DESENVOVIMENTO

ANATOMIA DE UM ATAQUE

1. IMPLANTAÇÃO
   1. A primeira fase, conhecida como implantação, é a fase em que se instala, na máquina da vítima, os componentes necessários para a infectar, criptografar ou bloquear o sistema (LISKA e GALLO, 2017).
   2. Download drive-by (download automático de malwares)
   3. Emails [sic] para phishing (campanhas maliciosas por e-mail)
   4. Exploração de vulnerabilidades em sistemas acessíveis pela internet
2. INSTALAÇÃO
   1. Como previamente explicado, passa-se à instalação assim que o payload alcançar o sistema da vítima.
   2. o início da formação do processo de comando e controle
3. COMANDO E CONTROLE
   1. deixar aberto um canal, qual varia conforme as diferentes variantes e famílias do malware, para garantir que as comunicações aconteçam
4. DESTRUIÇÃO
   1. É nesta fase que se dá a encriptação dos arquivos, podendo alcançar qualquer tipo, ou o bloqueio do sistema. Algumas variantes conseguem criptografar até o nome dos arquivos, dificultando ainda mais a identificação daqueles que foram afetados ou mesmo até onde os invasores prejudicaram o sistema
5. EXTORSÃO
   1. Deflui-se a exibição de uma tela informando às vítimas o acontecido, bem como fornecendo informações sobre o método de pagamento e instruções para realiza-lo.

RANSOWARE: DEFENDENDO-SE DA EXTORSÃO DIGITAL

CAPÍTULO 4: PROTEGENDO AS ESTAÇÕES DE TRABALHO E OS SERVIDORES

ALGUMAS PRECAUÇÕES IMPORTANTES, PARA EVITAR ATAQUES

* MACROS E PDFS NO COTIDIANO
  + Desabilitar a execução de macros
  + Fazer bloqueio de extensões costumeiramente utilizadas nos ataques no Gateway SMTP
* VARRENDO A CAIXA DE ENTRADA DOS EMAILS
  + FIREEYE NX
  + PALOALTO FIREWAL (com Wildfire ativado)
  + Arquivos suspeitos, se forem executados, somente em Sandbox (ambiente virtualizados)
  + Evitar mapeamento de drives na rede
  + Eliminar o software Adobe Flash (comumente atacados por kits de exploits)
* USAR SOFTWARES DE INVENTÁRIOS PARA MONITORAR SOFTWARES E VERSÕES USADOS NO AMBIENTE DE REDE
  + CORVIL
  + TRIPWIRE
  + SOFTWARE END-POINT MANAGEMENT DA SYMANTEC

*Em suma, manter os softwares atualizados é primordial*.

INTERROMPENDO A SEQUÊNCIA DE UM ATAQUE

SEQUÊNCIA DO ATAQUE

1. O Ransoware deve executar e de descompactar para coletar informações do sistema
2. Precisar alterar informações de registro para que seja considerado um processo válido dentro do sistema
3. Os mais sofisticados desativam e apagam os registros das cópia de sombra
4. A maioria precisa obter acesso a uma chave pública para poder criptografar os arquivos, para isso, precisam acessar a infraestrutura de comando e controle do sistema
5. Listar os arquivos
6. Ler e criptografar os arquivos
7. Se for o caso, apagar os arquivos originais
8. Remover a chave de criptografia do computador local

INTERROMPENDO

Antes, necessário saber como negociar as políticas de segurança

1. Desabilitar macros via política de grupos, por exemplo
2. Limitar os diretórios onde os arquivos podem ser executados. Proibindo, por exemplo, nos diretórios, no caso do SO Windows:
   1. \Downloads
   2. \Temp
   3. %AppData%\
3. Impedir execução automática de PEs (Portable Executables, ou executáveis portáteis) através, por exemplo, do uso do software AppLocker (Windows 7 e no Windos Server 2008)
4. Desabilitar escritas no registry para contas locais, ficando na responsabilidade de uma equipe de suporte treinada as instalações dos softwares que forem solicitados
5. Impedir a desativação e/ou exclusão dos pontos de restauração do sistemas com o uso de ferramentas tais como SentinelOne ou Carbon Black
6. Bloquear o acesso ao host C&C (command-and-control, ou comando e controle), geralmente usando HTTP, na porta 80. Novamente, ferramentas como Carbon Black, Cylance, FireEye, etc., podem ajudar nessa atividade. Ainda nesse contexto, estudar a possiblidade de bloquear no firewall extensões do tipo: biz, click, info, org, pl, pw, ru, su, work e xyz.
7. Interrompendo o ataque durante o processo de criptografia. Importante observar nesse ponto:
   1. Muitos ransowares usam a API Crypto do Windows (crypt32.dll);
   2. Nesse contexto, poderia ser programada para que encerre qualquer processo não confiável que chama a API crypto um determinado número de vezes, caracterizando uma atitude suspeita. Esse valor iria variar para mais ou menos, conforme as experiências nos ataques.
   3. A observação que se faz é que nem todos os ransowares poderão usar a criptografia nativa do Windows, mas sim suas próprias. Mas reitera-se, boa parte, deles a usam, daí o método poder ser eficaz em muitas ocasiões.
   4. Outra abordagem seria encerrar automaticamente qualquer processo não confiável que esteja copiando e/ou apagando um número grande de arquivos.

AGINDO RAPIDAMENTE

Maior integração e controle por todos os responsável pela administração da informação no suporte técnico de TI.

EFICÁCIA DO ESET ANTIVÍRUS

CAPÍTULO 5: PROTEGENDO A FORÇA TRABALHO

1. CONHECENDO OS RISCOS
   1. Sistemas e informações críticos que podem ser gravemente comprometidos, até mesmo de forma irreversível.
   2. Priorizar aquilo for mais crítico.
   3. Importância de fazer um levantamento que identifique o que está em rede.
2. EVITANDOS COMPROMETIMENTOS
   1. Scanning de anexos de email
   2. Monitorando os sites/links
3. TREINAMENTO E CONSCIENTIZAÇÃO
   1. Montar programa educacional
   2. Simulação
   3. Encontros periódicos (à exemplo da SIPAT, criar a Semana Interna de Prevenção de Acidentes em Tecnologia da Informação - SIPATI)
4. PÓS INVASÃO
   1. Análise de pontos de vulnerabilidades e aplicação das correções (pontos fortes, fracos e oportunidades de melhorias)
   2. Reforçar treinamento dos usuários

CAPÍTULO 6: USANDO DADOS DE INTELIGÊNCIA CONTRA AMEAÇAS E RANSOWARES

CONHECENDO OS MÉTODOS DE ENTREGA MAIS RECENTES

* Mais uma vez, os e-mails
* Documentos .pdf e .doc

INDICADORES DE REDE MAIS RECENTES

* Manter uma base atualizada contendo lista de IPs e URLs de alguma forma associados aos canais de comando e controle dos ransowares. (Tentar conseguir uma tabela com essa listagem atualizada e colocar no artigo).

INDICADORES COMPORTAMENTAIS MAIS RECENTES

* De olho nos processos anômalos
* De olho nos acessos de usuários anômalos

RANSOMWARE, EXTORSÃO DIGITAL - Brasil Escola (PÁGINA 25)

ADEQUAÇÃO JURÍDICA E COOPERAÇÃO INTERNACIAL

* RANSOWARE NA LEGISLAÇÃO BRASILEIRA
  + Ausência de tipificação específica
* CONVENÇÃO DE BUDAPESTE