

Capítulo 3 – Panorama Atual na Área de Segurança

- 3.1 – Introdução
- 3.2 – Ameaças recentes
 - 3.2.1 – Vírus
 - 3.2.2 – Worms
 - 3.2.3 – Vulnerabilidades
- 3.3 – Estatísticas
 - 3.3.1 – CERT
 - 3.3.2 – CAIS
- 3.4 – Perfil dos atacantes
 - 3.4.1 – Hackers e Crackers
 - 3.4.2 – Script Kiddies
 - 3.4.3 - Motivação

3.1 – Introdução

- Instalar um SO numa máquina conectada diretamente à Internet pode levar a um comprometimento em poucos minutos
 - tempo insuficiente até para baixar as últimas atualizações do sistema instalado
- Panorama atual da rede:
 - lugar público
 - cheio de informações valiosas
 - cheio de vândalos, *hackers*, *crackers*, vírus, *worms* e outras ameaças

3.2 – Ameaças recentes

3.2.1 – Vírus

- Primeiro vírus conhecido: ping-pong
- Hoje, existem aproximadamente 100 mil vírus catalogados
- Os primeiros vírus eram transmitidos por disquetes e somente arquivos executáveis podiam ser infectados
- Hoje, a maior forma de contágio é o e-mail
- Hoje, vários tipos de arquivos podem ser contaminados:
 - e.g.: .com, .exe, .doc, .xls, .bat, .cpl, .htr, .js, .scr, etc.

- Apesar de existirem vírus para outros SO's (Linux, MacOS, BSD), essa quantidade é infinitamente menor, se comparado ao Windows
- Por que o Windows tem, proporcionalmente ao número de usuários, muito mais vírus que outros SOs ?
- Antivírus são programas capazes de detectar e remover os vírus de uma máquina
 - podem ter recursos avançados como verificação de vírus em e-mail, e também verificação de vírus em arquivos em tempo real quando estão sendo acessados pelo SO
- Antivírus utiliza assinaturas de vírus para detectar arquivos infectados
 - Assinaturas de vírus: conjunto de informações que identificam unicamente um determinado vírus
 - As assinaturas devem ser frequentemente atualizadas

- Para tomar conhecimento de novos vírus e como eles funcionam basta visitar as páginas dos principais fabricantes de antivírus
 - Symantec: <https://www.broadcom.com/products/cyber-security>
 - McAfee: <https://www.mcafee.com/enterprise/pt-br/threat-center.html>
 - Trend Micro: <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/>
 - F-Secure: <https://www.f-secure.com/br-pt>
 - Kaspersky: <https://www.kaspersky.com.br/>
- Computador com antivírus desatualizado há mais de uma semana é considerado altamente vulnerável
- Nem sempre a atualização das assinaturas é feita a tempo de conter a contaminação
- Em questão de horas um vírus pode ter se espalhado para outros continentes

3.2.2 – Worms

- Parecidos com vírus
- Principal diferença: um *worm* tenta infectar uma máquina enquanto o vírus tenta infectar um arquivo
- Ao infectar uma máquina, o passo seguinte do *worm* é procurar (ou sortear) endereços de rede para tentar infectar outras máquinas na rede
- Utiliza-se de vulnerabilidades conhecidas, e-mail, permissões de acesso, compartilhamentos, etc.
- Muitos *worms* utilizam múltiplas formas de replicação
 - O *Worm Code Red*, em 2001, em apenas 14 horas, infectou cerca de 360.000 computadores
- Prevenção de *worms* se faz através de atualizações frequentes do SO
- Na grande maioria dos casos, os *worms* exploram vulnerabilidades já conhecidas, com atualizações já disponíveis nos sites dos fabricantes

3.2.3 – Vulnerabilidades

- São falhas presentes em um programa, protocolo ou SO
 - Normalmente causadas por erros de especificação ou erros de programação
 - Solução “simples”: fabricante lança uma correção, chamada de *patch*
 - Quando existem muitas correções, o fabricante as agrupa num *service pack*
- O usuário deve fazer o download dessas correções
 - Muitas vezes o fabricante disponibiliza formas automáticas de aplicar correções
 - e.g.: Windows Update da Microsoft, SUSE Updater da Novell, apt do Debian, dnf do RedHat

- Falhas de especificação são mais difíceis de se solucionar
 - especificação de protocolo ou produto deve ser revista
 - as alterações devem preservar a compatibilidade com sistemas que ainda não foram atualizados
 - problemas como o *syn flood* e ataques *smurf*, que são vulnerabilidades no próprio protocolo TCP/IP, até hoje não têm uma solução perfeita
- Listas de discussão fornecem informações sobre vulnerabilidades, além de sites de fabricantes
 - <https://www.microsoft.com/en-us/security>
 - <http://www.debian.org/security/>
- Descobertas de vulnerabilidades, geralmente vêm acompanhadas de uma “*prova por conceito*”: programas capazes de explorar aquela vulnerabilidade
 - **exploits**: programas criados para explorar determinada vulnerabilidade em um sistema. Tem como objetivo inicial provar que uma determinada vulnerabilidade é perigosa

3.3 – Estatísticas

- Estatísticas sobre o número de vulnerabilidades e o número de incidentes reportados a cada ano
 - Importantes para acompanhamento da evolução das vulnerabilidades e incidentes de segurança

3.3.1 – CERT

- Estatísticas sobre:
 - incidentes
 - vulnerabilidades
 - alertas de segurança publicados
 - notas de segurança publicadas
 - mensagens de correiro eletrônico atendidas
 - chamadas telefônicas recebidas
- <https://www.cert.br/stats/>



Centro de Estudos, Resposta
e Tratamento de Incidentes
de Segurança no Brasil

► Sobre o CERT.br

► CSIRTs

► Estatísticas

- Incidentes
- Amplificadores
- DNS Malicioso
- Honeyports
- Spam

► Cursos

► Projetos

► Publicações

► Palestras

► Links

► FAQ

► Mapa do site

► Contato

Twitter

RSS

Busca

ok

Buscar em CERT.br

Núcleo de Informação e Coordenação do Ponto BR

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br

Você está em: CERT.br > Estatísticas > Incidentes

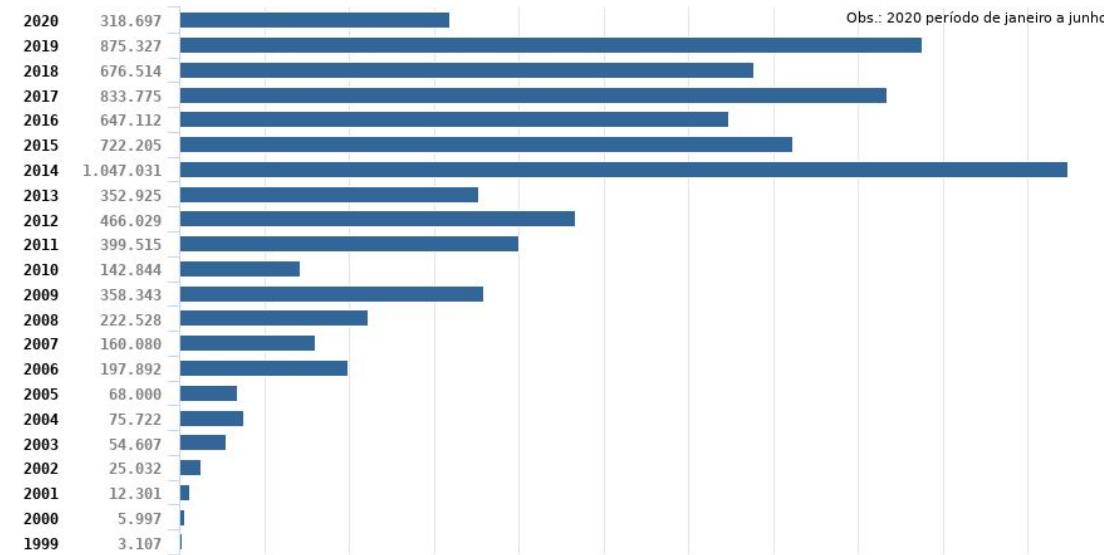
Estatísticas dos Incidentes Reportados ao CERT.br

| 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999 |

Valores acumulados: 1999 a 2020 (janeiro a junho) [novo](#)

Total de Incidentes Reportados ao CERT.br por Ano

Ano total



Obs.: 2020 período de janeiro a junho



Acessibilidade do site

3.3.2 – CAIS



3.4 – Perfil dos atacantes

- Quem são as pessoas que produzem os ataques?
- O que elas pensam?
- Quais são as suas motivações?
- Por que fazem esse tipo de coisa?

3.4.1 – Hackers

- O termo *hacker* foi por muito tempo associado a pessoas mal-intencionadas
- *Hacker* é uma pessoa que detém muitos conhecimentos sobre a área de computação
 - sistemas operacionais
 - software
 - programação
 - segurança
 - redes
 - Internet
- Tem interesse em descobrir coisas novas (inclusive vulnerabilidades)
- Não possui motivação destrutiva

3.4.2 – Crackers

- *Cracker* é um *hacker* com propósitos maldosos de invadir e violar a integridade dos sistemas

3.4.3 – Script kiddies

- Pessoas que possuem pouco conhecimento em informática e têm aspirações a *hacker/cracker*
- Utilizam os *exploits* criados por terceiros (*hackers*) para invadir sistemas vulneráveis
- Têm pouca idade
- Não estão interessados em algo específico, simplesmente querem invadir um site qualquer
- São responsáveis por boa parte dos ataques na Internet, e provavelmente serão os responsáveis caso o seu site seja atacado
- <https://www.honeynet.org/>



The HoneyNet Project

The HoneyNet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. With Chapters around the world, our volunteers have contributed to fight against malware (such as Conficker), discovering new attacks and creating security tools used by businesses and government agencies all over the world.

[Learn More](#)

The HoneyNet Project

HOT TOPICS



Analysis



Android



Encryption



Chapters



Honeypot



Data mining

3.4.4 – Motivação

- O que leva uma pessoa a invadir um sistema?
 - impunidade, delinquência, tentativa de chamar a atenção, notoriedade, para mostrar que pode, para mostrar aos amigos, e muitas outras
 - https://cdn.ttgtmedia.com/searchSecurity/downloads/Honeynet_Ch16.pdf
- Geralmente, um invasor não quer invadir a sua rede especificamente, mas uma rede qualquer que seja fácil de invadir
- Seguindo o princípio do ponto mais fraco, torne a sua rede forte o suficiente para o atacante tentar atacar outra rede e não a nossa
- Em alguns casos, o atacante pode ter muitos conhecimento em informática e interesses específicos

➤ Kevin Mitnick e Tsutomu Shimomura

- *Hacker (ou cracker?) mais famoso do mundo*
- Sua história virou livros e filme
- Hoje Mitnick trabalha numa empresa de segurança
- **Livros:**
 - “**Mitnick, A Arte de Enganar**”, escrito pelo próprio Mitnick
 - “O Pirata Eletrônico e o Samurai”
 - “Takedown”, escrito por Shimomura
- **Filme:**
 - “**Takedown, A Caçada Virtual**”
- Links:
 - <http://www.takedown.com/>
 - <http://www.freedomdowntime.com>
 - http://pt.wikipedia.org/wiki/Kevin_Mitnick

