

PROTEÇÃO DE DADOS NO BRASIL

Audiência Pública



Altair Olivo Santin
**CESeg: Comissão Especial em Segurança da
Informação e de Sistemas Computacionais**



CÂMARA DOS DEPUTADOS
Comissão de Defesa do Consumidor

18.06.2019

Investimento em Segurança da Informação

Cenários de Violação de Segurança

Investimento em Privacidade da Informação

Cenários de Violação de Privacidade

Considerações

Necessidades para mudar o futuro

Referencial Curricular do bacharelado em CiberSegurança

Agenda



**Segurança em Redes e
Sistemas Operacionais**



**Segurança em Comércio
Eletrônico**



Uso de Criptografia



**Investimento em
Capacitação /
Treinamento de Pessoal**



**Boas Práticas, baseadas
em Normas**

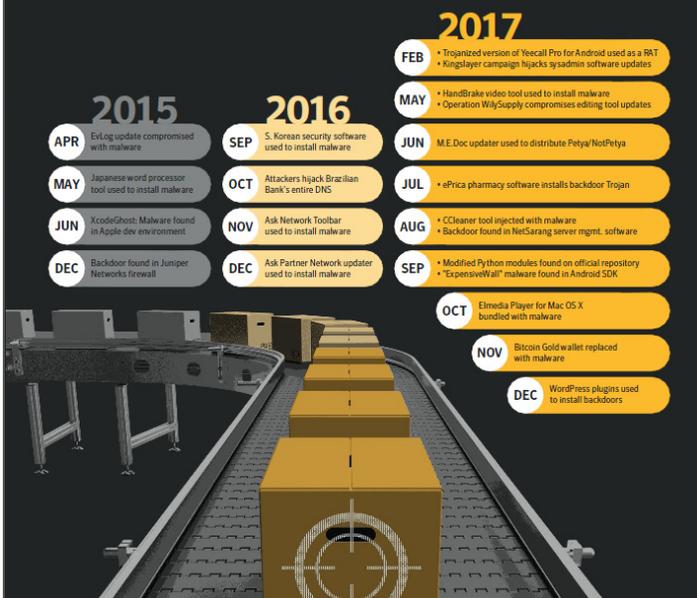


**Governança de TI com
Processos para Segurança
da Informação**

Investimento em Segurança da Informação

Lado Empresa

Supply chain attacks



Overall email malware rate

In 2017, the rate for email-borne malware fell to 1 in 412 (0.2 percent) from 1 in 131 (0.8 percent) in 2016.

Year	1 in
2015	220
2016	131
2017	412



[ENABLE FILTERS]

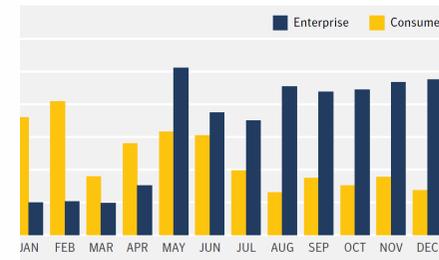
Total notifications: 299 of which 127 single ip and 172 mass defacements

Legend:
 H - Homepage defacement
 M - Mass defacement (click to view all defacements of this IP)
 R - Redefacement (click to view all defacements of this site)
 L - IP address location
 ★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	L	★	Domain
11:08	RMX team	H	M				telescopicseatingsystems.com
11:03	/ExCaKun			R			www.connect-personal.ru/ExCaKu...
11:02	MedoxEL	H	R				apisweb.net
11:01	M4L36H05T		M				arendadesoi.ru/jiwa.php
11:01	M4L36H05T		M				gipsometal.ru/jiwa.php
11:01	M4L36H05T		M				injekto.ru/jiwa.php
11:01	M4L36H05T		M				simpur.ru/jiwa.php
11:01	M4L36H05T		M				gipsometall.ru/jiwa.php
11:01	M4L36H05T		M				eggsservice.ru/jiwa.php
11:01	M4L36H05T		M				gipsometal2000.ru/jiwa.php
10:39	pajaR_19		M				emmayou.com/ly.php
10:39	pajaR_19	M	R				hannahyou.com/ly.php
10:39	pajaR_19	M	R				iconexpo.com/ly.php
10:39	pajaR_19	M	R				read1kbooks.com/ly.php
10:39	pajaR_19	M	R				koreanlit.com/ly.php
10:17	/Ikari404	M	R				1wb.me/z.htm
10:17	/Ikari404	M	R				liken.store/z.htm
10:17	/Ikari404	M	R				wncer.us/z.htm
10:17	/Ikari404	M	R				layla.furniture/z.htm
10:17	/Ikari404	M	R				4voip.us/z.htm
10:17	/Ikari404	M	R				itech2.us/z.htm
10:17	/Ikari404	M	R				www.itech2.co/z.htm
10:17	/Ikari404	M	R				socialgc.com/z.htm
10:17	/Ikari404	M	R				9compare.com/z.htm
10:11	Z3z3-HaCKEr	H	R				www.anupamshaadi.com

e vs. consumer ransomware detections by month

Ransomware attacks against consumers dominated in the early part of 2017, while attacks against enterprises dominated following the WannaCry outbreak in May.



Overall phishing rate

The phishing rate declined from 1 in 2,596 in 2016 to 1 in 2,995 in 2017.

Year	1 in
2015	1,846
2016	2,596
2017	2,995

Cenários de Violação de Segurança

Fonte: Symantec Internet Security Threat Report 2018



Malware

92%

Increase in new downloader variants

80%

Increase in new malware on Macs



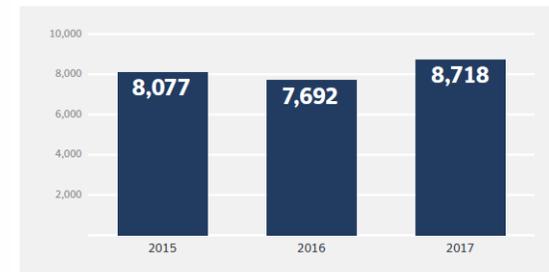
IoT attacks by source country

This table shows the country of origin, based on IP address, of the attacking devices.

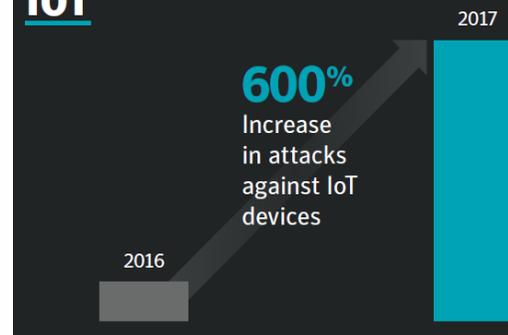
Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

Total number of vulnerabilities

This shows a 13 percent increase in the number of reported vulnerabilities recorded in 2017.

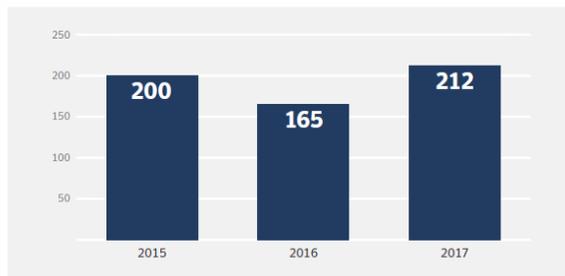


IoT



Vulnerabilities disclosed in industrial control systems

There was an increase of 29 percent in the number of recorded vulnerabilities affecting industrial control system (ICS) technology in 2017.



Cenários de Violação de Segurança

Fonte: Symantec Internet Security Threat Report 2018



Data Privacy Officer |
Time interdisciplinar



Desenvolvimento de
Cultura de
Privacidade



Inventário de dados |
política de retenção
de dados / backup



Revisão / Ajuste de
Contratos | Código
de Conduta para
Proteção de Dados



Gestão de
Consentimentos |
Política e avisos de
Privacidade



Ferramentas de
Compliance /
Privacidade (e.g.
Nymity)



Resposta a incidentes
/ violações de
Privacidade / Dados



*Processo custoso e
contínuo, mas
necessário*

Investimento em Privacidade da Informação

Baseado na LGPD

Facts about the Attack on Anthem

On January 26, 2015

78 Million patient records were exposed.

The breach is believed to be the work of a well-resourced cyberespionage group, which Symantec calls **Black Vine**. They appear to have access to a wide variety of resources to let it conduct multiple, simultaneous attacks over a sustained period of time. They used:

- ▶ attacker-owned infrastructure
- ▶ zero-day exploits
- ▶ custom-developed malware

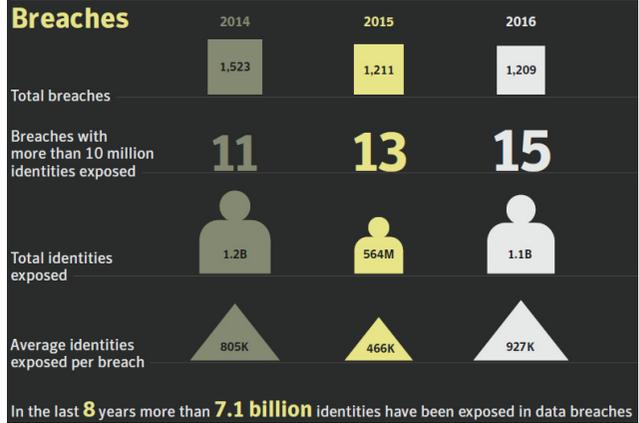
Three variants are named:
1) **Hurix**, 2) **Sakurel**, and 3) **Mivast**

detected as Trojan.Sakurel Backdoor.Mivast



- All variants have the following capabilities:
- Open a back door
 - Execute files & commands
 - Delete, modify, and create registry keys
 - Gather and transmit information about the compromised computer

Breaches



In the last 8 years more than **7.1 billion** identities have been exposed in data breaches

Notable targeted attack groups

Sandworm <small>≈ 2014</small> Aliases / <i>Quedagh, BE-2 APT</i> Tools, tactics, & procedures (TTP) Spear phishing, vulnerabilities, zero-days, custom back door programs, destructive payloads Motives Espionage, sabotage Target categories & regions Governments, international organizations, energy, Europe, US Recent activities Limited to destructive attacks against Ukrainian media and energy targets	Housefly <small>≈ 2001</small> Aliases / <i>Equalizer</i> Tools, tactics, & procedures (TTP) Watering holes, infected CD-ROMs, infected USB keys, vulnerabilities, zero-days, custom back door and information-stealing programs, worms programs Motives Espionage Target categories & regions Targets of interest to nation-state attackers Recent activities Breached in 2016, with tools and exploits leaked
Fritillary <small>≈ 2010</small> Aliases / <i>Coy Bear, Office Monkeys, EuroAPT, Curyduke, APT29</i> Tools, tactics, & procedures (TTP) Spear phishing, custom back door programs Motives Espionage, subversion Target categories & regions Governments, think tanks, media, Europe, US Recent activities Associated with Democratic National Committee (DNC) attacks	Strider <small>≈ 2011</small> Aliases / <i>Romsec</i> Tools, tactics, & procedures (TTP) Advanced surveillance tool Motives Espionage Target categories & regions Embassies, airlines, Russia, China, Sweden, Belgium Recent activities Uncovered by Symantec in 2016
Swallowtail <small>≈ 2007</small> Aliases / <i>Fancy Bear, APT28, Tsar Team, Sednit</i> Tools, tactics, & procedures (TTP) Spear phishing, watering holes, infected storage devices, vulnerabilities, zero-days, custom back door and information-stealing programs Motives Espionage, subversion Target categories & regions Governments, Europe, US Recent activities Associated with WADA and DNC hacks	Suckfly <small>≈ 2014</small> Aliases / <i>None</i> Tools, tactics, & procedures (TTP) Custom back door programs signed using stolen certificates Motives Espionage Target categories & regions E-commerce, government, technology, healthcare, financial, shipping Recent activities Targeted attacks using multiple stolen code-signing certificates
Cadelle <small>≈ 2012</small> Aliases / <i>None</i> Tools, tactics, & procedures (TTP) Custom back door programs Motives Espionage Target categories & regions Airlines, telecommunications, Iranian citizens, governments, NGOs Recent activities Surveillance on domestic targets in Iran and eigs in the Middle East	Buckeye <small>≈ 2009</small> Aliases / <i>APT3, UPS, Gothic Panda, TG-0110</i> Tools, tactics, & procedures (TTP) Spear phishing, zero-days, custom back door programs Motives Espionage Target categories & regions Military, defense industry, media, education, US, UK, Hong Kong Recent activities Shifted focus from Western targets to Hong Kong
Appleworm <small>≈ 2012</small> Aliases / <i>Lazarus</i> Tools, tactics, & procedures (TTP) Spear phishing, 0Day attacks, disk wiping, zero-days, custom back door and information-stealing programs, destructive payloads Motives Espionage, sabotage, subversion Target categories & regions Financial, military, governments, entertainment, electronics Recent activities Subject to disruption operations in early 2016. Links with Bangladesh bank attackers	Tick <small>≈ 2006</small> Aliases / <i>None</i> Tools, tactics, & procedures (TTP) Spear phishing, watering holes, custom back door programs Motives Espionage Target categories & regions Technology, broadcasting, aquatic engineering, Japan Recent activities Long-standing campaigns against targets in Japan



Cenários de Violação de Privacidade

Fonte: Symantec Internet Security Threat Report 2016 e 2017



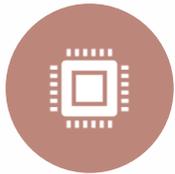
As empresas que oferecem novas tecnologias não se preocupam com segurança, num primeiro momento



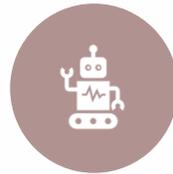
Pessoas são “seduzidas” a usar novas tecnologias, mas em geral não avaliam os riscos de segurança



Pessoas cometem os mesmos erros ou erros similares no transcorrer do tempo



Mesmos ataques continuam funcionando, em diferentes tecnologias



Novos ataques /violações de segurança / Privacidade surgem constantemente



O número de relatos de ataques /ou violações bem sucedidos aumenta sempre

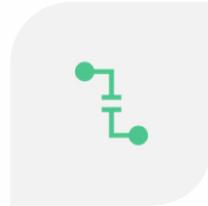
Considerações



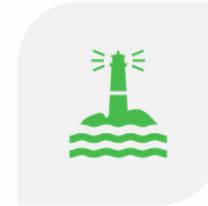
Segurança e Privacidade da informação **são ortogonais em vários aspectos** e precisam de tratamento diferenciado



Segurança e Privacidade da informação **ainda não são concebidas e incorporadas ao projeto de sistemas desde o seu início (by design)**



Sistemas falham porque os **ambientes** tecnológicos são e serão cada vez mais **heterogêneos e complexos**



Pessoas não são treinadas para lidar com as necessidades de segurança e privacidade e, em geral, também não sabem o que exigir dos sistemas que usam



A estimativa é que em 2022 haja algo como **1.8 milhões* de vagas de emprego não preenchidas** na área de CiberSegurança no mundo

*www.csoonline.com/article/2953258/it-careers/cybersecurity-jobmarketfigures-2015-to-2019-indicate-severe-workforce-shortage.html

Considerações



Investimento forte em formação de profissionais, pesquisadores e graduados, em cursos de segurança e privacidade da informação



Investimento forte e contínuo em capacitação de educadores para termos futuros jovens conscientes de necessidades de segurança e privacidade



Investimento forte e contínuo em capacitação da população, desenvolvimento de campanhas de conscientização, em especial para pessoas “tecnologicamente vulneráveis”



Incentivo forte e contínuo à pesquisa, desenvolvimento e inovação, para melhorar a competitividade do país no mercado mundial



Representação da CESeG e demais comissões especiais da SBC na ANPD

Necessidades para mudar o futuro

O Referencial Curricular (RF) esta em elaboração e considera os seguintes aspectos de Segurança:

Segurança de Dados

- conceitos básicos de criptografia, comunicação seguras fim-a-fim, forense digital, integridade de dados e autenticação e exclusão de dados

Segurança de Software

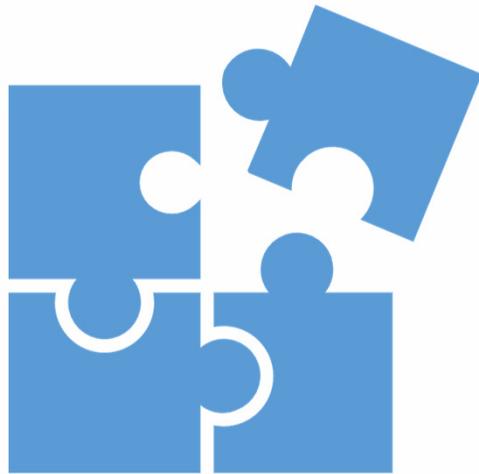
- princípios fundamentais de desenvolvimento e implementação, análise e testes, *deploy* e manutenção, documentação e ética

Segurança de Componentes

- vulnerabilidade dos sistemas de componentes, obtenção de componentes, teste de componentes, engenharia reversa de componentes

Segurança de Conexão

- mídia física, interface física e conectores, arquitetura de hardware, arquitetura de sistemas distribuídos, arquitetura de rede de computadores, segurança de sistemas, implementação de rede de computadores, serviços de redes de computadores e defesa de rede de computadores



Segurança de Sistemas

- *system thinking*, segurança de software, manutenção de sistemas, acesso a sistemas, controle de sistemas, arquitetura comum de sistemas, conexão segura

Segurança de Pessoas

- gestão de identidade, engenharia social, conformidade pessoal com normas de cibersecurity/regras/políticas/ética, conscientização e entendimento, privacidade social e comportamental, segurança e privacidade de dados pessoais, e privacidade e segurança usável

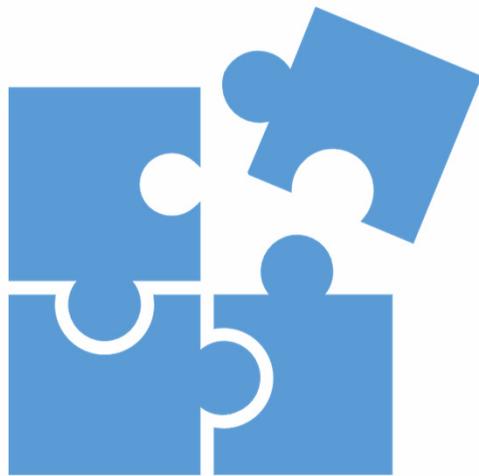
Segurança organizacional

- gestão de risco, política e governança de segurança, privacidade de dados, leis, ética, conformidade, ferramentas de analítica, administração de sistemas, planejamento de cibersegurança, continuidade do negócio, desastre e recuperação e gestão de incidentes, gestão de programa de segurança, segurança pessoal, segurança de operações

Segurança Societal

- abrange o espectro global de: cibercrimes, direito digital, ética digital, políticas digitais e privacidade

O RF é inspirado no documento da iniciativa internacional do GRCC, “Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity” (<http://cybered.acm.org/>).



<http://www.sbc.org.br>

altair.santin@pucpr.br

[sb.org.br](mailto:sbc@sb.org.br)

