GTER 46 | GTS 32

CYBERWARFARE, MERCADO DE VULNERABILIDADES E O QUE TUDO ISSO TEM A VER COM VOCÊ

Vinícius Oliveira Ferreira

vinicius.olifer@gmail.com

Vinicius Ferreira

- Desenvolvedor de Aplicações e *Subject Matter Expert* nas áreas de Redes e Segurança.
- Professor de Graduação e Pós-Graduação.
- Mestre em Ciência da Computação pela Unesp e o Lab. ACME! de pesquisa em Cibersegurança.
- Entusiasta de Desenvolvimento Seguro.
- Certificado Security+

Disclaimer

- Todas as declarações nesta apresentação são de minha responsabilidade e em nenhum momento falo pelo meu empregador.

AGENDA

- ❑ Cyberwarfare e APTs
- ❑ Mercado de Vulnerabilidades
- ❑ Impactos sobre o Ecossistema
- ❑ Reduzindo os Riscos

AGENDA

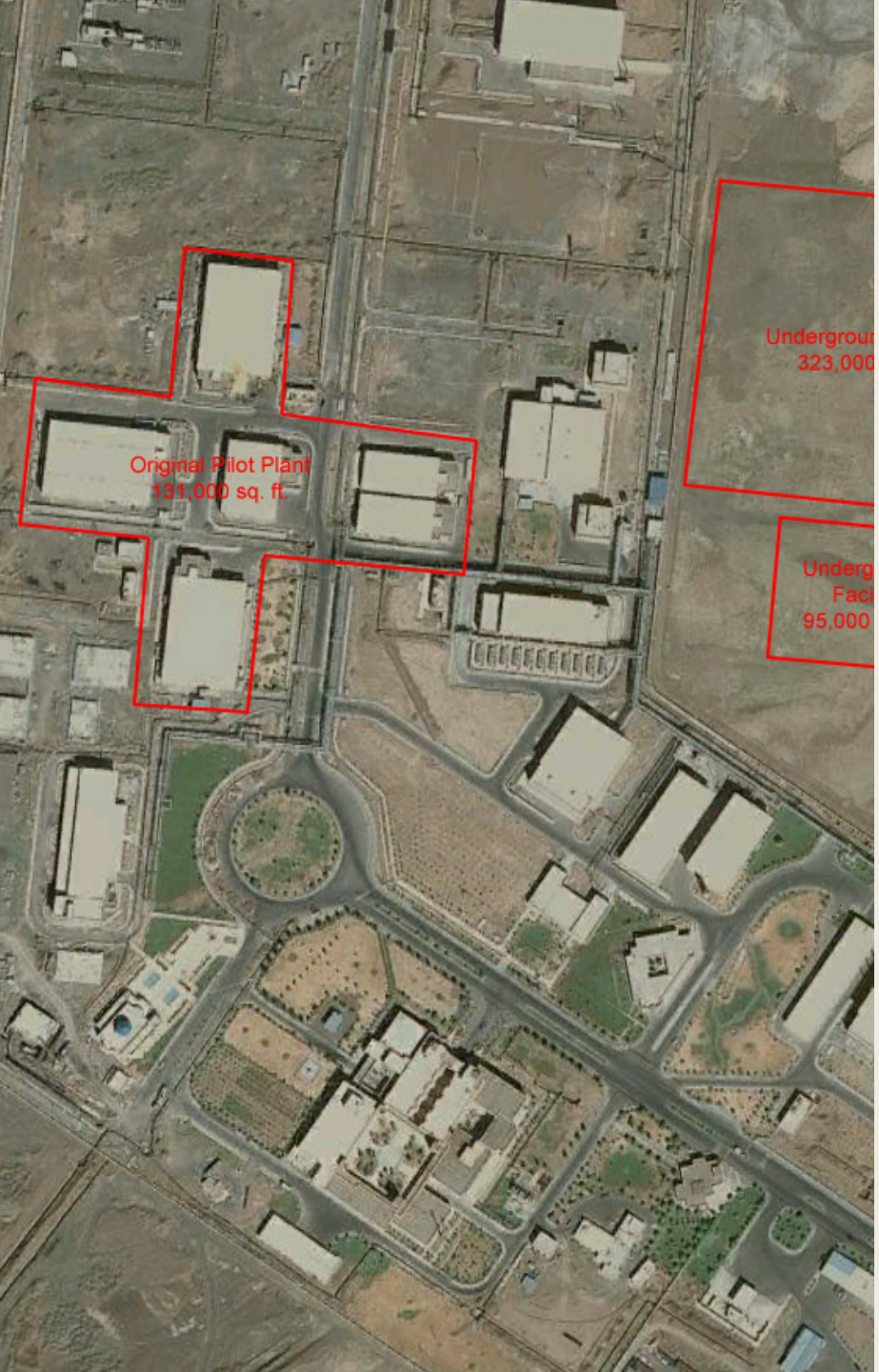
- ❑ Cyberwarfare e APTs
- ❑ Mercado de Vulnerabilidades
- ❑ Impactos sobre o Ecossistema
- ❑ Reduzindo os Riscos

Estônia - 2007

Governo decide recolocar o monumento do ‘Soldado de Bronze’, em homenagem aos soldados do exercito vermelho.

Bancos, órgãos governamentais, meios de comunicação passam a ser atingidos por severos ataques DDoS.

Ataques foram atribuídos a **Rússia**, marcando o inicio de uma série de ataques **patrocinados por nações** [1].



Stuxnet - 2010

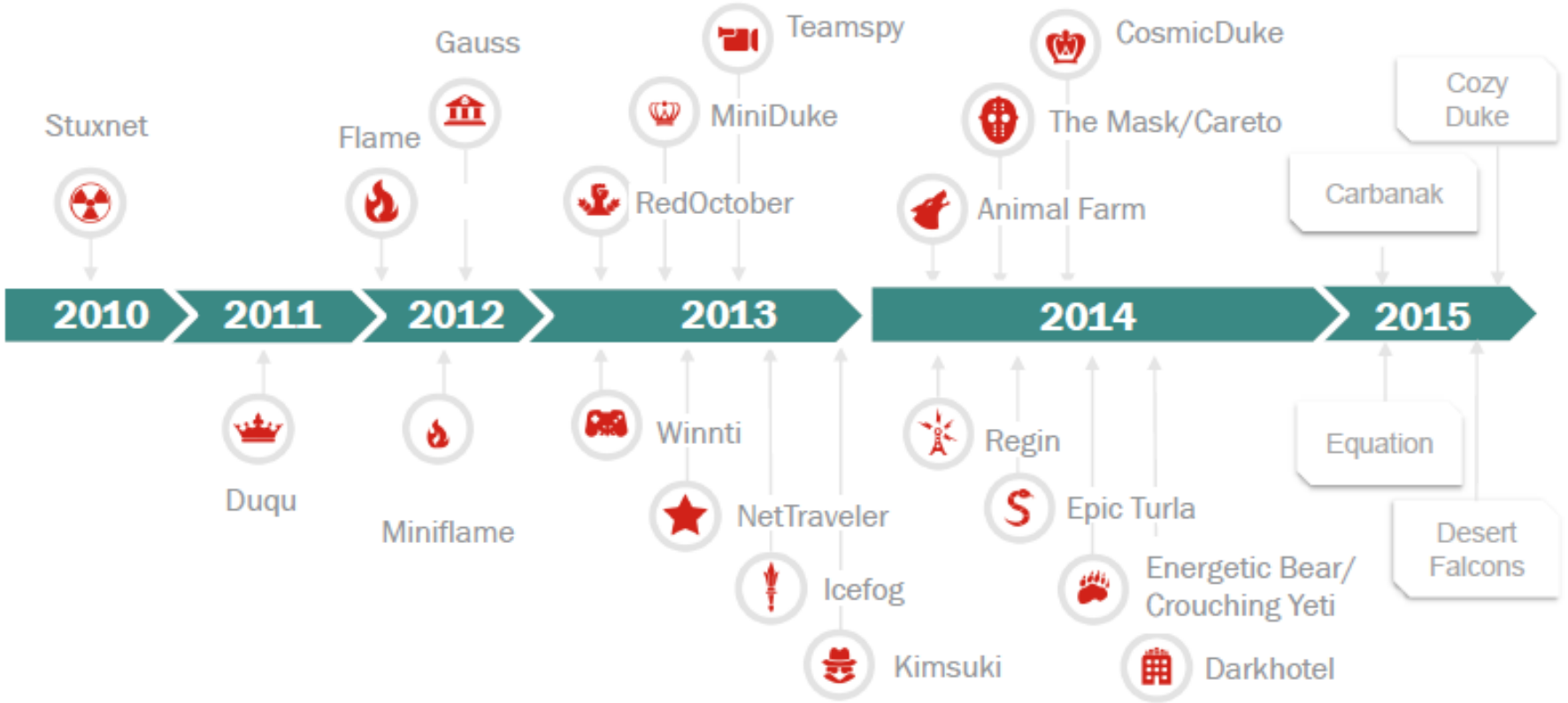
Operação contra as instalações nucleares de Natanz, no Irã, com objetivo de e danificar as centrifugas de enriquecimento de urânio.

Atrasou o programa nuclear Iraniano por período que pode ir de 18 a 24 meses [2].

Atribuído a Estados Unidos e Israel.

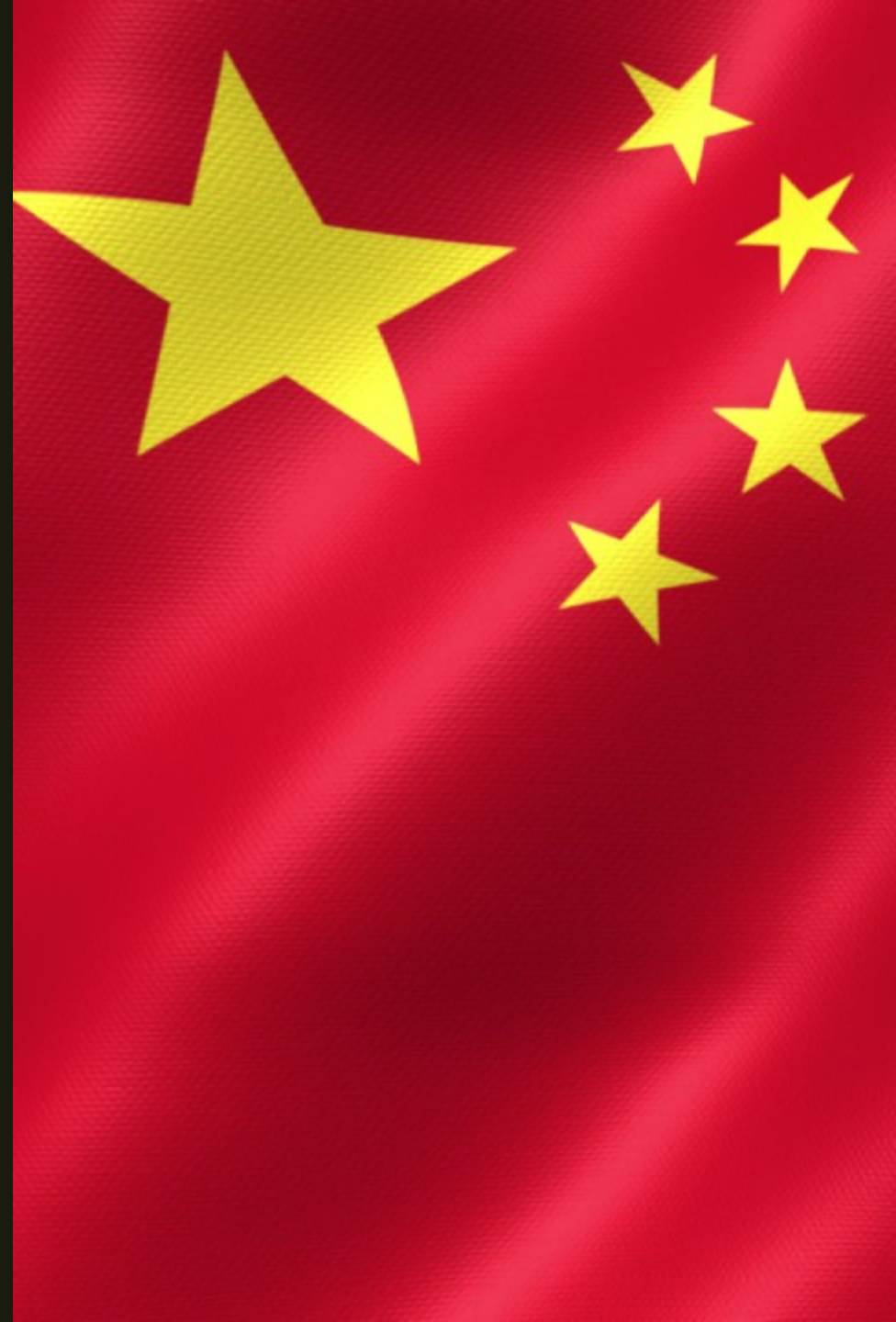
APT mais sofisticada até a data de sua descoberta.

APT ATTACKS


Stuxnet
Gauss
Flame
Teamspy
MiniDuke
RedOctober
CosmicDuke
The Mask/Careto
Animal Farm
Cozy Duke
Carbanak
2010
2011
2012
2013
2014
2015
Duqu
Miniflame
Winnti
NetTraveler
Icefog
Kimsuki
Regin
Epic Turla
Energetic Bear/ Crouching Yeti
Darkhotel
Equation
Desert Falcons

China [3]

- APT 16
- Aurora Panda (APT17)
- Comment Crew
- Shell_Crew
- Emissary Panda
- APT3 (UPS)
- Hurricane Panda
- Icefog
- Ke3chang
- NetTraveler
- Night Dragon
- IXESHE
- Putter Panda
- Hellsing
- Naikon



Rússia [3]

- Energetic Bear
  - *Setor energético*
- Sandworm
- AOT28/Fancy Bear
  - *SOURFACE*
  - *CORESHELL*
  - *PawnStorm*
  - *STRONTIUM*
  - *CHOPSTICKS*
- The Dukes
- Snake

EUA [3]

- Olympic Games
  - *Stuxnet*
  - *Duqu*
  - *Flame*
  - *Gaus*
  - *miniFlame*
- Equation Group
  - *DOUBLEFANTASY*
  - *EQUATIONDRUG*
  - *GRAYFISH*
  - *EXTRABACON and EPICBANANA*
  - *EternalBlue*
- Regin
- Project Sauron ?

Coreia do Norte [3]

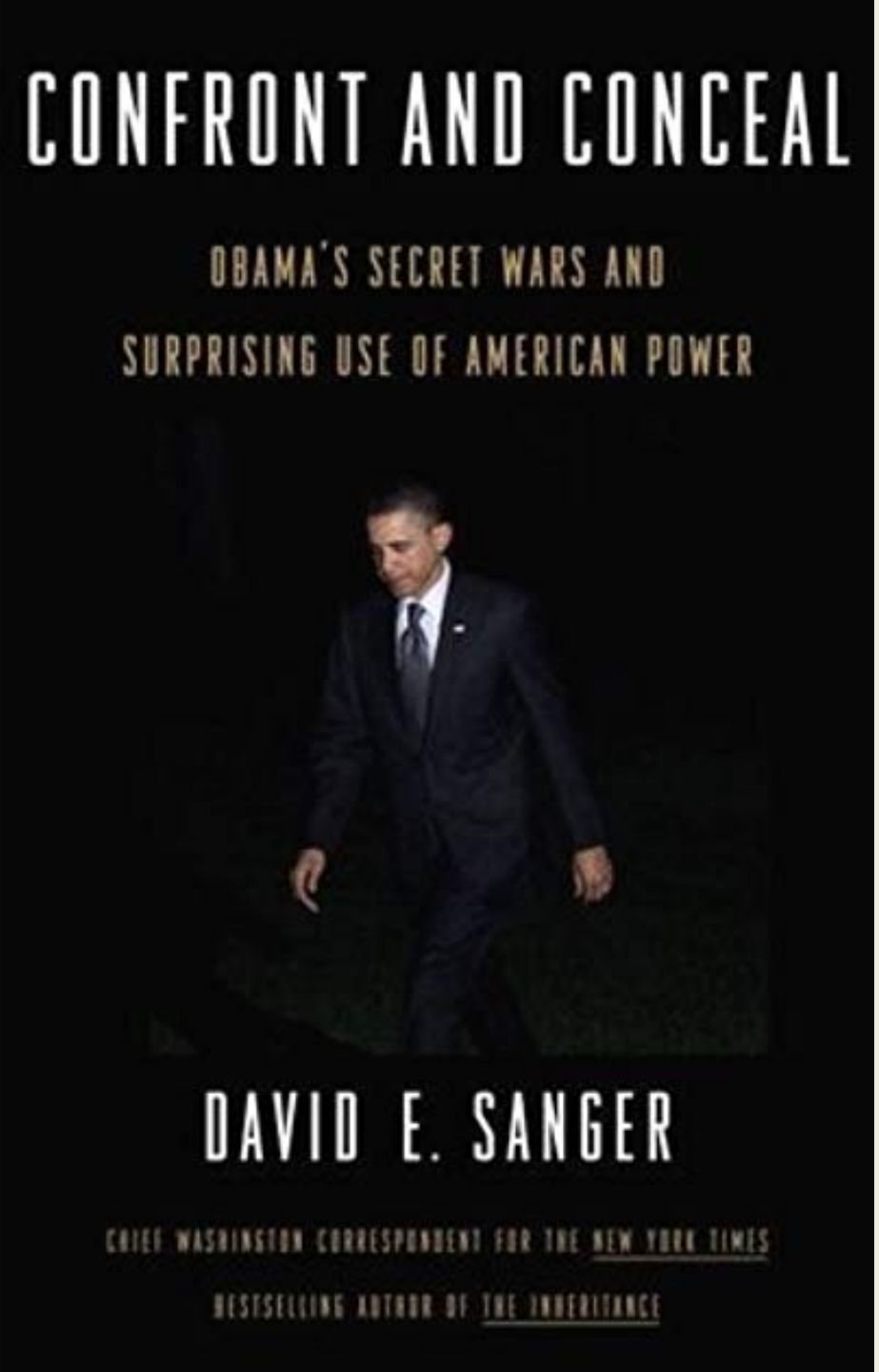
- Silent Chollima
  - *Operation Troy (a.k.a Dark Seoul);*
  - *Kimsuky operation;*
  - *Sony Pictures Attack.*

Irã [3]

- Shamoon attacks
- Clever Kitten
- Operation Saffron Rose
- OpClever
- Rocket Kitten

Paquistão [3]

- Transparent tribe



Por que Ciberguerra?

- Infraestruturas críticas controladas pelos sistemas computacionais.
- Custos reduzidos e alto potencial de impacto.
- Dificuldades de atribuição favorecem as “Covert Operations”.
- Dificuldades na classificação de um ato de guerra.

AGENDA

- ❑ Cyberwarfare e APTs
- ❑ Mercado de Vulnerabilidades
- ❑ Impactos sobre o Ecossistema
- ❑ Reduzindo os Riscos

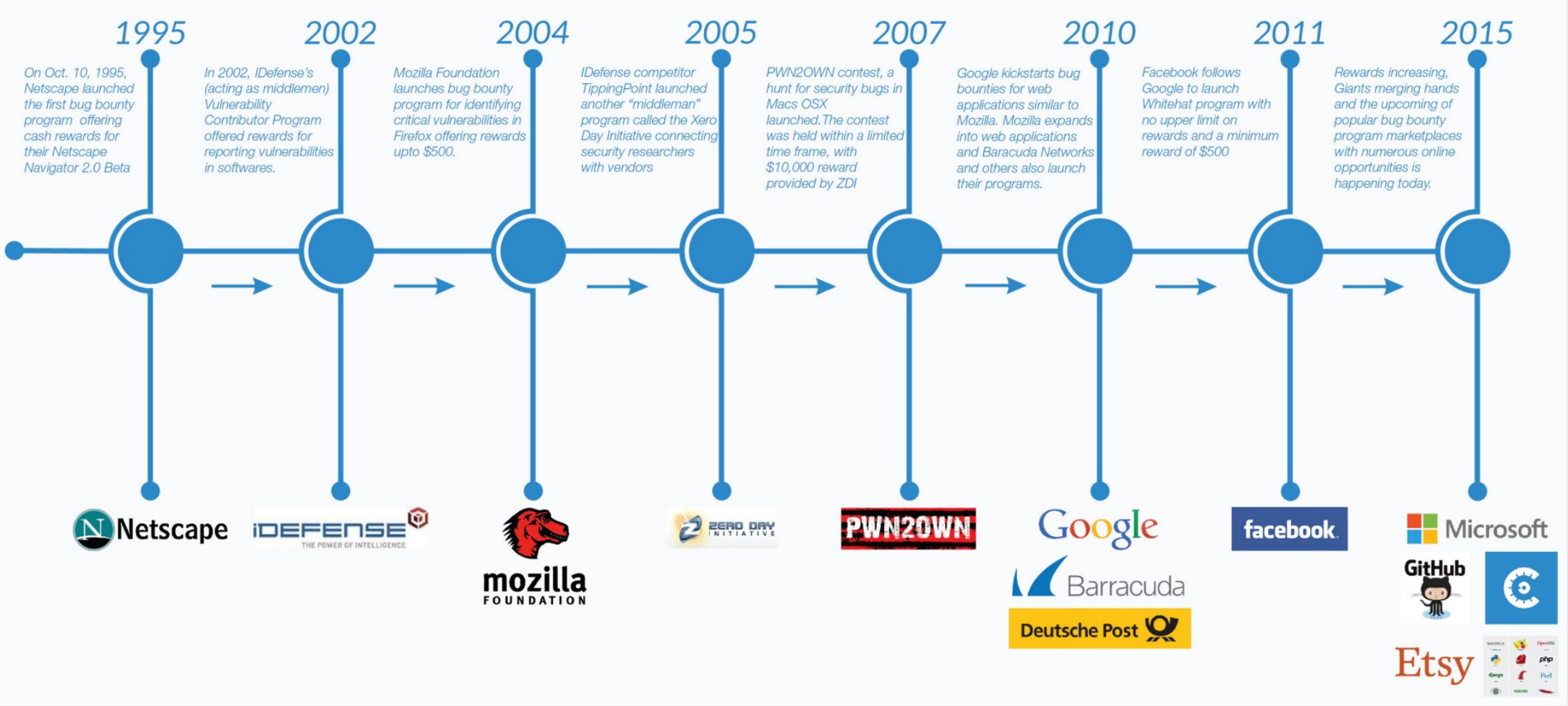
Mercado de Vulnerabilidades

- White Market – Bug Bounties
  - *Vulnerabilidades são negociadas com o propósito de serem corrigidas.*
- Os Players deste mercado podem ser divididos em diferentes categorias de acordo com seu modelo de negócios e incentivos:
  - *Security Vendors: ZDI*
  - *Plataformas de Bug-Bounty: HackerOne, BugCrowd, Hackaflag**
  - *Organizações: Microsoft, Google, Facebook*

bugcrowd

Mercado de Vulnerabilidades

- White Market – Bug Bounties



Valores – *White Market*

- HackerOne em 2015 reportou o pagamento médio de $650 USD por *bug* [4].
- BugCrowd reportou que seu pagamento médio é de $294.70 USD por *bug* [4].
- Pelo programa “Hack the Pentagon” foram pagos prêmios de de $100 - $15,000 [4].
- Companhias individuais podem pagar até centenas de milhares de dólares a depender da falha. Ex: Apple, Microsoft, Google.

Black Market

- Black-Market: *exploits* para criação de *bots*; roubo de informações online.
- Valor médio: $30,000–$50,000

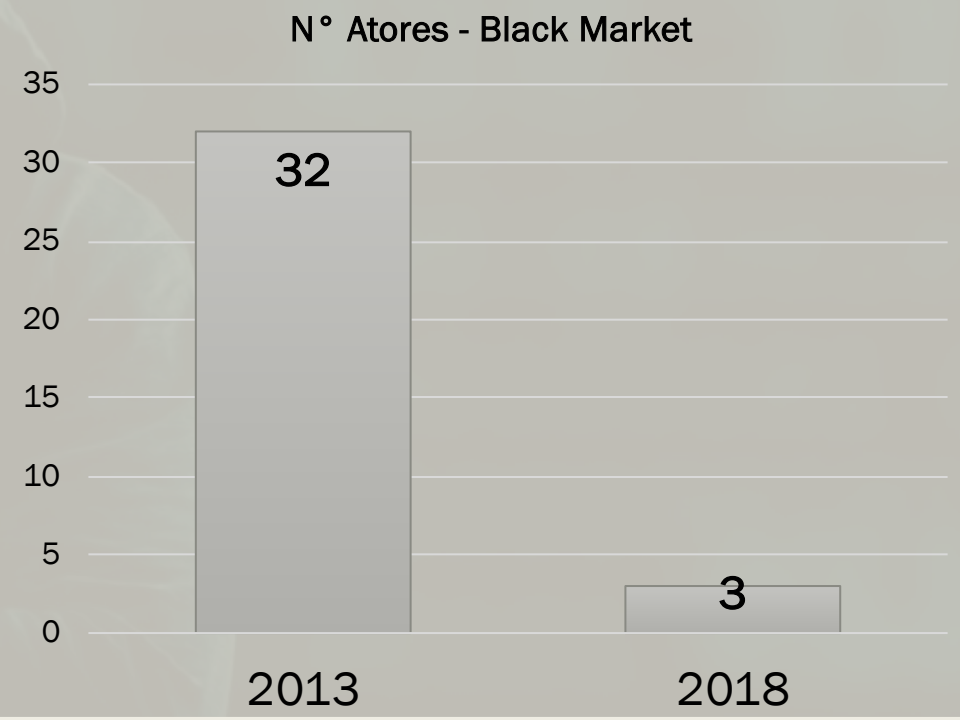
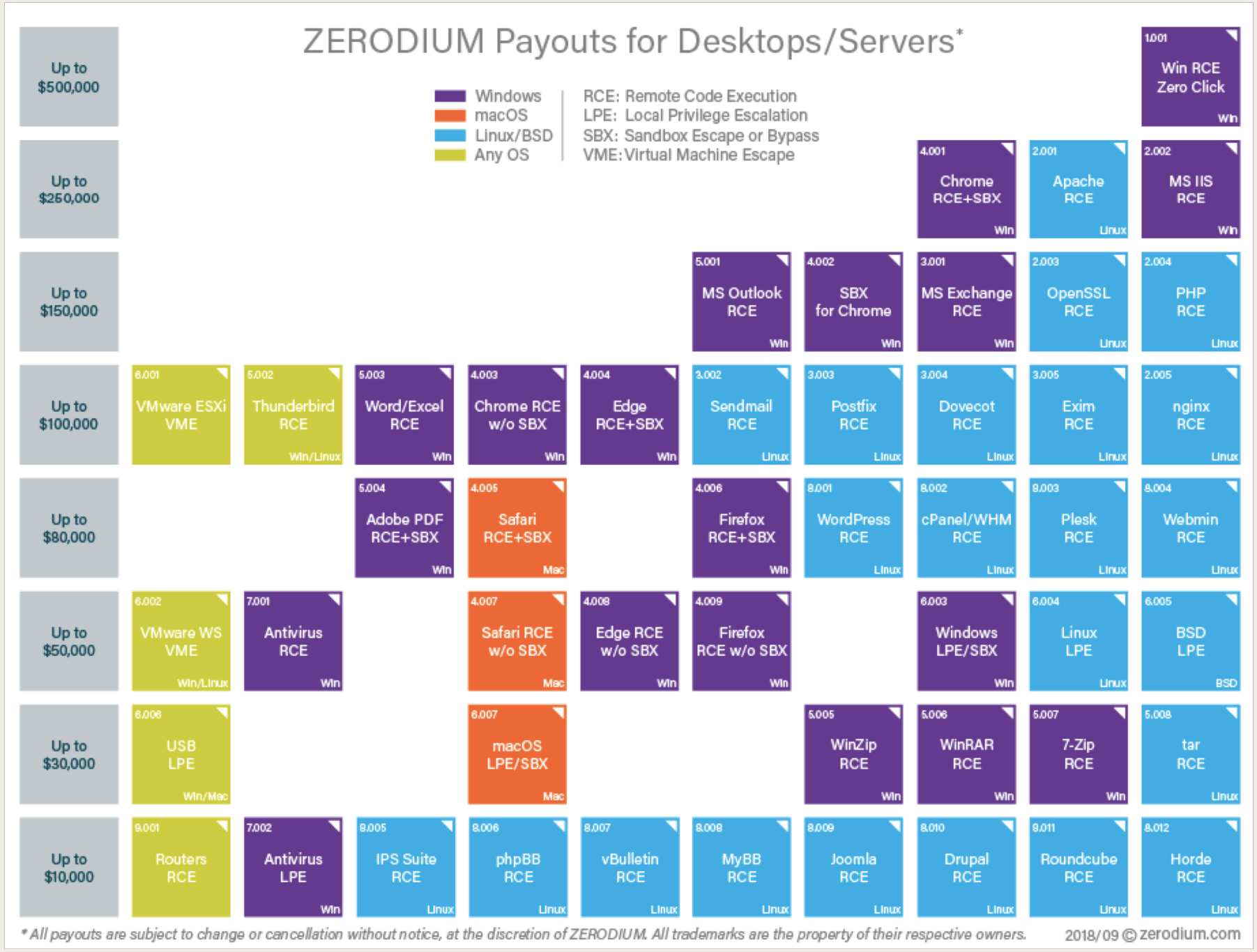
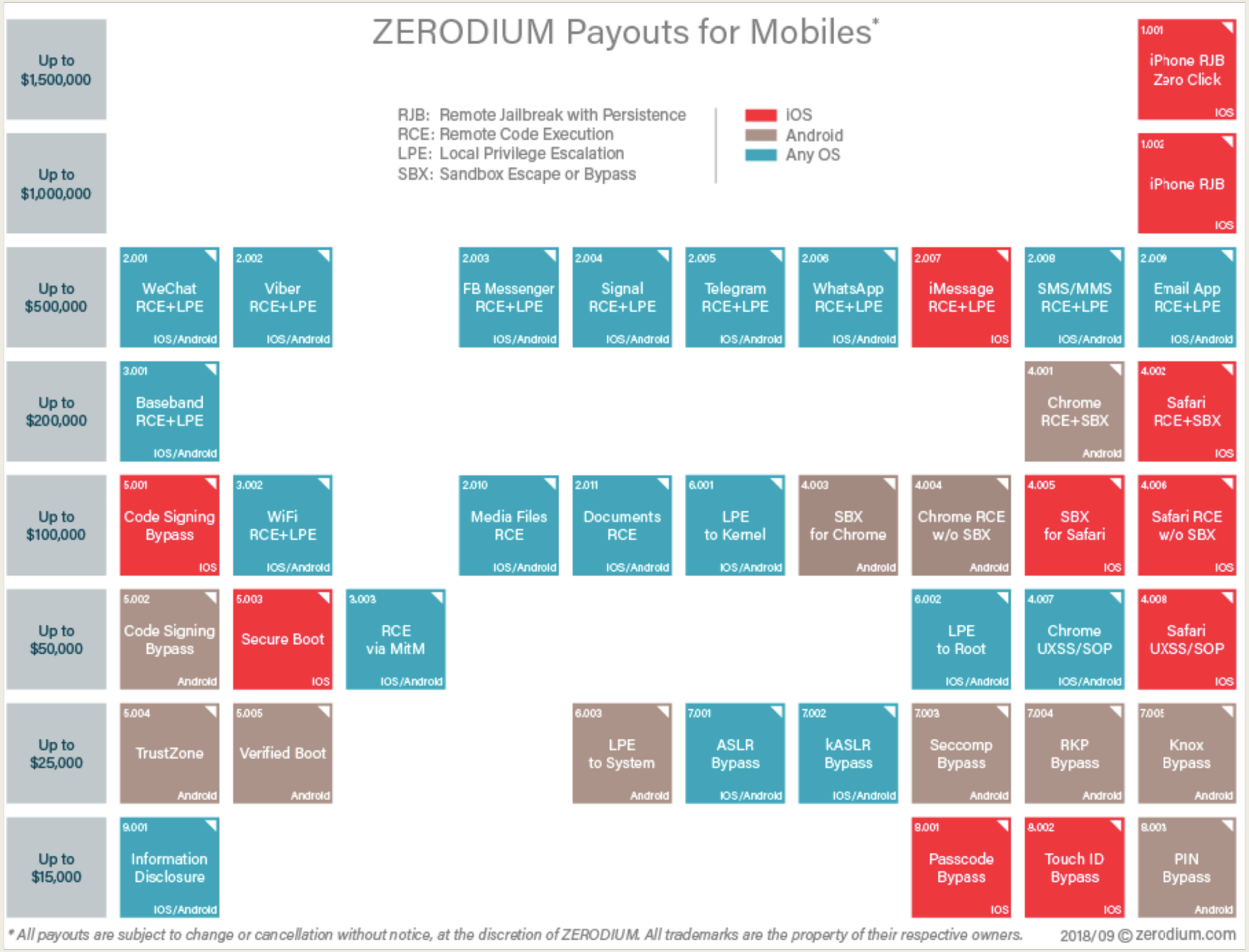


Gráfico baseado nas informações apresentadas em [5]

Grey Market

- Vulnerabilidades vendidas a governos, *Defense Contractors*, Brokers
  - *Instituições legítimas!*
- Vulnerabilidades não são corrigidas e não se sabe para que o *exploit* será usado
  - *Alguns Brokers fornecem algumas garantias (e.g. somente fazer negócios com estados democráticos de direito).*
- Altos preços
  - *Governos não sem importam com preços.*
  - *Comercialização de Exploits prontos para uso.*


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $500,000
1.001 Win RCE Zero Click Win
Up to $250,000
4.001 Chrome RCE+SBX Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $150,000
5.001 MS Outlook RCE Win
4.002 SBX for Chrome Win
3.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $100,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
5.003 Word/Excel RCE Win
4.003 Chrome RCE w/o SBX Win
4.004 Edge RCE+SBX Win
3.002 Sendmail RCE Linux
3.003 Postfix RCE Linux
3.004 Dovecot RCE Linux
3.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $80,000
5.004 Adobe PDF RCE+SBX Win
4.005 Safari RCE+SBX Mac
4.006 Firefox RCE+SBX Win
8.001 WordPress RCE Linux
8.002 cPanel/WHM RCE Linux
8.003 Plesk RCE Linux
8.004 Webmin RCE Linux
Up to $50,000
6.002 VMware WS VME Win/Linux
7.001 Antivirus RCE Win
4.007 Safari RCE w/o SBX Mac
4.008 Edge RCE w/o SBX Win
4.009 Firefox RCE w/o SBX Win
6.003 Windows LPE/SBX Win
6.004 Linux LPE Linux
6.005 BSD LPE BSD
Up to $30,000
6.006 USB LPE Win/Mac
6.007 macOS LPE/SBX Mac
5.005 WinZip RCE Win
5.006 WinRAR RCE Win
5.007 7-Zip RCE Win
5.008 tar RCE Linux
Up to $10,000
9.001 Routers RCE
7.002 Antivirus LPE Win
8.005 IPS Suite RCE Linux
8.006 phpBB RCE Linux
8.007 vBulletin RCE Linux
8.008 MyBB RCE Linux
8.009 Joomla RCE Linux
8.010 Drupal RCE Linux
8.011 Roundcube RCE Linux
8.012 Horde RCE Linux
* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.
2018/09 © zerodium.com


ZERODIUM Payouts for Mobiles*
RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $1,500,000
1.001 iPhone RJB Zero Click iOS
Up to $1,000,000
1.002 iPhone RJB iOS
Up to $500,000
2.001 WeChat RCE+LPE iOS/Android
2.002 Viber RCE+LPE iOS/Android
2.003 FB Messenger RCE+LPE iOS/Android
2.004 Signal RCE+LPE iOS/Android
2.005 Telegram RCE+LPE iOS/Android
2.006 WhatsApp RCE+LPE iOS/Android
2.007 iMessage RCE+LPE iOS
2.008 SMS/MMS RCE+LPE iOS/Android
2.009 Email App RCE+LPE iOS/Android
Up to $200,000
3.001 Baseband RCE+LPE iOS/Android
4.001 Chrome RCE+SBX Android
4.002 Safari RCE+SBX iOS
Up to $100,000
5.001 Code Signing Bypass iOS
3.002 WiFi RCE+LPE iOS/Android
2.010 Media Files RCE iOS/Android
2.011 Documents RCE iOS/Android
6.001 LPE to Kernel iOS/Android
4.003 SBX for Chrome Android
4.004 Chrome RCE w/o SBX Android
4.005 SBX for Safari iOS
4.006 Safari RCE w/o SBX iOS
Up to $50,000
5.002 Code Signing Bypass Android
5.003 Secure Boot iOS
3.003 RCE via MitM iOS/Android
6.002 LPE to Root iOS/Android
4.007 Chrome UXSS/SOP iOS/Android
4.008 Safari UXSS/SOP iOS
Up to $25,000
5.004 TrustZone Android
5.005 Verified Boot Android
6.003 LPE to System Android
7.001 ASLR Bypass iOS/Android
7.002 kASLR Bypass iOS/Android
7.003 Seccomp Bypass Android
7.004 RKP Bypass Android
7.005 Knox Bypass Android
Up to $15,000
9.001 Information Disclosure iOS/Android
8.001 Passcode Bypass iOS
8.002 Touch ID Bypass iOS
8.003 PIN Bypass Android
* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.
2018/09 © zerodium.com

The Washington Post
Democracy Dies in Darkness

National Security

U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show

The NSA designs most of its own implants, but it devoted $25.1 million this year to "additional covert purchases of software vulnerabilities" from private malware vendors, a growing gray-market industry based largely in Europe.


The Washington Post
Democracy Dies in Darkness
National Security
REUTERS
Business
Markets
World
Politics
TV
More
TECHNOLOGY NEWS
APRIL 28, 2016 / 10:30 PM / 3 YEARS AGO
FBI paid under $1 million to unlock San Bernardino iPhone: sources
Mark Hosenball
2 MIN READ
growing gray-market

The Washington Post
Democracy Dies in Darkness

MOTHERBOARD

HACKING | By Lorenzo Franceschi-Bicchierai | Apr 25 2018, 2:58pm

Startup Offers $3 Million to Anyone Who Can Hack the iPhone

A new startup in Dubai is offering six and seven figure payouts for zero-day exploits for Android, iOS, Windows and Mac.

Zero Days, Thousands of Nights

The Life and Times of Zero-Day Vulnerabilities and Their Exploit

Lillian Ablon, Andy Bogart

stories.[10] But even then, prices can vary. One vulnerability research firm we spoke to noted that their prices for exploits are three to five times those quoted in Zerodium's published price list (Zerodium, 2016).[11] Someone familiar with buying and selling

RAND CORPORATION

Grey Market - Valores

- Exploits ‘unicórnios’ vendidos na casa dos milhões, mas de modo geral, os preços variam de **$50k – $100k USD** ou de **$150k-$300k USD** a depender do *exploit* [4].
  - *Custo estimado para pesquisa e desenvolvimento de um exploit 0-day **$30k.***

Zero Days, Thousands of Nights

The Life and Times of Zero-Day Vulnerabilities and Their Exploits

Lillian Ablon, Andy Bogart

Implications for Offense

At the most basic level, any serious attacker can always get an affordable zero-day for almost any target. However, other tangible costs (acquiring products to find the vulnerabilities in, setting up test infrastructure, maintaining and porting the exploit to

RAND CORPORATION

AGENDA

- ❑ Cyberwarfare e APTs
- ❑ Mercado de Vulnerabilidades
- ❑ Impactos sobre o Ecossistema
- ❑ Reduzindo os Riscos

Impactos da Ascenção do Grey Market

- Os altos prêmios do Grey Market atraem mais talentos e propiciam os incentivos naturais para um aumento da sofisticação nas vulnerabilidades encontradas.
  - *Mitigações disponibilizadas pelo Kernel (e.g. non-executable stack, stack canaries, ASLR, etc.) não tem sido suficientes para a contenção dos ataques quando se existem os recursos necessários.*

- Por definição, as vulnerabilidades comercializadas neste mercado não são notificadas aos *vendors* para correção.

Money Talks

Dados vazados no ataque a HackingTeam indicaram negociações com países como: **Etiópia, Barém, Egito, Cazaquistão, Marrocos, Sudão, Arzeibajão e outros**

BUSINESS INSIDER

'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit

Rob Price Aug. 15, 2016, 12:17 PM

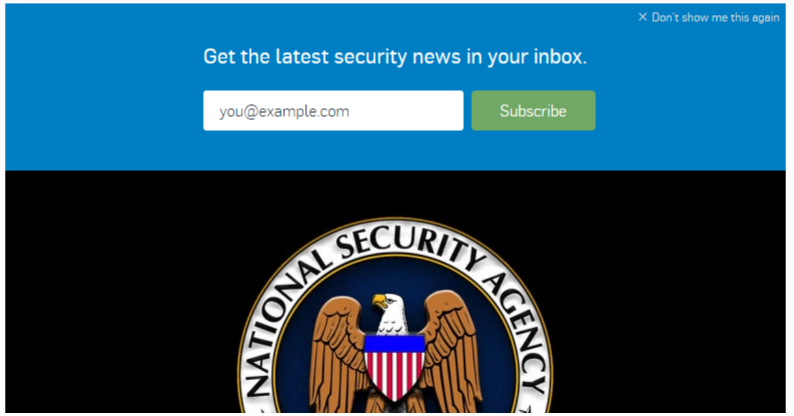
Cybersecurity experts are searching for answers after an unidentified group claimed on Monday to have hacked into "Equation Group" — an elite cyber-attack group associated with the NSA.

The National Security Agency's Utah Data Center in Bluffdale, Utah. Rick Bowmer/AP

Did "The Shadow Brokers" hack NSA cyberweapons worth $500M?

16 AUG 2016 18

Data loss



NSA Hacked? 'Shadow Brokers' Crew Claims Compromise Of Surveillance Op

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO

AGO/2016

Microsoft Office Windows Surface Xbox Deals Support More Sig

Microsoft Support Contact us

MS17-010: Security update for Windows SMB Server: March 14, 2017

Email

Print

Subscribe RSS Feeds

Applies to: Windows Server 2016 Datacenter, Windows Server 2016 Essentials, Windows Server 2016 Standard, Windows 10, Windows 10 Version 1511, Windows 10 Version 1607, Windows Server 2012 R2 Datacenter, Windows Server 2012 R2 Standard, Windows Server 2012 R2 Essentials, Windows Server 2012 R2 Foundation, Windows 8.1 Enterprise, Windows 8.1 Pro, Windows 8.1, Windows RT 8.1, Windows Server 2012 Datacenter, Windows Server 2012 Standard, Windows Server 2012 Essentials, Windows Server 2012 Foundation, Windows Server 2008 R2 Service Pack 1, Windows Server 2008 R2 Datacenter, Windows Server 2008 R2 Enterprise, Windows Server 2008 R2 Standard, Windows Web Server 2008 R2, Windows Server 2008 R2 Foundation, Windows 7 Service Pack 1, Windows 7 Ultimate, Windows 7 Enterprise, Windows 7 Professional, Windows 7 Home Premium, Windows 7 Home Basic, Windows 7 Starter, Windows Server 2008 Service Pack 2, Windows Server 2008 Foundation, Windows Server 2008 Standard, Windows Server 2008 for Itanium-Based Systems, Windows Web Server 2008, Windows Server 2008 Enterprise, Windows Server 2008 Datacenter, Windows Vista Service Pack 2, Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Starter, **Less**

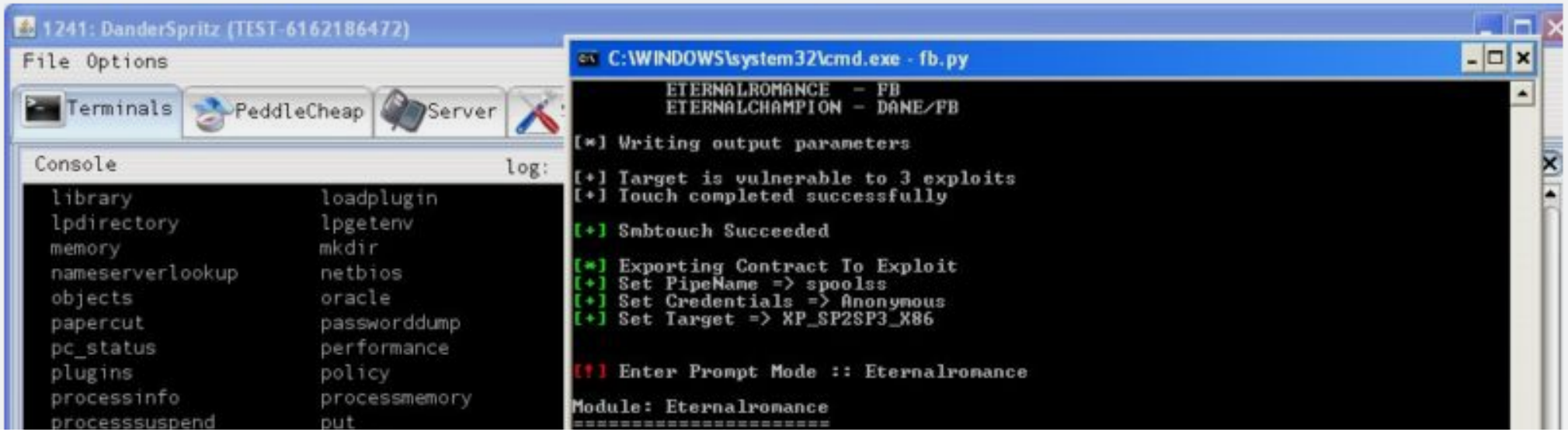
MAR/2017

RISK ASSESSMENT —

NSA-leaking Shadow Brokers just dumped its most damaging release yet

Windows zero-days, SWIFT bank hacks, slick exploit loader among the contents.

DAN GOODIN - 4/14/2017, 2:27 PM



APR/2017

Ferramentas vazadas:

- ETERNALROMANCE—Remote privilege escalation (SYSTEM) exploit (Windows XP to Windows 2008 over TCP port 445)
- ENTERNALCHAMPION, ETERNALSYSTEM—Remote exploit up to Windows 8 and 2012
- **ETERNALBLUE — Remote Exploit via SMB & NBT (Windows XP to Windows 2012)**
- EXPLODINGCAN—Remote IIS 6.0 exploit for Windows 2003
- EWORKFRENZY—Lotus Domino 6.5.4 and 7.0.2 exploit
- ETERNALSYNERGY—Windows 8 and Windows Server 2012
- FUZZBUNCH—Exploit Framework (Similar to Metasploit) for the exploits.

APR/2017


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
MAI/2017

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$188,000,000

Snack company Mondelez (parent company of Nabisco and Cadbury)

$300,000,000

Danish shipping company Maersk

$10 BILLION

Total damages from NotPetya, as estimated by the White House

$384,000,000

French construction company Saint-Gobain

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

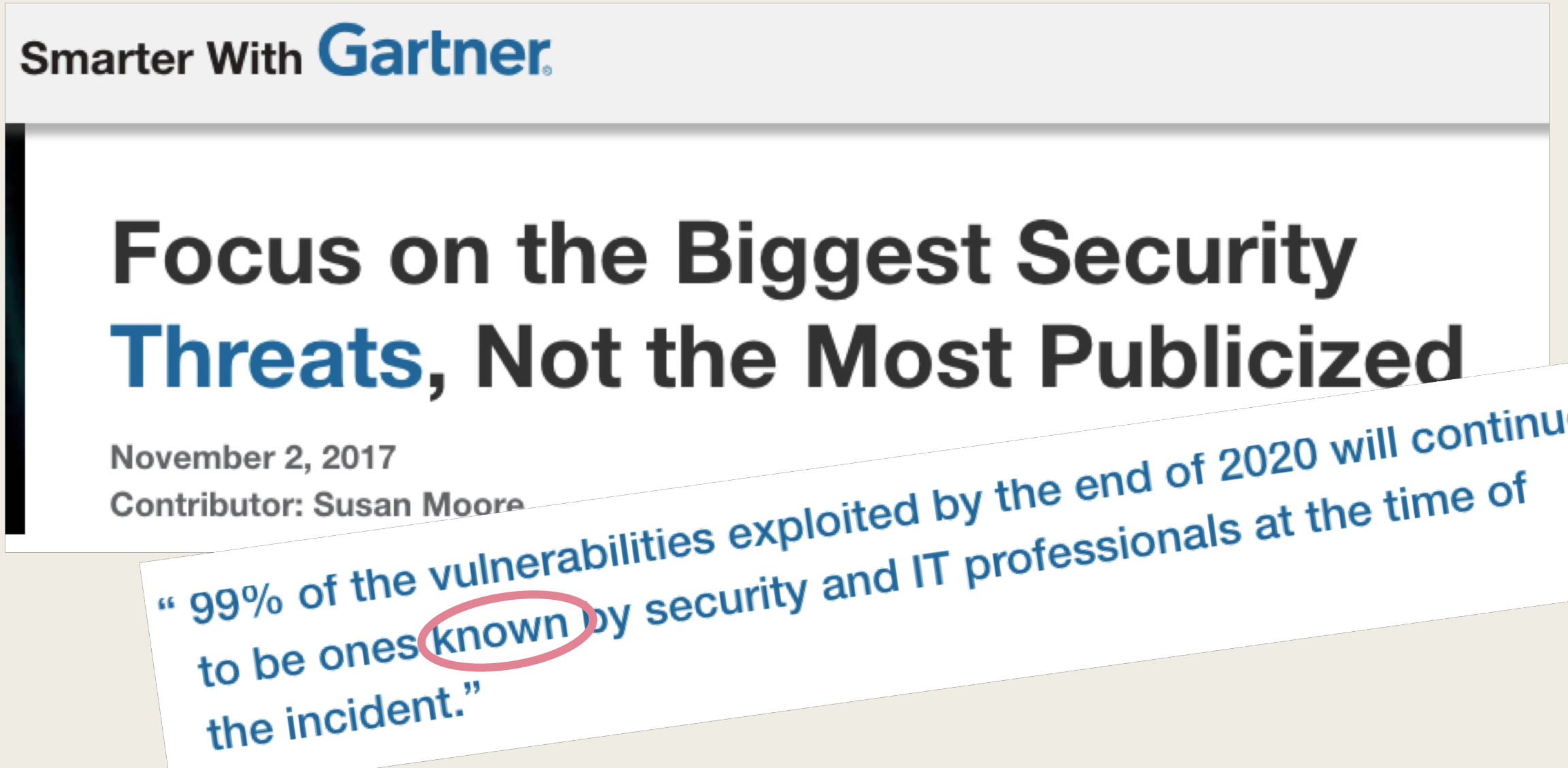
$870,000,000

Pharmaceutical company Merck

AGENDA

- ❑ Cyberwarfare e APTs
- ❑ Mercado de Vulnerabilidades
- ❑ Impactos sobre o Ecossistema
- ❑ Reduzindo os Riscos

0-day is not really your problem!



0-day is not really your problem!

and implementing those patches. For most attacks, a zero-day is not needed unless penetrating the target requires it. Generally, consumer-grade malware and tactics will get into almost any network, or "half-days" will suffice. That said, it is generally thought that if one can afford

Patch Managment

- A instalação de patches e atualizações de segurança é a forma mais eficaz para se prevenir infecções por malware que se dissemina pela exploração de vulnerabilidades.

- Patch Management compreende o *deploy* organizado de correções de Segurança de acordo com seu parque tecnológico.
  - *Controlar de forma manual todas as versões de todas as suas aplicações em todos os seus servidores costuma ser trágico!*

Uma questão de tempo

- Aceitar esta realidade leva a maior maturidade na implantação dos controles de segurança.
  - *Ênfase em contenção e plano de resposta a incidentes.*

Referências

[1] How a cyber attack transformed Estonia. Disponível em: <https://www.bbc.com/news/39655415>. Acesso em: 9 de dezembro de 2018.

[2] Obama Order Sped Up Wave of Cyberattacks Against Iran. Disponível em: <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>. Acesso em: 11 de dezembro de 2018.

[3] LEMAY, A.; CALVET, J.; MENET, F.; FERNANDEZ, J. M. Survey of publicly available reports on advanced persistent threat actors. Computers and Security, v. 72, p. 26–59, 2018. Elsevier Ltd.

[4] ABLON, L.; BOGART, A. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. 2017.

[5] Why the market for zero-day vulnerabilities on the dark web is vanishing. Disponível em: <https://www.fifthdomain.com/industry/2018/09/25/why-the-market-for-zero-day-vulnerabilities-on-the-dark-web-is-vanishing/>. Acesso em: 9 de dezembro de 2018.

vinicius.olifer@gmail.com

Vinicius Oliveira Ferreira

@viniciusofer

SECURITYIN
Security into your software