Christian Batista de Lima Rego

RA: 824126605

Professor Calvetti USJT – Butantã

Atividade 3 – Pesquisar 2 ataques cibernéticos nos últimos 5 anos e produzir um texto com as informações solicitadas.

Ataque de Ransomware: BlackCat (ALPHV)

Data do Ataque: O ataque foi descoberto em novembro de 2021.

Tipo de Ataque: Ransomware.

Descrição do Ataque: O BlackCat, também conhecido como ALPHV, é um Ransomware (O ransomware criptografa arquivos e exige um resgate em criptomoedas para liberar os dados.) que utiliza técnicas avançadas de criptografia e ataque para comprometer sistemas. Em novembro de 2021, o grupo de ransomware BlackCat foi associado a uma série de ataques a organizações em vários setores. Os atacantes também infiltram dados antes da criptografia e ameaçam vazá-los se o resgate não for pago.

Vulnerabilidades Exploradas:

CVE (**Common Vulnerabilities and Exposures** ou **Vulnerabilidades e exposições comuns)** é um sistema de identificação e catalogação de vulnerabilidades e exposições de segurança em software e hardware, facilitando a comunicação e a correção de falhas de segurança.

- **CVE:** O BlackCat não está associado a uma vulnerabilidade específica de CVE; em vez disso, explora vulnerabilidades gerais de segurança, como falta de patch em sistemas e fraquezas na segurança de rede.
- **Descrição:** Os ataques frequentemente se aproveitam de falhas na configuração de segurança, como ausência de autenticação forte, sistemas desatualizados e redes vulneráveis.

Impactos e/ou Prejuízos: O ataque causou danos significativos a diversas organizações, resultando em perda de dados, interrupção das operações e custos elevados com recuperação e resgate. A estimativa de danos financeiros para as vítimas varia, mas pode chegar a milhões de dólares.

Tipos de Proteção que poderiam ter sido aplicadas para evita-lo:

- **Atualizações Regulares:** Manter sistemas e software atualizados para corrigir vulnerabilidades conhecidas.
- **Backups:** Implementar e testar regularmente backups de dados para garantir a recuperação em caso de ataque.
- **Treinamento:** Treinar funcionários sobre práticas de segurança e reconhecimento de ataques de phishing (phishing são tentativas fraudulentas de obter informações confidenciais, como senhas e dados bancários, enganando vítimas por meio de mensagens falsas ou sites que imitam fontes confiáveis) que podem ser usados para inicializar o ransomware.

- **Fonte:** Coluna da The Record sobre BlackCat Ransomware

Ataque de Supply Chain: Kaseya VSA

Data do Ataque: O ataque foi descoberto em Julho de 2021.

Tipo de Ataque: Ataque de Supply Chain (Ransomware REvil).

Descrição do Ataque: O ataque ao Kaseya VSA foi um ataque à cadeia de suprimentos que afetou clientes do software de gerenciamento de TI da Kaseya. Os atacantes comprometeram uma atualização do software VSA, que permitiu a distribuição de ransomware para cerca de 1.500 organizações ao redor do mundo. O ransomware REvil, também conhecido como Sodinokibi, criptografa arquivos em sistemas infectados e exige resgate em criptomoedas. É notório por suas demandas de alto valor e suas táticas de extorsão.

Vulnerabilidades Exploradas:

- **CVE:** A vulnerabilidade explorada foi identificada como CVE-2021-30116.
- **Descrição:** CVE-2021-30116 é uma vulnerabilidade crítica na função de gerenciamento remoto do VSA da Kaseya, que permite a execução remota de código sem autenticação. **VSA** (**Virtual Server Agent**) é um software de gerenciamento de TI que facilita a administração remota de servidores e dispositivos, monitorando e automatizando tarefas em ambientes de rede complexos).

Impactos e/ou Prejuízos: O ataque causou interrupção significativa nos serviços das empresas afetadas, paralisando operações e resultando em grandes custos de recuperação e possíveis perdas de dados. Estimativas indicam que os danos podem ter sido na casa dos milhões de dólares.

Tipos de Proteção que poderiam ter sido aplicadas para evita-lo:

- **Segurança da Cadeia de Suprimentos:** Fortalecer a segurança ao longo da cadeia de suprimentos para garantir que atualizações e software de terceiros sejam auditados e monitorados.
- **Autenticação e Controle de Acesso:** Implementar controles de acesso rigorosos e autenticação multifator para proteger sistemas críticos.
- **Monitoramento de Segurança:** Estabelecer monitoramento contínuo e detecção de anomalias para identificar rapidamente qualquer comportamento suspeito ou invasão.

- **Fonte:** Coluna TechCrunch sobre o ataque Kaseya.