Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 02/2016 – Ataques de Ransomware através de campanhas de Phishing

1. Descrição do Problema

Temos recebido dos órgãos de Inteligência e de nossos colaboradores, Alertas sobre ataques de "Ransomware" tendo como alvo os domínios da Administração Pública Federal, em particular, os órgãos relacionados, direta ou indiretamente, com a organização dos Jogos Olímpicos e Paralímpicos Rio2016.

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

Os atacantes possivelmente utilizarão contas de correio comprometidas (contas funcionais) de órgãos de Governo para propagar códigos maliciosos (malwares), conhecidos como "droppers" que farão o download do Ramsoware (código encriptador).

Os códigos maliciosos são, geralmente, enviados em arquivos com "java scritps" compactados (zip, rar, etc) atachados via E-mail. A infeção também pode ocorrer através de documentos do MS-Office que contenham macros com códicos obfuscados com *Visual Basic Scrip*t (VBS) e em arquivos "batch", os quais resultam no download e execução do executável do Ransomware.

Outra possiblidade é a utilização de sítios comprometidos (ataques de drive-by) para infecção de navegadores vulneráveis a injeção de Java-scripts.

3. Ameaças

- Recentemente, recebemos a informação sobre um ataque de Ransomware, onde foi encontrado traços de código do "Hidden Tear", um ransomware "educacional" publicado no GitHub, o qual está sendo amplamente usado em ataques desse tipo.
- Aparentemente, o grupo "Anonymous" baixou o código fonte do "Hidden Tear", mudou o código e recompilou.
- O FBI emitiu, em 11 de Julho de 2016, alerta sobre uma variante de Ransomware chamada de "Locky", que tem sido extensivamente utilizado em campanhas de "spam" e "Phishing Message" para distribuir código capaz de encriptar numerosos tipos de arquivos, locais ou em compartilhamentos de Rede.
- O locky se comunica com Servidores de Comando e Controle (C2) para informar aos operadores o sucesso na infecção e obter a chave de encriptação e o código identificador da vítima. O locky também contém um algorítmo, que gera domínios para a comunicação com a sua Infraestrutura de Comando e Controle.
- As redes infectadas, normalmente, fazem requisições com métodos "HTTP" POST de arquivos tipo: main.php, submit.php e mais recentemente userinfo.php, dentre outros.
- Uma vez executado, o Locky estabelece, via Registro, um processo persistente na tentativa de deletar "shadow copies" usando o Comando "vssadmin" e encriptar arquivos dos usuários, tais como: documentos, arquivos de mídias, códigos-fonte, dentre outros.

- O FBI afirma que a recuperação é quase impossível, sem a chave de encriptação, devido ao tipo de criptografia forte utilizada, portanto a política de Backup é a medida mais eficaz para evitar a perda de dados.
- Não é recomendável, em nenhuma hipótese, o pagamento de valores aos atacantes.
- Segue em anexo uma lista de domínios de Comando e Controle utilizados pelo Locky.

4. Sugestões para Mitigação Problema

- Ajustar os filtros de e-mail para bloquear, ou alertar arquivos anexados com extensão zip, rar, etc;
- 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;
- Garantir o backup atualizado dos arquivos locais e dos Armazenados em Servidores de Arquivos;
- Rever a política de privilégios administrativos nas máquinas clientes, a fim de restringir a instalação /execução de binários e ou executáveis desconhecidos;
- Isolar a máquina da rede, ao primeiro sinal de infecção por malware;
- Verificar o tráfego de máquinas internas para domínios não usuais ou suspeitos. (vide relação anexa);
- Monitorar as conexões internas e não usuais entre máquinas da rede, a fim de evitar o movimento lateral de propagação do malware; e
- Manter navegadores atualizados e verificar necessidade de habilitar a execução de Java-Script;
- Por fim, manter o antivírus, aplicação de "Patchs" de segurança e a "*blacklist"* (filtro "antispam") de e-mail atualizados.

Referências:

- https://www.us-cert.gov/ncas/alerts/TA16-091A
- https://info.publicintelligence.net/FBI-LockyRansomware.pdf
- https://www.cyphort.com/drive-by-ransomware-infection-in-the-wild/

Brasília-DF, 05 de agosto de 2016.

Equipe do CTIR Gov