Relatório Técnico de Incidente Cibernético - PayFlex

Este relatório técnico detalha as etapas de um ataque cibernético sofrido pela empresa fictícia PayFlex, especializada em carteiras digitais e pagamento por aproximação (NFC). A análise é direcionada a uma equipe de segurança de TI júnior, apresentando vulnerabilidades exploradas, mecanismos de ocultação, ferramentas usadas pelos atacantes e recomendações de prevenção.

1. Etapas do Ataque

- Phishing: Envio de e-mail spoofed solicitando atualização de senha via bit.ly.
- Redirecionamento ao site falso replicando a intranet.
- Injeção de script JavaScript ofuscado para roubo de credenciais.
- Captura e exfiltração de credenciais em menos de 15 minutos.
- Uso de credenciais para acesso ao sistema de RH e movimentação lateral.
- Injeção de vírus modular nos servidores de banco de dados.
- Exfiltração de dados sensíveis (nomes, CPFs, cartões) e sabotagem de backups.
- DDoS massivo como distração no site principal.

2. Diagrama de Fluxo do Ataque

3. Vulnerabilidades Exploradas

- Falta de treinamento em identificação de phishing.
- Ausência de verificação de URL encurtada.
- Inexistência de autenticação multifator.
- Pouco monitoramento de comportamento de rede anômalo.

4. Ferramentas Possíveis dos Atacantes

- **LOIC/HOIC:** ferramentas de código-aberto que geram enormes volumes de tráfego (TCP, UDP ou HTTP) para sobrecarregar e derrubar servidores alvo.

- **Botnets**: redes de dispositivos infectados e controlados à distância, usadas para enviar em massa dados roubados sem levantar suspeitas.

- **Scripts personalizados em Node.js ou Python para C2:** pequenos programas instalados em máquinas comprometidas que mantêm um canal oculto com o servidor do invasor, permitindo envio de comandos e extração de informações.

5. Medidas de Prevenção

- **Proofpoint**: identifica e bloqueia e-mails de phishing antes de chegarem à caixa de entrada, usando machine learning e reputação de remetente para filtrar ameaças em tempo real.
- **Cofense**: combina inteligência humana e análise automatizada de URLs e anexos em sandbox para detectar e neutralizar campanhas de phishing que escapam de filtros tradicionais .
- **Mimecast**: faz varredura em tempo real de links e anexos, isolando e convertendo conteúdo suspeito

em ambiente seguro antes de entregar o e-mail ao usuário.

- **MFA (Autenticação Multifator**): exige dois ou mais fatores (por exemplo, senha + código SMS ou app de autenticação), de modo que mesmo que a senha seja comprometida, o acesso é barrado sem o segundo fator
- **SIEM (Splunk, ELK):** agrega, normaliza e correlaciona logs e eventos de diversas fontes em tempo real, facilitando a detecção de padrões anômalos e gerações de alertas de segurança automatizados.
- **EDR (CrowdStrike):** monitora continuamente endpoints, detecta comportamentos maliciosos com análise em nuvem e permite resposta imediata a incidentes, isolando cargas maliciosas e facilitando a investigação.
- **Single Sign-On com SAML/OAuth:**
    - SAML permite ao usuário autenticar-se uma única vez em um provedor de identidade e acessar múltiplas aplicações sem nova verificação, centralizando o controle de acesso.
    - OAuth entrega tokens de autorização entre serviços, permitindo acesso delegado sem expor credenciais, usado frequentemente em fluxos de SSO e APIs seguras.

Referências:

1. Symantec. What Is Phishing? https://www.symantec.com/security-center
2. MITRE ATT&CK. Phishing (T1566). https://attack.mitre.org/techniques/T1566
3. Stallings, W. Computer Security: Principles and Practice. Pearson, 2018.
4. Anderson, R. Security Engineering. Wiley, 2020.
5. Kaspersky. Anatomy of a Cyber Attack. https://www.kaspersky.com/resource-center
6. OWASP. Top 10 Phishing Prevention. https://owasp.org
7. IEEE Communications. DDoS Attack Mitigation Techniques.
8. ACM. Command and Control of Botnets.