Recomendações para PREVENÇÃO dos Órgãos
05/11/2020 – 16:25

Ambiente de INTERNET

1. Habilitar assinaturas de Ransomware no IPS;
2. Ativar assinaturas de proteção para as CVEs: CVE-2020-1472;
3. Bloquear Regras de acesso ANY para HTTP e HTTPS para internet;
4. Restringir acesso WEB a destinos não especificados e com reputação comprometida, analisando os endereços IP ou domínios em bases online;
5. Identificar e bloquear (caso necessário) Endereços IP que estejam com volume de tráfego suspeito para a Internet;

Ambiente de MONITORAÇÃO

6. Criação de “Arquivos Canário”, com checksum monitorado por ferramenta de infraestrutura (Arquivos que seriam alterados apenas por um ransomware, mas nunca por um administrador ou script de sistema).
7. Monitorar assinaturas de IPS e logs (SIEM) para eventos suspeitos de tentativas de escalação de privilégio, como exemplo da CVE 2020-1472 e conexões TCP Netlogon suspeitas com origem em redes externas.

Ambiente de INTRANET

8. Garantir atualização dos endpoints e ativação das funcionalidades avançadas
9. Bloqueios imediatos de arquivos com esta assinatura:

    MD5 (svc-new/svc-new) = 4bb2f87100fca40bfbb102e48ef43e65
    MD5 (notepad.exe) = 80cfb7904e934182d512daa4fe0abbfb
    SHA1 (notepad.exe) = 9df15f471083698b818575c381e49c914dee69de
    SHA1 (svc-new/svc-new) = 3bf79cc3ed82edd6bfe1950b7612a20853e28b09

10. Verificar com o fabricante da solução de endpoint protection funcionalidades que podem ser habilitadas para proporcionar ou aprimorar a proteção contra Ransomware;
11. Ativar assinaturas de proteção para as CVEs: CVE-2020-1472, CVE-2019-5544 e CVE-2020-3992;
12. Habitar, caso disponível, a funcionalidade de firewall e IPS de endpoint para identificar situações de exploração de vulnerabilidades ou ações maliciosas de forma lateral, no ambiente de rede local;
13. Verificar na solução de endpoint protection os registros de riscos de segurança e malwares identificados para tentar identificar um possível vetor de ataque, e se prevenir de futuras ações;
14. Verificar se os atualizações do sistema operacional e aplicações dos servidores e estações de trabalho foram realizadas;
15. Caso possível, desabilitar temporariamente mapeamentos de rede para tentar conter a propagação das ações de um malware;
16. Solicitar aos usuários realizar a troca de senha fazendo uso de uma política de senha previamente definida;
17. Bloquear acessos à internet sem Filtro de Conteúdo (servidores e estações de trabalho) - (Curto prazo)
18. Habilitar filtro de reputação no FCW para toda Rede
19. Revisão dos acessos via Netbios e internet em todos os Firewalls
20. Levantar e propor o bloqueio dos acessos de servidores à internet que não estejam usando filtro de conteúdo
21. Cancelar, temporariamente os poderes dos Administradores do AD (Active Directory)
22. Verificar usuários “logados” no AD, efetuar o sign out destes usuários.
23. Lançar informes aos usuários que acessam VPN com estações particulares para atualizarem antivírus
24. Mudar a permissão dos compartilhamento de rede para SÓ LEITURA , (não vai parar o serviço e evita perda de dados, e disseminação)

Ambiente de SERVIDORES E BACKUP

25. Caso os servidores possuam usuários locais configurados, desabilitá-los ou alterar a senha utilizadas por eles
26. Desabilitar o CIM Server no VMware ESXi (76372)
    https://www.vmware.com/security/advisories/VMSA-2020-0023.html
    https://kb.vmware.com/s/article/76372 (How to Disable/Enable CIM Server on VMware ESXi)

OUTRAS AÇÕES

27. Revisar acessos privilegiados em todas as consoles de gerência (Firewall, IPS, Anti-DDoS, Filtro de Conteúdo, Virtualizadores e ativos de rede)
28. Verificar e apagar contas que não são utilizadas nos ativos

CVEs e Referências possivelmente relacionados:

Active Directory:
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

Correção:
https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

VMWARE:
https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5544

Solução de Contorno:
https://kb.vmware.com/s/article/76372

Artigo sobre uso de “arquivos canário”:
https://www.researchgate.net/publication/240496151_CANARY_FILES_GENERATING_FAKE_FILES_TO_DETECT_CRITICAL_DATA_LOSS_FROM_COMPLEX_COMPUTER_NETWORKS)

Monitoração de “arquivos canário” com ferramenta livre Zabbix: chave de agente “vfs.file.cksum”:
https://www.zabbix.com/documentation/current/manual/config/items/itemtypes/zabbix_agent

Bases de reputação IP para referência e consulta:
https://auth0.com/
https://www.abuseipdb.com/
https://www.virustotal.com/gui/

Em breve serão liberadas orientações de contorno e pós-ataque.