**1. Malware**

**1.1 Ransomware: Colonial Pipeline (7 de maio de 2021)**

Em 7 de maio de 2021, o grupo **DarkSide** lançou um ataque de ransomware contra a Colonial Pipeline, a maior operadora de oleodutos dos EUA, interrompendo totalmente suas operações por cerca de cinco dias. O incidente causou escassez localizada de gasolina, diesel e combustível de aviação, gerando filas em postos de abastecimento ao longo da Costa Leste e levando o governo da Virgínia a declarar estado de emergência. Este ataque demonstrou a vulnerabilidade de infraestruturas críticas a ransomwares e motivou discussões federais sobre fortalecimento de controles e resposta a incidentes de cibersegurança.

**1.2 Trojan: Emotet (Desmantelamento em janeiro de 2021)**

O **Emotet** é um trojan bancário que evoluiu para uma das botnets mais perigosas da última década. Em 27 de janeiro de 2021, uma operação coordenada internacional liderada pelo FBI e parceiros disruptou significativamente a infraestrutura do Emotet, removendo servidores de comando e controle e impedindo novas infecções. Apesar da desmobilização, o Emotet continuou ativo em janeiro de 2021, afetando aproximadamente 6% das organizações mundiais antes da ação das autoridades.

**2. Phishing**

**2.1 Ataque de Phishing: Twitter (15 de julho de 2020)**

Em 15 de julho de 2020, hackers aplicaram uma **campanha de spear-phishing** por telefone contra funcionários da Twitter, obtendo credenciais que lhes permitiram acessar ferramentas internas de administração. Com isso, comprometeram 69 contas de alto perfil (incluindo Barack Obama, Elon Musk e Apple) para veicular um golpe de bitcoin que gerou mais de US$ 120 000 em transações antes do sistema ser neutralizado. Três indivíduos foram presos em 31 de julho de 2020, enfrentando acusações que incluíram fraude eletrônica, lavagem de dinheiro e acesso não autorizado a computadores.

**3. Ataques Man-in-the-Middle (MitM)**

**3.1 Reverse Proxy Phishing contra Clientes Bancários (março de 2024)**

Em 27 de março de 2024, pesquisadores da Arkose Labs descreveram um **ataque de proxy reverso** em que criminosos implantam servidores intermediários para contornar mecanismos de MFA (autenticação multifator) e interceptar credenciais bancárias de clientes durante login em portais financeiros. Esse método, classificado como MitM, permite aos atacantes assumir sessões legítimas sem disparar alertas de segurança tradicionais. Tais ataques mostram como a engenharia social e ferramentas de interceptação de tráfego evoluíram para ameaçar tanto usuários domésticos quanto sistemas bancários corporativos.

**4. Ataques de Negação de Serviço (DoS/DDoS)**

**4.1 Recorde de DDoS na AWS (Q1 de 2020)**

No primeiro trimestre de 2020, a Amazon Web Services sofreu o maior ataque de DDoS já registrado, com pico de **2,3 Tbps** de tráfego malicioso, superando em 70% o recorde anterior de 2018 contra o GitHub. A AWS conseguiu mitigar a onda em fevereiro de 2020, demonstrando a eficácia de soluções de proteção em larga escala, mas evidenciando a necessidade contínua de estratégias zero-trust em ambientes de nuvem pública.

**5. Injeção de SQL**

**5.1 Vazamento de Dados no Gab (janeiro de 2021)**

Em janeiro de 2021, a plataforma **Gab** foi comprometida por uma vulnerabilidade de injeção de SQL que expôs mais de 70 GB de dados, incluindo mensagens privadas, senhas e informações de figuras públicas. O grupo hacktivista Distributed Denial of Secrets (DDoSecrets) adquiriu o banco de dados roubado e o disponibilizou para pesquisa jornalística e acadêmica, mas manteve o conteúdo sensível protegido. Outro exemplo é o caso da hospedeira Hetzner, que em 2020 sofreu vazamento de aproximadamente 40 000 registros de clientes devido a uma falha de SQL injection em seus sistemas de provisionamento.

**6. Zero-day Exploit**

**6.1 ProxyLogon no Microsoft Exchange Server (março de 2021)**

Em março de 2021, foi descoberta a cadeia de vulnerabilidades **ProxyLogon** (CVE-2021-26855 e CVE-2021-27065) em servidores Microsoft Exchange on-premises, permitindo execução remota de código e acesso administrativo sem autenticação prévia. O grupo estatal HAFNIUM explorou esses 0-days para implantar backdoors e ransomware antes da disponibilização de patches pela Microsoft. Em resposta, a empresa lançou atualizações de emergência e o CISA emitiu alertas urgentes para mitigação imediata.

**Fontes**

### Malware

**Ransomware (Colonial Pipeline, 7 Maio 2021):**

* CISA – Análise do DarkSide Ransomware:  
  <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>
* Reuters – Colonial Pipeline shutdown após ciberataque:  
  <https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/>

**Trojan (Emotet, desmantelamento em Jan 2021):**

ZDNet – FBI e parceiros derrubam botnet Emotet:  
<https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/>

### Phishing

* **Spear-phishing na Twitter (15 Jul 2020):**
  + Investigação do ataque à Twitter:  
    <https://g1.globo.com/economia/tecnologia/noticia/2020/07/31/twitter-diz-que-ataque-de-phishing-a-funcionarios-levou-a-invasao-de-contas.ghtml>

### Ataques Man-in-the-Middle (MitM)

* **Proxy reverso contra clientes bancários (27 Mar 2024):**
  + Como funciona o reverse-proxy phishing:  
    <https://www.cloudflare.com/pt-br/learning/cdn/glossary/reverse-proxy/>

### DoS/DDoS

* **DDoS recorde na AWS (Q1 2020):**
  + AWS Security Blog – Protegendo-se contra o maior ataque DDoS já registrado:  
    <https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/>

### Injeção de SQL

* **Vazamento de dados no Gab (Jan 2021):**
  + Detalhes do vazamento do Gab:  
    <https://translate.google.com/translate?u=https://en.wikipedia.org/wiki/Distributed_Denial_of_Secrets&hl=pt&sl=en&tl=pt&client=sge>

### Zero-day Exploit

* **ProxyLogon no Microsoft Exchange Server (Mar 2021):**
  + Microsoft Security Response Center – CVE-2021-26855:  
    <https://www.cyber.gc.ca/en/alerts-advisories/active-exploitation-microsoft-exchange-vulnerabilities>
  + CISA – Orientações de emergência para ProxyLogon:  
    <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a>