Recent Malware Incidents — Summary, Attack Methods, and Mitigations

AUTHOR: TOM SHINJO THOMAS

1) CL0P / MOVEit exploitation (May 2023 — ongoing impacts)

Summary: The CL0P ransomware group exploited an SQL injection zero-day in Progress MOVEit Transfer (CVE-2023-34362) to gain unauthorized access to file transfer servers, exfiltrate sensitive data, and extort victims. This incident affected hundreds of organizations worldwide and produced a long tail of victim notifications and follow-up remediation work.

Attack method / technical details: • Threat actors located exploitable MOVEit instances and executed SQL injection against the vulnerable web-facing API. • The attackers used the SQLi to create a web shell (commonly observed as `human2.aspx` / "LEMURLOOT") enabling interactive access to the server. • From the web shell they enumerated files, exfiltrated data, and deployed CL0P extortion processes (data leak sites, ransom demands). • The vulnerability allowed unauthenticated attackers to manipulate administrative API endpoints, making it particularly dangerous for internetfacing deployments.

Mitigation / resolution: • Progress (MOVEit vendor) released security updates and patches; operators were urged to apply patches immediately. • U.S. agencies (CISA, FBI) and other national CERTs published advisories, indicators of compromise (IOCs), and step by step mitigation guidance (block vulnerable endpoints, rotate credentials, hunt for web shells). • Affected organizations performed incident response: removed web shells, restored from clean backups where possible, notified affected parties, and engaged forensic teams. • Law enforcement and CERTs published IOCs and detection signatures to help defenders hunt residual infections.

References: CISA advisory and vendor bulletins with technical details and mitigation guidance.

References (web sources used below): • CISA / FBI advisory on CL0P / MOVEit exploitation. (source id: cite turn0search4) • Progress MOVEit vulnerability details and CVE notes. (source id: cite turn0search16)

---

2) Operation ENDGAME — International disruption of initial-access malware (May 2025)

Summary: Operation ENDGAME (Season 2, May 2025) was a coordinated law enforcement action across multiple countries that targeted botnets and **initial access** malware families (e.g., Bumblebee, Qakbot, Trickbot, DanaBot). The operation disrupted servers, neutralized domains, and led to seizure of infrastructure and crypto assets.

Attack method / technical details (for covered families): • These families typically delivered **initial access** via phishing, malicious attachments, or purchase/abuse of compromised credentials. • Malware established persistence, performed credential theft, and provided a foothold for follow on payloads such as ransomware or remote access tools. • Botnets and initial access services acted as an on ramp for ransomware affiliates, selling or renting access to higher level operators.

Mitigation / resolution: • Law enforcement and international partners seized or disabled command-and-control servers and neutralized hundreds of domains and servers used to manage the botnets. • The operation provided victim remediation support (removal guidance and account remediation) and published IoCs to help defenders clean infected hosts. • Outcomes included arrests/charges, server seizures, and a measurable reduction in the availability of infrastructure used to spread ransomware — though agencies stressed continued vigilance because actors can rebuild infrastructure.

References: Europol and international coverage of Operation ENDGAME (press release and reporting). (source ids: cite turn1search8 turn1news20)

---

3) BlackSuit (aka Royal) ransomware — coordinated disruption (Aug 2025)

Summary: BlackSuit (a rebrand/descendant of groups often tracked as "Royal") is a ransomware operation that targeted healthcare and other sectors. In August 2025, the U.S. Department of Justice and international partners executed coordinated disruption actions that seized servers, domains, and approximately $1M in laundered proceeds.

Attack method / technical details: • BlackSuit used multi-stage intrusions often beginning with initial-access malware or exploited credentials to gain a foothold. • Once inside, operators deployed ransomware across networks, exfiltrated data for double-extortion, and used elaborate laundering to convert payments to crypto and fiat. • The group ran an extortion site to pressure victims into paying and operated affiliate-style infrastructure common to modern RaaS (ransomwareas-a-service) models.

Mitigation / resolution: • International law enforcement seized control of key infrastructure (servers and domains) and froze or seized cryptocurrency proceeds. • Agencies published disruption results and victim guidance; partners worked to notify victims and provide remediation assistance. • The takedown reduced BlackSuit's operational capacity and recovered funds, but authorities warned that affiliates and successor groups may attempt to reconstitute operations, so continued monitoring and hardening were recommended.

References: DOJ press release and industry reporting on the August 11, 2025 coordinated action. (source ids: cite turn1search1 turn1search5)

Common lessons & recommended controls

1. **Patch and reduce attack surface:** Keep internet-facing services patched (MOVEit is a canonical example). 2. **Detect initial access early:** Monitor for phishing, credential misuse, and anomalous web shells. Hunt for IOCs published after incidents. 3. **Network segmentation & backups:** Limit lateral movement and ensure clean, immutable backups and tested restore procedures.
4. **Threat intelligence & collaboration:** Use vendor/agency advisories and participate in information-sharing; law enforcement disruption actions amplify impact when defenders share intelligence.