Vírus

Vírus de Script

- SCRIPT = UM CONJUNTO DE INSTRUÇÕES QUE DEVEM SER EXECUTADAS.
- ESCRITO EM LINGUAGEM DE SCRIPT (EX: VBSCRIPT E JAVASCRIPT).
- RECEBIDO AO ACESSAR UMA PÁGINA WEB OU POR E-MAIL (COMO UM ARQUIVO ANEXO OU COMO PARTE DO PRÓPRIO E-MAIL ESCRITO EM FORMATO HTML.
- PODE SER AUTOMATICAMENTE EXECUTADO, DEPENDENDO DA CONFIGURAÇÃO DO NAVEGADOR OU DO PROGRAMA LEITOR DE E-MAILS.

Vírus de Macro

- TIPO ESPECÍFICO DE VÍRUS DE SCRIPT.
- ESCRITO EM LINGUAGEM DE MACRO.
- INFECTA DOCUMENTOS QUE USAM ESSA LINGUAGEM (DO EXCEL, DO WORD, DO POWER POINT, ETC).
- QUANDO O SOFTWARE CARREGA UM ARQUIVO, EXECUTA O CÓDIGO MALICIOSO.
- SE PROPAGA FACILMENTE ATRAVÉS DO COMPARTILHAMENTO DE DOCUMENTOS INFECTADOS.

Vírus de Arquivo

- VÍRUS DE PROGRAMA OU VÍRUS PARASITÁRIO.
- É O MAIS TRADICIONAL.
- INFECTA ARQUIVOS EXECUTÁVEIS, SOBRESCREVENDO O CÓDIGO ORIGINAL.
- REPLICA-SE AO LOCALIZAR OUTROS ARQUIVOS EXECUTÁVEIS OU INFECTANDO ARQUIVOS QUE FORAM REQUISITADOS PARA A EXECUÇÃO DE UM PROGRAMA.

`.EXE` `.COM` `.VBS` `.OVL` `.DLL` `.CMD` `.PIF` `.SYS` `.SRC` `.BAT` `.ASP`

Vírus de Boot

- VÍRUS DE SETOR OU VÍRUS DE INICIALIZAÇÃO.
- BOOT = PROCEDIMENTO DE INICIALIZAÇÃO DO COMPUTADOR DURANTE O CARREGAMENTO DO SISTEMA OPERACIONAL.
- ESCONDE-SE NO PRIMEIRO SETOR DA MEMÓRIA.
- É ATIVADO QUANDO O COMPUTADOR É LIGADO E É CARREGADO ANTES MESMO DO SISTEMA OPERACIONAL.
- PODE AFETAR DISPOSITIVOS MÓVEIS DE ARMAZENAMENTO. (EX: PENDRIVES)
- A FORMATAÇÃO RÁPIDA DO PENDRIVE NÃO GARANTE A REMOÇÃO COMPLETA DO VÍRUS.

Vírus Stealth

- VÍRUS FURTIVO.
- PROJETADO PARA NÃO SER DETECTADO PELO ANTIVÍRUS.
- É CAPAZ DE SE REMOVER DA MEMÓRIA TEMPORARIAMENTE.

Vírus Timebomb

- VÍRUS BOMBA RELÓGIO.
- APÓS INFECTAR A MÁQUINA, FICA LATENTE (OCULTO), SE REPLICANDO.
- É PROGRAMADO PARA SER ATIVADO EM UM MOMENTO ESPECÍFICO.

SE INSTALAM NOS COMPUTADORES PELA AÇÃO DO USUÁRIO.

Vírus Polimórfico

- VÍRUS MUTANTE.
- É CAPAZ DE ASSUMIR MÚLTIPLAS FORMAS A CADA INFECÇÃO COM O INTUITO DE BURLAR O ANTIVÍRUS.
- MUDA SUA ASSINATURA, MANTENDO SUAS FUNCIONALIDADES, MAS ALTERANDO O SEU PADRÃO DE BITS.
- ALTERAM A ROTINA DE ENCRIPTAÇÃO E A DE DECRIPTAÇÃO.
- GERA VARIAÇÕES DE SI MESMO UTILIZANDO-SE DE CHAVES DE ENCRIPTAÇÃO DIVERSAS.

Vírus Metamórfico

- É UMA VARIAÇÃO DO VÍRUS POLIMÓRFICO.
- SE REESCREVE COMPLETAMENTE A CADA INFECÇÃO.
- PODE MUDAR DE TAMANHO E DE COMPORTAMENTO.
- MUDA SUA ASSINATURA E SUA FUNCIONALIDADE.

Observações Gerais

- SE PROPAGA ANEXANDO-SE OU HOSPEDANDO-SE EM ARQUIVOS E PROGRAMAS;
- NÃO É AUTOEXECUTÁVEL;
- NÃO É AUTOSSUFICIENTE;

COMPOSTO DE 3 PARTES: MECANISMO DE INFECÇÃO, MECANISMO DE ATIVAÇÃO E CARGA ÚTIL.

@mapasdathai

@mapasdathai

Principais Malwares

Worm

VERME

- CAPAZ DE SE REPLICAR AUTOMATICAMENTE, ENVIANDO CÓPIAS DE SI MESMO.
- CONSOME MUITOS RECURSOS, AFETA O DESEMPENHO DA REDE E PODE LOTAR O DISCO RÍGIDO.
- WORMS NÃO INFECTAM ARQUIVOS. SÃO AUTÔNOMOS.
- SÃO CAPAZES DE ENTRAR EM UMA MÁQUINA SEM QUALQUER INTERAÇÃO COM O USUÁRIO.

PROCESSO DE INFECÇÃO E PROPAGAÇÃO

- 1ª FASE: SCANNING (IDENTIFICAÇÃO DOS COMPUTADORES-ALVO P/ OS QUAIS TENTARÁ SE COPIAR);
- 2ª FASE: ENVIO DE CÓPIAS;
- 3ª FASE: ATIVAÇÃO DAS CÓPIAS (EM REGRA, PRECISA SER EXECUTADO PARA QUE A INFECÇÃO OCORRA)

Spywares

SOFTWARE ESPIÃO

- SOFTWARE ESPIÃO QUE COLETA DADOS DA MÁQUINA OU DA REDE E DISPONIBILIZA-OS A TERCEIROS.
- PODE SER LEGÍTIMO OU MALICIOSO, DEPENDENDO DA FORMA COMO FOI INSTALADO.
- PRECISA SER EXPLICITAMENTE EXECUTADO PELO USUÁRIO.

- KEYLOGGER: CAPTURA AS TECLAS DIGITADAS PELO USUÁRIO.
- SCREENLOGGER: CAPTURA A POSIÇÃO DO CURSOR E A TELA APRESENTADA NO MOMENTO EM QUE O MOUSE É CLICADO.
- ADWARE: PROJETADO P/ APRESENTAR PROPAGANDAS.

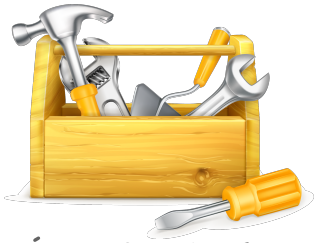
Backdoor

PORTA DOS FUNDOS

- PROGRAMA QUE PERMITE O RETORNO DE UM INVASOR A UM COMPUTADOR COMPROMETIDO.
- PODE SER INCLUÍDO POR OUTROS CÓDIGOS MALICIOSOS QUE TENHAM PREVIAMENTE INFECTADO O COMPUTADOR OU POR INVASORES QUE EXPLORAM VULNERABILIDADES NOS PROGRAMAS INSTALADOS NA MÁQUINA.
- GARANTE ACESSO REMOTO FUTURO. (ABRE AS PORTAS TCP)

Rootkit

KIT DO ADMINISTRADOR



- CONJUNTO DE PROGRAMAS E TÉCNICAS QUE PERMITE ESCONDER E ASSEGURAR A PRESENÇA DE UM INVASOR OU DE OUTRO CÓDIGO MALICIOSO EM UM COMPUTADOR.
- É UM DOS MALWARES MAIS SOFISTICADOS QUE EXISTEM.
- NÃO É USADO P/ OBTER O ACESSO, MAS SIM P/ MANTÊ-LO.
- COMPROMETE O SISTEMA OPERACIONAL, ALTERANDO TUDO QUE ELE INFORMA, DE ACORDO COM O QUE QUER O INVASOR.

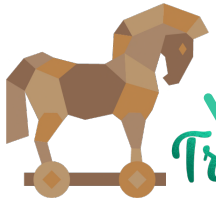
Bot

DIMINUTIVO DE ROBOT = ROBÔ

- PROGRAMA QUE DISPÕE DE MECANISMOS DE COMUNICAÇÃO COM O INVASOR QUE PERMITEM QUE A MÁQUINA INVADIDA SEJA CONTROLADA REMOTAMENTE.
- SE PROPAGA AUTOMATICAMENTE EXPLORANDO VULNERABILIDADES DOS PROGRAMAS.
- COMPUTADOR INFECTADO = ZUMBI.
- BOTNET = REDE DE ZUMBIS PRONTA PARA EXECUTAR AÇÕES EM MASSA SOB COMANDO DO INVASOR.

Trojan

CAVALO DE TROIA



- PROGRAMA QUE, ALÉM DE EXECUTAR AS FUNÇÕES PARA AS QUAIS FOI APARENTEMENTE PROJETADO, TAMBÉM EXECUTA FUNÇÕES MALICIOSAS.
- PRECISA EXPLICITAMENTE SER EXECUTADO P/ SER INSTALADO.
- NÃO SE PROPAGA.
- PODE SER CONSIDERADO UM TIPO DE VÍRUS.
- SUA ATUAÇÃO MALICIOSA É EXTREMAMENTE VERSÁTIL, PODENDO REALIZAR ATIVIDADES TÍPICAS DE OUTROS MALWARES
- TIPOS DE TROJAN: DOWNLOADER, DROPPER, BACKDOOR, DOS, DESTRUTIVO, CLICKER, PROXY, SPY E BANKER.

Outros Malwares

Ransomware

- EXTORSÃO OU EXTELIONATO VIRTUAL.
- RANSOM = RESGATE.
- TORNA INACESSÍVEIS OS DADOS ARMAZENADOS EM EQUIPAMENTOS E EXIGE PAGAMENTO DE UM RESGATE PARA RESTABELECER O ACESSO AO USUÁRIO.

- RANSOMWARE LOCKER: IMPEDE O ACESSO AO EQUIPAMENTO.
- RANSOMWARE CRYPTO: IMPEDE O ACESSO AOS DADOS UTILIZANDO CRIPTOGRAFIA.

- PREVENÇÃO: FAZER BACKUPS REGULARMENTE.

Bombas lógicas

- SOFTWARE MALICIOSO PROGRAMADO PARA CAUSAR DANOS QUANDO SATISFEITA UMA DETERMINADA CONDIÇÃO (UMA DEPENDÊNCIA LÓGICA).

- EX: EXCLUIR ARQUIVOS SE DETERMINADO USUÁRIO FICAR + DE 30 DIAS SEM EFETUAR LOGIN.

- GERALMENTE SÃO INSTALADAS POR UM USUÁRIO AUTORIZADO, COMO UM ADMINISTRADOR DE REDE.

Sniffer

FAREJADOR

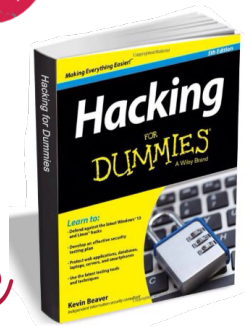
- ANALISADOR DE PACOTES DE DADOS CAPAZ DE MONITORAR, INTERCEPTAR E REGISTRAR TRÁFEGO DE DADOS EM SEGMENTOS DE REDE.

- USO LEGÍTIMO → POR ADMINISTRADORES DE REDES, PARA DETECTAR PROBLEMAS E MONITORAR A REDE.

- USO MALICIOSO → PARA CAPTURAR INFORMAÇÕES SENSÍVEIS QUE ESTEJAM TRAFEGANDO POR MEIO DE CONEXÕES SEM CRIPTOGRAFIA.
  → MODO PROMÍSCUO

Hijacker

- MODIFICA O REGISTRO DO SISTEMA OPERACIONAL, ALTERANDO O FUNCIONAMENTO DO NAVEGADOR.
  MODIFICA A PÁGINA INICIAL, ABRE PÁGINAS AUTOMATICAMENTE, INSERE BOTÕES, ETC.
- O DESENVOLVEDOR DO HIJACKER GERALMENTE GANHA DINHEIRO POR REDIRECIONAR O USUÁRIO PARA PÁGINAS PATROCINADAS.
  EX: HAO123 😤



Exploits

- FERRAMENTA CRIADA POR HACKERS, QUE EXPLORAM VULNERABILIDADES DOS SISTEMAS PARA PERMITIR QUE ATACANTES SEM CONHECIMENTO AVANÇADO POSSAM FAZER INVASÕES.

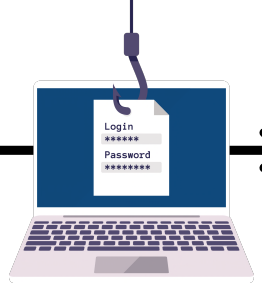
- PODEM EXPLORAR VULNERABILIDADES ZERO-DAY.
  → DESCONHECIDAS PELOS ADMINISTRADORES DE UM SISTEMA

@mapasdathai

Ataques e golpes

Engenharia social

- TÉCNICA POR MEIO DA QUAL UMA PESSOA PROCURA PERSUADIR OUTRA A EXECUTAR DETERMINADAS AÇÕES.
- É UTILIZADA PARA OBTER INFORMAÇÕES SENSÍVEIS DO USUÁRIO, ATRAVÉS DE SUA INGENUIDADE OU DE SUA CONFIANÇA.



Phishing Scan

- O ATACANTE UTILIZA UMA ARMADILHA VIRTUAL PARA OBTER INFORMAÇÕES SENSÍVEIS, COMO SENHAS DE BANCO.

ARMADILHAS COMUNS:

- PÁGINAS FALSAS DE COMÉRCIO ELETRÔNICO OU DE INTERNET BANKING;
- PÁGINAS FALSAS DE REDES SOCIAIS OU DE COMPANHIAS AÉREAS;
- E-MAILS COM FORMULÁRIOS COM CAMPOS P/ DADOS PESSOAIS E FINANCEIROS;
- E-MAILS QUE INDUZEM A CLICAR EM LINKS P/ CÓDIGOS MALICIOSOS;
- SOLICITAÇÃO DE RECADASTRAMENTO.

Força bruta

- ADVINHAR, POR TENTATIVA E ERRO, UM NOME DE USUÁRIO E SENHA.
- MESMO QUE O ATACANTE NÃO DESCUBRA A SENHA, A VÍTIMA PODE TER SUA CONTA BLOQUEADA POR CAUSA DAS VÁRIAS TENTATIVAS SEM SUCESSO.
- DEPENDENDO DE COMO É UTILIZADO, PODE RESULTAR EM UM ATAQUE DE NEGAÇÃO DE SERVIÇO (DoS).

FALSIFICAÇÃO/MASCARAMENTO DE IP

IP Spoofing

- TÉCNICA USADA QUANDO O MECANISMO DE AUTENTICAÇÃO DE UMA REDE É BASEADO EM ENDEREÇOS IP.
- O ATACANTE PODE CLONAR O IP DE UM USUÁRIO LEGÍTIMO, E CONSEGUE ACESSO NÃO AUTORIZADO FAZENDO-SE PASSAR POR ELE.
- EM RESUMO, O IP SPOOFING GERA PACOTES COM O ENDEREÇO IP FORJADO.

DENIAL OF SERVICE

DoS

- O ATACANTE BUSCA RETIRAR DE OPERAÇÃO UM SERVIÇO, UM COMPUTADOR OU UMA REDE CONECTADA À INTERNET, ESGOTANDO SEUS RECURSOS.
- DDoS - DISTRIBUTED DENIAL OF SERVICE (ATAQUE DISTRIBUÍDO DE NEGAÇÃO DE SERVIÇO): OCORRE QUANDO UM CONJUNTO DE EQUIPAMENTOS É USADO DE FORMA COORDENADA EM UM ATAQUE.

FALSIFICAÇÃO / MASCARAMENTO DE E-MAIL

E-mail Spoofing

- O ATACANTE ALTERA CAMPOS DO CABEÇALHO DE UM EMAIL, PARA APARENTAR QUE FOI ENVIADO DE DETERMINADA ORIGEM QUANDO, NA VERDADE, FOI ENVIADO DE OUTRA.
- É POSSÍVEL GRAÇAS A CARACTERÍSTICAS DO PROTOCOLO SMTP, QUE PERMITEM QUE CAMPOS DO CABEÇALHO SEJAM FALSIFICADOS.

Pharming

- TIPO DE PHISHING QUE ENVENENA A TABELA DE CACHE DO SERVIDOR DNS, REDIRECIONANDO O TRÁFEGO PARA SITES FRAUDULENTOS.

EXEMPLO: VOCÊ DIGITA WWW.BB.COM.BR NA BARRA DE ENDEREÇOS, MAS É REDIRECIONADO PARA O SITE WWW.BB.NET.BR DE FORMA TRANSPARENTE (SEM PERCEBER). NA PÁGINA FALSA O GOLPISTA PODE CAPTURAR SEUS DADOS BANCÁRIOS.

BOATO

Hoax

- MENSAGEM QUE POSSUI CONTEÚDO ALARMANTE OU FALSO.
- PODE CONTER CÓDIGOS MALICIOSOS QUE SÃO PROPAGADOS COMO "CORRENTES".
- ESPALHAM DESINFORMAÇÃO NA INTERNET.
- AUMENTAM EXCESSIVAMENTE A CARGA DE SERVIDORES DE E-MAIL E O CONSUMO DA BANDA DE REDE.
- COMPROMETEM A REPUTAÇÃO DE PESSOAS/ENTIDADES REFERENCIADAS NA MENSAGEM.

@mapasdathai