Ransomware: Uma Análise sob a Perspectiva do Red Team e do Blue Team

Autor: Gabriel José Biudes Lino

18 de Setembro de 2025

Sumário

Introdução

O *ransomware* é uma das maiores ameaças à segurança digital atualmente, impactando empresas de todos os setores e tamanhos. Ataques bem-sucedidos podem interromper operações críticas, causar prejuízos financeiros significativos e comprometer a confiança de clientes e parceiros. Por isso, entender como esses ataques acontecem e como se defender é essencial para qualquer organização que queira manter sua resiliência digital.

Para isso, utilizamos duas perspectivas complementares: o **Red Team**, que simula o comportamento do atacante, identificando vulnerabilidades e pontos críticos, e o **Blue Team**, que atua na defesa, mitigação e resposta a incidentes. O Red Team segue frameworks reconhecidos, como o MITRE ATT&CK, para mapear as fases do ataque e as técnicas mais comuns utilizadas em campanhas de *ransomware*. Já o Blue Team se apoia em frameworks de boas práticas, como o NIST Cybersecurity Framework, para estruturar processos de identificação, proteção, detecção, resposta e recuperação.

Essa visão integrada permite que a organização compreenda não apenas o ciclo de ataque, mas também os controles e medidas necessários para reduzir riscos, proteger ativos críticos e garantir a continuidade dos negócios. Ao adotar essa abordagem, líderes e equipes de segurança podem tomar decisões mais informadas e proativas, transformando o conhecimento sobre ameaças em ações concretas de defesa e resiliência.

Red Team: MITRE ATT&CK

O framework **MITRE ATT&CK** é uma base de conhecimento amplamente utilizada para entender, categorizar e analisar o comportamento de atacantes no ambiente cibernético. Ele organiza técnicas de ataque em *táticas*, representando os objetivos de alto nível do atacante, e *técnicas*, que detalham os métodos específicos utilizados para atingir esses objetivos.

Visão Geral Ampliada

Ataques de *ransomware* seguem tipicamente várias fases dentro do ATT&CK, desde a obtenção de acesso inicial até a execução e persistência do malware, passando por escalonamento de privilégios, movimentação lateral e exfiltração de dados. Nesta seção ampliada, para cada fase apresentamos: (1) descrição, (2) técnicas ATT&CK relevantes com identificadores, (3) exemplos históricos ou famílias de malware associadas, (4) artefatos / sinais de detecção, e (5) mitigações recomendadas.

Acesso Inicial

Objetivo: obter um ponto de entrada no ambiente alvo.

- **Serviços remotos externos (T1133) — RDP, VPN:**
  - *Exemplo:* campanhas que abusam de credenciais expostas em RDP (e.g. ataques envolvendo Brute-force contra portas RDP); grupos usam acessos RDP para deploy inicial de Cobalt Strike / loaders.
  - *Sinais:* múltiplas tentativas de login falhas provenientes de poucos IPs; conexões RDP de horários incomuns; uso de contas de serviço para login interativo.
  - *Mitigação:* habilitar 2FA/ MFA para VPN/RDP, bloquear acesso direto à internet com VPN/Jump hosts, monitorar e limitar tentativas de login (throttling), usar bloqueio por geolocalização quando apropriado.
- **Exploração de aplicações públicas (T1190):**
  - *Exemplo:* exploração de RCE em aplicações web públicas (vulnerabilidades como SQLi, command injection, deserialização).
  - *Sinais:* padrões anômalos em logs HTTP (padrões de injeção), requisições com payloads estranhos, tráfego POST com grande payload para endpoints não usuais.

  - *Mitigação:* WAF com regras atualizadas, scanner de vulnerabilidades programado, correção rápida de CVEs, hardening de aplicações.

- **Phishing / Spear-phishing (T1566):**
  - *Exemplo:* campanhas com anexos Office maliciosos que carregam macros, ou links para sites de credenciais (credential harvesting).
  - *Sinais:* usuários abrindo links de domínio novo, envio massivo de e-mails com mesmo payload, criação de contas de e-mail semelhantes a domínios internos.
  - *Mitigação:* proteção de e-mail (SPF, DKIM, DMARC), sandboxing de anexos, treinamento de phishing, políticas de bloqueio de macros por padrão.

- **Comprometimento da cadeia de suprimentos (T1195):**
  - *Exemplo:* ataques tipo supply-chain (e.g. NotPetya/ShadowPad/ CCleaner) onde software legítimo é manipulado para distribuir malware.
  - *Sinais:* assinaturas de software inválidas, atualizações vindas de servidores não reconhecidos, picos incomuns de downloads do mesmo instalador.
  - *Mitigação:* verificação de assinatura de binários, segmentação de rede para servidores de atualização, revisão de dependências de terceiros e contratos de segurança com fornecedores.

- **Ameaça interna / compra de acesso (T1078 & variante):**
  - *Exemplo:* afiliados comprando credenciais ou acesso de funcionários para saltar etapas iniciais.
  - *Sinais:* criação de acessos fora do processo normal, logins em horários estranhos, transferência de arquivos para destinos externos por contas internas.
  - *Mitigação:* revisão de privilégios com princípio do menor privilégio, monitoramento de atividades de contas privilegiadas, programas de conscientização e controles administrativos.

Execução de Código Malicioso

Objetivo: executar payloads ou comandos que permitam controlar o host.

- **Execução pelo usuário (T1204):** usuários executando binários recebidos por e-mail ou download — mitigação: políticas de execução, application allowlisting (AppLocker, Software Restriction Policies).

- **Interpretadores de comando e script (T1059):** uso de PowerShell, cmd, bash para automatizar ações. *Sinais:* comandos ofuscados em logs do PowerShell (ModuleLogging/ScriptBlockLogging), execução de cmdlets pouco usuais.

- **Exploits para execução em cliente / WMI (T1203 / T1047):** WMI frequentemente usado para orquestrar execução remota. *Mitigação:* registrar e correlacionar eventos de WMI, restringir uso de WMI a contas administrativas conhecidas.

Persistência

Objetivo: manter acesso após reinícios ou renovação de credenciais.

- **Contas válidas e criação de contas (T1078 / T1136):** criação de usuários com nomes próximos aos legítimos. *Sinais:* novas contas administrativas, elevação de grupos.
- **Execução automática na inicialização (T1547), Tarefas agendadas (T1053):** criação/modificação de serviços e tasks. *Detecção:* alterações em chaves de registro de run/autorun, novas scheduled tasks.
- **Uso de software de administração remota:** AnyDesk/TeamViewer usados como backdoor — monitorar instalações e sessões atípicas.

Escalonamento de Privilégios

Objetivo: ganhar permissões mais elevadas para acessar recursos sensíveis.

- **Exploração para escalonamento (T1068):** vulnerabilidades locais usadas para elevar privilégios. *Mitigação:* patching rápido, Application Control, proteção de memória (ASLR, DEP).
- **Injeção em processos (T1055):** inquilinação de processos confiáveis (ex.: injeção em explorer.exe, svchost). *Sinais:* processos com flags anômalas, handles abertos para LSASS por processos não esperados — monitorar com EDR.
- **Abuso de mecanismos de elevação (T1548):** técnicas que exploram UAC ou serviços com permissões incorretas — auditar serviços com direitos elevados.

Evasão de Defesa

Objetivo: evitar detecção por ferramentas de segurança.

- **Evasão de defesa (T1211), Impairing Defenses (T1562):** desativação de AV/EDR, modificação de políticas de segurança.
- **Modificação / remoção de evidências (T1070):** limpeza de logs, truncamento de eventos.
- **Signed binary proxy execution (T1218):** abuse de binários legítimos assinados (Living-off-the-Land Binaries) para executar código malicioso (ex.: mshta, regsvr32).
- *Mitigação:* EDR com heurísticas, monitoramento de alteração de serviços AV, proteção de logs com replicação remota, bloqueio e análise de execução de LOB (living off the land) quando usado fora de contexto.

Coleta de Credenciais

Objetivo: obter senhas, hashes, tickets Kerberos.

- **Força bruta (T1110):** ataques contra serviços de autenticação.
- **Dumping de credenciais (T1003):** ferramentas como Mimikatz, ou dumping de LSASS em memória. *Sinais:* leitura anômala de processos críticos, presença de ferramentas de dumping, execuções de processos com acesso a LSASS.
- **Roubo/falsificação de tickets Kerberos (T1558):** Pass-the-Ticket / Golden Ticket. *Mitigação:* segmentação de contas de serviço, rotação de senha, uso de LAPS, restringir uso de contas com SPN.

Movimentação Lateral

Objetivo: propagar controle para outros hosts e ambientes.

- **Serviços remotos (T1021), Exploração de serviços remotos (T1210):** RDP, SMB, WinRM, PsExec, WMI. *Sinais:* execuções remotas de comandos, conexões SMB anômalas, uso de ferramentas de gerenciamento remoto.
- **Mitigação:** segmentação da rede, microsegmentação, firewalling interno, monitoramento de autenticações inter-host, bloqueio de protocolos desnecessários.

Coleta e Exfiltração de Dados

Objetivo: reunir ativos relevantes e transferi-los para fora.

- **Coleta local e em drives de rede (T1005/T1039):** pesquisa por arquivos sensíveis (extensões específicas, padrões de dados).
- **Arquivamento (T1560) e exfiltração via serviços web (T1567):** compressão e upload para serviços legítimos (Google Drive, Dropbox) ou para servidores controlados.
- *Sinais:* criação de grandes arquivos comprimidos, conexões criptografadas para destinos externos incomuns, uso de contas cloud não autorizadas.
- *Mitigação:* DLP, controle de upload para serviços em nuvem, inspeção de tráfego TLS (quando possível), regras de egress filtering.

Implantação de Ransomware

Objetivo: encriptar dados e impedir recuperação, geralmente junto com extorsão.

- **Inibição da recuperação e encriptação (T1490):** apagar snapshots, desabilitar backups, encriptar arquivos em massa.

- **Campanhas RaaS:** afiliados utilizam plataformas RaaS (ex.: Conti, LockBit, BlackCat em várias operações) — esses modelos aumentam a escala de ataques.
- *Sinais:* processo de encriptação rápido com criação de arquivos com novas extensões, notas de resgate, alteração massiva de metadados de arquivos.
- *Mitigação:* cópias de segurança offsite com proteção contra alteração, testes regulares de restore, playbooks de resposta e isolamento rápido de segmentos afetados.

Indicadores de Comprometimento (IoCs) e Exemplos

- **Nomes/famílias frequentemente observadas:** Mimikatz (credential dumping), Cobalt Strike (post-exploit), QakBot/TrickBot (infostealers e loaders), Conti/LockBit/BlackCa (ransomware).
- **IoCs comuns:** domínios de C2 com padrões incomuns, hashes de executáveis conhecidos, endereços IP de servidores de comando, nomes de arquivos de ransom note.
- **Artefatos em host:** scheduled tasks não documentadas, serviços com descrições vazias, arquivos em locais temporários com nomes estranhos.

Consultas de Detecção (genéricas) — exemplos

As queries abaixo são propositalmente genéricas para uso em SIEM (Splunk/Elastic) — adapte ao seu ambiente.

Detecção de PowerShell ofuscado (exemplo genérico):

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

Detecção de dump de LSASS / leitura anômala do processo:

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

Detecção de compressão em massa seguida de upload:

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

> Nota: adapte campos e índices para sua implementação de SIEM. Para regras formais, traduza esses exemplos para Sigma ou regras nativas do seu EDR/SIEM.

Exemplo: Linha do Tempo de Ataque (mapeada para ATT&CK)

1. **Dia 0 — Acesso Inicial:** spear-phishing (T1566) com macro => vítima executa carregador (T1204).
2. **Dia 1 — Execução e Persistência:** loader baixa Beacon/Cobalt Strike (T1059) e cria scheduled task (T1053).
3. **Dia 2 — Credencial e Escalonamento:** dump de credenciais com Mimikatz (T1003); abuso de ferramentas legítimas para movimentação lateral (T1218).
4. **Dia 3 — Lateralidade e Exfil:** movimento lateral via SMB/RDP (T1021), coleta de documentos sensíveis (T1005), compressão e upload para servidor externo (T1567).
5. **Dia 5 — Deploy Ransomware:** desligamento de backups e execução de encriptação em massa (T1490).

Blue Team: NIST Cybersecurity Framework

O **NIST Cybersecurity Framework (CSF)** é uma das principais referências internacionais para a gestão de riscos em cibersegurança. Desenvolvido pelo National Institute of Standards and Technology (NIST), o CSF organiza as práticas de segurança em cinco funções fundamentais: *Identify* (Identificar), *Protect* (Proteger), *Detect* (Detectar), *Respond* (Responder) e *Recover* (Recuperar). Essas funções permitem estruturar uma abordagem integrada, desde a prevenção até a recuperação de incidentes.

No contexto de ataques de *ransomware*, aplicar o CSF de forma consistente é essencial para reduzir a probabilidade de infecção, mitigar impactos, responder rapidamente e restaurar operações críticas.

1. Identify (Identificar)

A primeira etapa busca criar uma compreensão clara do ambiente tecnológico, mapeando ativos, processos e riscos associados. Sem visibilidade, é impossível proteger de forma eficaz.

- **Inventário de ativos:** Manter um catálogo atualizado de servidores, endpoints, dispositivos de rede, aplicações críticas e dados sensíveis. Exemplo: classificar dados financeiros e de clientes como *high value assets*.
- **Mapeamento de dependências:** Identificar integrações com fornecedores e cadeias de suprimento digitais, reduzindo o risco de ataques indiretos (como supply chain attacks).
- **Avaliação de vulnerabilidades:** Utilizar scanners (como Nessus ou OpenVAS) para identificar falhas em sistemas expostos, incluindo SQL injection, RCEs ou serviços mal configurados.
- **Gerenciamento de contas e privilégios:** Documentar funções de usuários, segregando acessos para evitar privilégios excessivos ou contas órfãs.
- **Inteligência de ameaças:** Monitorar campanhas de Ransomware-as-a-Service (RaaS), domínios usados em malvertising e fóruns onde acessos a empresas são comercializados.

2. Protect (Proteger)

Aqui entram os controles técnicos e administrativos para dificultar a exploração por atacantes.

- **Controle de acesso:** Implementar autenticação multifator (MFA) em RDP e VPN, aplicar o princípio do menor privilégio e revisar permissões regularmente.
- **Proteção de dados:** Adotar a regra *3-2-1* de backup (3 cópias, 2 mídias diferentes, 1 offline ou off-site) e criptografia para dados em repouso e em trânsito.
- **Treinamento e conscientização:** Realizar simulações de phishing, campanhas de segurança e treinamentos periódicos. Funcionários bem treinados são a primeira linha de defesa contra spear phishing.
- **Segurança de endpoints:** Utilizar EDR/XDR, antivírus atualizado, firewalls e segmentação de rede (ex: separar servidores críticos de estações de trabalho).
- **Gerenciamento de patches:** Garantir a aplicação rápida de atualizações em sistemas operacionais, navegadores e softwares expostos. Exemplo: corrigir falhas conhecidas como ProxyShell ou Log4Shell.
- **Políticas e procedimentos:** Definir guias claros para configurações seguras, acesso remoto e armazenamento de credenciais.

3. Detect (Detectar)

Mesmo com boas proteções, é inevitável que tentativas de ataque ocorram. A função *Detect* foca no monitoramento e identificação rápida de anomalias.

- **SIEM e análise de logs:** Centralizar e correlacionar eventos de servidores, endpoints, proxies e firewalls para detectar padrões suspeitos.
- **Detecção baseada em comportamento:** Identificar tentativas de dumping de LSASS, criação de contas suspeitas, escalonamento de privilégios e movimentação lateral.
- **Honeypots e armadilhas:** Implantar sistemas isca para detectar varreduras e movimentos maliciosos precocemente.
- **Alertas automatizados:** Configurar notificações para atividades críticas, como execução de PowerShell anômalo, acessos fora do horário comercial ou uso de ferramentas como Mimikatz.

4. Respond (Responder)

Uma vez detectado o ataque, é crucial agir rapidamente para conter e mitigar danos.

- **Isolamento de ativos comprometidos:** Retirar sistemas infectados da rede para evitar propagação. Exemplo: segmentar VLAN ou desabilitar portas de switch.

- **Desabilitar persistência:** Revisar e remover contas, tarefas agendadas, chaves de registro ou RATs (TeamViewer, AnyDesk) utilizados pelo atacante.
- **Erradicação de malware:** Remover binários maliciosos, scripts e artefatos relacionados, garantindo que o atacante não mantenha presença.
- **Comunicação e coordenação:** Notificar equipes internas (TI, jurídico, compliance) e, quando necessário, acionar órgãos reguladores ou parceiros de resposta.
- **Planos de resposta a incidentes:** Seguir um roteiro estruturado, como playbooks específicos para ransomware.

5. Recover (Recuperar)

A função final garante o retorno das operações, além de aprendizado para evitar recorrência.

- **Restauração de backups:** Testar e validar cópias de segurança antes da reintegração, garantindo que não foram comprometidas.
- **Revisão pós-incidente:** Realizar *lessons learned*, identificando falhas exploradas e corrigindo vulnerabilidades. Exemplo: endurecer políticas de e-mail após phishing bem-sucedido.
- **Atualização de controles:** Refinar monitoramentos, políticas e treinamentos de acordo com as lições aprendidas.
- **Comunicação transparente:** Informar stakeholders, clientes e órgãos competentes sobre a recuperação, reforçando a confiança.
- **Testes de continuidade:** Realizar simulações de desastres e testes de restauração periódicos para garantir resiliência futura.

Conclusão

O estudo das perspectivas do **Red Team** e do **Blue Team** evidencia a importância de compreender tanto a mentalidade do atacante quanto as estratégias de defesa em um ambiente corporativo. A análise detalhada das TTPs de ransomware por meio do framework MITRE ATT&CK permite identificar pontos críticos de vulnerabilidade e antecipar as ações de agentes maliciosos, fornecendo uma visão estruturada das fases do ataque, desde o acesso inicial até a implantação do malware e a exfiltração de dados.

Por outro lado, a aplicação do **NIST Cybersecurity Framework** demonstra como organizações podem estruturar controles preventivos, mecanismos de detecção, processos de resposta e planos de recuperação. A integração das cinco funções — *Identify, Protect, Detect, Respond* e *Recover* — possibilita uma abordagem proativa e sistêmica, reduzindo significativamente os riscos associados a incidentes de ransomware.

A combinação dessas duas abordagens reforça a necessidade de uma segurança cibernética baseada em inteligência, na qual a compreensão das táticas do atacante orienta a implementação de controles eficazes, enquanto a execução de medidas defensivas fortalece a resiliência da organização. Além disso, destaca-se a relevância de treinamentos constantes, atualização de ferramentas de segurança, gestão adequada de backups e monitoramento contínuo, que são fundamentais para mitigar impactos financeiros, operacionais e reputacionais decorrentes de ataques de ransomware.

Em síntese, este trabalho reforça que a segurança digital não é apenas uma questão tecnológica, mas também estratégica. Conhecer o ciclo completo de um ataque e aplicar frameworks reconhecidos permite que empresas transformem a ameaça em oportunidade de aprimorar processos, fortalecer controles e promover uma cultura de segurança contínua, garantindo a continuidade e a confiabilidade dos negócios diante de cenários de risco cada vez mais complexos.