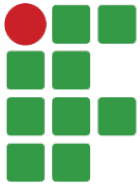
Códigos (não apenas) Maliciosos

Segurança Computacional

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau

Malware

- ***Malicious software*** ou código malicioso.
- Não é sinônimo de **vírus**, embora seja frequentemente tratado como se fosse.
  - Todo vírus é um *malware*
  - Nem todo *malware* é um vírus
- Códigos maliciosos variam quanto
  - à natureza
  - às características de replicação
  - à necessidade de execução do usuário
  - à necessidade de pagamento do usuário
  - ...

Malware

Marca de roupas Guess sofre vazamento de dados após ransomware

13/07/2021 às 14:00 • 1 min de leitura

Nilton Kleina
via nexperts

0 Compartilharam 0 Comentários

A marca de vestuário e dona de rede de lojas Guest começou a entrar em contato com consumidores que podem ter sido vítimas de um vazamento de dados. A companhia foi vítima de um ransomware em fevereiro de 2021 e, após investigações, detectou vulnerabilidades que podem ou não envolver roubo e uso de informações pessoais de clientes.

A rede de lojas da Guest envolve 1.041 unidades espalhadas pelo mundo, mas apenas 1,3 mil pessoas foram afetadas pelo vazamento. Detalhes como o número do Social Security (o equivalente nos Estados Unidos ao nosso RG), carteira de habilitação, passaporte e até dados bancários ficaram expostos a cibercriminosos — sendo que estes são os mais preocupantes, já que podem incluir detalhes completos de cartões de crédito.

Fonte: `https://www.tecmundo.com.br/seguranca/220950-marca-roupas-guess-sofre-vazamento-dados-ransomware.htm`

Malware

Fonte: `https://www.cnnbrasil.com.br/business/2021/07/03/novo-ataque-de-ransomware-tem-como-alvo-principal-fornecedor-de-ti-dos-eua`

Malware

Novo malware evasivo rouba dados e apaga seu HD se você tentar detectá-lo

48.003 Visualizações
Por Leonardo Rocha
05 mai 2015 - 12h 45

Um grupo de pesquisadores do Talos Group da Cisco Systems descobriu a existência de um novo tipo de malware que é capaz de tomar medidas impressionantes para evitar processos de detecção e análise. Entre as ações mais desesperadas de que o software nocivo é capaz está deletar todos os dados do seu disco rígido e, dessa forma, deixar seu computador inoperável.

Nomeado Rombertik pelos cientistas, o malware é um programa complexo que indiscriminadamente coleta

ataforma-mo...

o que o usuário da máquina infectada faz na internet, com o provável

Malware

Governo de Atlanta segue com computadores bloqueados por ransomware

Por Patrícia Gnipper | 02 de Abril de 2018 às 12h02

Há quase duas semanas os computadores do governo da cidade norte-americana de Atlanta permanecem sequestrados por cibercriminosos. São pelo menos 13 os departamentos afetados, e a cidade está tentando funcionar do jeito antigo, registrando processos em papel, já que não podem contar com os sistemas para tal.

O ransomware SamSam exige o pagamento de US$ 51 mil para a liberação das máquinas, mas o governo local já havia afirmado que não pagaria o resgate, buscando outras maneiras de reviver suas máquinas. Alguns computadores já voltaram a ser usados, mas vários outros seguem bloqueados. Por conta disso, alguns funcionários estão dividindo laptops durante o final de semana, na tentativa de reconstruir alguns documentos perdidos.

Entre os arquivos corrompidos, foram encontrados alguns contendo tags adicionadas aos títulos, como, por exemplo, "weapologize" ("pedimos desculpas", em português), ou ainda "imsorry" ("sinto muito"). O problema se agrava porque é possível que os servidores de backup também tenham sido afetados, ainda que as autoridades municipais não tenham revelado essa informação de maneira clara.

O SamSam é especialista em descobrir e explorar vulnerabilidades de sistemas, adivinhando senhas consideradas fracas para concluir sua invasão. Ao ter a palavra-passe "em mãos", o ransomware usa ferramentas de recuperação de senhas para conseguir controlar o restante da rede. Dessa maneira, os criminosos não precisam efetivamente invadir a infraestrutura, deixando todo o trabalho para o ransomware.

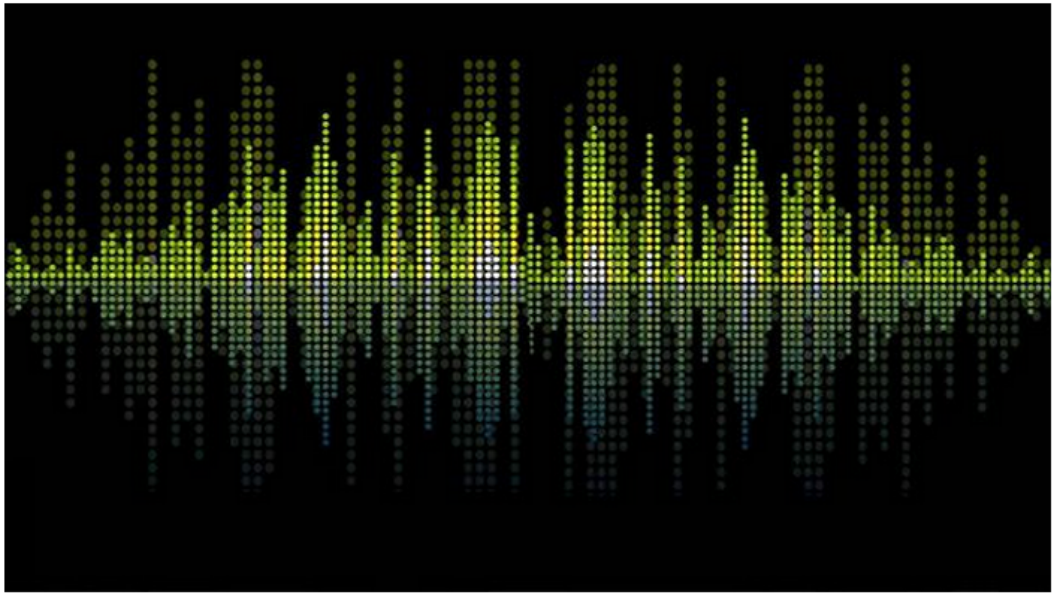
Fonte: `https://canaltech.com.br/seguranca/governo-de-atlanta-segue-com-computadores-bloqueados-por-ransomware-111012/`

Malware

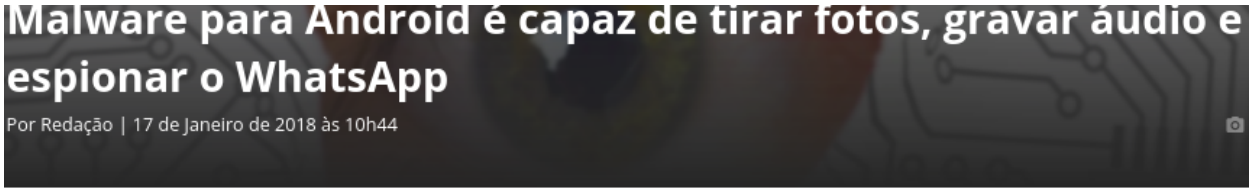
CIENTISTAS CRIAM MALWARE QUE SE PROPAGA PELO SOM

SEGURANÇA FLÁVIO CROFFI @ 3 DEZ 2013 | 12:35 PM

Cientistas do **Instituto Fraunhofer de Comunicação** desenvolveram um novo conceito de malware que se propaga pelo som. Ele pode se comunicar com máquinas próximas apenas utilizando as caixas de som ou microfones dos computadores.



Malware



Malware para Android é capaz de tirar fotos, gravar áudio e espionar o WhatsApp

Por Redação | 17 de Janeiro de 2018 às 10h44

Um "espião mobile no estilo de Hollywood". É com essas palavras que a Kaspersky Labs, uma das principais empresas de segurança da informação do mundo, abre sua revelação sobre o Skygofree, citado como um dos malwares mais sofisticados já desenvolvidos para o Android, capaz de uma série de operações que vão desde capturar as mensagens do WhatsApp até tirar fotos ou gravar áudio sem a autorização do usuário.

Infectando celulares a partir de páginas maliciosas, que se passam pelos domínios legítimos de operadoras de telefonia, o Skygofree se instala no smartphone sem a anuência dos usuários, assumindo privilégios administrativos e abrindo o caminho para a realização de suas operações. Na sequência, executa a programação configurada por seu controlador remoto, realizando uma ou várias ações, de acordo com o ordenado.

E é justamente aqui que entra o que chamou a atenção dos especialistas da Kaspersky, com o rol de ferramentas do Skygofree sendo altamente avançado. Em uma de suas ferramentas mais sofisticadas, o malware é capaz de ativar a gravação de áudio, tirar fotos ou capturar vídeos de acordo com dados de geolocalização. Basicamente, é possível espionar os usuários de acordo com o lugar em que eles estão.

Nesse mesmo quesito, o smartphone infectado também pode ser ordenado a se conectar a uma rede sem fio sob controle de hackers, mais uma vez sem a autorização do usuário. A partir daí todos os dados trocados entre o aparelho e a rede podem ser interceptados, mesmo que sigam de maneira criptografada, aumentando ainda mais as capacidades da praga.

Fonte: `https://canaltech.com.br/android/malware-para-android-e-capaz-de-tirar-fotos-gravar-audio-e-espionar-o-whatsapp-106718/`

Malware

Figura: G DATA Mobile Malware Report. Fonte: `https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_Mobile_Malware_Report_H1_2016_EN.pdf`

Malware

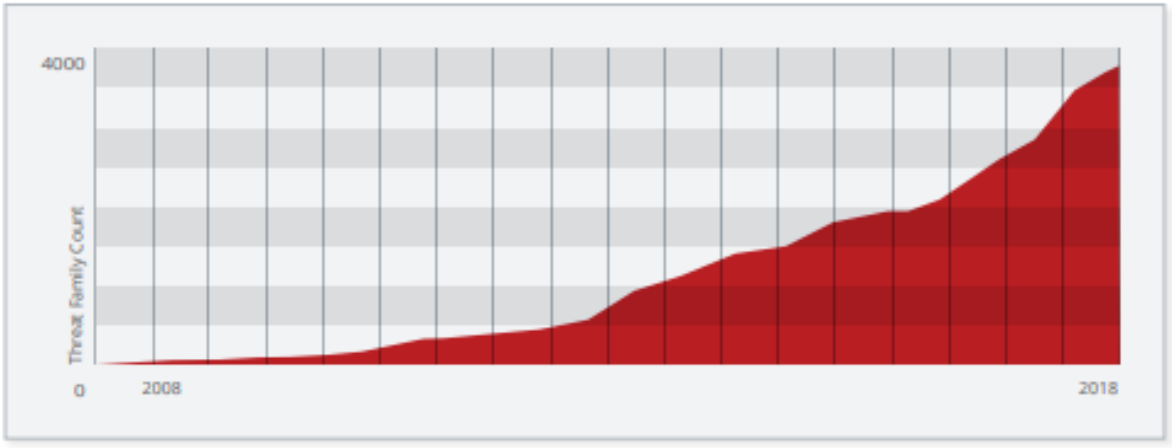


Figure 7. There are more than 4,000 mobile threat families and variants in the McAfee sample database today.

Figura: Gráfico da base de dados da McAfee. Fonte: `https://www.mcafee.com/br/resources/reports/rp-mobile-threat-report-2018.pdf`

Malware

- O *malware* realiza algum tipo de ação indesejada pelo usuário.
  - Rouba dados
  - Exibe propagandas
  - Consome recursos
  - Abre portas
  - Altera/exclui arquivos
  - Executa/altera/mata processos
- Há outro termo utilizado, denominado *maldoc*, que define documentos maliciosos, tais como arquivos .DOC e .PPT. Essa distinção (maldoc/malware) faz diferença para analistas de malware definirem o tipo de análise a ser realizada no(s) arquivo(s).

Malware

Como eles agem?

- Explorando vulnerabilidades de programas
- Por autoexecução de dispositivos, como pendrives
- Por acesso a *websites* maliciosos, utilizando navegadores vulneráveis
- Por ação direta de atacantes (invasores)
- Por execução de arquivos previamente infectados, obtidos em anexos de e-mails, via mídias removíveis, em *websites* ou diretamente de outros computadores (através de compartilhamento de recursos).

Malware

O que leva alguém a desenvolver um malware?

- Vantagens financeiras
  - Monetização por acesso a *website*
  - Venda de dados
  - Divulgação de produtos
  - Mineração de criptomoeda
- Vandalismo
- Satisfação pessoal

Malware

Vírus

tec

Maior | Menor Enviar por e-mail Comunicar erros Link http://www1.folha.uol.c

15/06/2004 - 10h22

Grupo desenvolve primeiro vírus que afeta celulares

da **Folha Online**

PUBLICIDADE

Um grupo de hackers escreveu um vírus que ataca os telefones celulares equipados com o sistema operacional Symbian, usado em aparelhos compatíveis com a tecnologia GSM. Algumas das empresas que usam o Symbian em seus telefones são a Nokia, Sony Ericsson, Siemens, FOMA, Motorola, Samsung, Panasonic e Benq. O vírus foi enviado para empresas que desenvolvem soluções antivírus, mas não chegou a ser espalhado para outros aparelhos.

A praga digital foi batizada de Cabir e é o primeiro vírus a atacar celulares, de acordo com a Kaspersky Labs, que desenvolve soluções de segurança. O Cabir foi escrito pelo "29a", um grupo de programadores que escrevem "vírus conceituais" --isto é, eles escrevem as pragas apenas para mostrar que é possível atacar um determinado sistema operacional ou explorar uma falha de um programa.

O "29a" é responsável por ter escrito os primeiros vírus para a plataforma .NET e para a versão de 64 bits do sistema operacional Windows, que nem chegou a ser lançado, informou o site "The Register" (www.theregister.co.uk).

Bluetooth

O Cabir se transfere como um SIS (arquivo de distribuição do Symbian), mas se disfarça como um aplicativo de segurança. Ele usa a tecnologia Bluetooth para localizar outros aparelhos equipados com o sistema operacional Symbian e se enviar automaticamente. O vírus, entretanto, não tem código destrutivo: sua função é se espalhar para outros celulares.

Para que um celular seja contaminado, o dono do telefone precisa confirmar o recebimento do arquivo e permitir sua instalação. A técnica desenvolvida pelo grupo "29a" tem justamente o objetivo de burlar essa

Malware

Vírus

- **Vírus** é um programa que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.
  - Assim como um vírus biológico, não pode se reproduzir sem uma célula hospedeira (programa ou arquivo).
- É um *malware* que **depende da execução do programa infectado** para se tornar ativo.
- Bastante propagado por e-mails, pendrives e *download* de programas não confiáveis.

Malware

Vírus

Vírus de pendrive impossível de ser removido tem código publicado na web

84.958 Visualizações
Por **Leonardo Müller**
02 out 2014 - 18h 27

Não é novidade para ninguém que pendrives podem propagar vírus de um PC para o outro com certa facilidade. Acontece que uma nova ameaça chamada BadUSB está prestes a mudar essa situação. Esse código consegue infectar o firmware de pendrives e, até o momento, não há nenhum procedimento eficaz para removê-lo de lá.

Como se isso não fosse problema suficiente, o BadUSB teve seu código publicado no GitHub. Com isso, qualquer pessoa que souber como usá-lo, poderá infectar milhões de pendrives e usá-los para atacar computadores de diversas

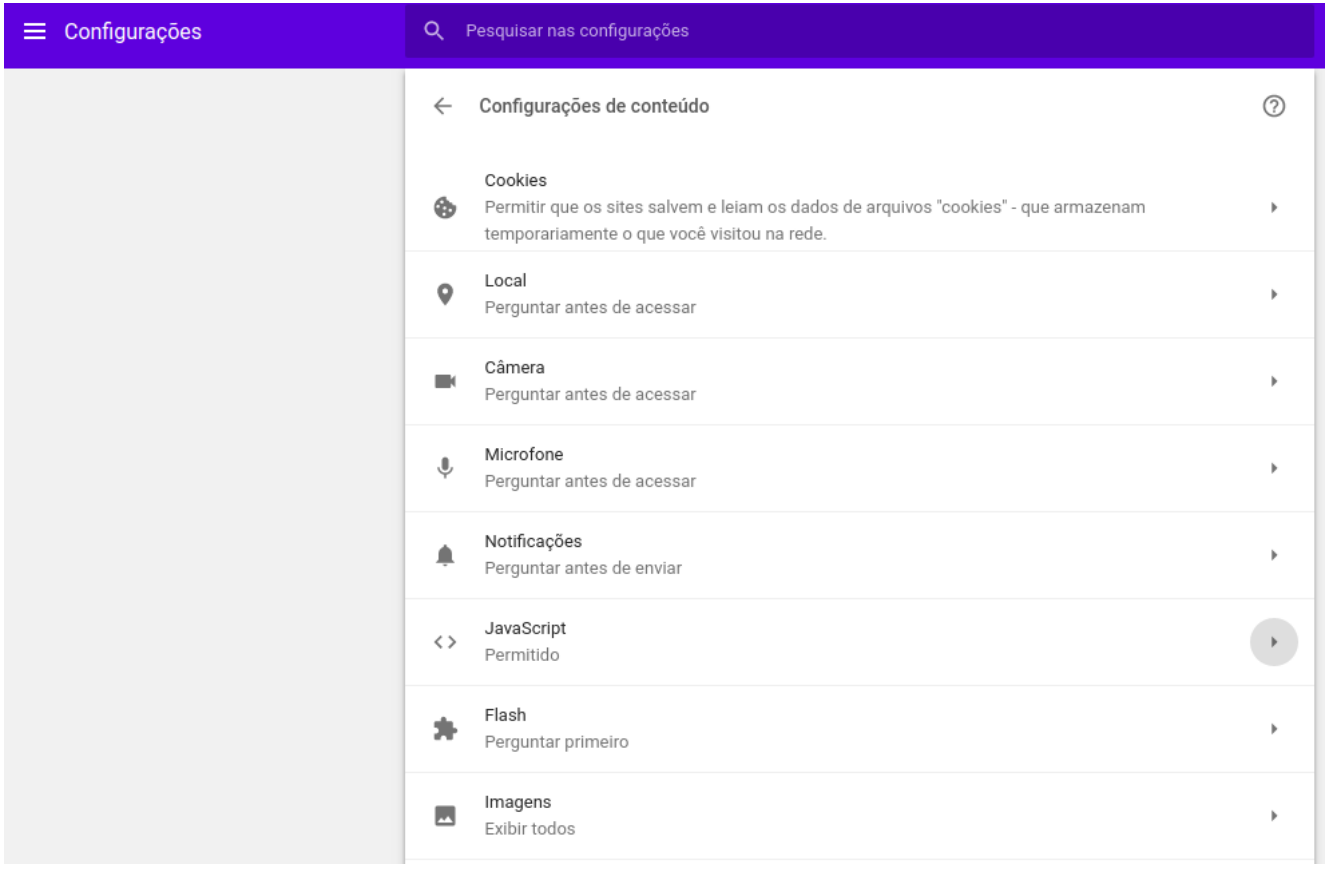
Malware

Vírus

- Há diferentes tipos de vírus:
- **Vírus propagado por e-mail**: arquivo anexo em e-mails. Quando executado, infecta arquivos e programas e envia cópias de si mesmo para os contatos.
- **Vírus de *script***: escrito em linguagem de *script*, é recebido ao acessar um *website* ou por e-mail, como um arquivo anexo ou como parte do e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador e do programa leitor de e-mails do usuario.

Malware

Vírus



Malware

Vírus

- **Vírus de macro**: tipo de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem, como os que compõem o Microsoft Office (Excel, Word e PowerPoint, entre outros).

- **Vírus de celular**: propaga-se entre celulares por bluetooth ou mensagens MMS (*Multimedia Message Service*). A infecção se dá quando um usuário permite o recebimento de um arquivo infectado e o executa. O vírus pode destruir ou alterar arquivos, remover contatos, efetuar ligações e drenar a carga da bateria, além de tentar se propagar para outros celulares.

Malware

Worm

- ***Worm***: programa que se replica automaticamente pela rede.
- Diferente do vírus, o *worm* nao se propaga por inclusão de cópias de si mesmo em outros programas ou arquivos, mas pela execução direta de suas cópias ou exploração automática de vulnerabilidades de programas instalados no computador.
- São responsáveis por consumir recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar, afetando o desempenho de redes e computadores.

Malware

Worm

- Ao infectar um computador, procura os próximos alvos.
- Depois, envia as cópias
  - Por e-mail
  - Por pasta compartilhada
  - Programas de bate-papo
  - ...
- Depois, é executado. Diretamente pela vítima ou por algum evento.
- Recomeça o ciclo.

Malware

Worm

notícias / vírus

Primeiro worm brasileiro ataca usuário do Facebook

Tipo de vírus se espalha via chat do site de relacionamentos

por Redação Galileu

O worns de redes sociais são um tipo de programa que rouba credenciais de acesso de usuários e tenta se espalhar por seus contatos via chat. Esse tipo de vírus era comum no MSN e Orkut entre usuários brasileiros. Com a popularização do Facebook no País, os ataques começaram mirar essa rede. A fabricante de antivírus Kaspersky acabou de identificar o primeiro worn brasileiro de Facebook.

>> Primeiro homem infectado com vírus de computador

Segundo a empresa, o ataque é feito por meio de uma página falsa preparada para enganar e infectar o usuário com o download de um programa. Se ele for executado, o programa se instala no computador e com ele são colocados vários arquivos maliciosos, como trojans bancários, vírus que capturam senhas de acesso ao Facebook, Twitter e Orkut.

Para infectar novos usuários, o aplicativo envia automaticamente uma mensagem pelo chat para os contatos do infectado com um link para download. Mas a disseminação do programa ainda não é tão grande. "Registramos infecções de usuários no Brasil e em Portugal, mas o número de vítimas é pequeno porque reportamos o problema ao Facebook, que tem bloqueado o link", diz Fábio Assolini, analista que descobriu o worn brasileiro. O programa é chamado IM-Worm.Win32.FBook.a.

Malware

Trojan

- Chamado de **Cavalo de Tróia**, *Trojan* ou *Trojan-horse*.
- Origem do nome: em uma guerra entre gregos e troianos, os gregos criaram um cavalo de madeira e o colocaram em frente aos muros da cidade de Tróia. Os troianos acreditaram ser um presente e carregaram o cavalo para dentro da cidade. À noite, saíram gregos de dentro do cavalo e Tróia acabou dominada por eles.

Malware

Trojan

- O Trojan recebe este nome porque aparenta ser um tipo de programa, mas não é.

Malware

Trojan

- O Trojan realiza atividades para as quais foi aparentemente projetado, mas também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

- Exemplos de trojans são os cartões virtuais animados, albuns de fotos, jogos e protetores de telas. Estes programas, geralmente, consistem em um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Malware

Trojan

Malware

Spyware

- **Spyware** é um software espião.
- Monitora as atividades de um host e encaminha aos atacantes.
- Pergunta: isto é sempre ilegítimo?

Malware

Spyware

- Pergunta: isto é sempre ilegítimo?
- Não. Imagine que você instalou um spyware no seu próprio computador para verificar se alguém está mexendo nele para fins indesejáveis.

Malware

Spyware

- Entretanto, muitas vezes são usados para comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário na internet. Especialmente e-mail, logins e senhas.

- Tipos de spywares: keylogger, screenlogger e adware.

Malware

Spyware

- **Keylogger**: armazena as teclas digitadas pelo usuário.
- **Screenlogger**: capaz de armazenar a posição do cursor e a tela apresentada no monitor. É utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, por exemplo.
- **Adware**: spyware que exibe propagandas.

Malware

Spyware

Figura: Spyware descoberto em 2006.

Malware

Spyware

- É possível criar um spyware legítimo?
- Suponhamos a seguinte situação: você não tem privilégios ou simplesmente não quer colocar senha no computador que utiliza e está desconfiado que, quando para de usá-lo por alguns instantes e se ausenta do recinto em que ele está, uma pessoa não autorizada usa o computador para ver conteúdo impróprio, entrar em redes sociais e em contas de e-mail pessoais.
- O usuário é cuidadoso. Ele acessa websites em guias anônimas e não encerra seus programas em execução. Além disso, ele não usa seu teclado para digitar, mas um teclado virtual, selecionando os caracteres com o mouse.

Malware

Spyware

- Que spyware podemos que criar para nos ajudar nesta situação?

Malware

Spyware

- Que spyware podemos que criar para nos ajudar nesta situação?
- Screenlogger! Alguma ideia de como fazer?

Malware

Backdoor

- **Backdoor** (porta dos fundos), ou *trapdoor* é um ponto de entrada secreto para um programa, que permite que alguém ciente da backdoor obtenha acesso sem passar pelos procedimentos normais de acesso.

- Usado por programadores quando se testa um programa que tem longos procedimentos de autenticação e o testador quer passar mais rapidamente por esta parte e quando o programador quer garantir que exista meio alternativo de ativação do programa caso a autenticação falhe por motivo não previsto.

Malware

Backdoor

- É uma ameaça quando utilizado para obter acesso não autorizado.
- Difícil implementar controles do sistema operacional para backdoors (STALLINGS, 2008).
- Programas de administração remota, como BackOrifice, NetBus, Sub-Seven, VNC e Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors (CERT.br, 2012).

Malware

Rootkit

- **Rootkit**: conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou outro código malicioso em um computador comprometido. Ele pode:

- Remover evidências, tais como arquivos de log.
- Instalar outros malwares, como backdoors, para assegurar acesso futuro ao computador.
- Esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões, etc.
- Mapear vulnerabilidades em outros computadores pela rede.
- Capturar informações da rede onde o computador comprometido está localizado, pela interceptação de pacotes.

Malware

Rootkit

Segurança

McAfee descobre rootkit que torna máquina vulnerável ao Conficker

Redação do IDG Now! 27/04/2009 - 16h23

São Paulo - Rootkit descoberto na semana passada afeta arquivos executáveis e HTML compartilhados em redes, principalmente de empresas.

Notícias Relacionadas

- Nova falha no Windows Vista pode permitir instalação de rootkit
- Nasa admite infecção de laptops em estação espacial por malware
- Relatório da Kaspersky

Um rootkit descoberto na semana passada pela McAfee está explorando arquivos executáveis e HTML compartilhados em rede, tornando a máquina vulnerável a outros malwares, incluindo o Conficker.

A McAfee informou nesta segunda-feira (27/04) que a variante do rootkit Virut afeta arquivos em redes locais, o que o torna ainda mais malicioso para empresas, e, após a infecção, não é possível recuperar os documentos.

Saiba mais sobre o Conficker:
> Dicas: saiba se proteger do Conficker
> Conficker: ferramenta indica PC infectado
> Microsoft oferece US$ 250 mil por criador da praga

Segundo a McAfee, é necessário destruir todos os arquivos

om/intent/tweet?original referer=... a praga.

+ Notícias Segurança

Site de encontros para militares é invadido e 170 mil cadastros são roubados

Twitter de Justin Bieber é invadido e post mal-educado é divulgado para 19 milhões

Redes sociais são mais perigosas que sites pornográficos

Apps que prometem mostrar quem visitou seu perfil no Facebook são golpes

Malware

Rootkit

DESCOBERTO PRIMEIRO ROOTKIT PARA TELEFONES

HARDWARE HD E SSD MOBILE TABLETS TECNOLOGIA SOFTWARE TOP DOWNLOADS
TUTORIAIS WINDOWS WINDOWS PHONE

BABOO @ 13 JUL 2007 | 12:00 AM

Uma operação altamente sofisticada de espionagem, que atingiu os celulares do primeiro ministro e de outros funcionários do alto-escalão do governo da Grécia,destacou as fragilidades em sistemas de telecomunicações que usam computadores antigos,de acordo com um relatório feito por dois professores universitários.

O caso de espionagem, que atingiu cerca de 100 pessoas, continua não solucionado, e ainda está sendo investigado. Para complicar ainda mais, há o questionável suicídio de um engenheiro da Vodafone na Grécia, em Março de 2005, que era o responsável pelo planejamento da rede invadida. Um estudo mais detalhado sobre a espionagem mostra uma operação extremamente detalhada e bem sucedida, de acordo com uma análise do IEEE Spectrum Online, site do Instituto de Engenharia Elétrica e Eletrônica.

O caso inclui o 'primeiro rootkit conhecido que foi instalado numa rede telefônica', afirmou Diomidis Spinellis, professor associado da Universidade de Administração e Economia de Atenas, que realizou o estudo da operação com Vassillis Prevelakis, professor assistente de ciência da computação da Universidade Drexel, na Filadélfia.

Um rootkit é um programa especial com o poder de esconder atividades maliciosas do sistema operacional, e sua detecção é extremamente difícil. O rootkit em questão permitiu a desativação de um log de transações e o monitoramento de chamadas a partir de quatro equipamentos da Telefonaktiebolaget LM Ericsson, feitos com tecnologias da Vodafone. O software permitia que os hackers ouvissem o conteúdo das conversas, e que uma segunda chamada de voz fosse redirecionada para outro lugar.

Malware

Rootkit

- O foco do rootkit é manter o acessoa privilegiado ao computador, e não obtê-lo.
- Facilita a vida dos atacantes:
  1. Após uma invasão, instala-se o rootkit;
  2. Para acessar novamente o computador da vítima, não é necessário recorrer novamente aos métodos utilizados para a invasão.
- Estão sendo incorporados em outros códigos maliciosos.

Malware

Ransomware

- **Ransomware**: código malicioso que torna equipamentos (*locker*) ou arquivos (*crypto*) inacessíveis e cobra uma quantia de resgate (normalmente em criptomoeda) para recuperá-los.
- Formas de infecção:
  - E-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link;
  - Explorando vulnerabilidades em sistemas desatualizados.
- Exemplo famoso: WannaCry.

Malware

Outros Tipos

- Há outros tipos:
  - Exploit
  - Flooder
  - Hijack
  - Bot (Zombie)
  - ...
- Há programas maliciosos que se encaixam em mais de uma categoria.

Malware

Resumo Comparativo

	Virus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Malware

Cuidados

- Manter antimalware e firewall pessoal instalados e atualizados.
- Manter softwares atualizados. Qualquer vulnerabilidade em versões anteriores pode tornar seu computador um alvo.
- Não abrir arquivos de origem duvidosa.
- Cuidar a URL de destino dos links.
- Não baixar e executar anexos de origem duvidosa.
- Não acessar websites duvidosos.
- Realizar logout quando não for utilizar mais o serviço.
- Utilizar computadores e redes confiáveis para acessar recursos críticos, como o sistema bancário.
- Utilizar perfis com privilégios de administrador somente se necessário.

Malware

Contramedidas

- Com base em Stallings (2008):
  - Usar antimalware para não permitir que o malware entre no sistema
  - Usar antimalware para detectar, identificar e remover o malware, restaurando o sistema ao ponto anterior à infecção, se necessário.
  - Usar antimalware com descriptografia genérica (detecta vírus polimórficos complexos com rapidez)
  - Usar softwares de bloqueio de comportamento, que monitora o comportamento do programa em tempo real e bloqueia ações potencialmente maliciosas.

Malware

- Será que é difícil criar um script malicioso?
  - Pode ser feito em e para qualquer Sistema Operacional.
  - Várias linguagens podem ser usadas (individual ou conjuntamente).

Scripts Maliciosos

```
for i in $(seq 0 5)
do
    mkdir $i
done
```

- O que faz este código?
- Em quatro linhas foi escrito um *script* que cria seis pastas no diretório atual.
- Pense: e se fizermos com um laço infinito?

Scripts Maliciosos

```
for i in $(seq 0 5)
do
    mkdir $i
done
```

- Digite este código e salve o arquivo como `aula.sh`.
- Para executá-lo, digite no terminal: `sh aula.sh`.

Scripts Maliciosos

```
for i in $(seq 0 5)
do
    mkdir $i
done
```

- E se o *script* for adicionado no agendador de trabalhos do sistema operacional (`crontab`)?
- Podemos definir sua execução em um momento específico.
- Podemos definir sua execução em *background*
  - `nohup sh aula.sh &> /dev/null &`

Scripts Maliciosos

```
for i in $(seq 0 5)
do
    mkdir $i
done
google-chrome www.sitedecoisafeia.com --
   incognito
```

- O que mudou?

Scripts Maliciosos

- Aprimorando nosso exemplo...

```
for i in $(seq 0 5)
do
    mkdir $i
    sleep 10
    google-chrome $(shuf -n 1 lista.txt) --
       incognito
done
```

Scripts Maliciosos

```
for i in $(seq 0 5)
do
    mkdir $i
    sleep 10
    google-chrome $(shuf -n 1 lista.txt) --
       incognito
done
```

- No arquivo `lista.txt`, insira uma url em cada linha e veja o resultado.

Scripts Maliciosos

- Para fazer, no Windows, scripts semelhantes a estes, cria-se os chamados arquivos Batch (de lote). São arquivos com extensão `.bat`.
- Exemplo: `win32sys.bat`

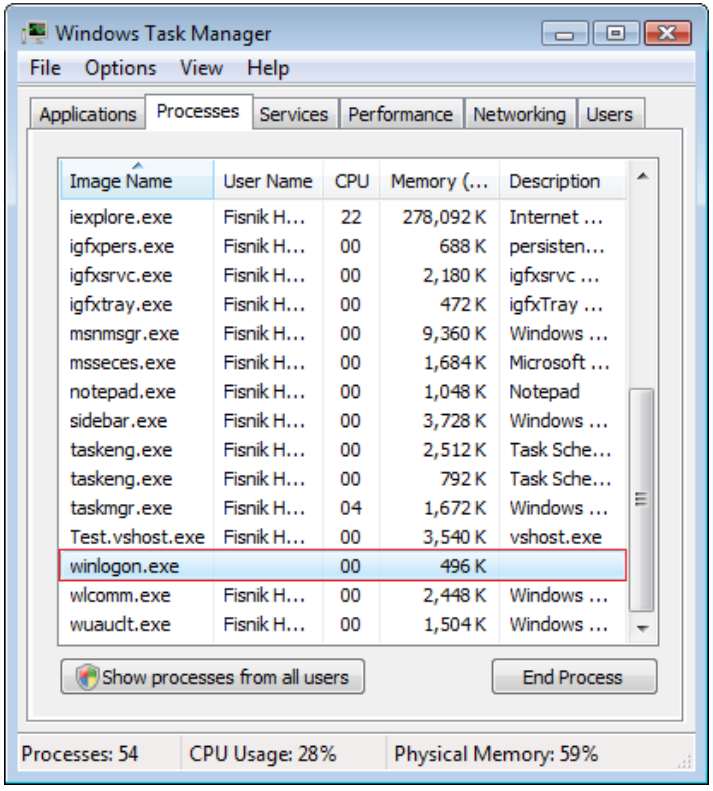
Cuidados

- Nunca executar um arquivo sem saber do que se trata.
- Manter os utilitários de proteção sempre atualizados.
- Restringir ao máximo os privilégios do usuário.
- Utilizar o perfil de administrador somente quando necessário (não criar o perfil de usuário com privilégios de administrador!).

Cuidados

- Podemos perceber quando *scripts* maliciosos estão sendo executados.
- Nos sistemas Unix, os comandos `ps` e `top` mostram os processos em execução. No Windows, o utilitário Gerenciador de Tarefas (`taskmgr.exe`) exibe os processos em execução.
- Engenharia reversa permite obter códigos equivalentes aos originais e identificar instruções maliciosas.
- Ferramentas como `strings` permitem encontrar códigos embutidos em arquivos (ex: PDF).

Cuidados


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (... Description
iexplore.exe Fisnik H... 22 278,092 K Internet ...
igfxpers.exe Fisnik H... 00 688 K persisten...
igfxsrvc.exe Fisnik H... 00 2,180 K igfxsrvc ...
igfxtray.exe Fisnik H... 00 472 K igfxTray ...
msnmsgr.exe Fisnik H... 00 9,360 K Windows ...
msseces.exe Fisnik H... 00 1,684 K Microsoft ...
notepad.exe Fisnik H... 00 1,048 K Notepad
sidebar.exe Fisnik H... 00 3,728 K Windows ...
taskeng.exe Fisnik H... 00 2,512 K Task Sche...
taskeng.exe Fisnik H... 00 792 K Task Sche...
taskmgr.exe Fisnik H... 04 1,672 K Windows ...
Test.vshost.exe Fisnik H... 00 3,540 K vshost.exe
winlogon.exe 00 496 K
wlcomm.exe Fisnik H... 00 2,448 K Windows ...
wuaudt.exe Fisnik H... 00 1,504 K Windows ...
Show processes from all users
End Process
Processes: 54 CPU Usage: 28% Physical Memory: 59%

Cuidados

- No Windows, ainda podemos ver se há algum arquivo suspeito sendo inicializado junto com o SO. Em algumas versões isto é feito no próprio Gerenciador de Tarefas, em outras é feito no `msconfig`.

- Entretanto, tenha em mente que nem sempre é simples encontrá-los. Um *script* malicioso pode ter sobrescrito algum arquivo legítimo, bem como pode alterar os nomes de seus arquivos dinamicamente, dificultando o seu descobrimento.

Códigos Bons

- Obviamente, pode-se aproveitar o conhecimento em programação de *scripts* para também fazer o bem, criar rotinas de defesa ou de identificação de incidentes. O que fazem os códigos abaixo?

```
apt update
cp -r /meus/arquivos/importantes/* /mnt/
   pendrive
grep -E "deauth|error|Failed password|
   warning" /var/log/*.log
ss -tuln | grep LISTEN
ss -tuna | grep ':22'
ps -eo pid,ppid,cmd,%mem,%cpu --sort=-%cpu |
    head
ufw status verbose
```

Códigos Bons

- O que faz o código abaixo?

```
find "$(pwd)" -type f -exec sh -c 'exiftool
   "{}" 2>&1 | grep -i "File format error"
   && echo "Arquivo corrompido: {}"' \;
```

- Executar a partir do diretório `IFC/Códigos/Segurança`.

Exercícios

1. Individualmente, faça um *script* que crie um arquivo de texto chamado `imagens`, que deve conter o link para cinco imagens do logotipo do Instituto Federal. O *script* deve abrir aleatoriamente três destas imagens em um navegador a cada três segundos. Utilize qualquer linguagem.

2. No mesmo *script*, coloque um comando para desligar ou hibernar o computador trinta segundos após abrir as imagens.

Resposta em `scriptmalicioso.sh`.

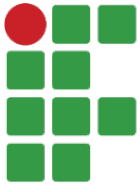
Referências

- CERT.br. Cartilha de Segurança para Internet, versao 4.0 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: `http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf`. Acesso em: 3 ago. 2015.
- CERT.br. Ransomware. Disponível em: `https://cartilha.cert.br/ransomware/`. Acesso em: 17 abr. 2018.
- STALLINGS, William. Criptografia e segurança de redes. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

Códigos (não apenas) Maliciosos

Segurança Computacional

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau