Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 07/2017 – Ataques de Ransomware *Bad Rabbit*

1. Descrição do Problema

Recebemos relatórios de infecções de *ransomware*, conhecidos como *Bad Rabbit*, em alguns países. Aparentando ser variante de *Petya*, *Bad Rabbit* é um *software* malicioso *ransomware* que infecta um computador e restringe o acesso do usuário à máquina infectada até que um resgate seja pago para desbloqueá-lo.

Sempre desencorajamos o pagamento do resgate, pois não garante a restauração do acesso. O uso de *software* sem as atualizações de segurança e sem suporte aumenta o risco de proliferação de ameaças, como ataques de *ransomware* à segurança da informação.

O CTIR Gov RECOMENDA a revisão de seus alertas **nº 02/2016 – Ataques de *Ransomware* através de campanhas de *Phishing*, nº 02/2017 – Ataques de *Ransomware Wanna Decryptor*, e nº 04/2017 – Ataques de *Ransomware Petrwrap/Petya***, disponíveis em www.ctir.gov.br, e que descrevem os recentes eventos de *ransomware*.

Notifique os incidentes do *Ransomware* no endereço ctir@ctir.gov.br. O CTIR Gov fornecerá informações atualizadas à medida que elas se tornem disponíveis.

1.1 O que é um Ransomware?

Pode ser entendido como um código malicioso que infecta dispositivos computacionais com o objetivo de sequestrar, capturar ou limitar o acesso aos dados ou informações de um sistema, geralmente através da utilização de algoritimos de encriptação (*crypto-ransoware*), para fins de extorsão.

Para obtenção da chave de decriptação, geralmente é exigido o pagamento (*ransom*) através de métodos online, tipo "*Bitcoins*".

2. Métodos de Ataques

Com base em análises realizadas, o *Bad Rabbit* se espalha para outros computadores na rede, tirando cópias de si mesmo na rede usando seu nome original e executando as cópias descartadas usando o *Windows Management Instrumentation* (WMI) e o *Service Control Manager Remote Protocol*. Quando o protocolo remoto do *Service Control Manage*r é usado, ele usa ataques de força bruta para levantamento das credenciais.

Entre as ferramentas *Bad Rabbit* incorporadas, se encontra o utilitário de código aberto *Mimikatz*, para a extração de credenciais. Também existem evidências dele usando o *DiskCryptor*, uma ferramenta legítima de criptografia de disco, para criptografar os sistemas de destino.

É importante notar que *Bad Rabbit* não explora quaisquer vulnerabilidades, ao contrário de *Petya* que usou o *EternalBlue* como parte de sua rotina.

3. Sugestões para Mitigação do Problema

- Mesmo não sendo comprovado o uso de vulnerabilidades, até o momento, mantenha seus sistemas atualizados para a versão mais recente ou aplique os *patch* conforme orientação do fabricante.
- Isolar a máquina da rede, ao primeiro sinal de infecção por *malware*;
- Verificar o tráfego de máquinas internas para domínios não usuais ou suspeitos;
- Monitorar as conexões internas e não usuais entre máquinas da rede, a fim de evitar o movimento lateral de propagação do *malware*;
- Garantir o *backup* atualizado dos arquivos locais e dos Armazenados em Servidores de Arquivos;
- Manter o antivírus, aplicação de "*Patchs*" de segurança e a "*blacklist*" (filtro "*antispam*") de e-mail atualizados;
- Rever a política de privilégios administrativos nas máquinas clientes, a fim de restringir a instalação /execução de binários e ou executáveis desconhecidos; e
- Por fim, realizar campanhas internas, alertando os usuários a não clicar em links ou baixar arquivos de e-mail suspeitos ou não reconhecidos como de origem esperada.

4. Referências

- http://dsic.planalto.gov.br/legislacao/RequisitosMnimosSIparaAPF.pdf/view
- http://www.ctir.gov.br/arquivos/alertas/2016/ALERTA_2016_02_AtaquesRansomware.pdf
- http://www.ctir.gov.br/arquivos/alertas/2017/ALERTA_2017_02_RansomwareWNCRY.pdf
- http://www.ctir.gov.br/arquivos/alertas/2017/ALERTA_2017_04_RansomwarePetrwrap.pdf
- http://blog.trendmicro.com/trendlabs-security-intelligence/bad-rabbit-ransomware-spreads-via-network-hits-ukraine-russia/
- https://www.us-cert.gov/ncas/current-activity/2017/10/24/Multiple-Ransomware-Infections-Reported

Brasília-DF, 25 de outubro de 2017.

Equipe do CTIR Gov