8 de novembro de 2020

Alerta Especial nº 06/2020
Nova campanha de ataques de Ransomware

Atualização: 8 de novembro de 2020 - 20:00

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) 9995-7859

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

IMPORTANTE:

- Este alerta foi confeccionado pelos órgãos em destaque no cabeçalho através de em um trabalho em conjunto e que tem o objetivo de fornecer informações oportunas sobre ações preventivas relativas à campanha massiva de ataques *Ransomware* que está ocorrendo.
- O arquivo contém todas as recomendações até a emissão deste alerta. As atualizações desde a última versão estão assinaladas na cor vermelha.
- Sempre obtenha este arquivo da fonte oficial, a partir do site https://www.ctir.gov.br
- Para garantir a integridade deste material, verifique a validade da assinatura digital do Secretário de Governo Digital.

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:

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. **(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
8. **(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 estas assinaturas:
   - 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 as 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 compartilhamentos 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.

EM CASO DE ALTERAÇÕES DO ARQUIVO DE TESTE "ArquivoCanário"

1. Se o arquivo canário foi criptografado (possui uma extensão não conhecida e está indisponível para acesso), característica de um ataque ransomware, desconecte o servidor da rede IMEDIATAMENTE por meio da plataforma de virtualização no caso de máquinas virtuais ou desconectando-o fisicamente da rede no caso de máquinas físicas. Em nenhuma hipótese o servidor deve ser desligado para que as evidências possam ser mantidas e, com isso, auxiliar no processo de investigação.
2. Comunique à ETIR do seu órgão sobre o ocorrido enviando todas as evidências possíveis, e comunique ao CTIR.Gov.
3. Garanta que o backup da máquina e dos logs referentes aos últimos 7 dias esteja disponível e que não seja expirado.
4. Caso trate-se de uma máquina virtual, crie um clone da máquina afetada, sem reconectar a máquina original nem o clone à rede, e disponibilize o arquivo da máquina clone para acesso à equipe da ETIR do seu órgão.

5. De posse do clone do servidor a ETIR deverá iniciar a investigação do ambiente, analisando logs de sistema operacional, do AD/LDAP e fluxos de rede, visando identificar o horário de início do processo de criptografia, o arquivo de ransomware envolvido, de que forma o arquivo foi transferido para o servidor, a origem do ataque e as vulnerabilidades exploradas. Caso seja necessário, os fornecedores das soluções deverão ser acionados para apoiar nas investigações.
6. Atividades adicionais dependentes das evidências encontradas:
7. Antes de iniciar o processo de recuperação do backup do servidor, é importante tratar e corrigir as vulnerabilidades que permitiram ao atacante comprometer o ambiente.
    - **Identificadas evidências de comprometimento de credenciais**
        i. Caso sejam identificadas evidências de comprometimento de credenciais, o órgão deverá providenciar a troca imediata das senhas das credenciais envolvidas.
        ii. O órgão deverá avaliar também a possibilidade de adotar um duplo fator de autenticação em suas soluções mais críticas.
    - **Identificadas evidências de exploração de vulnerabilidades**
        i. Caso sejam encontradas vulnerabilidades exploradas durante o ataque, o órgão deverá providenciar a aplicação dos patches necessários acionando os fornecedores caso seja preciso.
    - **Identificadas evidências de endereços de origem dos ataques**
        i. Caso sejam identificados os endereços IP de origem dos ataques, tais IP`s deverão ser bloqueados nas ferramentas de proteção de perímetro, tais como Firewalls, IPS, WAF, a fim de impedir novas tentativas de invasão da mesma origem.
8. Após a identificação dos vetores de ataque e vulnerabilidades exploradas, inicie a recuperação do servidor a partir do backup, certificando-se de aplicar todas as correções e patches necessários antes de disponibilizá-lo novamente em produção.

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

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.

5. 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].

6. 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 pela Secretaria de Governo Digital SGD - 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
  - http://reputation.serpro.gov.br/

- Microsoft Windows Elevação de privilégio (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/

7. Próximo alerta

- Previsto para 09/11/2020 as 16hs

8. Assinaturas

SERPRO
Assinado Digitalmente por:
LUIS FELIPE SALIN MONTEIRO
CPF/CNPJ: 77205995000
Assinado em: 08/11/2020
Sua autenticidade pode ser confirmada no endereço: <http://www.serpro.gov.br/assinador-digital>

Secretaria de Governo Digital
Ministério da Economia

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

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