Ransomware: An Analysis from the Red Team and Blue Team Perspectives

Author: Gabriel José Biudes Lino

September 18, 2025

Contents

Introduction

Ransomware is one of the greatest threats to digital security today, impacting organizations across all sectors and sizes. Successful attacks can disrupt critical operations, cause significant financial losses, and undermine the trust of customers and partners. Therefore, understanding how these attacks occur and how to defend against them is essential for any organization seeking to maintain digital resilience.

To that end, we use two complementary perspectives: the **Red Team**, which simulates attacker behavior by identifying vulnerabilities and critical points, and the **Blue Team**, which focuses on defense, mitigation, and incident response. The Red Team follows recognized frameworks such as MITRE ATT&CK to map attack phases and the most common techniques used in ransomware campaigns. The Blue Team relies on best-practice frameworks like the NIST Cybersecurity Framework to structure processes for identification, protection, detection, response, and recovery.

This integrated view allows the organization to understand not only the attack lifecycle but also the controls and measures necessary to reduce risk, protect critical assets, and ensure business continuity. By adopting this approach, leaders and security teams can make more informed and proactive decisions, turning threat knowledge into concrete defensive and resilience actions.

Red Team: MITRE ATT&CK

The **MITRE ATT&CK** framework is a widely used knowledge base for understanding, categorizing, and analyzing attacker behavior in the cyber domain. It organizes attack techniques into *tactics*, representing the attacker's high-level objectives, and *techniques*, which detail the specific methods used to achieve those objectives.

Expanded Overview

Ransomware attacks typically follow several phases within ATT&CK, from initial access to execution and persistence of malware, through privilege escalation, lateral movement, and data exfiltration. In this expanded section, for each phase we present: (1) description, (2) relevant ATT&CK techniques with identifiers, (3) historical examples or associated malware families, (4) artifacts / detection signals, and (5) recommended mitigations.

Initial Access

Objective: obtain an entry point into the target environment.

- **External remote services (T1133) — RDP, VPN:**
  - *Example:* campaigns that abuse exposed RDP credentials (e.g., brute-force attacks against RDP ports); groups use RDP access for initial deployment of Cobalt Strike / loaders.
  - *Signals:* multiple failed login attempts from a few IPs; RDP connections at unusual hours; use of service accounts for interactive login.
  - *Mitigation:* enable 2FA/MFA for VPN/RDP, block direct internet access with VPN/jump hosts, monitor and throttle login attempts, use geo-blocking when appropriate.
- **Exploitation of public-facing applications (T1190):**
  - *Example:* exploitation of RCE in public web applications (vulnerabilities such as SQLi, command injection, deserialization).
  - *Signals:* anomalous patterns in HTTP logs (injection patterns), requests with strange payloads, POST traffic with large payloads to unusual endpoints.
  - *Mitigation:* WAF with updated rules, scheduled vulnerability scanning, rapid patching of CVEs, application hardening.

- **Phishing / Spear-phishing (T1566):**
  - *Example:* campaigns with malicious Office attachments that load macros, or links to credential-harvesting sites.
  - *Signals:* users opening links from newly registered domains, mass-sent emails with the same payload, creation of email accounts mimicking internal domains.
  - *Mitigation:* email protections (SPF, DKIM, DMARC), attachment sandboxing, phishing training, default macro-blocking policies.
- **Supply chain compromise (T1195):**
  - *Example:* supply-chain attacks (e.g., NotPetya / ShadowPad / CCleaner) where legitimate software is tampered with to distribute malware.
  - *Signals:* invalid software signatures, updates coming from unrecognized servers, unusual spikes in downloads of the same installer.
  - *Mitigation:* verify binary signatures, network segmentation for update servers, review third-party dependencies and security clauses in vendor contracts.
- **Insider threat / purchase of access (T1078 & variant):**
  - *Example:* affiliates buying credentials or employee access to skip early stages.
  - *Signals:* access created outside normal procedures, logins at odd hours, file transfers to external destinations by internal accounts.
  - *Mitigation:* privilege review with least-privilege principle, monitoring of privileged account activity, awareness programs and administrative controls.

Execution of Malicious Code

Objective: execute payloads or commands that allow control of the host.

- **User execution (T1204):** users running binaries received via email or download — mitigation: execution policies, application allowlisting (AppLocker, Software Restriction Policies).
- **Command and scripting interpreters (T1059):** use of PowerShell, cmd, bash to automate actions. *Signals:* obfuscated commands in PowerShell logs (ModuleLogging/ScriptBlockLogging), execution of unusual cmdlets.
- **Exploits for client execution / WMI (T1203 / T1047):** WMI often used to orchestrate remote execution. *Mitigation:* log and correlate WMI events, restrict WMI usage to known administrative accounts.

Persistence

Objective: maintain access after reboots or credential renewals.

- **Valid accounts and account creation (T1078 / T1136):** creation of user accounts with names similar to legitimate ones. *Signals:* new administrative accounts, group elevation.

- **Registry run keys / startup folder (T1547), Scheduled tasks (T1053):** creation/modification of services and tasks. *Detection:* changes in run/autorun registry keys, new scheduled tasks.
- **Use of remote administration software:** AnyDesk/TeamViewer used as backdoors — monitor atypical installations and sessions.

Privilege Escalation

Objective: gain higher permissions to access sensitive resources.

- **Exploitation for privilege escalation (T1068):** local vulnerabilities used to elevate privileges. *Mitigation:* fast patching, Application Control, memory protection (ASLR, DEP).
- **Process injection (T1055):** hollowing of trusted processes (e.g., injection into explorer.exe, svchost). *Signals:* processes with anomalous flags, handles opened to LSASS by unexpected processes — monitor with EDR.
- **Abuse of elevation control mechanisms (T1548):** techniques exploiting UAC or misconfigured services — audit services with elevated rights.

Defense Evasion

Objective: avoid detection by security tools.

- **Defense evasion (T1211), Impairing defenses (T1562):** disabling AV/EDR, modifying security policies.
- **Modification / removal of artifacts (T1070):** log clearing, event truncation.
- **Signed binary proxy execution (T1218):** abuse of legitimate signed binaries (Living-off-the-Land Binaries) to execute malicious code (e.g., mshta, regsvr32).
- *Mitigation:* EDR with heuristics, monitoring AV service changes, protecting logs with remote replication, blocking and analyzing LOLBin execution when used out of context.

Credential Access

Objective: obtain passwords, hashes, Kerberos tickets.

- **Brute force (T1110):** attacks against authentication services.
- **Credential dumping (T1003):** tools like Mimikatz, or LSASS memory dumping. *Signals:* anomalous reads of critical processes, presence of dumping tools, process executions accessing LSASS.
- **Theft / forging of Kerberos tickets (T1558):** Pass-the-Ticket / Golden Ticket. *Mitigation:* service account segmentation, password rotation, use of LAPS, restricting SPN-enabled accounts.

Lateral Movement

Objective: propagate control to other hosts and environments.

- **Remote services (T1021), Exploitation of remote services (T1210):** RDP, SMB, WinRM, PsExec, WMI. *Signals:* remote command executions, anomalous SMB connections, use of remote management tools.
- **Mitigation:** network segmentation, microsegmentation, internal firewalls, monitoring inter-host authentications, blocking unnecessary protocols.

Collection and Exfiltration

Objective: gather relevant assets and transfer them outside.

- **Local and network drive collection (T1005/T1039):** searching for sensitive files (specific extensions, data patterns).
- **Archive (T1560) and exfiltration via web services (T1567):** compression and upload to legitimate services (Google Drive, Dropbox) or attacker-controlled servers.
- *Signals:* creation of large compressed files, encrypted connections to unusual external destinations, use of unauthorized cloud accounts.
- *Mitigation:* DLP, upload control to cloud services, TLS traffic inspection (when possible), egress filtering rules.

Ransomware Deployment

Objective: encrypt data and prevent recovery, often coupled with extortion.

- **Inhibit system recovery and encryption (T1490):** delete snapshots, disable backups, mass file encryption.
- **RaaS campaigns:** affiliates leverage RaaS platforms (e.g., Conti, LockBit, BlackCat across multiple operations) — these models scale attacks.
- *Signals:* rapid encryption processes with creation of files with new extensions, ransom notes, mass changes to file metadata.
- *Mitigation:* offsite backups with tamper protection, regular restore testing, response playbooks, and fast isolation of affected segments.

Indicators of Compromise (IoCs) and Examples

- **Frequently observed names/families:** Mimikatz (credential dumping), Cobalt Strike (post-exploitation), QakBot/TrickBot (infostealers and loaders), Conti/LockBit/BlackCa (ransomware).

- **Common IoCs:** C2 domains with unusual patterns, hashes of known executables, command server IP addresses, ransom note filenames.
- **Host artifacts:** undocumented scheduled tasks, services with empty descriptions, files in temporary locations with strange names.

Detection Queries (generic) — examples

The queries below are intentionally generic for use in SIEM (Splunk/Elastic) — adapt them to your environment.

Detection of obfuscated PowerShell (generic example):

```
index=wineventlog EventCode=4104
| where ScriptBlockText like "%FromBase64String%" OR ScriptBlockText like "%IEX %"
```

Detection of LSASS dump / anomalous process read:

```
process_name IN ("procdump.exe","rundll32.exe","taskmgr.exe")
AND parent_process_name="explorer.exe"
AND event_type="process_create"
```

Detection of mass compression followed by upload:

```
file_name endswith ".zip" OR file_name endswith ".7z"
| join [search index=proxy "upload" OR "PUT"]
```

> Note: adapt fields and indexes for your SIEM implementation. For formal rules, translate these examples into Sigma or your EDR/SIEM native rules.

Example: Attack Timeline (mapped to ATT&CK)

1. **Day 0 — Initial Access:** spear-phishing (T1566) with macro => victim executes loader (T1204).
2. **Day 1 — Execution and Persistence:** loader downloads Beacon/Cobalt Strike (T1059) and creates scheduled task (T1053).
3. **Day 2 — Credential and Privilege Escalation:** credential dump with Mimikatz (T1003); abuse of legitimate tools for lateral movement (T1218).
4. **Day 3 — Lateral Movement and Exfiltration:** lateral movement via SMB/RDP (T1021), collection of sensitive documents (T1005), compression and upload to external server (T1567).
5. **Day 5 — Ransomware Deployment:** backup shutdown and mass encryption execution (T1490).

Blue Team: NIST Cybersecurity Framework

The **NIST Cybersecurity Framework (CSF)** is one of the leading international references for cybersecurity risk management. Developed by the National Institute of Standards and Technology (NIST), the CSF organizes security practices into five core functions: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. These functions enable an integrated approach, from prevention to incident recovery.

In the context of *ransomware* attacks, applying the CSF consistently is essential to reduce infection likelihood, mitigate impacts, respond quickly, and restore critical operations.

1. Identify

The first step seeks to build a clear understanding of the technological environment, mapping assets, processes, and associated risks. Without visibility, effective protection is impossible.

- **Asset inventory:** Maintain an updated catalog of servers, endpoints, network devices, critical applications, and sensitive data. Example: classify financial and customer data as *high value assets*.
- **Dependency mapping:** Identify integrations with suppliers and digital supply chains, reducing the risk of indirect attacks (such as supply chain attacks).
- **Vulnerability assessment:** Use scanners (such as Nessus or OpenVAS) to identify flaws in exposed systems, including SQL injection, RCEs, or misconfigured services.
- **Account and privilege management:** Document user roles, segregating access to avoid excessive privileges or orphan accounts.
- **Threat intelligence:** Monitor Ransomware-as-a-Service (RaaS) campaigns, domains used in malvertising, and forums where corporate accesses are traded.

2. Protect

This phase includes technical and administrative controls to make exploitation more difficult for attackers.

- **Access control:** Implement multi-factor authentication (MFA) for RDP and VPN, apply the principle of least privilege, and regularly review permissions.

- **Data protection:** Adopt the *3-2-1* backup rule (3 copies, 2 different media, 1 offline or off-site) and encryption for data at rest and in transit.
- **Training and awareness:** Conduct phishing simulations, security campaigns, and periodic training. Well-trained employees are the first line of defense against spear phishing.
- **Endpoint security:** Deploy EDR/XDR, updated antivirus, firewalls, and network segmentation (e.g., separating critical servers from workstations).
- **Patch management:** Ensure timely application of updates in operating systems, browsers, and exposed software. Example: patching known vulnerabilities like ProxyShell or Log4Shell.
- **Policies and procedures:** Define clear guidelines for secure configurations, remote access, and credential storage.

3. Detect

Even with good protection, attack attempts are inevitable. The *Detect* function focuses on monitoring and quickly identifying anomalies.

- **SIEM and log analysis:** Centralize and correlate events from servers, endpoints, proxies, and firewalls to detect suspicious patterns.
- **Behavior-based detection:** Identify attempts to dump LSASS, create suspicious accounts, escalate privileges, and perform lateral movement.
- **Honeypots and traps:** Deploy decoy systems to detect scans and malicious movements early.
- **Automated alerts:** Configure notifications for critical activities such as anomalous PowerShell execution, off-hours access, or use of tools like Mimikatz.

4. Respond

Once an attack is detected, it is crucial to act quickly to contain and mitigate damage.

- **Isolation of compromised assets:** Remove infected systems from the network to prevent propagation. Example: VLAN segmentation or disabling switch ports.
- **Disable persistence:** Review and remove accounts, scheduled tasks, registry keys, or RATs (TeamViewer, AnyDesk) used by the attacker.
- **Malware eradication:** Remove malicious binaries, scripts, and related artifacts, ensuring the attacker cannot maintain presence.
- **Communication and coordination:** Notify internal teams (IT, legal, compliance) and, when necessary, involve regulators or response partners.
- **Incident response plans:** Follow a structured playbook, such as ransomware-specific response guides.

5. Recover

The final function ensures operations return to normal and that lessons are learned to avoid recurrence.

- **Backup restoration:** Test and validate backup copies before reintegration, ensuring they were not compromised.
- **Post-incident review:** Conduct *lessons learned*, identifying exploited flaws and correcting vulnerabilities. Example: strengthen email policies after a successful phishing incident.
- **Control updates:** Refine monitoring, policies, and training according to lessons learned.
- **Transparent communication:** Inform stakeholders, clients, and authorities about recovery, reinforcing trust.
- **Continuity testing:** Conduct disaster simulations and periodic restoration tests to ensure future resilience.

Conclusion

The study of both the **Red Team** and **Blue Team** perspectives highlights the importance of understanding both the attacker's mindset and defensive strategies in a corporate environment. The detailed analysis of ransomware TTPs through the MITRE ATT&CK framework enables the identification of critical vulnerability points and anticipation of malicious actions, providing a structured view of the attack phases — from initial access to malware deployment and data exfiltration.

On the other hand, the application of the **NIST Cybersecurity Framework** demonstrates how organizations can structure preventive controls, detection mechanisms, response processes, and recovery plans. Integrating the five functions — *Identify, Protect, Detect, Respond*, and *Recover* — enables a proactive and systemic approach, significantly reducing the risks associated with ransomware incidents.

The combination of these two approaches reinforces the need for intelligence-driven cybersecurity, where understanding attacker tactics guides the implementation of effective controls, while defensive measures strengthen organizational resilience. Furthermore, it emphasizes the relevance of continuous training, security tool updates, proper backup management, and continuous monitoring, all of which are critical to mitigating financial, operational, and reputational impacts from ransomware attacks.

In summary, this work highlights that cybersecurity is not only a technological matter but also a strategic one. Understanding the full attack lifecycle and applying recognized frameworks enables companies to transform threats into opportunities to improve processes, strengthen controls, and promote a culture of continuous security — ensuring business continuity and reliability in increasingly complex risk scenarios.