White Paper: Comprehensive Analysis of Cybercriminal Behavior Throughout the Intrusion Lifecycle

Kirk Lurie

This white paper offers actionable insights for cybersecurity practitioners. By integrating behavioral analysis with frameworks such as MITRE ATT&CK and the Cyber Kill Chain/Unified Kill Chain, it maps adversary tactics and techniques throughout the full intrusion lifecycle. Real-world case studies, including SolarWinds, Colonial Pipeline, Equifax, MOVEit/CLOP mass extortion, and Microsoft Exchange/Hafnium, illustrate how these behavioral patterns manifest, underscoring the urgency of proactive defense strategies.

Frameworks for Behavioral Mapping

The MITRE ATT&CK framework (n.d.-c) provides a comprehensive knowledgebase of adversary tactics, techniques, and procedures (TTPs). It emphasizes pre-attack tactics such as Reconnaissance (MITRE, n.d.-a) and Resource Development (MITRE, n.d.-b), as well as post-compromise actions like Lateral Movement, Exfiltration, and Impact. The Cyber Kill Chain (Lockheed Martin, 2015) and Unified Kill Chain (Pols, 2019) further contextualize these behaviors, describing the progression from initial reconnaissance through exploitation and impact. These frameworks enable organizations to systematically track and anticipate adversary actions, supporting more effective threat detection and response.

Cybercriminal Profiles and Psychological Drivers

Cybercriminals encompass a range of profiles, each shaped by distinct motivations and psychological traits:

- *Opportunistic Attackers*: Driven by financial stress or personal gain, these individuals may lack deep technical backgrounds but act impulsively, often rationalizing their behavior as necessary.
- *Disgruntled Insiders*: Motivated by resentment from perceived injustice or lack of recognition, these actors exploit privileged access for retribution.
- *Thrill-Seekers*: Highly skilled individuals motivated by curiosity and the excitement of overcoming technical barriers. These attackers often seek recognition within online communities.
- *Socially Isolated Individuals*: Seeking validation or control in cyberspace, these persons are compensating for real-world social deficits.

- *Teenage Cybercriminals*: Often motivated by curiosity and a desire to learn, these individuals may not fully understand the legal or ethical implications of their actions, highlighting the need for educational and mentorship interventions.
- *Antisocial/Narcissistic Personalities*: Displaying a lack of empathy, remorse, or guilt, these individuals derive pleasure from causing harm and may escalate their activities over time.

Understanding these diverse profiles enables organizations to anticipate, prevent, and detect malicious activity more effectively.

Key Stressors, Motivators, and Psychological Traits

Individuals are driven to cybercrime by a combination of external and internal pressures:

- *Stressors:* Financial hardship, workplace dissatisfaction, relationship struggles, and social isolation can distort judgment and lower inhibitions, making cybercrime more appealing. Technical challenges and the thrill of overcoming defenses also can act as stressors.
- *Motivators:* Financial gain, retribution, curiosity, notoriety, and the desire for validation drive cybercriminals, often combining practical needs with psychological desires.
- *Psychological Traits:* Rationalization of actions, lack of empathy, thrill-seeking, and resourcefulness are common traits. Some offenders demonstrate antisocial or narcissistic tendencies, reinforcing their detachment from consequences.

These factors influence not just the decision to commit cybercrime, but also the methods and persistence displayed.

Behavioral Breakdown by Phase

Pre-Crime (Preparation & Reconnaissance)

Cybercriminals operate strategically and opportunistically in this phase. They gather intelligence on targets (employee emails, tech stacks, business processes) using Open-Source Intelligence (OSINT) and active scanning, and acquire resources (domains, VPS, malware/exploits). The psychological landscape is marked by anticipation, excitement, anxiety, and paranoia, with stressors including the urgency to exploit vulnerabilities and technical challenges. Operational security is prioritized, and empowerment grows as infrastructure and attack vectors are readied, balanced by the calculated risks of exposure or failure.

During Crime (Execution & Exploitation)

The psychological profile shifts to intense focus and situational awareness. Activities include phishing, exploiting vulnerabilities, password spraying, privilege escalation, lateral movement, and data exfiltration. Success leads to adrenaline and excitement, often accompanied by a lack of empathy or guilt. Overconfidence may fuel riskier behavior. Stress and agitation are ever-present due to the threat of detection or technical obstacles. Escalation and repeat offenses often result from enjoying the crime and being detached from consequences.

Post-Crime (Cover-Up, Monetization, Persistence)

Cybercriminals seek to evade detection, monetize their actions, and maintain persistence. This phase is characterized by relief, vigilance, and continued thrill. Steps include log tampering, disabling security tools, selling data, extortion, and establishing backdoors for future access. The perpetrator may obsessively monitor investigations, taunt victims, or escalate activities. Physical and emotional symptoms can manifest, and the lack of empathy persists. Escalation and risk-taking may increase if the offender enjoys causing distress.

Detection & Mitigation Playbook

The table below offers detection and mitigation technique based on the phase or behavior.

Phase/Behavior	MITRE ATT&CK Mapping	Observable Indicators	Detection & Controls	Metrics to Track
Pre: Reconnaissance	TA0043, T1595	Cloud/VPS scanning; typo-squatted domains	Blocklists, anomaly detection, brand monitoring, DMARC/DKIM/SPF	Lookalike domains; scan volumes by ASN
Pre: Resource Development	TA0042, T1583	New domains/certs; registered C2	Threat intel ingestion, domain/cert monitoring, takedowns	Detection speed of lookalikes
During: Initial Access	TA0001	Auth anomalies, spikes in 401/403, suspicious logs	MFA, patch SLAs, phishing-resistant auth, geo-velocity rules	Patch latency; privileged accounts with MFA
During: Lateral Movement	TA0008, T1021/T1027	Kerberoasting, SMB/RDP bursts, new admin sessions	Network segmentation, JIT admin, EDR analytics	Containment time for lateral activity
During: Exfiltration/Impact	TA0010, TA0040	High egress, archive creation,	DLP, egress filtering, immutable	Restore objectives;

		shadow IT transfers	backups, ransomware playbooks	data-loss prevented
Post: Defense Evasion	TA0005	Cleared logs, stopped agents, modified audit policies	Secure log forwarding, tamper-proof telemetry, least privilege	Critical log coverage; EDR tamper protection

Note: Autonomous System Number (ASN); Command and Control (C2); Data Loss Prevention (DLP); DomainKeys Identified Mail (DKIM); Domain-Based Message Authentication, Reporting & Conformance (DMARC); Endpoint Detection and Response (EDR); Multifactor Authentication (MFA); Service Level Agreements (SLAs); Sender Policy Framework (SPF); Server Message Block/Remote Desktop Protocol (SMB/RDP); and Virtual Private Server (VPS).

Case Studies

Equifax Breach (2017)

- Pre-crime: In the lead-up to the breach, attackers conducted extensive scans for known vulnerabilities in Equifax's online interfaces, homing in on Apache Struts CVE-2017-5638 (Vulnerability History Project, 2017). Although a patch had been released and publicized, Equifax failed to update its public-facing dispute portal. This omission left a critical backdoor open for adversaries to exploit, demonstrating the difficulty large organizations face in keeping legacy and externally exposed assets properly inventoried and patched.
- During crime: Once inside, attackers established persistence by creating footholds within the network, escalated their privileges, and harvested credentials. For weeks, they moved laterally, seeking and exfiltrating sensitive data, and ultimately compromising the personal information of roughly 147 million Americans, including Social Security numbers, birth dates, addresses, and some credit card data. Poor network segmentation and weak internal monitoring exacerbated the period of no detection.
- Post-crime: Public disclosure of the breach prompted rigorous scrutiny from regulators, Congress, and industry watchdogs. The Government Accountability Office (GAO, 2018) and United States Senate Permanent Subcommittee on Investigations (U.S. Senate, 2019) identified major gaps in Equifax's cyber governance, asset management, and patch processes. The breach, which resulted in widespread reforms, stands as an example for the financial and critical infrastructure sectors regarding vulnerability management, asset tracking, network segmentation, and board-level cybersecurity oversight.

MOVEit Transfer/Clop Mass Extortion (2023)

- Pre-crime: Early in 2023, the Clop ransomware group targeted MOVEit Transfer, a popular file transfer solution, for a zero-day SQL injection vulnerability. Prior to the public's awareness and the release of a patch, Clop systematically scanned for

vulnerable installations and developed custom web shells to facilitate persistent access (CISA & FBI, 2023).

- During crime: Once the vulnerability was exploited, Clop rapidly gained control of thousands of organizations' systems across the globe. They used automated tooling to steal data at scale, taking advantage of the delay between attack and patch availability for maximum impact.
- Post-crime: Clop launched mass extortion campaigns, threatening to publicly leak stolen data unless ransoms were paid. Cybersecurity authorities released urgent advisories, emphasizing the importance of third-party risk management, quick vulnerability response, and robust controls for vendor access.

Colonial Pipeline Ransomware Attack (2021)

- Pre-crime: The DarkSide ransomware group targeted Colonial Pipeline, identifying a legacy VPN account that was still active and unprotected by multifactor authentication (FBI, 2021). This weak point served as the entry vector for the attack.
- During crime: Once inside, DarkSide swiftly deployed ransomware, encrypting critical systems and forcing a shutdown of pipeline operations. This disruption led to fuel shortages across the U.S. East Coast, and the attackers demanded a ransom for decryption keys and to prevent data leakage. Colonial Pipeline paid a portion of the ransom, and law enforcement later recovered some of the funds (Department of Justice, 2021).
- Post-crime: The attack spurred the industry to accelerate the adoption of multifactor authentication, reinforce network segmentation, and improve incident response planning. It also brought about new regulatory guidance for critical infrastructure entities (CISA & FBI, 2023; Department of Energy, 2021).

Microsoft Exchange/Hafnium (2021)

- Pre-crime: The Hafnium advanced persistent threat (APT) group discovered a chain of zero-day vulnerabilities (ProxyLogon) in on-premises Microsoft Exchange servers (CISA, 2021a). These flaws allowed attackers to bypass authentication, obtain administrative access, and prepare for widespread exploitation.
- During crime: Hafnium leveraged automated attacks to deploy web shells for persistent access, steal emails, and harvest credentials from thousands of organizations. The scale and speed of exploitation were amplified by the lack of immediate patching and insufficient detection mechanisms.
- Post-crime: The response included global emergency patching campaigns, mass forensic investigations, and public advisories. The incident highlighted the critical need for aggressive vulnerability management and continuous monitoring.

SolarWinds Supply Chain Compromise (2019–2021)

- Pre-crime: Nation-state actors infiltrated SolarWinds' software development environment, injecting malicious code (SUNBURST backdoor) into legitimate Orion software updates (MITRE, n.d.-d). This supply chain attack was exceptionally stealthy, leveraging trusted software channels.
- During crime: Compromised updates were distributed to thousands of customers, enabling attackers to move laterally across networks by abusing federated identity systems and forging security tokens. Their persistent access reached into both cloud and on-premise environments.
- Post-crime: The breach triggered a global reevaluation of supply chain security, prompting reforms in risk management, adoption of zero trust architectures, and more robust monitoring and software assurance practices throughout the industry (CISA, 2021b; FERC & E-ISAC, 2021).

Practical Detection & Response Recommendations

To proactively defend against sophisticated cyber threats and large-scale supply chain attacks, organizations should treat early warning indicators, such as the registration of lookalike domains, broad internet scanning for vulnerabilities, and credential stuffing attempts, not as isolated events but as potential precursors to more significant incidents. Automating brand monitoring and attack surface management speeds detection and response to these signals, reducing adversaries' window of opportunity. To minimize the risk of initial compromise, it is essential to patch all external-facing systems within clearly defined SLAs and to enforce phishing-resistant MFA, such as FIDO or WebAuthn, particularly for privileged administrative accounts. Strengthening identity security is also critical. Organizations should safeguard token signing certificates, closely monitor for anomalous OAuth application consents and privilege escalations, and implement regular rotation and robust protection of sensitive credentials and secrets.

To limit lateral movement within the environment, adopting network segmentation and implementing Just-In-Time (JIT) and Just-Enough-Administration (JEA) principles can significantly reduce the attack surface. Disabling legacy protocols and monitoring internal network traffic for unusual activity further constrains attacker mobility. Given the high likelihood of data exfiltration attempts, organizations should deploy egress controls, utilize DLP technologies where appropriate, and continuously monitor for abnormal file archiving and unauthorized cloud synchronization behaviors.

Building resilience against ransomware requires maintaining immutable, offline backups and regularly practicing restoration procedures to ensure rapid recovery. In addition, organizations should establish clear decision frameworks for responding to ransom or extortion demands, documenting these processes in advance to support swift and coordinated action during a crisis.

Managing third-party risk is another vital component of a comprehensive defense strategy. It involves maintaining an up-to-date inventory of all critical software-as-a-service (SaaS) applications and software supply chain dependencies, subscribing to vendor advisories for timely threat intelligence, and periodically testing emergency disablement plans to ensure business continuity if a supplier is compromised.

Finally, incident response readiness should be enhanced by conducting tabletop exercises based on realistic threat scenarios, pre-establishing secure, out-of-band communication channels, and rehearsing evidence collection procedures and coordination with legal and public relations teams. These measures collectively help organizations anticipate, detect, and effectively respond to complex cyber incidents, reducing their overall exposure and impact.

Conclusion

Understanding the behavioral and psychological dimensions of cybercriminals, mapped to established frameworks and illustrated through real-world case studies, is vital for effective cybersecurity. Proactive detection, rapid response, and continuous improvement in technical and governance controls are essential techniques to withstand the evolving threat landscape. Organizations must integrate behavioral insights, technical controls, and incident readiness to anticipate and mitigate cyber risks across all phases of the attack lifecycle.

References

CISA. (2021a). *Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. https://www.cisa.gov/news-events/directives/ed-21-02-mitigate-microsoft-exchange-premises-product-vulnerabilities

CISA. (2021b). *Remediating networks affected by SolarWinds and Active Directory/M365 compromise*. https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise

CISA. (2023). *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years*. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

CISA & FBI. (2021, March 10). *Joint CSA: AA21-062A: Compromise of Microsoft Exchange Server*. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

CISA & FBI. (2023). *CISA and FBI release advisory: CL0P ransomware gang exploiting MOVEit vulnerability*. https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability

Department of Energy. (2021). *Colonial Pipeline cyber incident*. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Department of Justice. (2021). *Department of Justice seizes $2.3 million in cryptocurrency paid to ransomware extortionists DarkSide*. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

FBI. (2021). *FBI statement on compromise of Colonial Pipeline networks*. https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

FERC & E-ISAC. (2021). *SolarWinds and related supply chain compromise* [White paper]. https://www.ferc.gov/sites/default/files/2021-07/SolarWinds%20and%20RelatedSupply%20Chain%20Compromise%20White%20Paper_1.pdf

GAO. (2018). *Data protection: Actions taken by Equifax and federal agencies in response to the 2017 breach* (GAO-18-559). https://www.gao.gov/products/gao-18-559

Lockheed Martin. (2015). *Seven ways to apply the Cyber Kill Chain with a threat intelligence platform*. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

MITRE. (n.d.-a). *MITRE ATT&CK: Reconnaissance (TA0043)*. https://attack.mitre.org/tactics/TA0043/

MITRE. (n.d.-b). *MITRE ATT&CK: Resource Development (TA0042)*. https://attack.mitre.org/tactics/TA0042/

MITRE. (n.d.-c). *MITRE ATT&CK: Site & Matrix*. https://attack.mitre.org/

MITRE. (n.d.-d). *SolarWinds Compromise (C0024)*. https://attack.mitre.org/campaigns/C0024/

Pols, P. (2019). *The unified kill chain: Raising resilience against cyber attacks* (White paper). https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs. (2019). How Equifax neglected cybersecurity and suffered a devastating data breach: Staff report. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/FINAL%20Equifax%20Report.pdf

Vulnerability History Project. (2017). *CVE-2017-5638*. https://vulnerabilityhistory.org/CVE-2017-5638

About Electrosoft

Electrosoft is a cybersecurity, digital engineering and intelligent automation firm delivering secure, scalable solutions for federal agencies. With 25 years of experience, the award-winning company combines deep mission expertise with modern engineering practices to help agencies operate securely, modernize with confidence and accelerate operational performance. Electrosoft is headquartered in Reston, Virginia. www.electrosoft-inc.com

About the Author

Kirk Lurie is a Program Director in Electrosoft's Federal/Civilian Operations Division. He possesses over 21 years of experience supporting the intelligence community, the National Institute of Standards and Technology, and reviewing risk and risk mitigation activities.