UNIVERSIDADE TUIUTI DO PARANÁ

RODRIGO FERREIRA DOS ANJOS

SOFTWARE MALICIOSO E ENGENHARIA SOCIAL

CURITIBA

2017

RODRIGO FERREIRA DOS ANJOS

SOFTWARE MALICIOSO E ENGENHARIA SOCIAL

Trabalho apresentado ao Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, da Universidade Tuiuti do Paraná, como requisito avaliativo do 2º bimestre da disciplina de Segurança e Auditoria de Software.
Professor: Patricia Rucker de Bassi.

CURITIBA

2017

SUMÁRIO

1 INTRODUÇÃO 3
2 O QUE É SOFTWARE MALICIOSO 4
2.1 DIFERENÇA ENTRE MALWARE, VIRUS, SPYWARE, ADWARE, WORMS E TROJANS 4
2.2 TIPOS DE MALWARES 5
2.3 O QUE É ROOTKIT 5
2.4 RELAÇÃO ENTRE SOFTWARE MALICIOSO E ENGENHARIA SOCIAL 6
2.5 COMO DETECTAR SOFTWARES MALICIOSOS E COMO NOS PROTEGER? 6
2.6 CURIOSIDADES 6
3 O QUE É ENGENHARIA SOCIAL 8
3.1 CICLO DE VIDA DA ENGENHARIA SOCIAL 8
3.2 TRAÇOS COMPORTAMENTAIS HUMANOS POSSIVEIS DE EXPLORAÇÃO 8
3.3 TECNICAS DA ENGENHARIA SOCIAL 8
3.4 ESTRATÉGIAS DE DEFESA 9
3.5 PROCEDIMENTOS EM CASO DE VIOLAÇÃO 9
3.6 COMO PROFISSIONAIS DA SI PODEM AGIR PARA EVITAR 10
4 CONCLUSÃO 11
REFERÊNCIAS 12

1 INTRODUÇÃO

A segurança da informação nos dias de hoje é de suma importância para as organizações. Desde muito tempo softwares maliciosos estão na rede de internet afim de prejudicar financeiramente estas empresas. Por isso, muito recurso é gasto com proteção (antivírus), para que estas estejam mais seguras.

Apesar destas ameaças serem muito tecnológicas e, com isso automática, existe muitos criminosos que usam técnicas de engenharia social para conseguir informações privilegiadas de pessoas/organizações.

2 O QUE É SOFTWARE MALICIOSO

É um programa de computador cujo seu objetivo é se infiltrar no sistema operacional do usuário de forma ilegal, com o objetivo de causar danos ou coletar informações sigilosas sobre uma pessoa ou rede. É comum que esses softwares sejam baixados em conjunto com alguma necessidade real do usuário, ou seja, quando o usuário vai até um site pesquisando sobre algum tipo de software que precisa, é comum esses softwares terem algum arquivo .exe não confiável, e assim que o mesmo é executado, ele se apodera de algumas informações da máquina, deixando ela vulnerável aos ataques.

2.1 DIFERENÇA ENTRE MALWARE, VIRUS, SPYWARE, ADWARE, WORMS E TROJANS

Existem diversos tipos de softwares maliciosos circulando pela interne, sejam em formato executável ou uma simples imagem, abaixo será detalhado a diferença entre cada um deles, mostrando o que fazem e como se apoderam das maquinas.

- Malware: Pode ser um programa ou um comando, pode ter diferentes propósitos como acessar a máquina do usuário e apagar todos os dados, ou apenas se infiltrar e coletar dados para divulgação dos mesmos;
- Vírus: O termo mais comum entre os usuários, este tem a capacidade de infectar uma máquina e fazer copias de si mesmo espalhando-se para os demais computadores, por isso chama-se de vírus, pela grande semelhança com doenças transmitidas por vírus;
- Spyware: Vem do inglês que traduzido para língua nativa significa espião, ou seja, um software malicioso que monitora seus hábitos de navegação para que assim possam os seus criadores possam agir. Comumente usado para roubos de senhas e informações pessoais;
- Adware: Não tem característica de prejudicar o computador, mas pode gerar um grande desconforto ao usuário. Bastante conhecido por executar ou baixar propagandas e anúncios automáticos;
- Worms: Traduzido do inglês, a palavra verme se assemelha muito com esse software malicioso, pois o mesmo é utilizado para se espalhar por

diversos computadores sem que nenhum usuário interfira no processo. Este tipo, não necessita que algum arquivo seja anexado para conseguir infectar diversas máquinas e seu consumo de banda é considerável;

- Trojan: Mais conhecido como cavalo de troia pela sua semelhança com a história antiga, o trojan é um conjunto de funções desenvolvidas para executar ações indesejadas.

2.2 TIPOS DE MALWARES

Malware nada mais é do que um nome (*Malicious Software)*, criado para fazer alusão a um software malicioso, abaixo segue os tipos de malwares mais comuns nos dias de hoje. Vale ressaltar que, todos os itens vistos até o momento, não atacam somente computadores desktops, mas sim, tablets, smatphones e servidores.

- Ransomware: Um tipo de malware que fornece ao hacker poder de bloquear uma máquina ou até mesmo sequestrar dados específicos e com ele, extorquir sua vítima até que o pagamento seja realizado. Instalado normalmente a partir de um link enviado por e-mail ou até mesmo uma imagem;
- Hijacker: Basicamente estes programas entram no computador sem que o usuário perceba e utiliza ActiveX e algumas brechas de segurança, modificando o registro Windows sequestrando e modificando a página inicial do browser, após isso surgem algumas barras, botões e algumas páginas começam a abrir na tela sem que o usuário tenha feito qualquer ação;
- Lammer: E um termo utilizado pelos hackers para depreciar crackers inexperientes, eles não se limitam a somente sites, mas quando invadem, modificam toda a estrutura e deixam sua marca em busca de fama na comunidade hacker.

2.3 O QUE É ROOTKIT

É um programa que fornece acesso administrativo ao computador infectado sem que o usuário tome ciência disso. Eles podem ser instalados de diversas maneiras, incluindo meios comerciais de produtos de segurança e extensões de

aplicativos. Não tem a característica de se espalhar sozinho, em vez disso, se tornam um componente de muita ameaça.

2.4 RELAÇÃO ENTRE SOFTWARE MALICIOSO E ENGENHARIA SOCIAL

A relação entre os dois casos é simples, a engenharia social tem como objetivo enganar pessoas, fornecendo informações pessoais ou sigilosas e aplicar o golpe conseguindo seu objetivo final, já o software malicioso em sua maioria, tem o mesmo objetivo, porém não precisa de interação humana, uma vez que o golpe poderá ser aplicado apenas com a instalação de um vírus na máquina do usuário.

Em ambas as situações ocorre o crime, o que varia são os níveis de golpe, sendo um diretamente e outro indiretamente.

2.5 COMO DETECTAR SOFTWARES MALICIOSOS E COMO NOS PROTEGER?

Para detectar um software malicioso são necessários alguns comandos ou passos simples de serem feitos, como por exemplo a sequência de comandos Ctrl + Alt + Delete, ou ainda Ctrl + Shift + Esc em outras versões do Windows, ele executa o gerenciador de tarefas e mostra tudo que está consumindo processamento. É importante ficar atento aos programas de nomes confusos, como por exemplo “hkcmd.exe”, esses costumam consumir 99% do processamento da CPU ou de memória. Após a identificação é necessário que se interrompa a execução e um antivírus seja acionado para remoção do mesmo.

Quanto a proteção, ainda como maneira mais eficaz temos o software de antivírus e atualizações que seu sistema operacional libera de tempos em tempos, fazendo correção de possíveis vulnerabilidades do sistema.

2.6 CURIOSIDADES

O primeiro software malicioso foi criado por Bob Thomas. Chamado de The Creeper, este "aplicativo" mostrava uma mensagem na tela com os dizeres "Eu sou assustador, pegue-me se for capaz!". Por causa deste software, foi criado o primeiro antivírus para removê-lo, chamado de The Reaper.

Bomba Lógica, um dos mais antigos vírus já inventado foi utilizado por uma ex-funcionário de empresa Omega após sua demissão. Timothy Lloyd deixou o código bomba no sistema da empresa e conseguiu roubar 10 milhões de dólares. Lloyd foi preso e condenado a 41 meses de prisão.

3 O QUE É ENGENHARIA SOCIAL

Conforme citado no capítulo anterior, a engenharia social é a habilidade de coletar informações confidencias pessoais ou de áreas importantes de uma instituição através do poder de persuasão. Ao contrário de softwares maliciosos, não é necessário nenhum equipamento de alta tecnologia e nem grandes conhecimentos na área. O criminoso basta ter empatia, conhecer as regras de segurança de uma determinada empresa para saber seus pontos falhos para que o ataque aconteça de maneira eficiente.

3.1 CICLO DE VIDA DA ENGENHARIA SOCIAL

O ciclo de vida da engenharia social não é algo que se possa medir em prazo, uma vez que, assim que o criminoso chega em seu objetivo, a meta desse caso é dada como encerrada. Portanto, considera-se que o ciclo de vida é relativamente proporcional com o tempo de execução do golpe.

3.2 TRAÇOS COMPORTAMENTAIS HUMANOS POSSIVEIS DE EXPLORAÇÃO

Como já visto, a segurança de um software não garante que uma empresa esteja livre de ataques dos crimes cibernéticos, pois a vulnerabilidade neste caso está nos seus funcionários. Um criminoso que pratica a engenharia social em sua grande maioria são pessoas persuasivas, simpáticas, com vontade de ser útil em todas as tarefas, buscas por novas amizades e vaidade profissional. Com esses requisitos básicos, ele consegue chegar mais próximo da sua vítima atingindo seu objetivo final.

3.3 TECNICAS DA ENGENHARIA SOCIAL

Essa técnica é muito utilizada por crackers para obter acesso não autorizados em sistemas, redes ou informações com grande valor estratégico para empresas. Abaixo, segue a lista de técnicas mais utilizadas pelos engenheiros sociais:

- Analise do Lixo – Poucas empresas tem o cuidado de verificar o que está sendo descartado pela sua empresa, porém essa pratica pode salvar a

empresa de um golpe, uma vez que o lixo descartado pode conter informações de grande valia para que o crime aconteça;

- Internet e Redes sociais – Quando um engenheiro social precisa se abastecer de informações sobre uma determinada empresa, ele usa o site da mesma para iniciar seus estudos e assim poder aplicar o golpe. Ele verifica as redes sociais da empresa e dos seus funcionários, assim vai ganhando munição para que seu ataque seja mais eficiente;
- Contato Telefônico – Após o criminoso ter coletado informações via analise do lixo, e estudo dos funcionários, cargos e análise sobre o seu alvo, chega a parte de fazer contato por telefone;
- Abordagem Pessoal – Aqui, o criminoso faz uma visita na empresa alvo, nessa etapa ele pode se passar por fornecedor, cliente, amigo de pessoas com cargos altos como diretores, além de conseguir detectar a falta de preparo e treinamento dos funcionários em abordar novos alvos, ou seja, funcionários em baixo nível com grande vulnerabilidade;
- *Phishing* – Uma das técnicas mais utilizadas para conseguir acesso a rede do alvo. O criminoso envia um e-mail com sentido de aguçar curiosidade ou algum sentimento que faça com que o usuário aceite o e-mail e realize as operações solicitadas. Nos casos mais comuns, entra e-mails de banco que solicita a instalação de um plug-in para que o ambiente fique mais seguro, com isso ele consegue se infiltrar no ambiente coletando informações necessárias.

3.4 ESTRATÉGIAS DE DEFESA

Como é uma pratica mais pessoal do que tecnológica, a melhor estratégia de defesa contra-ataques de engenheiros sociais além de software de antivírus, é adotar uma cartilha de política de segurança e reforçar esse tema com seus funcionários. Importante também é fazer um encontro anual reforçando as boas práticas de segurança, reforçando a arquitetura de segurança, sensibilizar e educar para que o aumentando da segurança quanto ao vazamento de informações privilegiadas dos funcionários.

3.5 PROCEDIMENTOS EM CASO DE VIOLAÇÃO

Quando detectado uma violação as informações ou algum computador, é recomendado que a empresa ou pessoa que sofreu o ataque vá até a delegacia de crimes cibernéticos munido de todas as informações e evidências necessárias para que as investigações deem início e que as autoridades possam agir e rastrear até chegar no seu alvo.

Em caso de ataques por computador, é recomentado o rastreio do IP e bloqueio do mesmo o quanto antes, essas medidas sendo tomadas assim que identificado, diminuem os riscos de maiores complicações.

3.6 COMO PROFISSIONAIS DA SI PODEM AGIR PARA EVITAR

O antivírus ainda é o maior aliado nas empresas, mas ele por si só, não garante a segurança das informações contidas em cada departamento. É importante, além do software de antivírus, investir em boa segurança de redes, ter uma política de segurança eficaz, educar e sensibilizar seus envolvidos sobre ataques de engenharia social.

Algumas empresas têm como recurso, bloquear redes sociais achando que assim, estarão livres de ataques *phishing*, o que é um engano já que esses ataques podem vir via e-mail empresarial. Portanto, pode-se dizer que a conscientização e a educação dos funcionários quanto a segurança, em conjunto com softwares de antivírus, são os melhores aliados para prevenir os ataques.

4 CONCLUSÃO

O estudo apresenta diferentes tipos de softwares maliciosos e como eles agem. Mostra como estes aplicativos são muito perigosos caso seus alvos não tenham a mínima segurança necessária.

Muitos criminosos utilizam engenharia social, técnica de conseguir convencer pessoas, com empatia a lhes passar informações privadas.

REFERÊNCIAS

CIPOLI, Pedro. O que é engenharia Social. *Canaltech*. Disponível em: https://canaltech.com.br/seguranca/O-que-e-Engenharia-Social/. Acesso em: 26 Nov. 2017.

HOMANN, Renan. Glossário do Mal: os diferentes tipos de malware que poderiam atingir você. *Tecmundo*, 2016. Disponível em: https://www.tecmundo.com.br/seguranca/8284-glossario-do-mal-conheca-os-diferentes-tipos-de-ataque-ao-computador.htm. Acesso em: 26 Nov. 2017.

RAFAEL, Gustavo de Castro. Engenharia Social: as técnicas mais utilizadas. *Profissionais de TI*, 2013. Disponível em: https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 26 Nov. 2017.

ROCHA, Leonardo. Guia: como descobrir processos suspeitos rodando no Windows. *Tecmundo*, 2014. Disponível em: https://www.tecmundo.com.br/gerenciador-de-tarefas/54287-domine-processos-gerenciador-tarefas-do-windows-dificuldade.htm. Acesso em: 26 Nov. 2017.

ROOTKIT. *Avast*. Disponível em: https://www.avast.com/pt-br/c-rootkit. Acesso em: 26 Nov. 2017.