users, and administration.

04 **Protect privileged credentials**

Limit access and investigate unexpected account changes.

05 **Reduce lateral movement**

Review segmentation and remote-service permissions.

06 **Detect attacker behavior**

Investigate tampering, unusual activity, and data transfers.

07 **Prepare for recovery**

Protect backups, test restoration, and rehearse response.

Blackpoint MDR

Contextual detection and 24/7 human-led investigation and containment across monitored environments.

EXPLORE MDR

EXPLORE ITDR

A team behind your team.

Turn threat intelligence into your next conversation.

> “My team is not really worried about responding to security alerts anymore.”
>
> **Nate Smith**, CTO, DTC

READ DTC’S SUCCESS STORY

For your clients

Ransomware can begin with a stolen account or a vulnerable system. We review access, patching, monitoring, and recovery together to help reduce risk.

For your next team review

Which accounts can reach critical systems? Which public-facing systems need attention? Can we detect unusual activity and restore from protected backups?

Ready-to-share social post

Know the threat. Know the moves. Explore Blackpoint Cyber’s ThreatDex to learn about ransomware groups and seven defensive priorities. #CybersecurityAwarenessMonth #Cybersecurity

Put your next move into action.

Explore Blackpoint’s technology and 24/7 SOC response.

TALK TO BLACKPOINT