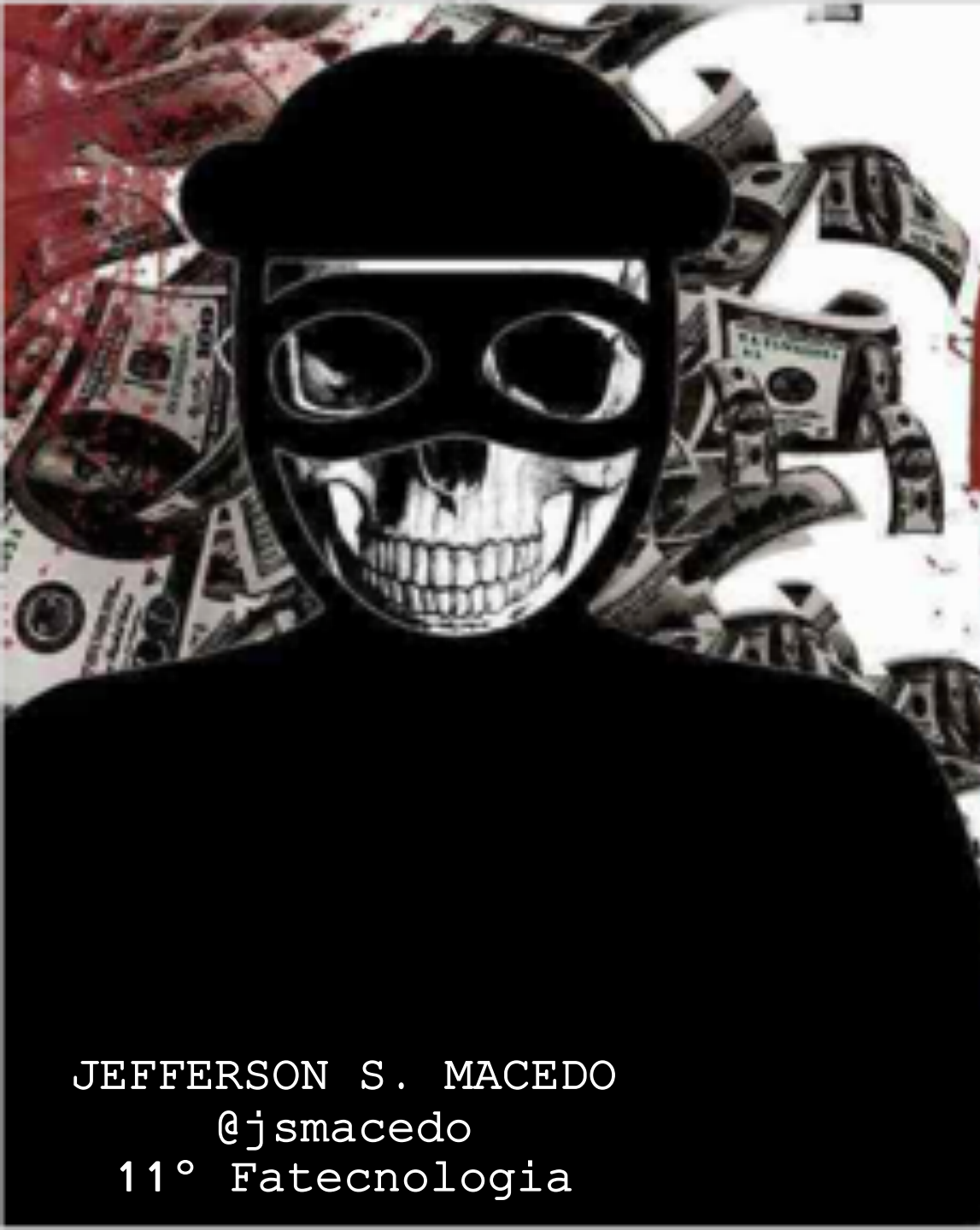


MERCADO NEGRO de Exploração de Vulnerabilidades

JEFFERSON S. MACEDO
@jsmacedo
11° Fatecnologia

AGENDA

- Quem Sou Eu?
- Vulnerabilidades e Como São Exploradas
- Um Pouco de História…
- Números!
- Quem Utiliza as Vulnerabilidades? Onde? Porque?
- Mercados de Vulnerabilidades
- Empresas Especializadas
- Nos Bastidores…
- De Qual Lado Você Ficará?

Quem sou eu?

- Consultor de Resposta a Incidentes e Serviços Proativos, IBM, X-Force IRIS, na América Latina.

- +10 anos de experiência profissional em Tecnologia da Informação, dos quais +5 são dedicados a Cibersegurança, Computação Forense e Auditoria Forense (Crimes de Colarinho Branco).

- Bacharelando em Direito (EPD)
- Bacharel em Sistemas de Informação (UMESP)
- Pós-Graduado em Computação Forense (Mackenzie)

- É pesquisador independente e membro de associações de investigação de crimes em meios digitais.

- **O conteúdo apresentado representa unicamente a minha opinião e não do meu empregador.**

Jefferson Souza Macedo

https://www.linkedin.com/in/jeffersonsmacedo

jefferson.macedo@protonmail.com

Vulnerabilidades e Como São Exploradas

- **Vulnerabilidade**

- **Exploit**

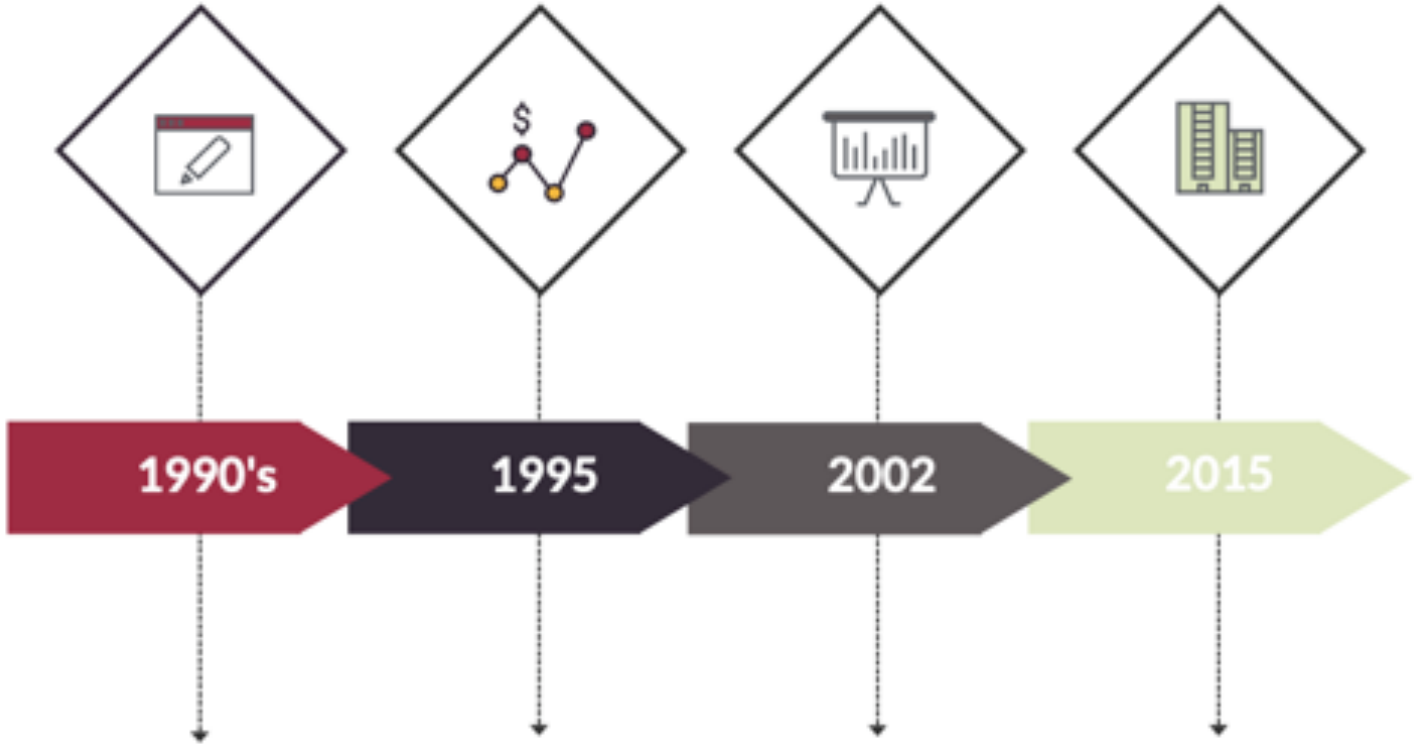
- **Vulnerabilidade não divulgada**

- **Zero Day**

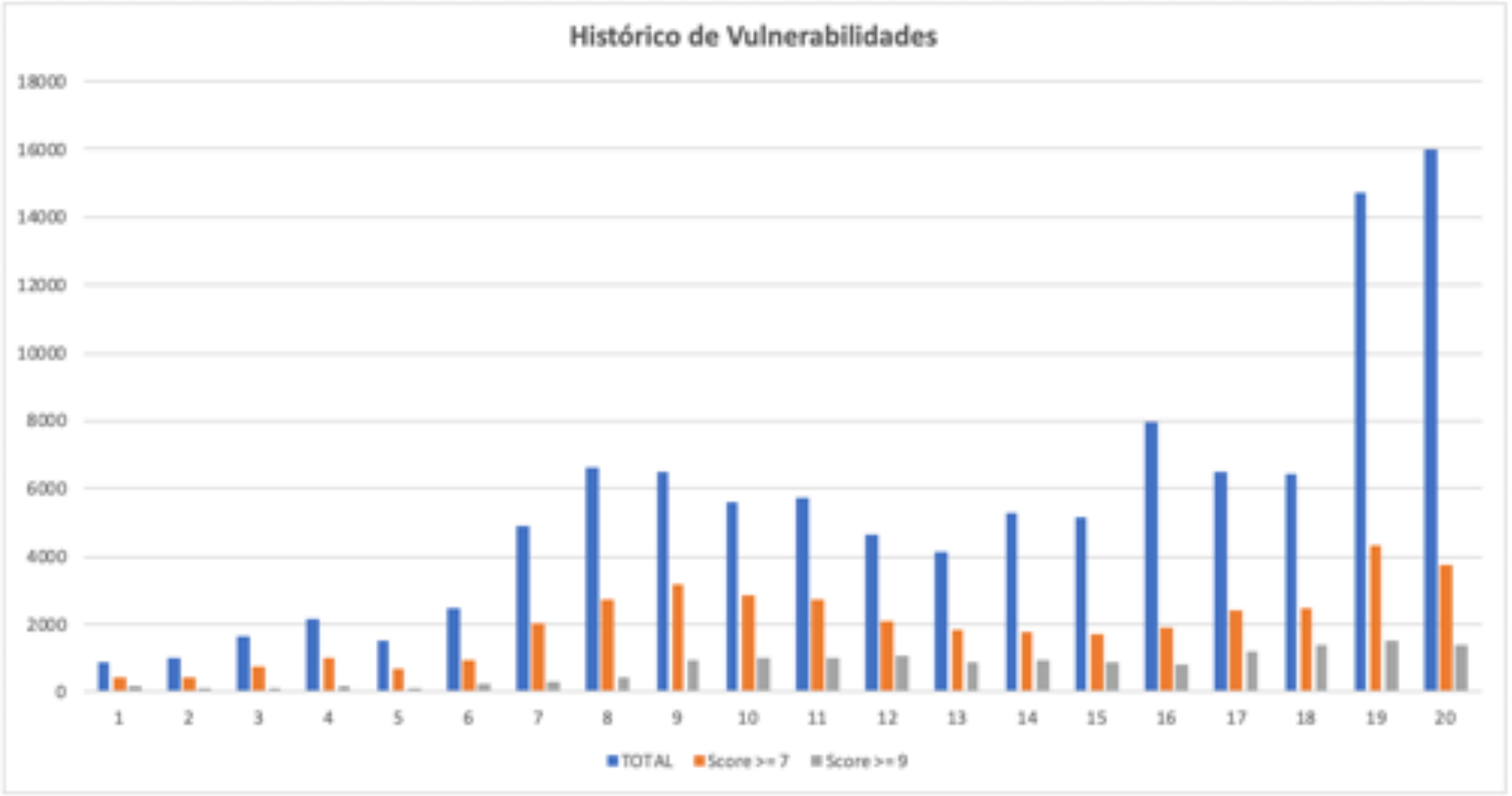
- **Vulnerabilidade Zero Day**

- Matéria-prima para a indústria de vigilância e espionagem.

Um Pouco de História...



Números!



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
TOTAL	894	1020	1677	2156	1527	2451	4935	6610	6520	5632	5736	4652	4155	5297	5191	7946	6480	6447	14714	16029
Score >= 7	423	452	772	1004	678	969	2041	2762	3159	2840	2719	2103	1824	1772	1737	1919	2401	2471	4325	3757
Score >= 9	164	144	150	159	134	222	309	427	980	1005	1033	1062	899	970	914	812	1204	1375	1524	1401

- O número de falhas críticas (CVSS v3) diminuiu em 8% na comparação entre 2017 e 2018.

Quem Utiliza as Vulnerabilidades? Onde? Porque?

Adversary	Category or Nation-State
SPIDER	ECRIME
CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
JACKAL	HACKTIVIST
TIGER	INDIA
KITTEN	IRAN
LEOPARD	PAKISTAN
PANDA	PEOPLE'S REPUBLIC OF CHINA
BEAR	RUSSIAN FEDERATION
CRANE	SOUTH KOREA
BUFFALO	VIETNAM

UNCOVER THE ADVERSARY

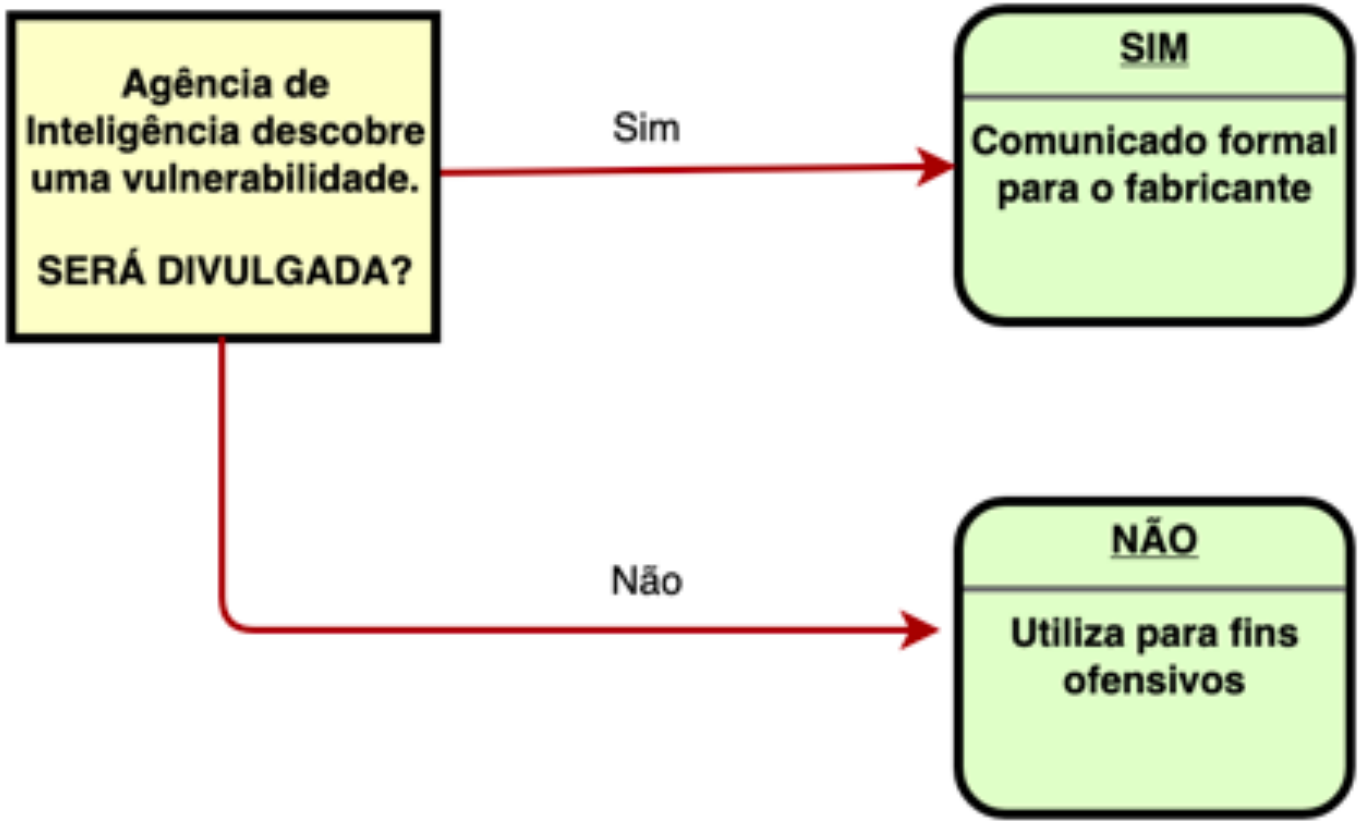
Mercados de Vulnerabilidades

- **White Market**
  - Bug Bounties;
    Security Vendors.

- **Gray Market**
  - Instituições legítimas;
  - Não se importam com preços;
  - Exploit será corrigido?

- **Black Market**
  - Não regulado;
  - Agentes anônimos;
  - Fins variados.

VPE (Vulnerability Equities Policy and Process)



*** Vulnerabilidade comprada de terceiro não passa por tal filtro.**

Empresas Especializadas

zerodium

azimuth

VUPEN security

Zerodium @Zerodium · Mar 5

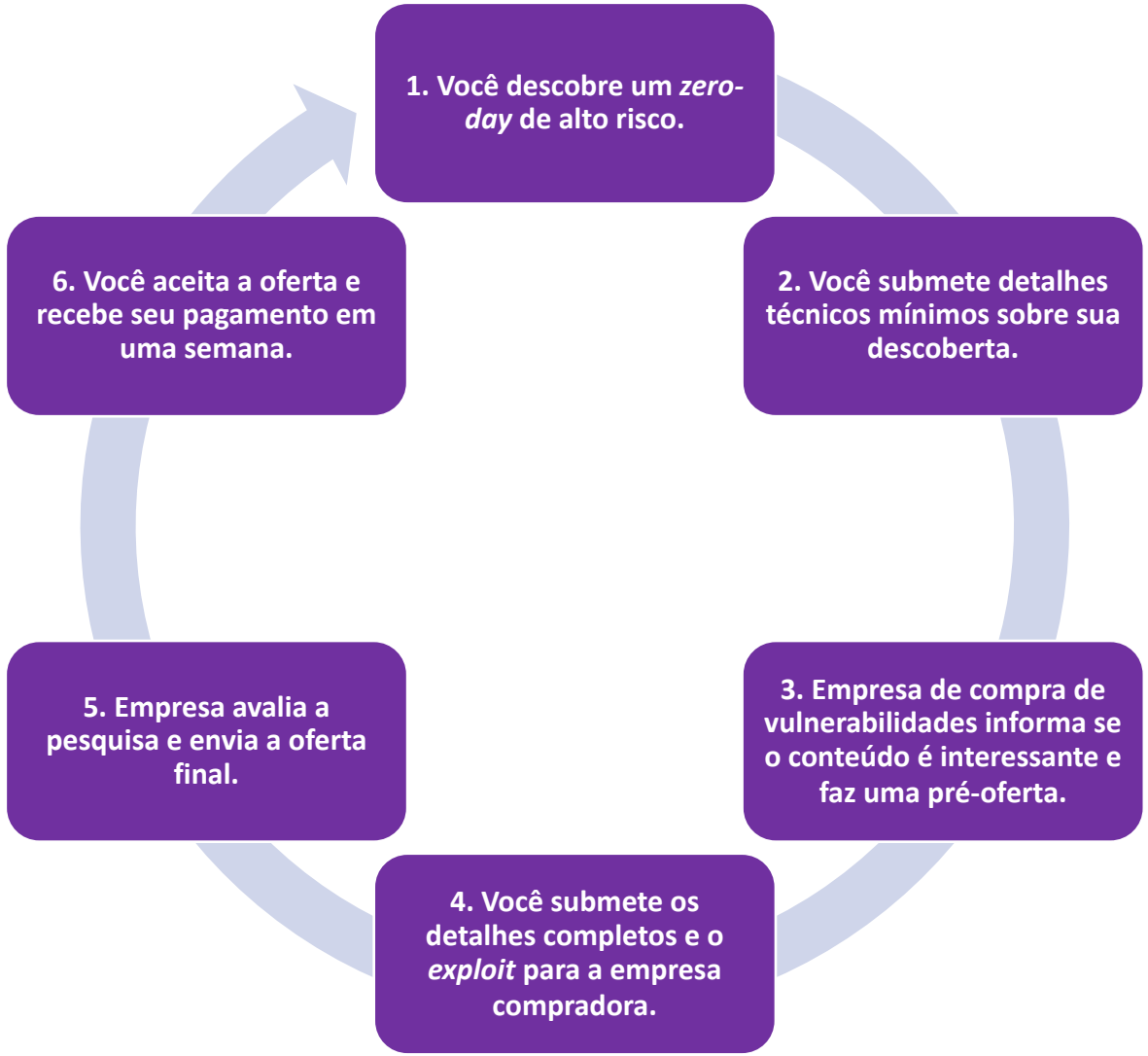
We're paying up to $500,000 for #0day exploits targeting VMware ESXi (vSphere) or Microsoft Hyper-V, and allowing Guest-to-Host escapes.
The exploits must work with default configs, be reliable, and lead to full access to the host. Contact us: zerodium.com/submit.html

14 123 221

Zerodium @Zerodium · Jan 7

Announcement: We are increasing our bounties for almost every product. We're now paying $2,000,000 for remote iOS jailbreaks, $1,000,000 for WhatsApp/iMessage/SMS/MMS RCEs, and $500,000 for Chrome RCEs.
More information at: zerodium.com/program.html#c…

Processo de Compra



Baseado em divulgação da Zerodium.

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 $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000						3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win	
Up to $250,000					5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux	
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux		4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux	
Up to $100,000		5.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.005 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.005 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	6.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

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 $2,000,000										1.001 iPhone RJB Zero Click iOS
Up to $1,500,000										1.002 iPhone RJB iOS
Up to $1,000,000							2.001 WhatsApp RCE+LPE iOS / Android	2.002 SMS/MMS RCE+LPE iOS / Android	2.003 iMessage RCE+LPE iOS
Up to $500,000	2.004 WeChat RCE+LPE iOS / Android			2.005 FB Messenger RCE+LPE iOS / Android	2.006 Signal RCE+LPE iOS / Android	2.007 Telegram RCE+LPE iOS / Android	2.008 Email App RCE+LPE iOS / Android	3.001 Chrome RCE+LPE Android	3.002 Safari RCE+LPE iOS
Up to $200,000	4.001 Baseband RCE+LPE iOS / Android		5.001 LPE to Kernel / Root iOS / Android	2.009 Media Files RCE+LPE iOS / Android	2.010 Documents RCE+LPE iOS / Android	3.003 SBX for Chrome Android	3.004 Chrome RCE w/o SBX Android	3.005 SBX for Safari iOS	3.006 Safari RCE w/o SBX iOS
Up to $100,000	6.001 Code Signing Bypass iOS / Android	4.002 WiFi RCE iOS / Android	4.003 RCE via MitM iOS / Android	5.002 LPE to System Android	7.001 Information Disclosure iOS / Android	7.002 [k]ASLR Bypass iOS / Android	8.001 PIN Bypass Android	8.002 Passcode Bypass iOS	8.003 Touch ID Bypass iOS

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

Nos bastidores...

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-Day Hunters Will Pay Over Twice as Much as Apple's New Bug Bounty Programme

Exodus Intelligence's new programme offers a potential payout of half a million dollars for Apple vulnerabilities.

FBI paid over $1.3 million to unlock San Bernardino iPhone

Nos bastidores...

Search: Search Extended search

0day Today Exploit Market and 0day Exploits Database

[private]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
26-01-2018	Twitter reset account Private Method 0day Exploit	tricks	49 856		R	D	-	✓	0.352	0day Today Team
07-01-2018	Instagram bypass Access Account Private Method Exploit	tricks	71 153		R	D	-	✓	0.352	smokzz
11-04-2018	Hotmail.com reset account 0day Exploit	tricks	19 169		R	D	-	✓	0.539	0day Today Team
07-08-2018	Facebook steal Group 0day Exploit	tricks	19 839		R	D	-	✓	0.475	0day Today Team
05-03-2019	Snapchat takeover any account 0day Exploit	tricks	5 713		R	D	-	✓	0.352	0day Today Team
03-02-2019	Tebillain Remote File Read Vulnerability	php	2 259		R	D	-	✓	0.088	Zedros
29-01-2019	Mod_Security <= 3.0 Bypass XSS Payload Vulnerability	tricks	3 083		R	D	-	✓	0.364	champloo
08-01-2019	facebook - Grabbing permanent access token which Never expires of your accounts and	Android	3 314		R	D	-	✓	0.352	deep007

[remote exploits]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
06-05-2019	LG Supersign EZ CMS - Remote Code Execution Exploit	hardware	15		R	D	C	✓	free	Alejandro Fanjul
06-05-2019	Xitami Web Server 2.5 - Remote Buffer Overflow (SEH + Egghunter) Exploit	windows	50		R	D	-	✓	free	ElSoufiane
03-05-2019	Blue Angel Software Suite - Command Execution Exploit	linux	218		R	D	-	✓	free	Paolo Serracino
03-05-2019	MailCarrier 2.51 HELP Remote Buffer Overflow Exploit	windows	183		R	D	-	✓	free	Vinaykumar Yennam
03-05-2019	Wordpress Social Warfare Plugin 3.5.3 - Remote Code Execution Exploit	php	166		R	D	C	✓	free	hash3liZer
03-05-2019	Ruby On Rails DoubleTap Development Mode secret_key_base Remote Code Execution Exploit	linux	333		R	D	C	✓	free	metasploit
03-05-2019	Windows PowerShell ISE / Filename Parsing Flaw Remote Code Execution Exploit	windows	169		R	D	-	✓	free	hyp3rlinx
01-05-2019	Freefloat FTP Server 1.0 - SIZE Remote Buffer Overflow Exploit	windows	179		R	D	-	✓	free	Kevin Randall

[local exploits]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
06-05-2019	NSClient++ 0.5.2.35 - Privilege Escalation Vulnerability	windows	11		R	D	-	✓	free	bzyo
01-05-2019	DeviceViewer 3.12.0.1 - user SEH Overflow Exploit	windows	151		R	D	C	✓	free	Hayden Wright
29-04-2019	SGI IRIX <= 6.5.5 sysmp() Onyx kernel memory disclosure Exploit	irix	195		R	D	-	✓	free	Hacker Fantastic
29-04-2019	SGI IRIX <= 6.4.x Run-Time Linker Arbitrary File Creation Exploit	irix	177		R	D	-	✓	free	Hacker Fantastic
25-04-2019	Lawavo CD Ripper 4.30 Local SEH Exploit	windows	249		R	D	-	✓	free	Achilles
24-04-2019	VirtualBox 6.0.4 r128413 - COM RPC Interface Code Injection Host Privilege Escalation	windows	315		R	D	C	✓	free	Google Security
24-04-2019	RARLAB WinRAR ACE Format Input Validation Remote Code Execution Exploit	windows	333		R	D	C	✓	free	Imran Dawoodjee
24-04-2019	Sony Smart TV Information Disclosure / File Read Vulnerabilities	hardware	327		R	D	C	✓	free	xen1thLabs

[web applications]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
06-05-2019	microASP (Portal+) CMS - (pagina.phtml?explode_tree) SQL Injection Vulnerability	asp	11		R	D	-	✓	free	felipe andrian
06-05-2019	PHPads 2.0 - (click.php3?bannerID) SQL Injection Vulnerability	php	15		R	D	-	✓	free	felipe andrian
06-05-2019	ReadyAPI 2.5.0 / 2.6.0 - Remote Code Execution Exploit	multiple	34		R	D	C	✓	free	Gilson Camelo
03-05-2019	Barco / AWIND OEM Presentation Platform Unauthenticated Remote Command Injection	hardware	181		R	D	C	✓	free	Jacob Baines
03-05-2019	Zotonic < 0.47.0 mod_admin - Cross-Site Scripting Vulnerability	multiple	124		R	D	C	✓	free	Ramón Janssen
03-05-2019	Instagram Auto Follow - Authentication Bypass Vulnerability	php	419		R	D	-	✓	free	VeyselXan
01-05-2019	Veeam ONE Reporter 9.5.0.3201 - Multiple Cross-Site Request Forgery Vulnerabilities	multiple	140		R	D	C	✓	free	Seyed Sadegh
01-05-2019	Veeam ONE Reporter 9.5.0.3201 - Persistent Cross-Site Scripting Vulnerability	multiple	121		R	D	-	✓	free	Seyed Sadegh

Contact us:

0day Today is the ultimate database
Our aim is to collect exploits
This was written solely for educ

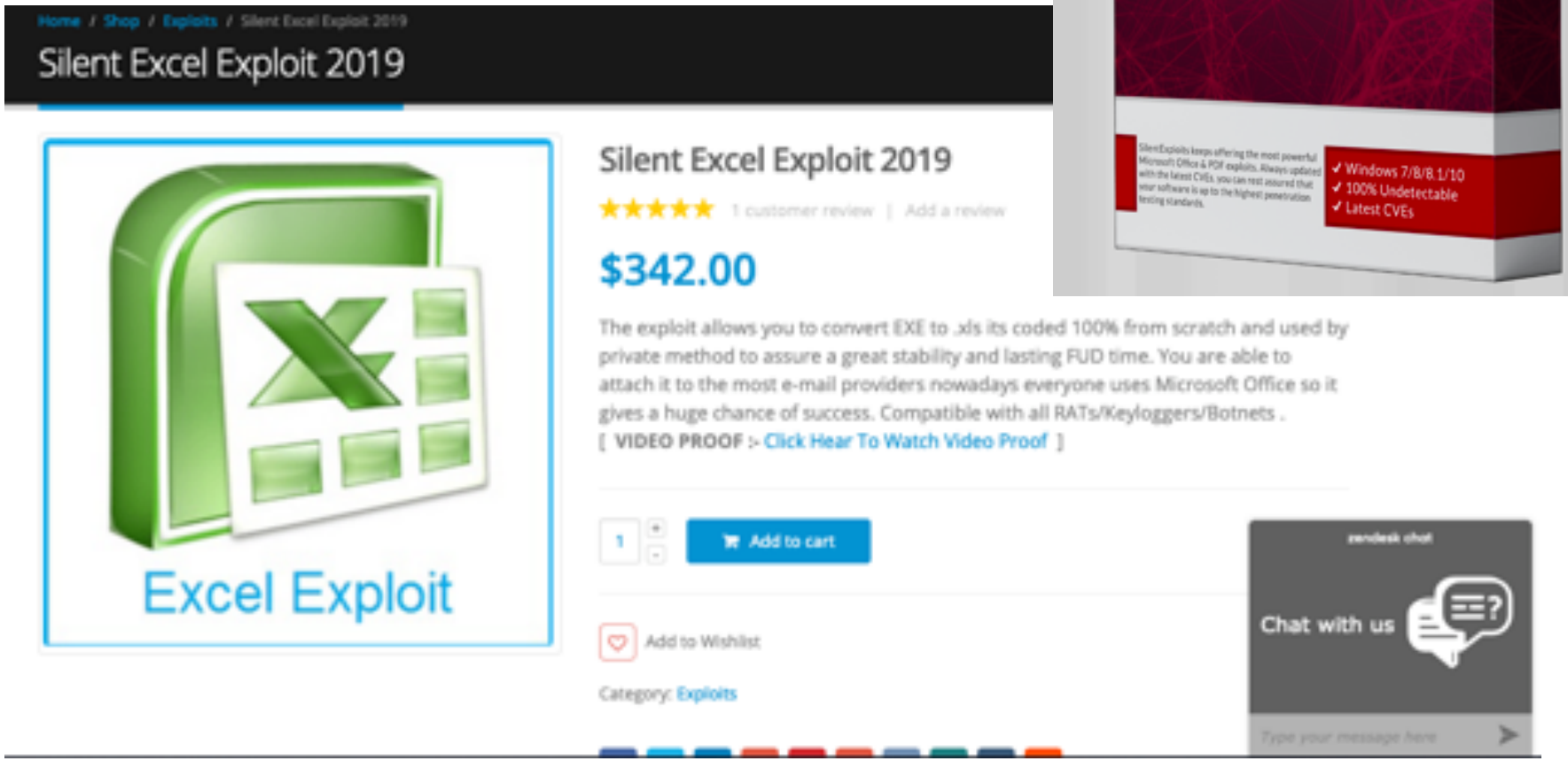
iOS 12.1.3 - cfprefsd Memory Corruption

Author	ZecOps	Risk	
Category	dos / poc	Date add	06
Platform	iOS		

```
1  // (c) 2019 ZecOps, Inc. - https
2  // Intended only for educational
3  // Use at your own risk.
4  // iOS 12.1.3 - cfprefsd Memory
5
6  #include <xpc/xpc.h>
7  #import <pthread.h>
8  #include <mach/mach.h>
9  #include <mach/task.h>
10 #include <dlfcn.h>
```

Nos bastidores...

Nos bastidores...



De qual lado você ficará?

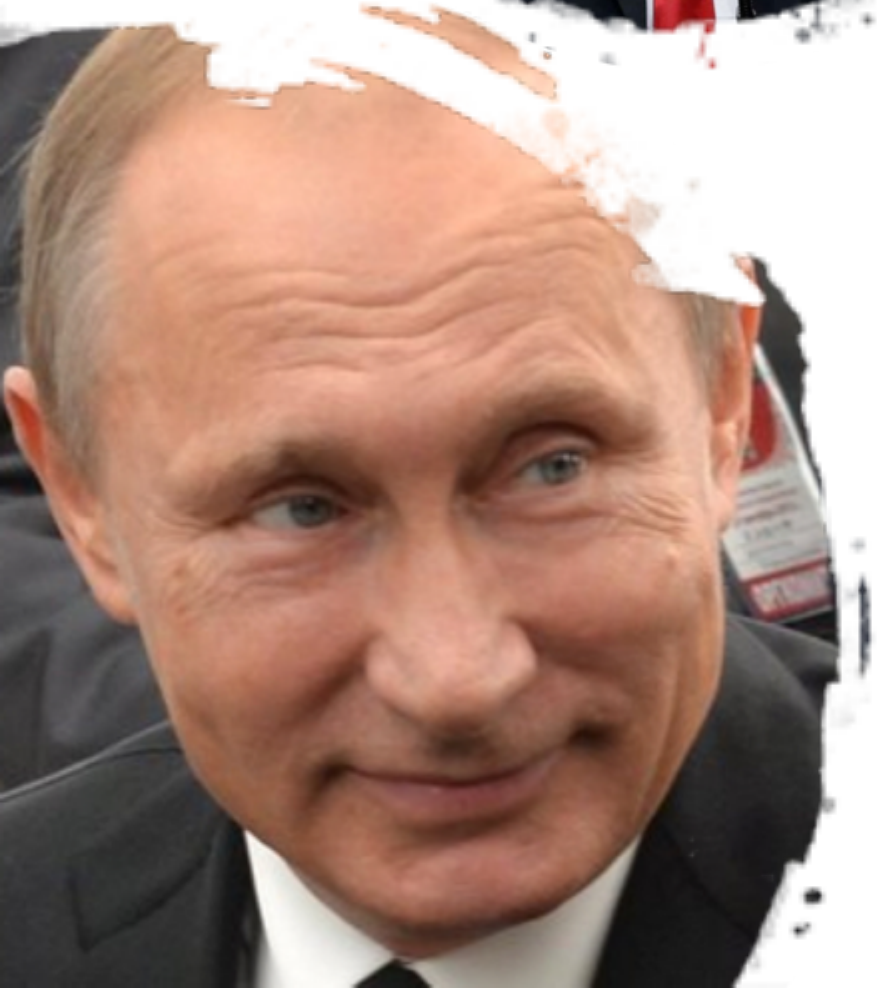
- *“Se você tivesse um 0day valioso, você venderia para alimentar sua família ou daria de graça para desenvolvedores de software alimentarem seus acionistas?”*

[Chaouki Bekrar, Fundador da Zerodium]


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Framework and Standard
COBIT
ISO/IEC
NIST
SANS/CSC
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics

Como ingressar na área de Segurança da Informação?

- *Eventos, eventos e mais eventos!*
  - *16 edição BSides SP: http://sp16.securitybsides.com.br*
  - *16 edição H2HC Conference: https://www.eventbrite.com.br/e/hackers-2-hackers-conference-registration-60034486766*
- *Podcast!*
  - *Segurança Legal: https://www.segurancalegal.com*
  - *Recorded Future: Threat Intel for Cybersecurity*



Agora que você sobreviveu até aqui...

OBRIGADO!!!

https://www.linkedin.com/in/jeffersonsmacedo

jefferson.macedo@protonmail.com