

Mestrado em Engenharia Informática (MEI)

Mestrado Integrado em Engenharia Informática

(MiEI)

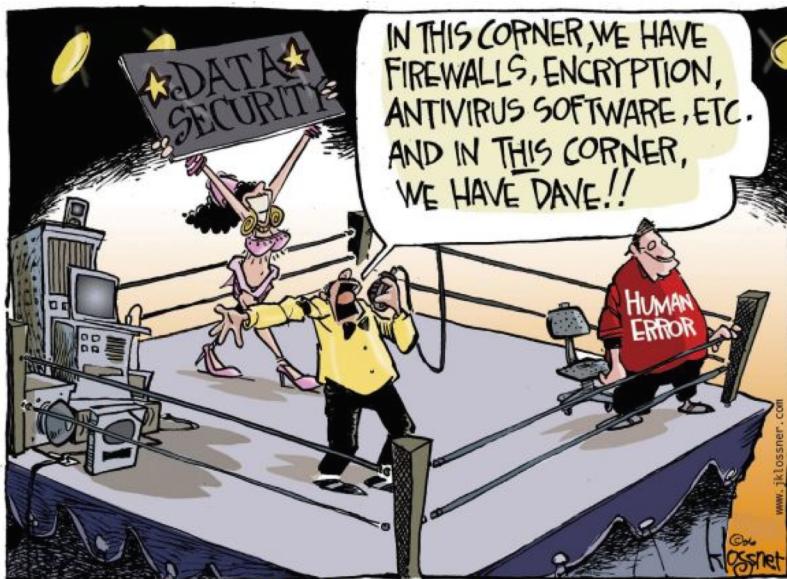
Perfil de Especialização **CSI** : Criptografia e Segurança da Informação

Engenharia de Segurança



Tópicos de Segurança de Software

- Ameaças de segurança ao software
- Categorias de ataques que exploram vulnerabilidades de software

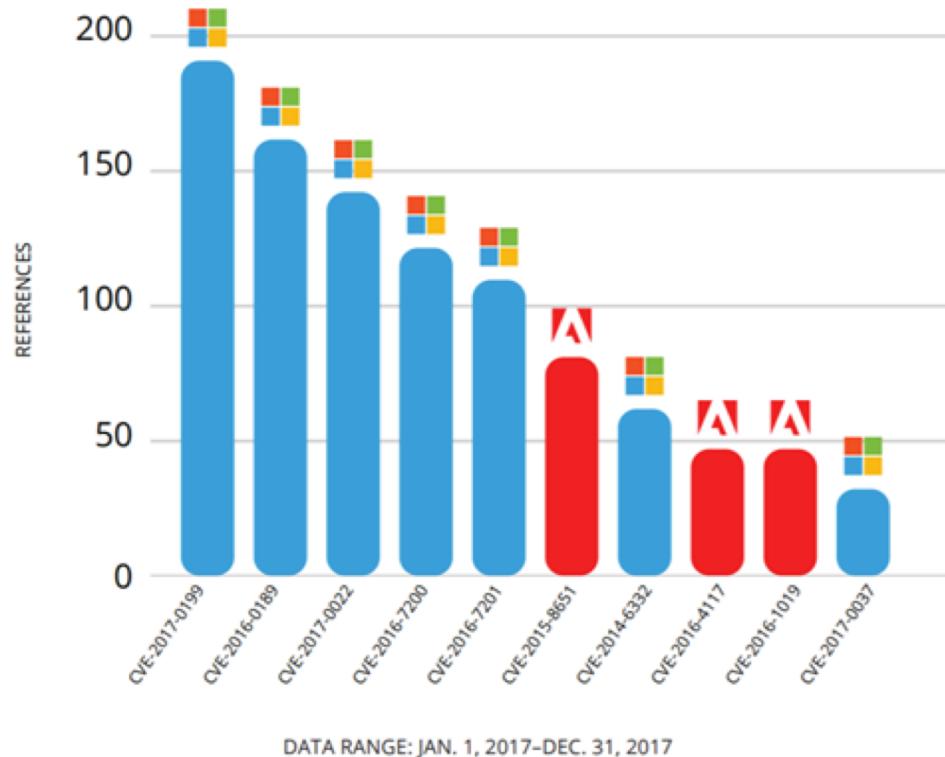


Copyright 2006 John Klossner, www.jklossner.com



Onde está o risco?

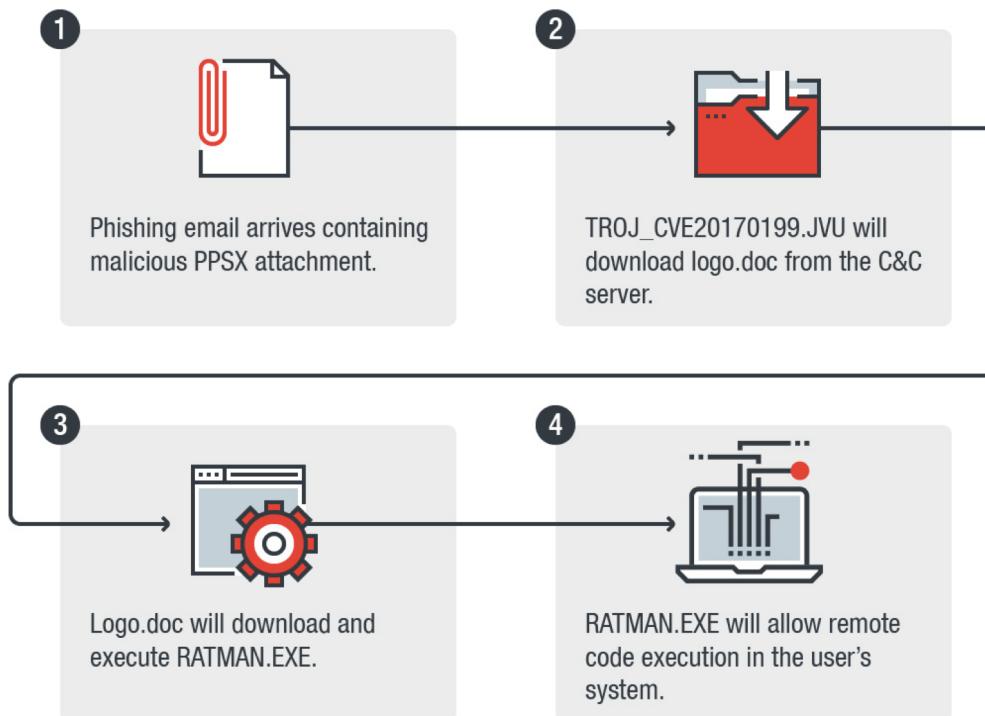
Top 10 Vulnerabilities Used by Cybercriminals



Infosec Institute – <http://resources.infosecinstitute.com/exploited-flaws-cybercriminal-organizations/>

Onde está o risco?

- CVE-2017-0199

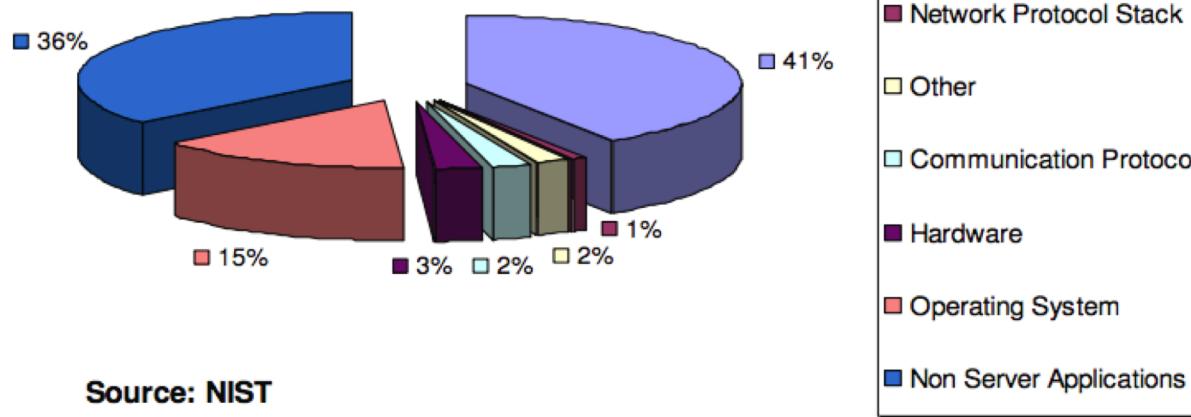


Trend Micro – <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-0199-new-malware-abuses-powerpoint-slide-show/>

O que está em risco?

Target Applications At Risk

92% of reported vulnerabilities
are in applications not in networks



O que está em risco?



ATTACK ORIGINS		ATTACK TYPES		ATTACK TARGETS		LIVE ATTACKS							
#	COUNTRY	#	PORT	SERVICE TYPE	#	COUNTRY	TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
4173	China	3124	1433	ms-sql-s	5672	United States	19:11:05.603	Taipei Taiwan	220.134.173.155	Tainan, TW	De Kalb Junction...	ms-wbt-server	3389
1108	United States	1497	53413	netis-router	2453	United Arab Emirates	19:11:05.540	Altanet	83.246.66.39	Hemmingen, DE	Hemmingen, DE	netbios-dgm	138
578	Netherlands	1246	22	ssh	196	Singapore	19:11:05.421	Adsl-Tt Net_Static Pool	85.105.195.176	Istanbul, TR	Roseville, US	telnet	23
429	Vietnam	989	5900	rfb	181	France	19:11:05.417	University Of Michigan College Of Engineering	141.212.122.195	Ann Arbor, US	San Francisco, US	http	80
350	Taiwan	776	3389	ms-wbt-server	170	Germany	19:11:05.353	China United Network Communications Corporati...	61.240.144.64	Beijing, CN	De Kalb Junction...	ssh	22
332	South Korea	486	23	telnet	146	Italy	19:11:05.348	China Tietong Telecommunications Corporation	222.42.230.121	Beijing, CN	Lynnwood, US	xsan-filesystem	50856
221	Canada	452	445	microsoft-ds	128	Canada	19:11:05.095	Chinanet Jiangsu Province Network	58.212.136.18	Nanjing, CN	Lynnwood, US	xsan-filesystem	50856
212	Spain	435	80	http	80	Hong Kong	19:11:05.091	Net-Core	217.16.1.178	Aix-En-Provence...	Aix-En-Provence...	netbios-dgm	138
189	Turkey	384	138	netbios-dgm	74	Spain	19:11:04.985	Net Servios De Comunicao S.A.	177.194.161.120	Ananindeua, BR	Oslo, NO	netis-router	53413

Norse – <http://map.norsecorp.com/> (14/Abr/2018)

Ameaças de segurança ao software

- Uma ameaça a um sistema de software é qualquer ator, agente, circunstância ou evento que tenha o potencial de causar danos a esse sistema ou aos dados ou recursos aos quais o sistema acede ou permite acesso.
- As ameaças podem ser categorizadas de acordo com sua intencionalidade:
 - não intencionais,
 - intencionais, mas não maliciosas
 - maliciosas (ataques).
- A maioria dos ataques contra software aproveitam ou exploram alguma vulnerabilidade ou fraqueza nesse software.
- Ameaças ao software estão presentes durante todo o seu ciclo de vida.

Ameaças de segurança ao software

Exemplo de ameaças ao software nas fases de desenvolvimento, distribuição e operação, categorizadas de acordo com sua intencionalidade.

Categoria da ameaça	Desenvolvimento	Distribuição	Operação
Não-intencional	<p>Erro de digitação no código-fonte por programador descuidado, altera a funcionalidade do software compilado a partir desse código-fonte.</p> <p>O programador que não conhece as práticas de codificação segura, escreve um módulo C que faz chamadas inseguras a bibliotecas externas.</p>	<p>O administrador de sistemas atribui accidentalmente permissões de escrita para todos os utilizadores, ao diretório no qual o software está instalado.</p>	<p>O utilizador pode efetuar um <i>input</i> extremamente longo porque o formulário de entrada HTML não valida e trunca os caracteres em excesso.</p>



Ameaças de segurança ao software

Exemplo de ameaças ao software nas fases de desenvolvimento, distribuição e operação, categorizadas de acordo com sua intencionalidade.

Categoria da ameaça	Desenvolvimento	Distribuição	Operação
Intencional, mas não maliciosa	<p>Para satisfazer o pedido do cliente para tornar o desempenho a prioridade principal, o programador elimina as funções de validação de <i>input</i> que adicionam sobrecarga de desempenho.</p> <p>O programador pressionado pela gestão para entregar o código-fonte num prazo apertado, não faz a revisão de segurança ao código .</p>	<p>O administrador atribui privilégios de "root" a um programa de software que foi implementado de tal modo que só pode ser executado como <i>root</i>.</p>	<p>O utilizador frustrado insere repetidamente combinações incomuns de comandos, de modo a contornar uma interface de <i>input</i> de dados do menu <i>pull-down</i>.</p> <p>O utilizador frustrado atualiza repetidamente e reenvia os mesmos dados de <i>input</i> para uma aplicação que não foi projetada para retornar uma confirmação de que os dados de <i>input</i> tinham sido recebidos.</p>



Ameaças de segurança ao software

Exemplo de ameaças ao software nas fases de desenvolvimento, distribuição e operação, categorizadas de acordo com sua intencionalidade.

Categoria da ameaça	Desenvolvimento	Distribuição	Operação
Maliciosa	O programador inclui intencionalmente três falhas exploráveis e um <i>backdoor</i> no seu código-fonte.	O instalador do sistema deixa a senha <i>default</i> da aplicação inalterada, para facilitar a vida do atacante com quem está em conluio.	O atacante inicia um ataque de SQL <i>injection</i> contra uma aplicação Web que utiliza base de dados.
	O integrador adiciona uma bomba lógica a um programa <i>open source</i> .	O administrador de sistemas configura intencionalmente o <i>firewall</i> de modo a permitir o acesso a URLs (<i>Uniform Resource Locators</i>) que contenham conteúdo executável.	O programador envia uma <i>string</i> de dados predefinida para uma aplicação Web que sabe que acionará a execução da bomba lógica que plantou nessa aplicação.

Categorias de ataques

- Categorias de ataques que exploram vulnerabilidades de software:
 - **Ataque de reconhecimento**
 - Ajuda o atacante a descobrir mais sobre o software e o seu ambiente, de modo que outros ataques subsequentes possam ser mais eficazes;
 - Os atacantes estão particularmente interessados na informação da versão do software e componentes COTS (*Commercial off-the-shelf*) e OSS (*Open-source software*) do ambiente, já que essas informações revelam se o software / ambiente inclui componentes com vulnerabilidades conhecidas que podem ser exploradas.
 - **Facilitador de ataques**
 - Tipo de ataques que facilitam a concretização de outros ataques;
 - Exemplos: ataques que exploram *buffer overflow* para execução de código malicioso; ataques para aumento de privilégios.
 - **Ataque de divulgação**
 - Revelam dados que não devem ser vistos pelo atacante (comprometimento da confidencialidade).
 - **Ataque de corrupção**
 - Adulteram e corrompem o *software* para alterar o seu modo de operação (comprometimento da integridade).
 - **Ataque de sabotagem**
 - Causa a falha do *software* ou evita que seja acedido pelos seus utilizadores;
 - Também conhecido como ataque de “*denial of service*” (comprometimento de disponibilidade).
 - **Ataque de código malicioso**
 - Insere lógica maliciosa no software, aciona a execução de código malicioso já incorporado no software ou entrega / executa malicioso no ambiente de execução do software.

Lista de ameaças STRIDE

A lista de ameaças baseada no STRIDE é útil para identificar as ameaças, do ponto de vista dos objetivos dos atacantes.

Tipo da ameaça	Exemplo	Controlo de segurança
<u>Spoofing</u> (falsificação)	Ação que tem por objetivo aceder e utilizar, de modo ilegal, as credenciais de outro utilizador, tais como <i>username</i> e <i>password</i> .	Autenticação
<u>Tampering</u> (adulteração)	Ação que tem por objetivo a alteração/modificação maliciosa de dados persistentes (por exemplo, numa base de dados), e a alteração de dados em trânsito entre dois computadores numa rede aberta (por exemplo, a Internet).	Integridade
<u>Repudiation</u> (repúdio)	Ação que tem por objetivo efetuar operações ilegais num sistema que não tem mecanismos para rastrear as operações proibidas.	Não-repúdio
<u>Information disclosure</u> (divulgação)	Ação que tem por objetivo ler um ficheiro a que não foi dado acesso, ou ler dados em trânsito.	Confidencialidade
<u>Denial of service</u>	Ação que tem por objetivo negar o acesso a utilizadores válidos (por exemplo, tornando um servidor web temporariamente indisponível ou inutilizável).	Disponibilidade
<u>Elevation of privilege</u>	Ação que tem por objetivo obter acesso privilegiado aos recursos, de forma a aceder indevidamente a informação ou a comprometer o sistema.	Autorização

Lista de ameaças STRIDE

Baseada em cada tipo de ameaça STRIDE, é possível identificar técnicas de atenuação das ameaças que podem ser utilizadas para atenuar cada ameaça concreta identificada.

Tipo da ameaça	Técnicas de atenuação/mitigação	Controlo de segurança
<u>Spoofing</u> (falsificação)	<ol style="list-style-type: none"> Autenticação apropriada Proteger dados/informação secreta Não guardar segredos 	Autenticação
<u>Tampering</u> (adulteração)	<ol style="list-style-type: none"> Autorização apropriada Hashes MACs Assinaturas digitais Protocolos invioláveis / resistentes a ataques 	Integridade
<u>Repudiation</u> (repúdio)	<ol style="list-style-type: none"> Assinaturas digitais Selos de tempo Registos de auditoria 	Não-repúdio
<u>Information disclosure</u> (divulgação)		Confidencialidade
<u>Denial of service</u>		Disponibilidade
<u>Elevation of privilege</u>		Autorização

Lista de ameaças STRIDE

Baseada em cada tipo de ameaça STRIDE, é possível identificar técnicas de atenuação das ameaças que podem ser utilizadas para atenuar cada ameaça concreta identificada.

Tipo da ameaça	Técnicas de atenuação/mitigação	Controlo de segurança
<u>Spoofing</u> (falsificação)		Autenticação
<u>Tampering</u> (adulteração)		Integridade
<u>Repudiation</u> (repúdio)		Não-repúdio
<u>Information disclosure</u> (divulgação)	1. Autorização 2. Protocolos avançados de privacidade 3. Encriptação 4. Proteger segredos 5. Não guardar segredos	Confidencialidade
<u>Denial of service</u>	1. Autenticação apropriada 2. Autorização apropriada 3. Filtragem 4. <i>Throttling</i> /Controlo 5. Qualidade de serviço	Disponibilidade
<u>Elevation of privilege</u>	1. Executar com os privilégios mínimos	Autorização



Ficha de trabalho

- Analise <https://www.csoonline.com/article/3217944/security/8-top-cyber-attack-maps-and-how-to-use-them.html>.

