Laboratório de Hardware

Malwares

Definição

- Malware é um termo geral usado para definir os tipos de softwares maliciosos, que são aqueles recursos que danificam, sequestram ou tiram do ar dispositivos, redes, sites e serviços de uma empresa.
- As pessoas que distribuem malware, conhecidas como criminosos cibernéticos, são motivadas pelo dinheiro e usarão os dispositivos infectados para iniciar ataques a fim de obter credenciais bancárias, coletar informações de identificação pessoal que podem ser vendidas, vender acesso a recursos de computação ou extorquir informações de pagamento das vítimas.
- Os criminosos cibernéticos utilizam malwares para as mais diversas finalidades, mas principalmente para obter vantagens financeiras sobre a vítima que, normalmente, são empresas de portes variados ou mesmo pessoas físicas.
- Nesse sentido, os criminosos têm acesso aos dados pessoais e financeiros de uma pessoa ou organização para roubar identidade e fazer operações de compras em nome da vítima.
- Outro motivo de praticar essas ações é para roubar o controle de uma rede de computadores para realizar ataques de negação de serviço contra outros sistemas, além de infectar dispositivos para minerar moedas virtuais, etc.

Funcionamento

- O malware funciona com o emprego de truques para impedir o uso normal de um dispositivo. Depois que um criminoso cibernético obteve acesso ao seu dispositivo por meio de uma ou mais técnicas diferentes – como email de phishing, arquivo infectado, vulnerabilidade de sistema ou software, unidade flash USB infectada ou site malicioso –, ele se aproveita da situação iniciando ataques adicionais, obtendo credenciais de contas, coletando informações de identificação pessoal para vender, vendendo acesso a recursos de computação ou extorquindo pagamentos das vítimas.
- Qualquer pessoa pode ser vítima de um ataque de malware. Embora algumas pessoas possam saber detectar certas maneiras pelas quais os invasores tentam atingir as vítimas com malware, por exemplo, sabendo como identificar um email de phishing, os criminosos cibernéticos são sofisticados e estão constantemente aprimorando seus métodos para ficarem atualizados com a tecnologia e as melhorias na segurança. Os ataques de malware também são diferentes, dependendo do tipo de malware. Alguém que seja uma vítima de um ataque de rootkit, por exemplo, pode nem mesmo saber, porque esse tipo de malware é desenvolvido para passar e permanecer despercebido pelo máximo de tempo possível.

Histórico

- Nos primórdios da computação, o malware era quase inofensivo, muitas vezes criado por entusiastas para demonstrar suas habilidades ou como piadas inofensivas.
- Um exemplo famoso é o vírus ‘Creeper’, que simplesmente exibia a mensagem “I’m the creeper, catch me if you can!” em computadores infectados na década de 1970.
- Com a expansão da internet, os ataques de malware tornaram-se mais perigosos e lucrativos.
- Na década de 1990 e início dos anos 2000, vírus como o ‘ILOVEYOU’ e o ‘MyDoom‘ causaram danos globais, apagando dados de usuários e causando prejuízos financeiros significativos. Estes ataques destacaram a necessidade de soluções de segurança mais robustas.
- No entanto, o cenário de ameaças continuou a evoluir. Os ataques de ransomware, como o famoso ‘Wanna Cry’ em 2017, começaram a criptografar dados de usuários e exigir resgates para a decriptografia.
- Esses ataques não apenas afetaram indivíduos, mas também grandes organizações, levando a interrupções operacionais e perdas financeiras enormes.
- Recentemente, a tendência tem sido o uso de malware em campanhas de ciberespionagem e guerra cibernética.
- Exemplos notáveis incluem o ‘Stuxnet’, que visou infraestruturas críticas, e o SolarWinds’, que comprometeu inúmeras organizações governamentais e privadas em uma sofisticada operação de espionagem.
- Essa trajetória histórica dos ataques de malware destaca a importância da cibersegurança e a necessidade de vigilância constante.
- À medida que a tecnologia continua a avançar, também avançam as técnicas usadas por cibercriminosos, tornando a luta contra o malware um desafio contínuo para indivíduos, empresas e governos ao redor do mundo.

Tipos de Malwares

- Vírus
  - Os vírus são desenvolvidos para interferir com o funcionamento normal de um dispositivo gravando, corrompendo ou excluindo os dados. Muitas vezes, eles se espalham para outros dispositivos enganando as pessoas para que abram arquivos nocivos.
- Worms
  - Em grande parte encontrados em anexos de email, mensagens de texto, programas de compartilhamento de arquivos, sites de redes sociais, compartilhamentos de rede e unidades removíveis, um worm se espalha por uma rede explorando vulnerabilidades de segurança e se copiando. Dependendo do tipo de worm, ele pode roubar informações confidenciais, mudar suas configurações de segurança ou impedir que você acesse arquivos.
- Trojans
  - O cavalo de troia conta com um usuário que faça seu download inadvertidamente porque ele parece ser um aplicativo ou arquivo legítimo. Após baixado, ele pode:
    - Baixar e instalar malware adicional, como vírus ou worms.
    - Usar o dispositivo infectado para fraude por clique.
    - Registrar os pressionamentos de tecla e sites que você visita.
    - Enviar informações (por exemplo, senhas, detalhes de login e histórico de navegação) sobre o dispositivo infectado a um hacker mal-intencionado.
    - Dar a um criminoso cibernético controle de um dispositivo infectado.

Tipos de Malwares

- Spyware
  - O spyware se instala em um dispositivo sem fornecer aviso adequado ou sem o consentimento da pessoa. Depois de instalado, ele pode monitorar o comportamento online, coletar informações confidenciais, alterar as configurações do dispositivo e diminuir o desempenho do dispositivo.
- Adware
  - Como o spyware, o adware se instala em um dispositivo sem o consentimento da pessoa. Mas, no caso do adware, o foco é exibir publicidade agressiva, muitas vezes em formato pop-up, para ganhar dinheiro com cliques. Esses anúncios frequentemente prejudicam o desempenho do dispositivo, deixando-o lento. Os tipos mais perigosos de adware também podem instalar software adicional, alterar as configurações do navegador e deixar o dispositivo vulnerável a outros ataques de malware.
- Software indesejado
  - Quando um dispositivo tem um software indesejado, o usuário pode experimentar uma experiência de navegação na web modificada, controle alterado de downloads e instalações, mensagens enganosas e mudanças não autorizadas nas configurações do dispositivo. Alguns softwares indesejados são colocados no mesmo pacote de outros softwares que as pessoas pretendem baixar.

Tipos de Malwares

- Malware sem arquivo
  - Esse tipo de ataque cibernético amplamente descreve aquele malware que não precisa de arquivos, como um anexo de email infectado, para violar uma rede. Por exemplo, ele pode chegar por meio de pacotes de rede mal-intencionados que exploram uma vulnerabilidade e depois instalam o malware que reside apenas na memória do kernel. Ameaças sem arquivos são especialmente difíceis de descobrir e remover porque a maioria dos programa antivírus não é desenvolvida para verificar firmware.
- Malware de macro
  - Macros são maneiras de automatizar rapidamente tarefas comuns. O malware de macro se aproveita dessa funcionalidade infectando anexos de email e arquivos ZIP. Para enganar pessoas para que abram os arquivos, os criminosos cibernéticos muitas vezes ocultam o malware em arquivos disfarçados como faturas, recibos e documentos legais. Antigamente, o malware de macro era mais comum porque as macros eram executadas automaticamente quando um documento era aberto. Mas, em versões recentes do Microsoft Office, as macros são desabilitadas por padrão, o que significa que os criminosos cibernéticos que infectam dispositivos dessa maneira precisam convencer os usuários a ativar as macros.
- Golpes de suporte técnico (Scams)
  - Problema enfrentado por todo o setor, os scams de suporte técnico usam táticas alarmistas para levar os usuários a pagarem por serviços desnecessários de suporte técnico que podem ter sido propagandeados como sendo a solução de um problema falso relacionado a um dispositivo, plataforma ou software. Com esse tipo de malware, um criminoso cibernético pode ligar diretamente para alguém fingindo ser um funcionário de uma empresa de software. Após ter ganhado a confiança da pessoa, o invasor muitas vezes estimula a vítima em potencial a instalar aplicativos ou dar acesso remoto a seus dispositivos.

Tipos de Malwares

- Kits de exploits e exploits
  - Os exploits usam as vulnerabilidades do software para ignorar as proteções de segurança de um computador a fim de infectar um dispositivo. Hackers mal-intencionados examinam sistemas desatualizados que contenham vulnerabilidades críticas e os exploram implantando malware. Ao incluir shellcode em um exploit, os criminosos cibernéticos podem baixar mais malware que infecta dispositivos e se infiltra nas organizações.
  - Os kits de exploits contêm uma coleção de exploits que examinam diferentes tipos de vulnerabilidades de software. Se alguma for detectada, os kits implantam um malware adicional. O software que pode estar infectado inclui Adobe Flash Player, Adobe Reader, navegadores da Web, Oracle Java e Sun Java. Angler/Axpergle, Neutrino e Nuclear são alguns tipos de kits de exploits comuns.
  - Os exploits e kits de exploits normalmente contam com sites mal-intencionados ou anexos de email para violar uma rede ou um dispositivo, mas, às vezes, eles também se escondem em anúncios de sites legítimos sem que o site saiba.
- Rootkits
  - Quando um criminoso cibernético usa um rootkit, ele oculta malware em um dispositivo pelo máximo de tempo possível, às vezes até por anos, para que roube informações e recursos de modo contínuo. Ao interceptar e alterar os processos padrão do sistema operacional, um rootkit pode alterar as informações que seu dispositivo reporta sobre o sistema. Por exemplo, um dispositivo infectado com um rootkit pode não mostrar uma lista precisa dos programas que estão em execução. Os rootkits também podem dar privilégios administrativos ou elevados de dispositivos a criminosos cibernéticos, para que eles possam controlar por completo um dispositivo e executar ações potencialmente mal-intencionadas, como roubar dados, espionar a vítima e instalar malware adicional.

Tipos de Malwares

- Mineradores de criptomoeda
  - Com o aumento da popularidade das criptomoedas, a mineração de criptomoedas se tornou uma prática lucrativa. Os mineradores usam os recursos de computação de um dispositivo para minerar criptomoedas. As infecções desse tipo de malware muitas vezes começam com um anexo de email que tenta instalar malware ou um site que usa vulnerabilidades em navegadores da web ou se aproveita do poder de processamento do computador para adicionar malware aos dispositivos.
  - Usando cálculos matemáticos complexos, os mineradores fazem a manutenção do livro-razão da blockchain para roubar recursos de computação que permitem a eles criar novas criptomoedas. A mineração de criptomoedas usa um poder de processamento significativo do computador, no entanto, para roubar quantias relativamente pequenas de criptomoedas. Por essa razão, os criminosos cibernéticos muitas vezes trabalham em equipes para maximizar e dividir os lucros.
  - Apesar disso, nem todos os mineradores de criptomoedas são criminosos. Pessoas e organizações às vezes adquirem potência eletrônica e de hardware para uma mineração legítima. O ato se torna criminoso quando um criminoso cibernético se infiltra em uma rede corporativa furtivamente a fim de usar o poder de computação dessa rede para minerar.

Tipos de Malwares

- Ransomware
  - Ransomware é um tipo de malware que ameaça a vítima destruindo ou bloqueando o acesso a dados críticos até que um resgate seja pago. Os ataques de ransomware operados por humanos visam atacar uma organização por meio de configurações incorretas comuns de sistema e segurança que se infiltram na organização, navegam em sua rede corporativa e se adaptam ao ambiente e a quaisquer pontos fracos. Um método comum de obtenção de acesso à rede de uma organização para distribuir ransomware é por meio do roubo de credencial, em que um criminoso cibernético poderia roubar as credenciais de um funcionário real para se passar por ele e obter acesso às suas contas.
  - Os invasores que usam ransomware operado por humanos atingem organizações grandes porque elas podem pagar um resgate maior do que o indivíduo médio — muitas vezes milhões de dólares. Devido aos altos riscos envolvidos em uma violação dessa escala, muitas organizações optam por pagar o resgate, em vez de ter seus dados confidenciais vazados ou arriscar novos ataques dos criminosos cibernéticos, mesmo que o pagamento não garanta a prevenção de nenhum dos resultados.
  - Conforme os ataques de ransomware operados por humanos crescem, os criminosos por trás dos ataques ficam mais organizados. Na verdade, muitas operações de ransomware agora usam um modelo de Ransomware como Serviço, o que significa que um conjunto de desenvolvedores criminosos cria o próprio ransomware e contrata outros criminosos cibernéticos para hackear a rede de uma organização e instalar o ransomware, dividindo os lucros entre os dois grupos a uma taxa acordada.

Tipos de Malwares

- Backdoor
  - Backdoor (em português, "porta dos fundos") é um método, geralmente secreto, de escapar de uma autenticação ou criptografia normais em um sistema computacional, produto ou dispositivo embarcado (por exemplo, um roteador doméstico), ou sua incorporação, por exemplo, como parte de um sistema criptográfico, um algoritmo ou um chipset.
  - Os backdoors costumam ser usados para proteger o acesso remoto a um computador ou obter acesso a texto simples em sistemas criptográficos.
  - Um backdoor pode assumir a forma de uma parte oculta de um programa, um programa separado (por exemplo, o Back Orifice pode subverter o sistema através de um rootkit), um código no firmware do hardware ou partes de um sistema operacional, como o Microsoft Windows.
  - Cavalos de Troia podem ser usados para criar vulnerabilidades em um dispositivo. Um destes pode parecer um programa inteiramente legítimo, mas quando executado, ele executa uma atividade que pode instalar um backdoor.
  - Embora alguns sejam secretamente instalados, outros backdoors são deliberadamente e amplamente conhecidos. Esses tipos têm usos "legítimos", como fornecer ao fabricante uma maneira de restaurar as senhas dos usuários. O backdoor pode ser usado para obter acesso a senhas, excluir dados em discos rígidos ou transferir informações dentro da nuvem.
  - Muitos sistemas que armazenam informações dentro da nuvem não conseguem criar medidas de segurança precisas. Se muitos sistemas estiverem conectados na nuvem, os hackers podem obter acesso a todas as outras plataformas através do sistema mais vulnerável.

Engenharia Social

- Engenharia social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor. No crime cibernético, esses golpes de "hacking humano" tendem a atrair usuários desavisados para expor dados, espalhar infecções por malware ou dar acesso a sistemas restritos. Os ataques podem acontecer on-line, em pessoa e por outros meios de interação.
- Os golpes promovidos com base em engenharia social são feitos a partir de como as pessoas pensam e agem. Sendo assim, os ataques de engenharia social são especialmente úteis para manipular o comportamento de um usuário. Quando um invasor entende o que motiva as ações de um usuário, ele pode enganar e manipular o usuário de forma eficaz.
- Além disso, os hackers tentam explorar a falta de conhecimento do usuário. Graças à velocidade da tecnologia, muitos consumidores e funcionários não reconhecem certas ameaças como os downloads automáticos. Os usuários podem também não perceber a verdadeiro valor dos dados pessoais, como o seu número do telefone, por exemplo. Por isso, muitos usuários não sabem exatamente como proteger a si mesmo e seus dados.
- Em geral, os invasores de engenharia social têm um dos seguintes objetivos:
  - Sabotagem: interrupção ou corrupção de dados para causar danos ou incômodos.
  - Roubo: obtenção de objetos de valor, como informações, acesso ou dinheiro.

Engenharia Social - Funcionamento

- A maioria dos ataques de engenharia social depende da comunicação real entre os atacantes e as vítimas. O invasor tende a motivar o usuário a se comprometer, em vez de usar métodos de força bruta para violar seus dados.
- O ciclo de ataque oferece a esses criminosos um processo confiável para enganar você. Os passos para o ciclo de ataque de engenharia social geralmente são os seguintes:
  1. Preparar reunindo informações sobre seu histórico ou de um grupo maior do qual você faz parte.
  2. Infiltrar-se estabelecendo um relacionamento ou iniciando uma interação, que começa pela construção de confiança.
  3. Explorar a vítima uma vez que a confiança e uma vulnerabilidade sejam estabelecidas para avançar com o ataque.
  4. Desvincular-se assim que o usuário tiver realizado a ação desejada.
- Esse processo pode ocorrer em um único e-mail ou ao longo de meses, em uma série de conversas nas redes sociais. Poderia até ser uma interação cara a cara. Mas, no fim das contas, tudo acaba em uma ação que você realiza, como compartilhar suas informações ou se expor a malwares.
- É importante ter cuidado com a engenharia social usada para confundir as pessoas. Muitos funcionários e consumidores não percebem que apenas algumas peças de informação podem dar acesso a hackers a várias redes e contas.
- Ao se passarem por usuários legítimos para os funcionários de suporte de TI, eles obtêm seus dados privados — como nome, data de nascimento ou endereço. A partir daí, é só uma questão de redefinir senhas e obter acesso praticamente ilimitado. Podem roubar dinheiro, espalhar malware de engenharia social e muito mais.

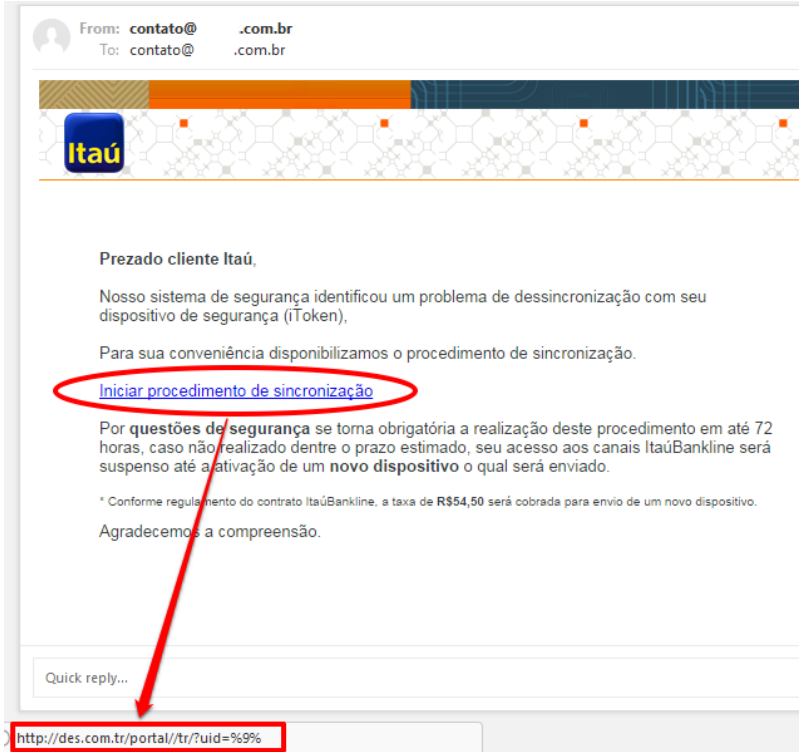
Engenharia Social - Phishing

- Um ataque de phishing se apresenta como uma fonte confiável a fim de roubar informações confidenciais por meio de emails, sites, mensagens de texto ou outras formas de comunicação eletrônica. Esses ataques fornecem um mecanismo de entrega para o malware. Ataques comuns roubam nomes de usuários, senhas, detalhes de cartão de crédito e informações bancárias. Esses tipos de ataques de malware podem levar a roubo de identidade ou de dinheiro diretamente a partir da conta bancária ou do cartão de crédito pessoal de alguém.
- Por exemplo, um criminoso cibernético pode se passar por um banco conhecido e enviar um email alertando alguém de que sua conta foi congelada devido a atividades suspeitas, pedindo que clique em um link no email para resolver o problema. Quando a pessoa clica no link, o malware é instalado.
- Os golpistas do phishing fingem ser uma instituição ou um indivíduo confiável na tentativa de persuadi-lo a expor dados pessoais e outros bens valiosos.
- Os ataques que utilizam o phishing são direcionados de duas maneiras:
    1. O spam de phishing, ou phishing em massa, é um ataque generalizado dirigido a muitos usuários. Esses ataques não são personalizados e tentam pegar qualquer pessoa desprevenida.
    2. O spear phishing e, por extensão, o whaling, utilizam informações personalizadas para direcionar usuários específicos. Os ataques de whaling visam especificamente alvos de alto valor, como celebridades, altos executivos e autoridades governamentais.
- Seja por meio de uma comunicação direta ou um formulário de um site falso, qualquer coisa que compartilhada vai diretamente para o bolso de um golpista. O usuário pode até ser enganado e baixar um malware contendo a próxima etapa do ataque de phishing

Engenharia Social - Phishing

- As chamadas telefônicas de phishing de voz (vishing) podem ser sistemas de mensagens automatizadas que gravam todas as suas entradas. Às vezes, uma pessoa ao vivo pode falar com você para aumentar a confiança e urgência.
- Textos de phishing por SMS (smishing) ou mensagens de aplicativos móveis podem incluir um link da web ou uma solicitação para seguir através de um e-mail fraudulento ou número de telefone.
- O phishing por e-mail é o meio mais tradicional de phishing, utilizando um e-mail urgente solicitando a sua resposta ou acompanhamento por outros meios. Links da web, números de telefone ou anexos de malware podem ser utilizados.
- O angler phishing ocorre nas redes sociais, onde um atacante imita a equipe de atendimento ao cliente de uma empresa confiável. Eles interceptam suas comunicações com uma marca para sequestrar e desviar sua conversa para mensagens privadas, onde então avançam com o golpe.
- Phishing de buscador é uma tentativa de colocar links para sites falsos no topo dos resultados da busca. Esses podem ser anúncios pagos ou usar métodos legítimos de otimização para manipular os rankings de busca.
- Links de phishing de URL tentam você a visitar sites de phishing. Esses links são comumente entregues em e-mails, mensagens de texto de redes sociais e anúncios online. Os ataques escondem links em textos ou botões de hiperlink, utilizando ferramentas de encurtamento de links ou URLs com grafias enganosas.
- O phishing em sessão aparece como uma interrupção na sua navegação normal na web. Por exemplo, você pode ver pop-ups de login falsos para as páginas que você está visitando no momento.

Engenharia Social - Phishing



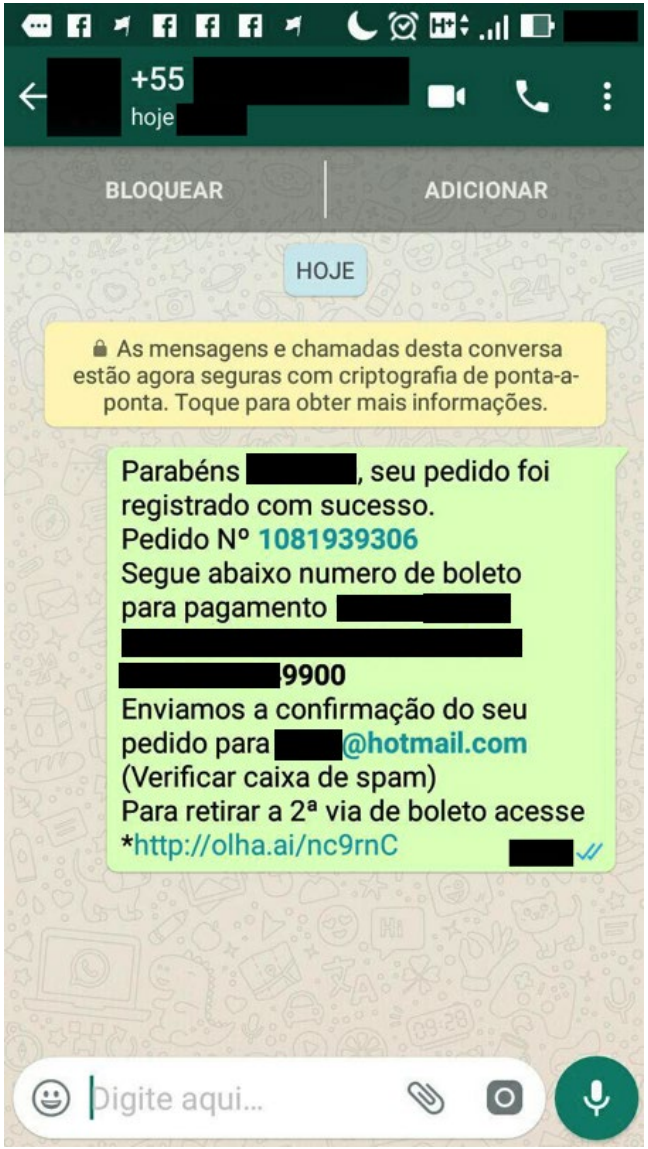
Engenharia Social - Baiting

- O baiting abusa de sua curiosidade natural para o convencer a se expor a um agressor. Tipicamente, o potencial de receber algo gratuito ou exclusivo é usado para manipulá-lo e explorá-lo. O golpe normalmente consiste em infectar você com malware.
- Os métodos populares de baiting podem incluir:
  - Pen drives deixados em espaços públicos, como bibliotecas e estacionamentos.
  - Anexos de e-mail incluindo detalhes sobre uma oferta gratuita ou software gratuito fraudulento.
  - Promoções falsas em redes sociais

Engenharia Social - Baiting

- O baiting abusa de sua curiosidade natural para o convencer a se expor a um agressor. Tipicamente, o potencial de receber algo gratuito ou exclusivo é usado para manipulá-lo e explorá-lo. O golpe normalmente consiste em infectar você com malware.
- Os métodos populares de baiting podem incluir:
  - Pen drives deixados em espaços públicos, como bibliotecas e estacionamentos.
  - Anexos de e-mail incluindo detalhes sobre uma oferta gratuita ou software gratuito fraudulento.
  - Promoções falsas em redes sociais

Engenharia Social - Baiting



Naomi Surugaba [azlin@moa.gov.my]

Actions

Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Antimalware - Antivirus

- O antivírus é um software que identifica e protege os dispositivos de malwares, também conhecidos como vírus. Esse programa pode ser instalado em computadores e dispositivos móveis, como celulares e tablets.
- A função mais simples de um antivírus é monitorar arquivos e outros programas de um dispositivo para detectar vírus. Quando novas aplicações são instaladas, o programa faz a verificação delas para saber se existe alguma ação suspeita. Se algo foi identificado, a instalação é bloqueada ou a nova aplicação é encaminhada para a quarentena.
- A quarentena é um espaço de proteção criptografado e gerenciado pelo antivírus, para que o possível vírus não se espalhe pelo sistema operacional do dispositivo. Arquivos e programas são encaminhados para a quarentena quando o antivírus ainda não identificou exatamente o tipo de vírus ou problema apresentado.
- Alguns antivírus podem ser específicos para um determinado tipo de vírus, como os antispywares, que são focados em combater spywares e adwares — dois tipos que contaminam navegadores para roubar dados bancários e apresentar banners indesejados.
- De modo geral, os programas devem se adaptar às necessidades de diferentes usuários. Por isso, uma versão para computador doméstico não funciona corretamente em um servidor de empresa. Nesse caso, é preciso ir atrás de uma versão corporativa do antivírus escolhido.
- Relatório de testes de antimalwares (AV-Comparatives.org)

Análise Heurística

- A análise heurística é um método de detecção de vírus que examina se há propriedades suspeitas no código
- Os métodos tradicionais de detecção de vírus envolvem a identificação de malware comparando o código de um programa com o código de tipos de vírus conhecidos que já foram encontrados, analisadose registrados em um banco de dados, o que é conhecido como detecção de assinaturas.
- Embora seja útil e ainda esteja em uso, o método de detecção de assinaturas também tornou-se mais limitado com o desenvolvimento das novas ameaças que se proliferaram.
- Para conter esse problema, o modelo heurístico foi projetado especificamente para identificar características suspeitas encontradas em vírus novos desconhecidos e versões modificadas de ameaças existentes, bem como amostras de malware conhecidas.
- Os criminosos virtuais estão desenvolvendo novas ameaças constantemente, e a análise heurística é um dos únicos métodos utilizados para lidar com o enorme volume dessas novas ameaças observadas diariamente.
- A análise heurística também é um dos poucos métodos capazes de combater vírus polimórficos (como são chamados os códigos maliciosos que mudam e se adaptam continuamente). A análise heurística é incorporada a soluções avançadas de segurança para detectar novas ameaças antes que possam causar danos, sem a necessidade de uma assinatura específica.

Análise Heurística - Funcionamento

- A análise heurística pode empregar várias técnicas diferentes. Um método heurístico, conhecido como análise heurística estática, envolve a descompilação de um programa suspeito e a análise de seu código fonte. Esse código é então comparado com vírus já conhecidos e que estão no banco de dados heurístico. Se uma porcentagem específica do código fonte corresponder a qualquer item no banco de dados heurístico, o código é sinalizado como uma possível ameaça.
- Outro método conhecido é a heurística dinâmica. Quando os cientistas querem analisar algo suspeito sem pôr as pessoas em perigo, eles mantém a substância em um ambiente controlado, como um laboratório seguro, e realizam testes. O processo de análise heurística é semelhante, mas em um mundo virtual.
- Ele isola o programa suspeito ou parte do código dentro de uma máquina virtual especializada, ou Sandbox, e dá ao programa antivírus a chance de testar o código e simular o que aconteceria se o arquivo suspeito pudesse ser executado. Ele examina cada comando à medida que é ativado e procura qualquer comportamento suspeito, como autorreplicação, substituição de arquivos e outras ações comuns aos vírus.