Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 004/2017 –Cogetic/VPGDI

Em 25 de outubro de 2017

Para: Gestores de TI das unidades da Fiocruz

Assunto: Ransomware Bad Rabbit

Prezados Gestores de TI da Fiocruz, segue alerta de segurança sobre Ransomware Bad Rabbit.

Descrição do problema

No dia 24 de outubro 2017 foi identificado um novo ataque propagado a partir da Rússia e Ucrânia de um novo *Ransomware* conhecido pelo nome *Bad Rabbit*. Apesar do potencial ofensivo ser menor que o *WannaCry* e *Petya*, faz-se necessário atenção ao ataque, tendo em vista os impactos esperados no caso de concretização.

Vetor do ataque

O ataque utiliza como vetor uma falsa atualização do Adobe Flash.

Dinâmica do ataque

O agente malicioso *Bad Rabbit Ransomware* utiliza como ferramenta o *DiskCryptor* para criptografia dos arquivos, *wordlists* (Mimikatz e Wmi) para obtenção de senhas fracas e SMB v1 para movimentação lateral, além de técnicas de evasão de *sandbox*.

Compartilhamento de redes visados para o ataque: admin / atsvc / browser / eventlog / lsarpc / netlogon / ntsvcs / spoolss / samr / srvsvc / scerpc / svcctl/ wkssvc;

Arquivos relacionados ao ataque e conhecidos até o momento:

- infpub.dat - 79116fe99f2b421c52ef64097f0f39b815b20907
- Win32/Diskcoder.D – Diskcoder
- dispci.exe - afeee8b4acff87bc469a6f0364a81ae5d60a2add

- Lockscreen - Win32/Diskcoder.D
- Mimikatz (32 bits) - 413eba3973a15c1a6429d9f170f3e8287f98c21c
- Win32/RiskWare.Mimikatz.X
- mimikatz (64 bits) - 16605a4a29a101208457c47ebfde788487be788d
- Win64/Riskware.Mimikatz.X
- install_flash_player.exe - fbbdc39af1139aebba4da004475e8839

Recomendações para mitigação do problema

- Manter ativada a função antimalware das soluções de Firewall/UTM/NGFW;
- Impedir o download de arquivos executáveis, monitorando inclusive o tráfego criptografado;
- Garantir que o filtro web esteja bloqueando sites categorizados como maliciosos;
- Revisar regras em serviços *antispam* para evitar a entrega de *phishings*;
- Verificar se os hosts possuem antivírus instalado e atualizado;
- Limitar a execução dos arquivos c:\windows\infpub.dat e c:\windows\cscc.dat;
- Adotar o uso de senhas fortes;
- Desativar o serviço SMB v1;
- Manter a política do menor privilégio na concessão de acessos;
- Realizar o monitoramento contínuo do ambiente;
- Isolar do restante da rede qualquer equipamento com comportamento suspeito;
- Bloquear acesso aos domínios http://1dnscontrol.com/flash_install.php e http://caforssztxqzf2nm.onion;

Referências

https://www.us-cert.gov/ncas/current-activity/2017/10/24/Multiple-Ransomware-Infections-Reported

https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html

https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

http://www.bbc.com/news/technology-41740768

https://realprotect.net/blog/notificacao-de-seguranca-medidas-de-prevencao-ransomware-bad-rabbit/?utm_campaign=notificacao_ransomware_bad_rabbit_final&utm_medium=email&utm_source=RD+Station

http://pages.checkpoint.com/bad-rabbit-ransomware-attack.html?utm_source=home%20hero&utm_medium=cp%20website&utm_campaign=CM_WR_17Q4_WW_RR%20Bad%20Rabbit%20Ransomware%20Attack

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações