Recomendações para PREVENÇÃO dos Órgãos v.4

07/11/2020 – 13:30h

GERAL

Notificação de ocorrência de incidentes pelos órgãos do Governo Federal

O ponto central para notificações de incidentes de segurança é o **CTIR Gov pelo celular +55 61 9995-7859 ou pelo e-mail ctir@ctir.gov.br**, com assunto: “nome do órgão” e o “**tipo do incidente: Ransonware**”.

Mais informações em https://www.ctir.gov.br/contato/

AÇÕES DE PREVENÇÃO

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;
6. **(CRÍTICA)** Fortalecer a inspeção de emails nas ferramentas de relay e antispam. Neste momento é importante que vetores de ataques como phishings e malwares sejam combatidos com campanhas de conscientização (Referência: https://cartilha.cert.br/golpes/). Sistemas de reputação também podem ser utilizados em alinhamento com as ferramentas disponíveis.
7. IPs categorizados como maliciosos na última hora:
   - O SERPRO disponibilizará a sua base de Reputation, atualizada a cada 12 horas.

54.36.148.255	185.191.171.23	125.95.20.92
189.6.246.8	185.26.92.74	23.97.242.129
54.36.149.92	185.25.35.9	119.60.5.37
89.248.171.134	54.36.148.86	94.200.76.222
54.36.148.44	176.31.3.253	103.95.199.151
54.36.148.74	54.36.148.35	23.96.117.144
185.191.171.3	54.36.148.8	54.36.148.49
185.191.171.20	54.36.148.23	74.125.151.31
201.47.114.144	54.36.148.127	63.143.42.242
54.36.148.79	54.36.148.57	54.36.148.40
45.143.221.154	23.96.117.179	54.36.148.190
46.229.173.67	37.59.222.68	54.36.148.113
54.36.148.106	165.22.42.137	54.36.148.78

8. **(CRÍTICA)** O SERPRO disponibilizou uma lista de reputação dos IPs. Essa lista foi criada pelo SOC e contém endereços maliciosos que tentaram atacar sites de Governo. A lista é atualizada em Tempo Real e pode ser acessada através do endereço: http://reputation.serpro.gov.br
9. **(CRÍTICA)** Aplicar imediatamente correções das seguintes vulnerabilidades:
   - CVE-2020-1472: permite escalação de privilégios quando um atacante consegue estabelecer uma conexão com o controlador de domínio usando NRPC (Netlogon Remote Protocol);

- CVE-2018-13379: afeta dispositivos do Fabricante Fortinet. Esta vulnerabilidade é considerada crítica e permite o download de informações e configurações dos dispositivos.

Ambiente de MONITORAÇÃO

1. 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).
2. 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.
3. **(CRÍTICA)** Sugestão de regra Yara para encontrar variantes do malware. Os órgãos podem usar estes padrões de string como parâmetros de inspeção em seus controles:

```
rule RansomwareESXi
{
    strings:
        $string1 = "ransomware.c" nocase
        $string2 = "cryptor.c" nocase
        $string3 = "logic.c" nocase
        $string4 = "enum_files.c" nocase
        $string5 = "aes.c" nocase
        $string6 = "rsa.c" nocase
        $string7 = "crtstuff.c" nocase
        $string8 = "mbedtls" nocase
    condition:
        all of them
}

rule BackdoorNotepad
{
    strings:
        $string1 = "c:\\windows\\INF\\config.dat" nocase
    condition:
        $string1
}
```

4. **(CRÍTICA)** Monitorar tentativas de acesso à porta TCP/UDP 427 com destino a administração de virtualização que não estejam aderentes às políticas de acesso à Gerência do Ambiente virtualizado;
5. Monitorar bloqueio de contas no Active Directory ou LDAP por tentativa de login falhas (account lockout).
6. Criar regra de monitoração de força bruta de autenticação em AD e autenticação Local. X tentativas falhas de login dentro intervalo Y seg.
7. **(CRÍTICA)** Monitorar tentativas de acesso por meio de ataque *pass-the-hash* (autenticação sem uso de senha):
    - userName != “ANONYMOUS LOGON”
    - Microsoft-Windows-Security-Auditing = 4624
    - Microsoft-Windows-Security-Auditing = 4625
    - LogonProcessName = 'NtLmSsp'

Ambiente de INTRANET

1. Garantir atualização dos endpoints e ativação das funcionalidades avançadas
2. **(CRÍTICA)** Bloqueios imediatos de arquivos com esta assinatura:

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

3. **(CRÍTICA)** Verificar com o fabricante da solução de *endpoint protection* funcionalidades que possam ser habilitadas para proporcionar ou aprimorar a proteção contra Ransomware;
4. **(CRÍTICA)** Ativar assinaturas de proteção para as CVEs: CVE-2020-1472, CVE-2019-5544 e CVE-2020-3992;
5. 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;
6. 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;
7. Verificar se os atualizações do sistema operacional e aplicações dos servidores e estações de trabalho foram realizadas;
8. Caso possível, desabilitar temporariamente mapeamentos de rede para tentar conter a propagação das ações de um malware;
9. Solicitar aos usuários realizar a troca de senha fazendo uso de uma política de senha previamente definida;
10. Bloquear acessos à internet sem Filtro de Conteúdo (servidores e estações de trabalho) - (Curto prazo)
11. Habilitar filtro de reputação no FCW para toda Rede
12. **(CRÍTICA)** Revisão dos acessos via Netbios e internet em todos os Firewalls
13. Levantar e propor o bloqueio dos acessos de servidores à internet que não estejam usando filtro de conteúdo
14. Cancelar, temporariamente os poderes dos Administradores do AD (Active Directory)
15. Verificar usuários “logados” no AD, efetuar o sign out destes usuários.
16. Lançar informes aos usuários que acessam VPN com estações particulares para atualizarem antivírus
17. Mudar a permissão dos compartilhamento de rede para SÓ LEITURA , (não vai parar o serviço e evita perda de dados, e disseminação)
18. Reparamos que o malware (que tivemos acesso) usa a mesma API de criptografia que o antigo WannaCry. Ele pode ser bloqueado com medidas nos principais antivírus corporativos como os exemplos abaixo:
    - Symantec - No SEP existe uma política de controle de aplicativo que bloqueia a criação de arquivos com extensão crypt criados pelo WannaCry.
    - TREND - Na Trend possui o recurso de controle de aplicativo semelhante ao do SEP (Symantec).
19. Ainda sobre os Antivírus, habilitar módulos de Machine Learning e de análise de comportamento.

Ambiente de SERVIDORES E BACKUP

1. **(CRÍTICA)** Desabilitar ou alterar a senha de usuários locais em servidores, caso existam;
2. **(CRÍTICA)** 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)
3. Possibilidade de habilitar 2FA (2º fator de autenticação) para autenticação em ativos críticos. Para os órgãos que possuem cofres de senhas, é possível que esta opção esteja disponível.
4. **(CRÍTICA)** Aplicar privilégios mínimos no Serviço de Diretório (Active Directory, LDAP) e desabilitar conta Guest (convidado):
5. **(CRÍTICA)** Separar as contas de administração e administração de Domain (Domain Admin);
6. **(CRÍTICA)** Criar GPO para efetuar o logoff de usuários, por inatividade no AD em vez de desconectá-los (*disconnect*);
7. **(CRÍTICA)** Criar auditoria de contas administrativas de Domínio.

8. **(CRÍTICA)** Revisar as políticas de backups dos principais sistemas e base de dados, inclusive testar uma amostragem de backup e garantir que a restauração está em conformidade.

OUTRAS AÇÕES

1. Revisar acessos privilegiados em todas as consoles de gerência (Firewall, IPS, Anti-DDoS, Filtro de Conteúdo, Virtualizadores e ativos de rede)
2. Verificar e apagar contas que não são utilizadas nos ativos.
3. Órgãos com saída pela INFOVIA poderão solicitar adição de portas para facilitar a monitoração exclusiva de INTERNET pelos seguintes canais: 0800-978-2337, css.serpro@serpro.gov.br ou https://cssinter.serpro.gov.br/SCCDPortalWEB/pages/dynamicPortal.jsf?ITEMNUM=2221

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/

Próximo informe será enviado em 07/11/2020 as 18hs

SERPRO
Assinado Digitalmente por:
LUIS FELIPE SALIN MONTEIRO
CPF/CNPJ: 77205995000
Assinado em: 07/11/2020
Sua autenticidade pode ser confirmada no endereço: <http://www.serpro.gov.br/assinador-digital>