7 de novembro de 2020

Alerta nº 03/2020
Nova campanha de ataques de Ransomware

Atualização: 7 de novembro de 2020

Por favor, entre em contato com o **CTIR Gov**, caso tenha alguma dúvida relacionada a esta publicação em sua Coordenação ou pelos contatos abaixo.

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-3477

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

Obs.: Os alertas, aqui disponibilizados, têm o objetivo de fornecer informações oportunas sobre problemas, vulnerabilidades e explorações de segurança atuais.

Dentro das trocas de informações entre CSIRTs, esta publicação está marcada como **TLP:WHITE***. Sujeito às regras padrão de direitos autorais, as informações do TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**).

1. Descrição do Problema

Com base nas estatísticas de eventos ocorridos no espaço cibernético, bem como nos diversos relatos que tem sido feitos por colaboradores, o CTIR Gov recomenda a divulgação, a todos os órgãos de governo e entidades vinculadas, do presente Alerta, sobre uma campanha nacional de ataques de *Ransomware* direcionado a sistemas VMware e Windows, que caracteriza-se por ações maliciosas para criptografar arquivos ou bancos de dados de instituições, a fim de exigir resgate em troca da descriptografia dos arquivos cifrados.

2. Impacto

Este ataque, sendo efetivo, impede o acesso aos dados em claro, os quais são criptografados e permanecem inacessíveis.

3. Dispositivos Afetados

Windows Server 2008 R2 (todas as versões)
Windows Server 2008 R2 Service Pack 1 (todas as versões)
Windows Server 2012 (todas as versões)
Windows Server 2012 R2 (todas as versões)
Windows Server 2016 (todas as versões)
Windows Server 2019 (todas as versões)
Windows Server versão 1809 Standard
Windows Server versão 1809 Datacenter
Windows Server versão 1903
Windows Server versão 1909
Windows Server versão 2004
VMWare ESXi 6.0
VMWare ESXi 6.5
VMWare ESXi 6.7
VMWare ESXi 7.0
VMware Cloud Foundation ESXi 3.X
VMware Cloud Foundation ESXi 4.X

4. Recomendações

As seguintes práticas são recomendadas para mitigar o risco a essa ameaça:

Recomendações Gerais

1. Não clicar em links de e-mails suspeitos;
2. Evitar a visita a *websites* que oferecem downloads de programas pirateados ou suspeitos;
3. Mesmo não sendo comprovada a existência de vulnerabilidades, manter os sistemas atualizados com a versão mais recente ou aplicar os *patches* conforme orientação do fabricante;
4. Isolar a máquina da rede ao primeiro sinal de infecção por *Malware*;
5. Garantir o *backup* atualizado dos arquivos locais e dos armazenados em Servidores de Arquivos;
6. Rever a política de privilégios administrativos nas máquinas clientes, a fim de restringir a instalação/execução de binários e ou executáveis desconhecidos;
7. Realizar campanhas internas, alertando os usuários a não clicar em *links* ou baixar arquivos de e-mails suspeitos ou não reconhecidos como de origem esperada.
8. Backup:
   a) Que haja uma política de backup (cópia de segurança) definida;
   b) Revisar as políticas de *backup* dos principais sistemas, executando testes em amostras para garantia de restauração;
   c) Armazenar as cópias de segurança em local protegido, em rede exclusiva e isolada dos demais ativos, com acesso restrito e controlado por Firewall, com o devido registro de conexões;

d) Se possível, armazenar os *backups* em mais de um local físico, separados geograficamente, de preferência em cofres à prova de furto, incêndio e alagamento, com acesso controlado.

Ambiente de INTERNET (*)

1. Habilitar assinaturas de *Ransomware* no IPS;
2. Ativar assinaturas de proteção para a CVE: 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 endereços IP que estejam com volume de tráfego suspeito para a Internet;
6. Fortalecer a inspeção de *emails* nas ferramentas de *relay* e *antispam*, usando-as em conjunto com sistemas de análise de reputação, configurando os filtros para o nível máximo de proteção.

Indicadores de Comprometimento (IoC)

Bloquear arquivos com as seguintes assinaturas:

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

IPs definidos como maliciosos

O SERPRO disponibilizou uma lista de reputação dos IPs em tempo real no link abaixo:
https://s3.i02.estaleiro.serpro.gov.br/blocklist/blocklist.txt

Ambiente de MONITORAÇÃO (*)

1. Utilizar ferramentas de monitoração de eventos para controle de arquivos de sistema ou verificação de integridade, como Inotify ou Iwatch no Debian;
2. Atualizar assinaturas de IPS e utilizar sistemas de gerenciamento de eventos e informações de segurança (SIEM) para correlacionamento de logs;
3. 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. Monitorar tentativas de acesso à porta 427 com destino à administração de virtualização;
5. Monitorar bloqueio de contas no Active Directory ou LDAP por tentativas falhas de login (account lockout).
6. Monitorar tentativas de autenticação por força bruta em AD e local;
7. Monitorar tentativas de acesso por meio de *pass-the-hash*

- 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. Verificar com o fabricante da solução de *endpoint protection* as funcionalidades que podem ser habilitadas para proporcionar ou aprimorar a proteção contra *Ransomware*;
3. Ativar assinaturas de proteção para as CVEs: CVE-2020-1472, CVE-2019-5544 e CVE-2020-3992;
4. 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;
5. 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;
6. Verificar se as atualizações do sistema operacional e aplicações dos servidores e estações de trabalho foram realizadas;
7. Caso possível, desabilitar temporariamente mapeamentos de rede para tentar conter a propagação das ações de um *malware*;
8. Solicitar aos usuários a troca de senha fazendo uso de uma política de senha previamente definida;
9. Bloquear acessos à internet sem Filtro de Conteúdo;
10. Habilitar filtro de reputação no FCW para toda a rede;
11. Não expor o protocolo SMB (Server Message Block) das máquinas Windows na Internet, filtrando todo o tráfego NetBIOS (portas 137, 139 e 445 TCP, além de 137 e 138 UDP);
12. Levantar e propor o bloqueio dos acessos de servidores à internet que não estejam usando filtro de conteúdo;
13. Revogar, temporariamente, os poderes dos Administradores do AD (Active Directory);
14. Verificar se há usuários administrativos autenticados no AD e efetuar o *logout* destes;
15. Estabelecer a necessidade de utilização de antivírus nas máquinas de usuários que acessam a rede interna da organização via VPN;
16. Em casos de suspeita de infecção na rede, mudar a permissão de compartilhamentos de arquivos para somente-leitura, a fim de evitar perda de dados e disseminação de artefatos maliciosos;
17. Configurar os sistemas de arquivos e antivírus para bloquear a criação de arquivos com extensão ".crypt".
18. Com relação a Antivírus, ainda, habilitar módulos de *Machine Learning* e de análise de comportamento;

Ambiente de SERVIDORES (*)

1. Caso os servidores possuam usuários locais configurados, desabilitá-los ou alterar as senhas utilizadas por eles;
2. 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. Habilitar 2FA (2º fator de autenticação) para autenticação em ativos críticos, tais como bancos de senhas;
4. Aplicar privilégios mínimos no AD e desabilitar a conta Guest (convidado);
5. Separar as contas de administração e administração de Domínio (Domain Admin);
6. Criar GPO para efetuar o *logoff* de usuários por inatividade no AD em vez de *disconnect*;
7. Criar auditoria de contas administrativas de Domínio.

CORREÇÕES DISPONÍVEIS

CVE-2018-13379
Aplicação imediata de correção dessa vulnerabilidade, que afeta dispositivos do Fabricante Fortinet.
Esta vulnerabilidade é considerada crítica e permite o download de informações e configurações dos dispositivos. Sua exploração ocorre quando o módulo de acesso remoto está ativado.

CVE-2020-1472
Aplicar a atualização KB4571702 de 11 de agosto de 2020.

CVE-2019-5544
Executar os *patches* de correção disponibilizados pela VMWare:
Para versões ESXi 6.7, aplicar o patch ESXi670-201912001.
Para versões ESXi 6.5, aplicar o patch ESXi650-201912001.
Para versões ESXi 6.5, aplicar o patch ESXi600-201912001.
Para versões Horizon DaaS 8.x, atualizar para a versão 9.0

CVE-2020-3992
Executar os *patches* de correção disponibilizados pela VMWare:
Para versões ESXi 7.0, aplicar o patch ESXi670-ESXi70U1a-17119627.
Para versões ESXi 6.7, aplicar o patch ESXi670-202011301-SG.
Para versões ESXi 6.5, aplicar o patch ESXi650-202011401-SG.
Para versões ESXi 6.5, aplicar o patch ESXi600-201903001.

Para versões VMware Cloud Foundation ESXi 3.X e 4.X, não há *patches* de correção até o momento.
Como solução de contorno, é necessário desabilitar o serviço OpenSLP através da interface de comando [https://nvd.nist.gov/vuln/detail/CVE-2020-3992].

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 credenciais ou 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

5. Referências

- Alerta CAIS RNP
- https://www.rnp.br/arquivos/documents/CAIS_Alerta_Multiplas_vulnerabilidades_cr%c3%adticas_em_plataformas.txt?RP7ZfG4CJoaecXaf6nsVXeWUXr_ovKuq=

- Adaptado das Recomendações confeccionadas pelo SERPRO (*) Recomendações para PREVENÇÃO dos Órgãos v.3 (06/11/2020, 18h35 - em PDF)

- https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-backup/

- Lista de reputação IPs confeccionada pelo SERPRO
- https://s3.i02.estaleiro.serpro.gov.br/blocklist/blocklist.txt

- Microsoft Windows Elevação de privilégio (CVE-2020-1472)
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

- VMWare Execução remota de código (CVE-2020-3992)
- https://www.vmware.com/security/advisories/VMSA-2020-0023.html

- Execução remota de código (CVE-2019-5544)
- https://www.vmware.com/security/advisories/VMSA-2019-0022.html

- RansomEXX:
- https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

- Active Directory:
- https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material
- 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/

Coordenação-Geral do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CGCTIR)

Informações: cgtir@presidencia.gov.br
Notificação de incidentes: ctir@ctir.gov.br