Departamento de Segurança da Informação e Comunicações – **DSIC** dsic.planalto.gov.br/
Centro de Tratamento de Incidentes de Redes do Governo – **CTIR Gov** www.ctir.gov.br/

Alerta nº 04/2018 – Atividade de Ameaça Avançada Persistente visando o setor de Energia e outros setores de Infraestrutura Crítica.

1. Descrição do Problema

Data de Publicação: 27/05/2018
Data de Atualização: 27/05/2018

Foi observado o ressurgimento de um grupo de hackers conhecido como *Dragonfly* que está direcionando ataques às infraestruturas do sistema de controle de energia e de empresas (ICS).
A Empresa Symantec informou possuir evidências que indicam que a campanha *Dragonfly* 2.0 está em andamento desde pelo menos dezembro de 2015 e identificou um aumento distinto e significativo na atividade em 2017.
Essa campanha faz uso de uma variedade de vetores de infecção em um esforço para obter acesso à rede de uma vítima, incluindo *e-mail phishing*, ataques de *watering hole* e programas com *trojan*.
A primeira atividade identificada dessa onda de ataques foi uma campanha maliciosa de *e-mail* que enviou e-mails "*Phishings*" com convite de uma festa de Ano Novo para uma empresa no setor de energia em dezembro de 2015.
O grupo realizou mais campanhas mal intencionadas de *e-mail* durante 2016 e até 2017. Os *e-mails* continham conteúdo muito específico relacionado ao setor de energia, bem como alguns relacionados a preocupações comerciais gerais. Uma vez aberto, o documento malicioso em anexo tentaria capturar as credenciais da rede das vítimas para enviar a um servidor fora da organização. Uma vez de posse das credencias de rede do usuário e o acesso remoto estabelecido, o invasor usa ferramentas publicamente disponíveis ou ferramentas de administração de dentro do ambiente da vítima para obter credenciais que permitam acesso a sistemas de seu interesse.

2. Possíveis Riscos

- Vazamento de credencias;
- Vazamento de dados sigilosos;
- Comprometimento parcial ou total da operação dos seus alvos.

3. Sugestões para Mitigação do Problema

- Impedir a comunicação externa de todas as versões do SMB e protocolos relacionados no limite da rede bloqueando as portas TCP 139 e 445 com a porta UDP relacionada 137;
- Bloquear o protocolo *WebDAV* (*Distributed Authoring and Versioning*) com base na *Web* em dispositivos de *gateway* de fronteira na rede;
- Monitorar logs VPN para atividade anormal (por exemplo, logs fora de hora, *logins* de endereço IP não autorizados e múltiplos *logins* simultâneos);
- Implantar filtros de *web* e de *e-mail* na rede. Configurar esses dispositivos para procurar nomes, fontes e endereços de nomes mais conhecidos;
- Bloquear esses antes de receber e baixar mensagens (*blacklist*). Esta ação ajudará a reduzir a superfície de ataque no primeiro nível de defesa da rede. Analise todos os e-mails, anexos e downloads (tanto no host como no gateway de correio) com uma solução antivírus respeitável que inclui serviços de reputação em nuvem;
- Segmentar todas as redes críticas ou sistemas de controle de sistemas e redes de negócios de acordo com as melhores práticas da indústria;
- Assegurar *logs* e visibilidade adequada nos pontos de entrada e saída;
- Garantir o uso da versão 5 do *PowerShell*, com o *log* aprimorado ativado. As versões mais antigas do *PowerShell* não fornecem registro adequado dos comandos do *PowerShell* que um invasor pode ter executado;

- Habilitar o log de módulo *PowerShell*, registro de blocos de script e transcrição. Enviar os logs associados a um repositório de *log* centralizado para monitoramento e análise;
- Implementar as estratégias de prevenção, detecção e mitigação. Consultar o Alerta CTIR.Gov 01/2016 - Comprometimento de Servidores de páginas através do *Web Shell*;
- Estabelecer um mecanismo de treinamento para informar Aos usuários finais sobre o uso correto de *e-mail* e *web*, destacando informações e análises atuais e incluindo indicadores comuns de *phishing*. Os usuários finais devem ter instruções claras sobre como denunciar *e-mails* incomuns ou suspeitos;
- Implementar listagem de listas de diretório de aplicativos. Os administradores de sistema podem implementar listas de diretório de aplicativos ou diretórios de aplicativos através da Política de Restrição de *Software* da *Microsoft*, *AppLocker* ou *software* similar. Os padrões de segurança permitem que aplicativos sejam executados a partir de *PROGRAMFILES*, *PROGRAMFILES* (X86), *SYSTEM32* e quaisquer pastas de software ICS. Todos os outros locais devem ser desativados a menos que uma exceção seja concedida;
- Bloquear conexões RDP originadas de endereços externos não confiáveis, a menos que exista uma exceção; rotineiramente revogar exceções de forma regular para validade;
- Armazenar os *logs* do sistema de sistemas de missão crítica durante, pelo menos, um ano dentro de uma ferramenta de gerenciamento de eventos de informações de segurança;
- Certificar-se de que as aplicações estão configuradas para registrar o nível de detalhe adequado para uma investigação de resposta a incidentes;
- Considerar implementar HIPS ou outros controles para evitar a execução de código não autorizado;
- Estabelecer controles de mínimos privilégios;
- Reduzir o número de contas de administrador de empresas e de domínio do *Active Directory*;
- Com base no nível de compromisso suspeito, redefinir todas as credenciais da conta de usuário, administrador e serviço em todos os sistemas locais e de domínio;
- Estabelecer uma política de senha para exigir senhas complexas para todos os usuários;
- Certificar-se de que as contas de administração de rede não possuem conectividade externa;
- Certificar-se de que os administradores de rede usem contas não privilegiadas para o e-mail e acesso à Internet;
- Usar e a autenticação de dois fatores para toda autenticação, com ênfase especial em interfaces externas e ambientes de alto risco (por exemplo, acesso remoto, acesso privilegiado e acesso a dados sensíveis);
- Implementar um processo de log e atividades de auditoria realizadas por contas privilegiadas;
- Habilitar o *log* e o alerta sobre escalas de privilégios e mudanças de função;
- Fazer uma busca periódica de informações publicamente disponíveis para garantir que nenhuma informação confidencial tenha sido divulgada. Revise fotografias e documentos para dados sensíveis que podem ter sido inadvertidamente incluídos;
- Atribuir pessoal suficiente para revisar *logs*, incluindo registros de alertas;
- Rever o risco de segurança independente (em oposição à conformidade);
- Criar e participar de programas de compartilhamento de informações; e
- Criar e manter a documentação do sistema e da rede para auxiliar na resposta a incidentes. A documentação deve incluir diagramas de rede, proprietários de ativos, tipo de ativos e um plano de resposta a incidentes.

5. Referências

- https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
- https://www.us-cert.gov/ncas/alerts/TA17-293A
- https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
- https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- https://www.us-cert.gov/ncas/alerts/TA15-314A