Projeto final de Segurança da Informação Análise de Ransomware

Discente: Isaac Corrêa de Oliveira
Docente: Rennan Jose Maia Da Silva

Introdução

No cenário contemporâneo da segurança da informação, o ransomware emergiu como uma das ameaças cibernéticas mais proeminentes e devastadoras. Caracterizado por sua capacidade de sequestrar dados e extorquir vítimas, seu impacto transcende o âmbito digital, gerando severas consequências financeiras, operacionais e reputacionais. Este documento explora o modus operandi dos ataques de ransomware, desde sua definição e ciclo de vida até os principais métodos de infecção. O objetivo é fornecer uma análise abrangente sobre essa ameaça, destacando seus perigos e, fundamentalmente, apresentando as melhores práticas para prevenção, mitigação e resposta a incidentes, servindo como um guia essencial para indivíduos e organizações.

1. O Que é Ransomware?

Ransomware é uma categoria de software malicioso (malware) projetada para impedir o acesso do usuário a seus arquivos ou dispositivos, geralmente por meio de criptografia. Uma vez que os dados da vítima são criptografados e tornados inacessíveis, os operadores do ataque exigem o pagamento de um resgate (ransom) para fornecer a chave de descriptografia. Tipicamente, a exigência de pagamento é feita em criptomoedas, como Bitcoin (BTC) ou Monero, devido à sua natureza descentralizada e à dificuldade de rastreamento das transações, o que garante maior anonimato aos cibercriminosos.

É crucial entender que, embora o termo "vírus" seja frequentemente usado de forma genérica, o ransomware é uma forma distinta de malware. Suas primeiras variantes surgiram no final da década de 1980, com o "AIDS Trojan" em 1989 sendo o caso pioneiro, distribuído via disquetes e exigindo pagamento por correio. A evolução tecnológica, especialmente a popularização da internet e das criptomoedas, transformou o ransomware em uma ameaça global de alto impacto.

2. *Modus Operandi* de um Ataque de Ransomware

A execução de um ataque de ransomware segue um ciclo de vida bem definido, geralmente dividido nas seguintes etapas:

- **2.1. Infiltração e Acesso:** O ransomware precisa primeiro obter acesso a um sistema ou rede alvo. Isso ocorre por meio de diversos vetores de ataque, sendo o phishing um dos mais comuns.
- **2.2. Execução e Criptografia:** Uma vez no sistema e ativado (geralmente por uma ação da vítima, como clicar em um link ou abrir um anexo), o malware inicia o processo de criptografia de arquivos ou dados, tornando-os inacessíveis. O processo técnico de criptoextorsão envolve um protocolo de três rodadas :
    1. **Preparação do Atacante:** O atacante gera um par de chaves criptográficas (pública e privada). A chave pública é incorporada ao malware antes de sua liberação.
    2. **Infecção e Demanda de Resgate da Vítima:** O malware gera uma chave simétrica aleatória e a utiliza para criptografar os dados da vítima. Em seguida, essa chave simétrica é criptografada usando a chave pública do atacante (criptografia híbrida). A chave simétrica original e os dados em texto claro são "zeroizados" (sobrescritos com zeros) para evitar recuperação.
    3. **Descriptografia e Liberação da Chave Simétrica pelo Atacante:** Após receber o pagamento, o atacante usa sua chave privada (que nunca é exposta à vítima) para decifrar a chave simétrica criptografada. Essa chave simétrica é então enviada de volta à vítima, que pode usá-la para decifrar seus dados.
- Em ataques modernos, é comum a tática de **dupla extorsão**, na qual os criminosos primeiro exfiltram (roubam) uma cópia dos dados sensíveis antes de criptografá-los. Se a vítima se recusar a pagar o resgate pela chave de descriptografia, os criminosos ameaçam vazar publicamente os dados roubados. A
- **tripla extorsão** leva isso um passo adiante, adicionando uma terceira técnica de pressão, como a exigência de resgate de clientes ou parceiros da vítima, ou a realização de ataques de negação de serviço distribuído (DDoS) contra a empresa.
- **2.3. Notificação e Extorsão:** Concluída a criptografia, o ransomware exibe uma nota de resgate na tela do usuário ou em arquivos de texto (.txt) salvos nas pastas afetadas. Esta nota informa a vítima sobre o ataque, estipula o valor do resgate, o método de pagamento (geralmente criptomoedas como Bitcoin ou Monero), e o prazo para pagamento, frequentemente com um cronômetro de contagem regressiva para aumentar a urgência. A ameaça é clara: caso o pagamento não seja efetuado, os arquivos podem ser perdidos para sempre ou, no caso da dupla extorsão, os dados roubados serão divulgados publicamente.

3. Principais Vetores de Infecção

Os cibercriminosos utilizam múltiplas técnicas para distribuir ransomware. As mais frequentes incluem:

- **E-mails de Phishing:** Um dos vetores mais prevalentes. Mensagens fraudulentas que se passam por comunicações legítimas (bancos, empresas de entrega, serviços online) e que contêm anexos maliciosos (documentos Word, PDFs com macros) ou links para sites comprometidos. Ao clicar no link ou abrir o anexo, o ransomware é baixado e executado.
- **Vulnerabilidades de Software:** Exploração de falhas de segurança não corrigidas (conhecidas como N-Day) ou desconhecidas pelo fabricante (Zero-Day) em sistemas operacionais, navegadores e outros aplicativos. O WannaCry, por exemplo, explorou a vulnerabilidade EternalBlue para se propagar automaticamente.
- **Protocolo de Área de Trabalho Remota (RDP):** Acessos RDP com senhas fracas ou mal configurados são um alvo primário para atacantes, que buscam acesso direto a redes corporativas para implantar o ransomware manualmente.
- **Malvertising:** Anúncios maliciosos veiculados em sites legítimos que, ao serem clicados (ou mesmo sem clique direto), redirecionam o usuário para páginas que instalam o malware automaticamente.
- **Kits de Exploit:** Toolkits que exploram vulnerabilidades em softwares populares como Adobe Flash, Java e Microsoft Silverlight para distribuir malware, incluindo ransomware.
- **Downloads de Fontes Não Confiáveis:** Softwares piratas, jogos e outros arquivos baixados de sites ou redes P2P suspeitas frequentemente carregam malwares embutidos.
- **Mídias Removíveis:** Dispositivos como pen drives e HDs externos infectados podem espalhar o ransomware quando conectados a um computador.

4. Impactos de um Ataque de Ransomware

Os danos causados por um ataque de ransomware são multifacetados e severos:

- **4.1. Impacto Financeiro:** Inclui o custo do pagamento do resgate (se efetuado), que pode ser exorbitante e variar de milhares a dezenas de milhões de dólares. O custo médio de um resgate pago pode ultrapassar US$ 300.000, e o custo médio de recuperação de um ataque pode chegar a quase US$ 2 milhões. Além disso, há prejuízos pela interrupção das operações (tempo médio de inatividade de 21 dias, com recuperação total podendo levar até 287 dias), os custos de remediação e recuperação dos sistemas (análise forense pode custar mais de US$ 70.000), e as possíveis multas regulatórias. Empresas com seguro cibernético tendem a pagar resgates 2,8 vezes maiores.
- **4.2. Perda Permanente de Dados:** Não há garantia de que os criminosos fornecerão a chave de descriptografia após o pagamento. Estudos mostram que apenas 8% das vítimas que pagaram o resgate conseguiram recuperar seus dados. Em 2024, a perda de dados

aumentou significativamente, com 27% das organizações que pagaram o resgate não conseguindo recuperar seus dados. Além disso, falhas no processo de criptografia ou descriptografia podem corromper os arquivos de forma irreversível.

- **4.3. Dano Reputacional:** A exposição de um incidente de segurança abala a confiança de clientes, parceiros e investidores, podendo resultar em perdas de negócios a longo prazo. Ataques com malware e ransomware foram os mais propensos a gerar danos à reputação, representando 60% dos incidentes com impacto reputacional. O Relatório Global de Riscos Cibernéticos 2025 da Aon revela que eventos cibernéticos com potencial de dano à reputação podem provocar, em média, uma queda de 27% no valor de mercado para os acionistas.
- **4.4. Consequências Legais e Regulatórias:** A violação de dados pode levar a sanções sob leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, resultando em multas e penalidades substanciais.

5. Medidas de Prevenção e Mitigação

A defesa contra ransomware exige uma abordagem em camadas (*defense-in-depth*) :

- **5.1. Conscientização e Treinamento:** Educar os usuários a reconhecer e-mails de phishing, links suspeitos e práticas seguras de navegação é a primeira linha de defesa.
- **5.2. Política de Backups Robusta:** Implementar a regra 3-2-1: ter três cópias dos dados, em duas mídias diferentes, com uma cópia mantida offline (ou em ambiente isolado). Testar a restauração dos backups periodicamente é crucial.
- **5.3. Gerenciamento de Patches:** Manter sistemas operacionais, softwares e firmwares sempre atualizados para corrigir vulnerabilidades conhecidas.
- **5.4. Segurança de E-mail e Endpoints:** Utilizar filtros de e-mail avançados para bloquear spam e phishing, e implementar soluções de proteção de endpoint (antivírus, EDR/XDR) que detectem comportamentos maliciosos.
- **5.5. Controle de Acesso:** Aplicar o Princípio do Menor Privilégio, garantindo que usuários e contas de serviço tenham apenas as permissões estritamente necessárias para suas funções.
- **5.6. Segmentação de Rede:** Isolar redes críticas para impedir que uma infecção se espalhe lateralmente por toda a infraestrutura.

6. O Que Fazer em Caso de Infecção?

Se um ataque ocorrer, ações rápidas podem limitar o dano:

- **6.1. Isolar o Dispositivo:** Desconecte imediatamente o computador infectado da rede (Wi-Fi e cabo) e de qualquer dispositivo externo para conter a propagação.
- **6.2. Não Pagar o Resgate:** A recomendação unânime de especialistas e agências de segurança é não ceder à extorsão. O pagamento não garante a devolução dos dados (apenas 8% das vítimas que pagaram recuperaram seus dados), financia futuras atividades criminosas e pode aumentar a probabilidade de ser alvo de ataques futuros. Em 95% dos casos, o pagamento ocorre porque a infraestrutura de TI está completamente comprometida e não há outra forma de recuperação.
- **6.3. Acionar o Plano de Resposta a Incidentes:** Notifique a equipe de TI ou o responsável pela segurança da informação imediatamente.
- **6.4. Avaliar e Restaurar:** Identifique a variante do ransomware (se possível) e determine o escopo do dano. Formate os sistemas afetados e restaure os dados a partir de um backup limpo e confiável.
- **6.5. Reportar o Crime:** Registre um boletim de ocorrência na delegacia de crimes cibernéticos local.

Conclusão

O ransomware representa uma ameaça persistente e em constante evolução, com um potencial destrutivo que afeta a continuidade dos negócios e a segurança de dados pessoais. Sua progressão, desde o "AIDS Trojan" até os complexos modelos de Ransomware-as-a-Service (RaaS) e as táticas de dupla e tripla extorsão, demonstra uma notável capacidade de adaptação por parte dos atacantes.

A prevenção, centrada na vigilância e na preparação técnica, é indiscutivelmente a estratégia mais eficaz. A conscientização sobre os vetores de ataque, como o phishing, é vital, mas deve ser complementada por defesas tecnológicas robustas e processos bem definidos. A profissionalização dos grupos de ransomware, que operam como verdadeiras "indústrias" com estruturas organizacionais e estratégias de negócio bem definidas, exige vigilância contínua e estratégias de segurança cibernética proativas e multifacetadas por parte de indivíduos e organizações. Em última análise, uma abordagem de defesa em profundidade, que integra tecnologia, processos e pessoas, é indispensável para construir resiliência e proteger ativos digitais contra essa forma disruptiva de crime cibernético.

Anexo:

Link de um projeto exemplo no GitHub
https://github.com/correaisaac/fake-ransomware-sim

Fontes:

What is Ransomware? | Ransomware protection - Malwarebytes, https://www.malwarebytes.com/ransomware

A guide to ransomware - NCSC.GOV.UK, https://www.ncsc.gov.uk/ransomware/home

O impacto financeiro de um ataque de ransomware em uma organização, https://www.storageja.com.br/post/qual-e-o-impacto-financeiro-de-um-ataque-de-ransomware-em-uma-organizacao

O que é ransomware?, https://www.storageja.com.br/post/qual-e-o-impacto-financeiro-de-um-ataque-de-ransomware-em-uma-organizacao

Ciclo de vida de um ataque Ransomware, https://www.purestorage.com/br/knowledge/life-cycle-of-a-ransomware-attack.html

O que é ransomware?, https://www.checkpoint.com/pt/cyber-hub/threat-prevention/ransomware/