Recomendação de Segurança 002/2016 - CGTI/VPGDI

Em 27 de junho de 2016

Para: Gestores de TI das unidades da Fiocruz

Assunto: *Ransomware*

Prezados Gestores,

O Ransomware é uma categoria de malware que, ao contaminar um host, criptografa os arquivos e cobra um valor de resgate para que a criptografia possa ser revertida. Apesar do conceito já existir há alguns anos, observa-se uma rápida evolução da ameaça e do seu grau de severidade. Hoje, estima-se que 93% dos casos de *phishing* estão relacionados a Ransomware. São características do Ransomware:

- A alta lucratividade (para aqueles que lançam o ataque);
- A difícil rastreabilidade;
- A difícil interrupção do ataque;
- A fácil propagação;
- A utilização de Bitcoin (moeda virtual) para o pagamento;
- O uso de modelos RaaS (Ransomware as a Service) para o gerenciamento dos ataques (ToX, FakBen, Encryptor RaaS, Ransom32, ORX Locker, Janus, Alpha Locker, Hidden Tear, entre outros);

A seguir são descritos alguns conceitos importantes sobre o tema e práticas recomendas para prevenção e tratamento da ameaça.

Tipos de Ransomware

O Ransomware se divide em dois tipos:

- Locker Ransomware: locker de máquina
- Crypto Ransomware: locker de dados

Extensões conhecidas em arquivos contaminados

Apesar de haver muitas variações, algumas extensões já são conhecidas. São elas: .crypt, .locky, .cryptxxx, .cerber, .aaaryp, .xtbl, etc.

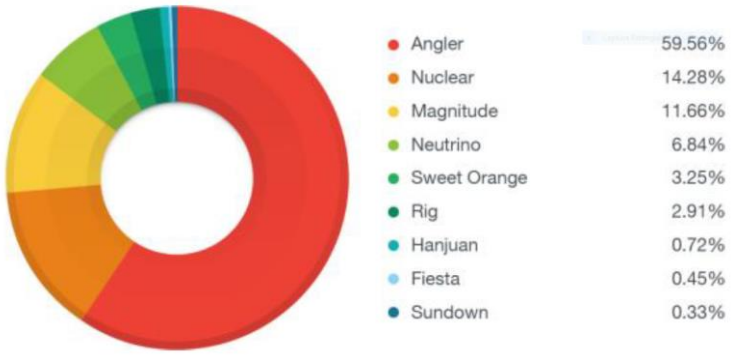
Plataformas vulneráveis

Já foram identificados casos de Ransomware em estações de trabalho Microsoft Windows, servidores Microsoft, MAC's, Smartphones e Tablets.

Principais formas de propagação

A propagação da ameaça pode se dar de diversas formas. As mais comuns são: e-mail, downloads, botnets, dispositivos em portas USB e versões desatualizadas de plug-ins como Oracle Java, Adobe Flash e Microsoft Silverlight.

Principais infraestruturas (Exploit kits) em uso



Boas práticas recomendadas para prevenção

A fim de mitigar a exposição à ameaça, algumas ações podem ser adotadas:

- Filtro web: proibir acesso a arquivos executáveis e a sites com reputação maliciosa.
- Filtro de e-mail: proibir recebimento de anexos com extensões maliciosas (.exe, .cpl, .js, .com, .pif, etc.), habilitar a checagem de reputação de URL, utilizar base de reputação, checagem de antispoofing e registro SPF.

- Sandbox: habilitar teste automatizado de segurança do arquivo antes do usuário final executar.
- Gestão ativa das Soluções de Segurança (MSS): analisar dados das soluções de segurança existentes a fim de identificar possíveis ameaças;
- Campanha de conscientização: realizar campanhas de sensibilização com funcionários, pois o risco muitas vezes é trazido do ambiente externo.
- Gestão de Vulnerabilidades: realizar regularmente varredura de vulnerabilidades, hardening e atualização do ambiente (Sistemas Operacionais, aplicativos de terceiros, tais como Java, Flash e Silverlight);
- Macros: desativar macros do pacote Office.
- Permissões de acesso e compartilhamentos: revisar regularmente as permissões de acesso e compartilhamento existentes;
- Manter backup regular dos dados;
- Adotar soluções de segurança com mecanismos contra Ransomware;
- Tráfego criptografado: realizar inspeção do tráfego criptografado.

Boas práticas na configuração do Officescan

- Aplicar o patch crítico 6054 (60/5/2016), disponível no Trend OfficeScan11.0 SP1, que disponibiliza recursos de análise baseada em comportamento;
- Ativar a configuração de análise baseada em comportamento acessando a opção: “Settings > Behavior Monitoring Settings”. Marcar as opções:

- Verificar através do ícone de status do agente (cliente) se a opção ‘Behavior Monitoring” está realmente ativada:

Procedimentos para tratamento

Uma vez identificada a manifestação da ameaça (ou sua suspeita), as seguintes ações devem ser adotadas, de acordo com o seu tipo.

Crypto Ransomware (Data Locker):

1. Isolar o host onde foi identificada a ameaça e que teve seus arquivos criptografados e buscar por extensões conhecidas (crypt, .locky, .CryptXXX, .Cerber, .aaa, etc);
2. Utilizar a ferramenta ATTK (Trend Micro Anti-Threat Toolkit) para limpeza (quando possível) e coleta de dados do host. Ao final da varredura será gerado um arquivo que deverá ser encaminhado à Real Protect através de um chamado.
3. Identificar a data e hora em que o arquivo de resgate que foi criado (exemplo: 'Locky_recover_instructions.txt', 'Recovery_xx.txt', 'Recovery_my_files.txt', etc.) e analisar os logs (filtro web e servidor de e-mail) a fim de identificar a origem do malware e bloquear novas infecções.
4. Tentar identificar o Ransomware responsável pela criptografia dos dados (Tesla Cryptxxx, Locky, Troldesh, Cerber, etc.
5. Verificar se houve infecção no servidor de arquivos em pastas mapeadas nessas estações. Verificar o Owner dos arquivos de resgate;
6. Tentar a restauração pelo "shadow copy (VSS)";
7. Avaliar o uso de ferramentas de terceiros para reverter o processo de criptografia, de acordo com o Ransomware identificado:
    a. TeslaCrypt: ESET TeslaCrypt Decryptor, BloodDolly's Tesla Decoder;

b. Rannoh, CryptXXX v1 e v2, Coinvault e Bitcryptor: Kaspersky Rannoh Decryptor;

c. Petya: Petya Sector Decrypter e https://petya-pay-no-ransom.herokuapp.com

d. Locky e Cerber: Não há conhecimento de ferramentas disponíveis até o momento;

Observação: Não havendo sucesso com as ferramentas descritas no item 7, pode-se 'tentar' a recuperação com ferramentas como GetDataBack, Recuva, File Recovery, Power Data Recovery, entre outros.

Locker Ransomware (Computer Locker)

1. Impedir a execução do arquivo 'Bewerbungsmappe-gepackt.exe'. Vale ressaltar que é raro encontrar este executável;
2. Colocar o HD em outra estação (secundário);
3. Executar o Petya Sector Extractor (extração de dados);
4. Utilizar os dados extraídos no passo anterior na ferramenta disponível no site http://petya-pay-no-ransom.herokuapp.com

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações