gov.br

ALERTA 09/2022

5-7 minutos

Notícias

Alerta sobre o ator malicioso VICE SOCIETY

Publicado em 21/03/2022 17h02 Atualizado em 28/03/2022 17h13

[TLP:WHITE]

1. O número de ataques de Ransomware é uma realidade cibernética, que as instituições precisam lidar. Ameaças à disponibilidade da informação por ações desta natureza impactam diretamente os negócios de organizações de todos os segmentos. As redes governamentais também são vítimas deste tipo de ameaça. Neste sentido, o CTIR Gov tem acompanhado o aumento de casos envolvendo o ator malicioso identificado como VICE SOCIETY.

2. VICE SOCIETY é um grupo que utiliza ataques do tipo "Ransomware" que pode infectar várias versões do sistema operacional Windows. O VICE SOCIETY atua contra diversos setores, utilizando como vetor de entrada, campanhas bem sucedidas de phishing, o reaproveitamento de credenciais vazadas e serviço remoto de impressão que esteja vulnerável (CVE-2021-34527). O referido grupo tem a capacidade de empregar algoritmos de encriptação, com objetivo de solictação de resgate, assim como replicar-se, por movimentação lateral,

através das redes corporativas.

3. O Centro de Prevenção, Tratamento e Resposta à Incidentes Cibernéticos de Governo (CTIR Gov) reforça as medidas de prevenção e reação a ataques de Ransomware citadas nos Alertas e Recomendações já publicados anteriormente, e destaca as seguintes ações:

- Criar ou reforçar campanhas de conscientização de usuários sobre como identificar e reportar e-mails de phishing e como se proteger de ataques de engenharia social;
- Definir uma política específica de controle de senhas administrativas de sistemas críticos, adotando a autenticação de multifator para acesso a estes recursos;
- Implementar o princípio de privilégio mínimo que garanta que usuários tenham o nível mínimo de acesso necessário para cumprir suas tarefas;
- Desabilitar as funções do servidor de impressão em todos os computadores onde ele não for necessário;
- Implementar regras de firewall baseadas em feeds de threat intelligence que bloqueiem acesso a sites ou IPs maliciosos, URLs de phishing, proxies anônimos, rede Tor e serviços de anonimização;
- Desativar o Windows PowerShell, caso não seja utilizado, uma vez que variantes de Ransomware usam este recurso para serem executados;
- Reduzir a superfície de ataque, evitando a utilização de protocolos inseguros ou programas de acesso remoto. Se acesso do tipo RDP for absolutamente necessário, restringir IPs de origem e exigir uso de autenticação de múltiplo fator (MFA);
- Promover a imediata segmentação ou segregação (air gap) de

ativos identificados como de maior risco na análise de risco da instituição;

- Atualizar os Sistemas Operacionais com os mais recentes patches de segurança, respeitando os procedimentos para garantir a disponibilidade com a aplicação de medidas mitigadoras;
- Monitorar continuamente dispositivos conectados à rede corporativa, com especial atenção a atividades anômalas relacionadas a processos de login; e
- Implementar e validar um Plano de Continuidade de Negócio (PCN).

4. Quando se trata de PCN, a gestão de backups de dados se destaca, quanto a este aspecto sugere-se:

- Adotar políticas de execução de backup, incluindo um plano de recuperação com base no impacto que sistemas e processos específicos possuem na organização, com procedimentos e testes de restauração;
- Definir um segmento de rede separado para dispositivos de armazenamento de backup, permitindo acesso apenas a servidores que estão sendo copiados;
- Utilizar a separação lógica de tarefas, definindo credenciais distintas da operação de rede e específicas para operações de backup; e
- Considerar manter cópias offline, desta forma inacessíveis a um usuário malicioso.

5. Recomenda-se ainda analisar, particularmente, as seguintes referências:

- https://msrc.microsoft.com/update-guide/vulnerability

/CVE-2021-34527

- https://www.cisa.gov/stopransomware
- https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

6. O CTIR Gov, em concordância com o previsto no Decreto 10.748/2021, solicita que as entidades responsáveis pelas Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos Setoriais orientem a constituency de seus respectivos setores sobre o tratado nesta recomendação, de acordo com suas diretrizes e políticas específicas.

7. Outrossim, cabe a leitura atenta, por parte de todos os Órgãos da Administração Pública Federal, do Decreto citado disponível em:

- https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022

8. Por fim, o CTIR Gov indica a consulta frequente aos alertas e recomendações divulgadas em:

- https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes

Equipe CTIR Gov

[TLP:WHITE]