BOLETIM DE SEGURANÇA

Ataques a cadeia de suprimentos, defenda-se!

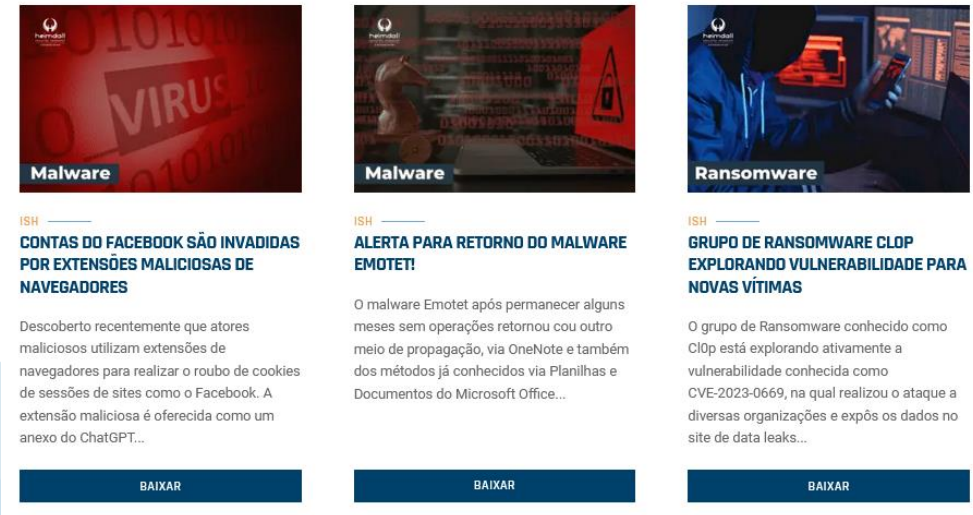
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Tabelas

Lista de Figuras

1 INTRODUÇÃO

Os ataques cibernéticos tornaram-se uma das ameaças mais prevalentes e destrutivas na atualidade, uma das frentes emergentes e preocupantes nesse cenário é o ataque à cadeia de suprimentos das organizações. Esses ataques visam explorar vulnerabilidades nas operações de fornecimento e distribuição de bens e serviços de uma empresa, que frequentemente envolvem múltiplos stakeholders, como fornecedores, fabricantes, distribuidores e varejistas.

O termo "cadeia de suprimentos" refere-se ao conjunto de processos e atividades relacionados à produção, transporte, armazenamento e entrega de produtos ou serviços ao cliente final. Na era da informação digital, essa cadeia é frequentemente suportada por sistemas informatizados que, se comprometidos, podem levar a interrupções significativas, perdas financeiras e danos à reputação das organizações.

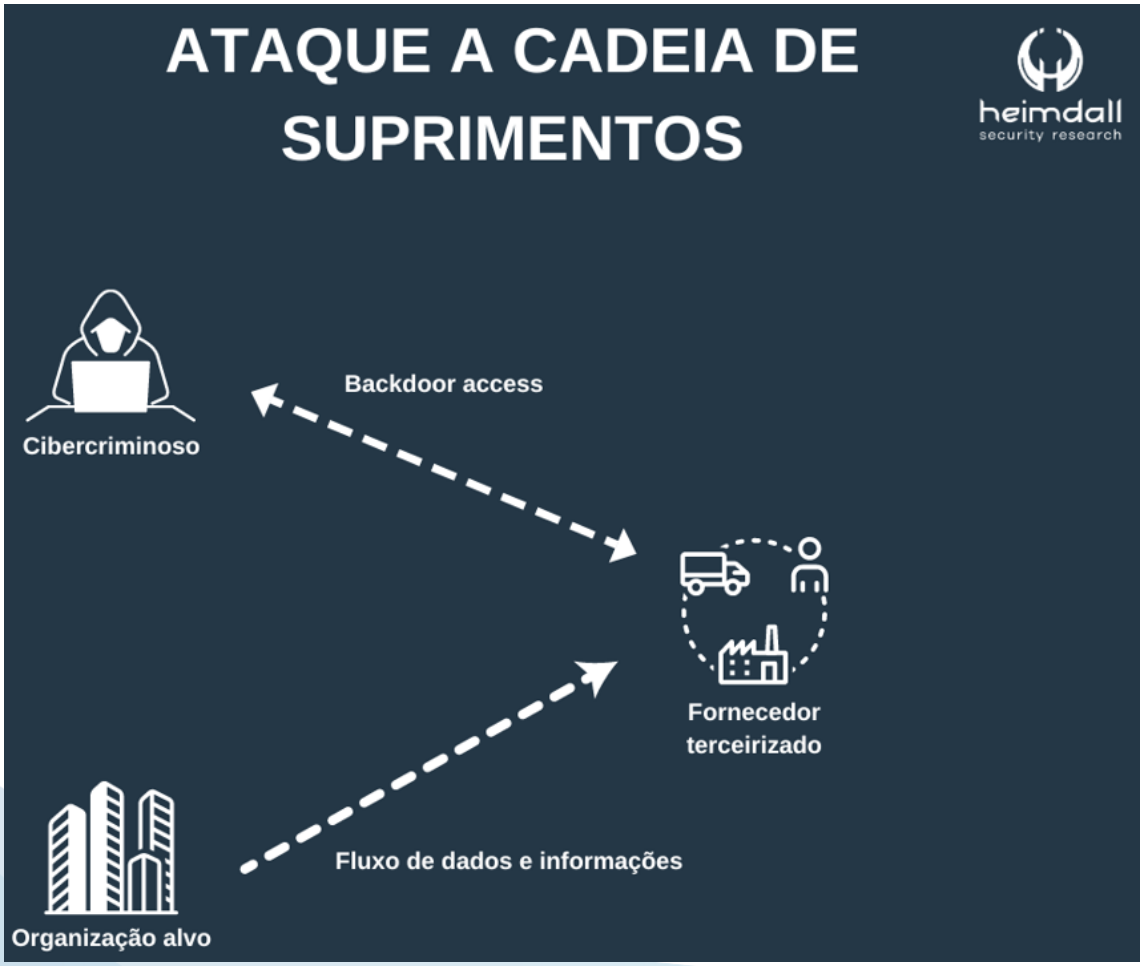


Figura 1 – Figura ilustrativa sobre ataques a cadeia de suprimentos.

2 FUNCIONAMENTO DE ATAQUES A CADEIA DE SUPRIMENTOS

Os ataques à cadeia de suprimentos exploram as conexões de confiança entre diferentes entidades. Cada organização, ao adotar software ou engajar-se com fornecedores, estabelece uma relação de confiança, que pode ser vulnerável. Neste contexto, o elo mais vulnerável dessa teia de confiança é o foco dos atacantes. Mesmo que uma empresa possua sólidas medidas de segurança, se um de seus fornecedores for vulnerável, esse fornecedor se tornará o ponto de entrada. Uma vez dentro da rede do fornecedor, os criminosos podem aproveitar essa relação de confiança para infiltrar-se na rede principal.

Um alvo comum nesse tipo de ataque são os Provedores de Serviços Gerenciados (MSPs), devido ao seu acesso extensivo às redes de seus clientes. Se um MSP é comprometido, os atacantes podem, com facilidade, estender sua presença para as redes dos clientes. Através desta estratégia, atacantes conseguem ampliar seu alcance e acessar redes que, de outra forma, seriam desafiadoras de invadir. O incidente com um desenvolvedor de soluções de TI para empresas e provedores de serviços gerenciados, onde os criminosos infectaram várias organizações através de ransomware, é um exemplo desta tática.

Além disso, há ataques à cadeia de suprimentos que utilizam softwares para disseminar malware. Um exemplo notável é o caso da empresa de desenvolvimento de software para empresas que ajuda a gerenciar suas redes, sistemas e infraestrutura de tecnologia da informação. Onde criminosos conseguiram acessar e modificar o processo de atualização do software da empresa. Com isso, quando as organizações atualizavam seu software, inadvertidamente permitiam o acesso dos invasores a suas infraestruturas.

3 TIPOS DE ATAQUES À CADEIA DE SUPRIMENTOS

Ataques à cadeia de suprimentos têm evoluído em termos de complexidade e escopo. Abaixo, detalhamos os tipos mais comuns e suas respectivas explicações:

Ataques de software

- Os atacantes comprometem softwares legítimos durante o processo de desenvolvimento ou atualização, inserindo códigos maliciosos. Quando a organização-alvo instala ou atualiza esse software, ela inadvertidamente introduz uma ameaça em sua rede.

Ataques de hardware

- Os atacantes inserem componentes maliciosos ou modificam componentes existentes de hardware durante o processo de manufatura ou transporte. Isso pode permitir que eles espionem, modifiquem ou interrompam as operações da organização que utiliza esse hardware.

Ataques via provedores de serviço

- Provedores de serviços, como os Provedores de Serviços Gerenciados (MSPs), têm acesso a redes e sistemas de seus clientes. Se os atacantes comprometem um MSP, eles podem usar esse acesso para atacar os clientes do MSP.

Ataques por infiltração de fornecedor

- Organizações muitas vezes dão acesso a suas redes para fornecedores confiáveis para fins de manutenção, suporte ou outros serviços. Atacantes podem comprometer esses fornecedores e usar esse acesso legítimo para entrar nas redes das organizações-alvo

Ataques de insiders maliciosos

- Embora não seja um ataque externo à cadeia de suprimentos, insiders (funcionários, ex-funcionários, parceiros) podem aproveitar seu conhecimento e acesso para comprometer a organização. Esses ataques podem ser motivados por ganhos financeiros, vingança ou outras razões.

Espionagem da cadeia de suprimentos

- Em vez de tentar comprometer diretamente uma organização, os atacantes podem espionar as comunicações entre a organização e seus fornecedores, buscando informações sensíveis ou pontos de acesso potenciais.

Esses ataques destacam a importância de ter uma visão abrangente da segurança, que não apenas se concentra nas próprias operações de uma organização, mas também em todos os parceiros, fornecedores e terceiros com os quais ela interage. A integridade da cadeia de suprimentos é crucial para garantir a segurança geral de uma organização

4 EXEMPLOS DE ATAQUES A CADEIA DE SUPRIMENTOS

Ataques à cadeia de suprimentos ganharam destaque nos últimos anos devido ao seu potencial de causar grandes interrupções e danos a organizações de alto perfil e seus clientes. Abaixo segue alguns dos ataques mais conhecidos:

- Em 2020, uma empresa de software de gestão de rede, foi comprometida por atacantes que inseriram um backdoor em uma de suas atualizações de software. Quando empresas e agências governamentais em todo o mundo instalaram a atualização comprometida, os atacantes ganharam acesso às suas redes.

- Em 2017, o ransomware NotPetya se espalhou globalmente, causando interrupções massivas. O vetor inicial de infecção foi um software contábil ucraniano. Atacantes comprometeram uma atualização deste software, que, quando instalada por empresas, espalhou o ransomware.

- Em 2017, uma versão legítima de um software de limpeza de PC, foi comprometida por atacantes. Eles inseriram um malware na ferramenta, e quando os usuários baixaram e instalaram a versão comprometida, também instalaram o malware.

- Em 2021, uma empresa de software de gestão de TI, foi comprometida. Os atacantes exploraram uma vulnerabilidade em seu software VSA e implantaram ransomware em redes de clientes que usavam o produto.

5 Conclusão

A segurança na cadeia de suprimentos é de extrema importância para organizações e governos, uma cadeia de suprimentos vulnerável não apenas expõe uma organização a riscos financeiros significativos, mas também pode comprometer a integridade e a confidencialidade de dados importantes. Em um ambiente interconectado, um ponto fraco em um fornecedor ou parceiro pode servir como porta de entrada para adversários cibernéticos, afetando todas as entidades interligadas. Falhas de segurança na cadeia de suprimentos podem resultar em interrupções operacionais, perda de propriedade intelectual, danos à reputação e perda de confiança dos clientes.

Além disso, à medida que a regulamentação em torno da cibersegurança se torna mais rigorosa, as organizações podem enfrentar penalidades legais e financeiras por negligenciar a segurança em sua cadeia de suprimentos. Portanto, proteger a cadeia de suprimentos de ataques cibernéticos é essencial para garantir a continuidade dos negócios, manter a confiança dos stakeholders e salvaguardar a integridade e a reputação de uma organização.

6 TTPs – MITRE ATT&CK

Tática	Técnica	Detalhes
Initial Access	T1195	Os adversários podem manipular produtos ou mecanismos de entrega de produtos antes de serem recebidos por um consumidor final com a finalidade de comprometer dados ou sistemas.

Tabela 1 – Tabel MITRE ATT&CK.

7 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da referida *ameaça*, como por exemplo:

- **Realize avaliação de risco**, identifique e avalie os riscos em toda cadeia de suprimentos. Isto inclui fornecedores, parceiros logísticos, sistemas de IT e quaisquer outras partes envolvidas.
- **Vetar parceiros**, assegure-se de que todos os parceiros na cadeia de suprimentos adotem práticas de segurança robustas. Isso pode incluir a realização de auditorias ou avaliações de terceiros.
- **Realize o monitoramento contínuo**, estabeleça um sistema de monitoramento para detectar atividades suspeitas em tempo real. Use soluções de segurança avançadas, como sistemas de detecção e prevenção de intrusões (IDS/IPS).
- **Atualizações e patches**, mantenha todos os sistemas atualizados com os patches mais recentes. Fornecedores de software frequentemente liberam atualizações para corrigir vulnerabilidades.
- **Segmentação da rede**, se possível, segmente sua rede para que um possível invasor não tenha acesso a toda a infraestrutura.
- **Autenticação multifatorial**, implemente autenticação multifatorial (MFA) para todos os acessos críticos.
- **Treinamento de conscientização**, forneça treinamento regular sobre segurança cibernética para todos os envolvidos na cadeia de suprimentos. Muitos ataques têm origem em engenharia social ou erros humanos.
- **Backup regular**, realize backups regulares de dados críticos e teste a restauração destes backups periodicamente.
- **Tenha um planos de resposta a incidentes**, desenvolva e teste um plano de resposta a incidentes. Este plano deve detalhar as etapas a serem tomadas em caso de um ataque cibernético.
- **Utilização de criptografia**, para proteger dados em trânsito e em repouso.
- **Gerenciamento de acessos**, estabeleça políticas de controle de acesso para garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis.

- **Ferramentas de gestão de vulnerabilidades**, implemente ferramentas que possam ajudar a identificar, classificar e remediar vulnerabilidades em sistemas e aplicativos.
- **Colaboração e comunicação**, estabeleça canais de comunicação claros com todos os parceiros da cadeia de suprimentos para trocar informações sobre ameaças e melhores práticas de segurança.
- **Revisão contratual**, assegure-se de que contratos com fornecedores e parceiros incluam cláusulas sobre padrões de segurança e responsabilidades em caso de falhas.
- **Inventário de ativos**, mantenha um inventário atualizado de todos os ativos digitais, softwares e hardware para que você saiba o que precisa proteger.
- **Políticas de segurança cibernética**, desenvolva políticas claras sobre segurança cibernética e garanta que todos os parceiros e fornecedores estejam cientes e em conformidade com elas.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Checkpoint**
- **Fortinet**
- **CISA**
- **Microsoft**

heimdall
security research
A DIVISION OF ISH