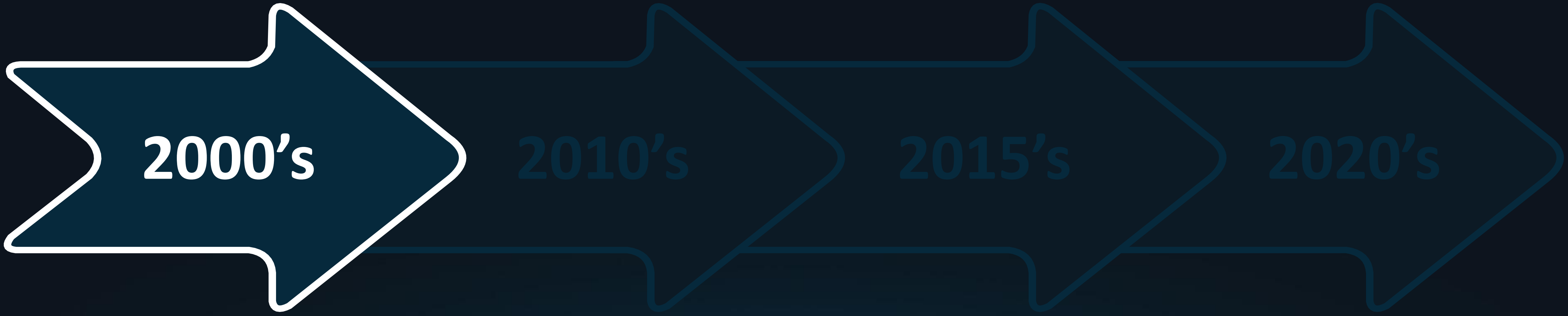
JSSI 2023

Patrowl

Évolution des méthodes offensives (à but défensif) dans le temps

C’est long le temps vous ne trouvez pas ?



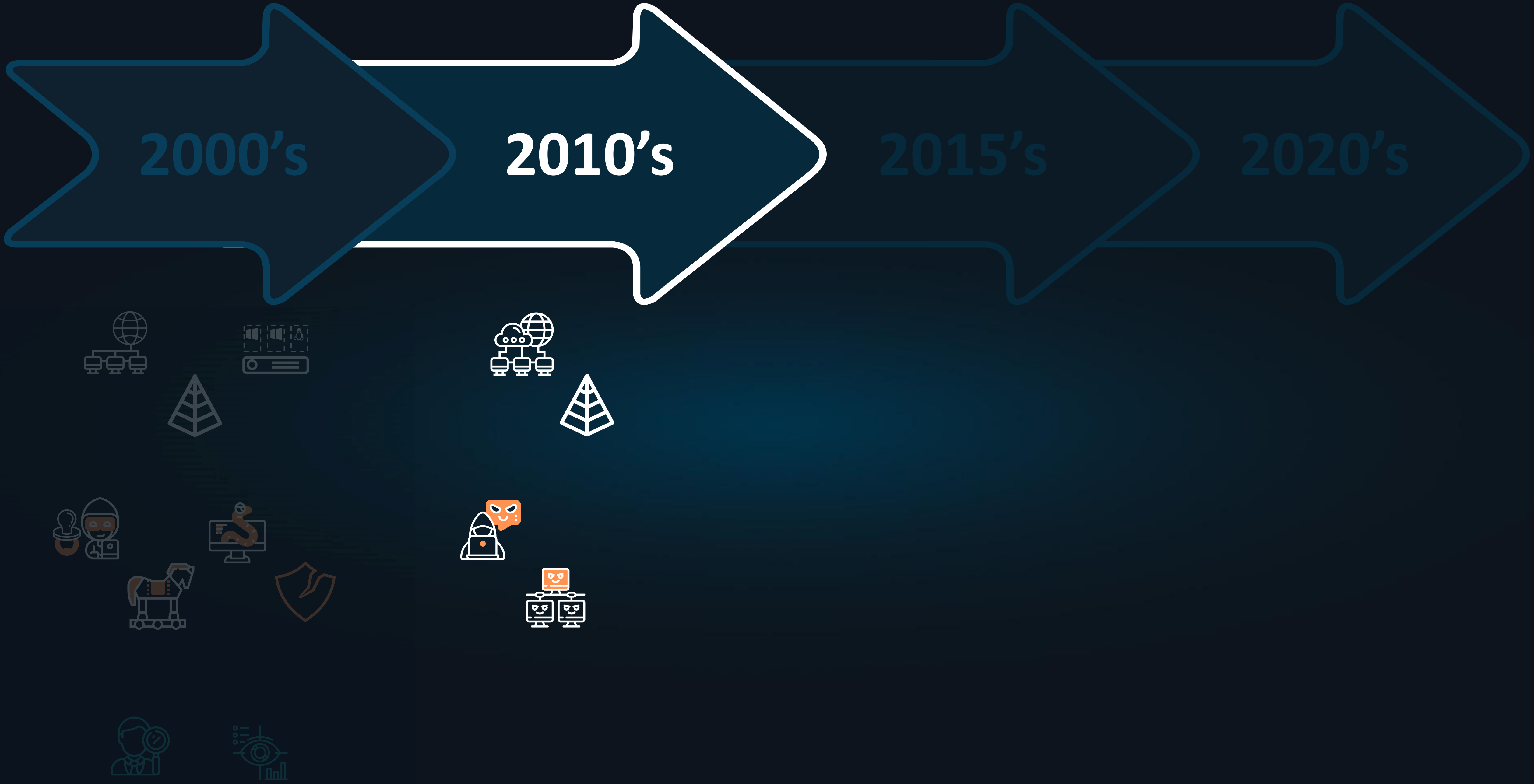
2000’s

2010’s

2015’s

2020’s

	Vulnerability management	Offensive Cybersecurity		
	Vulnerability Scanner			
Attack Surface	◐			
Continuous watch	○			
Qualification of vulnerabilities	○			
Prioritizing and contextualizing	◐			
Remediation plan	○			
Remediation follow-up	○			
Re-test	○			
Available for non-expert	○			

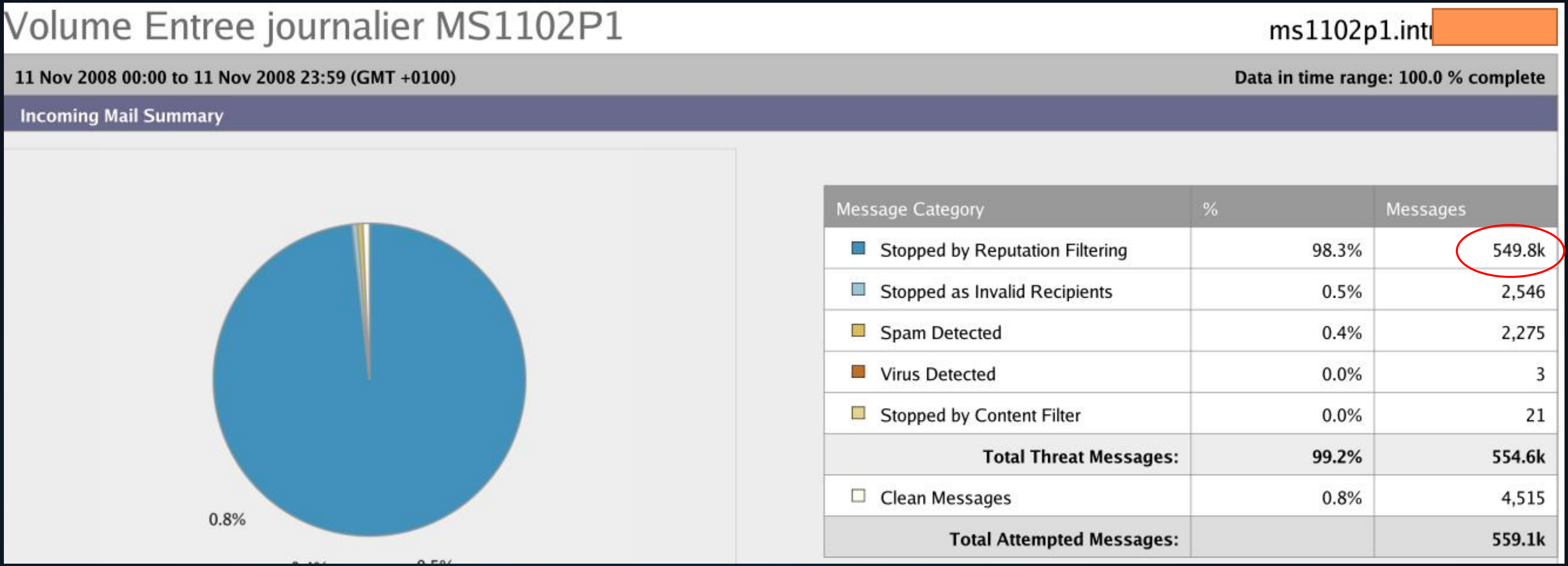


2000’s

2010’s

2015’s

2020’s



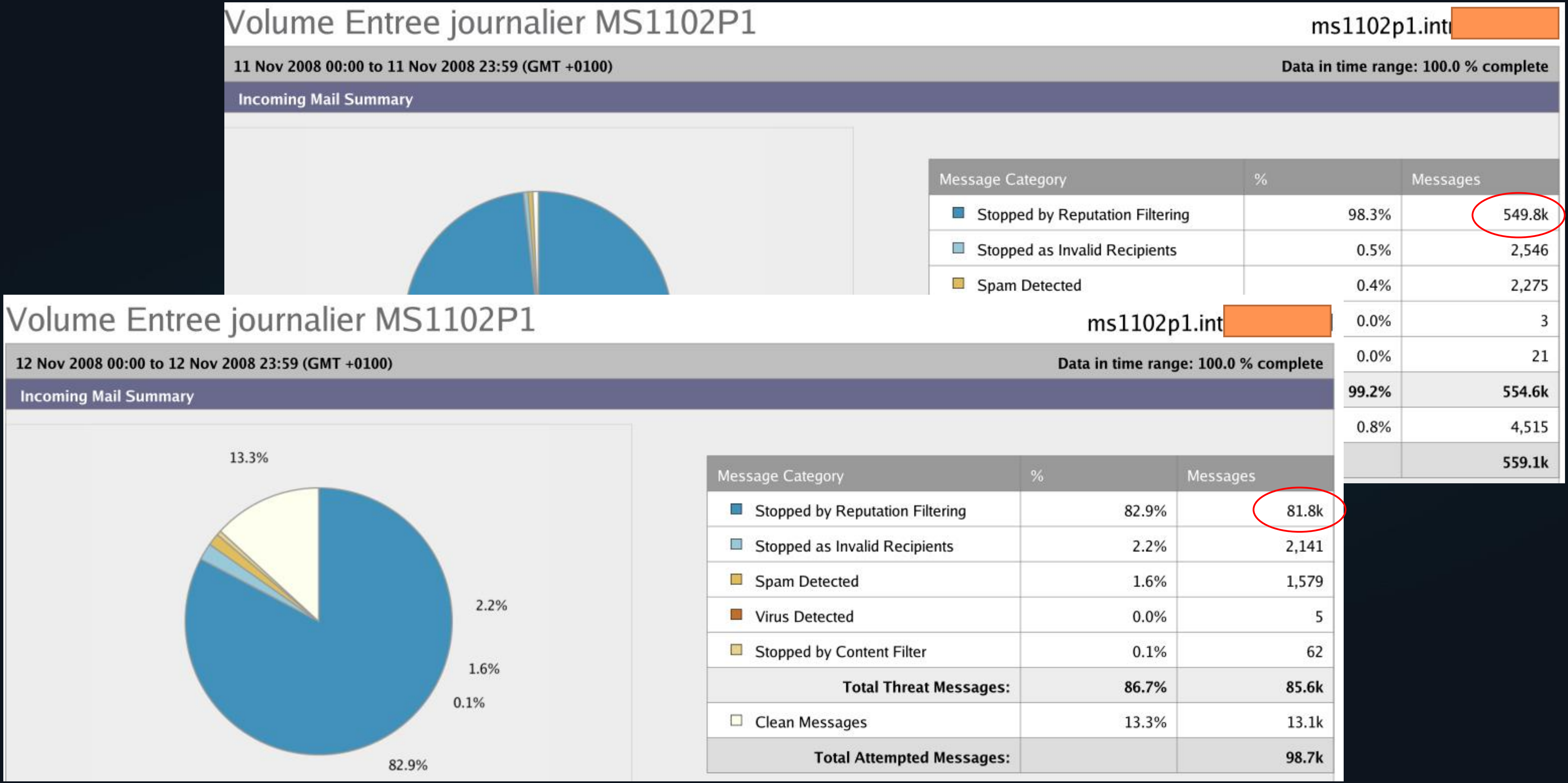
Volume Entree journalier MS1102P1

ms1102p1.intr[redacted]

11 Nov 2008 00:00 to 11 Nov 2008 23:59 (GMT +0100) **Data in time range: 100.0 % complete**

Incoming Mail Summary

Message Category	%	Messages
🟦 Stopped by Reputation Filtering	98.3%	549.8k
🟦 Stopped as Invalid Recipients	0.5%	2,546
🟨 Spam Detected	0.4%	2,275
🟧 Virus Detected	0.0%	3
🟨 Stopped by Content Filter	0.0%	21
Total Threat Messages:	**99.2%**	**554.6k**
□ Clean Messages	0.8%	4,515
Total Attempted Messages:		**559.1k**



Volume Entree journalier MS1102P1

ms1102p1.int[redacted]

11 Nov 2008 00:00 to 11 Nov 2008 23:59 (GMT +0100) — Data in time range: 100.0 % complete

Incoming Mail Summary

Message Category	%	Messages
🟦 Stopped by Reputation Filtering	98.3%	549.8k
🟦 Stopped as Invalid Recipients	0.5%	2,546
🟨 Spam Detected	0.4%	2,275
	0.0%	3
	0.0%	21
	99.2%	**554.6k**
	0.8%	4,515
		559.1k

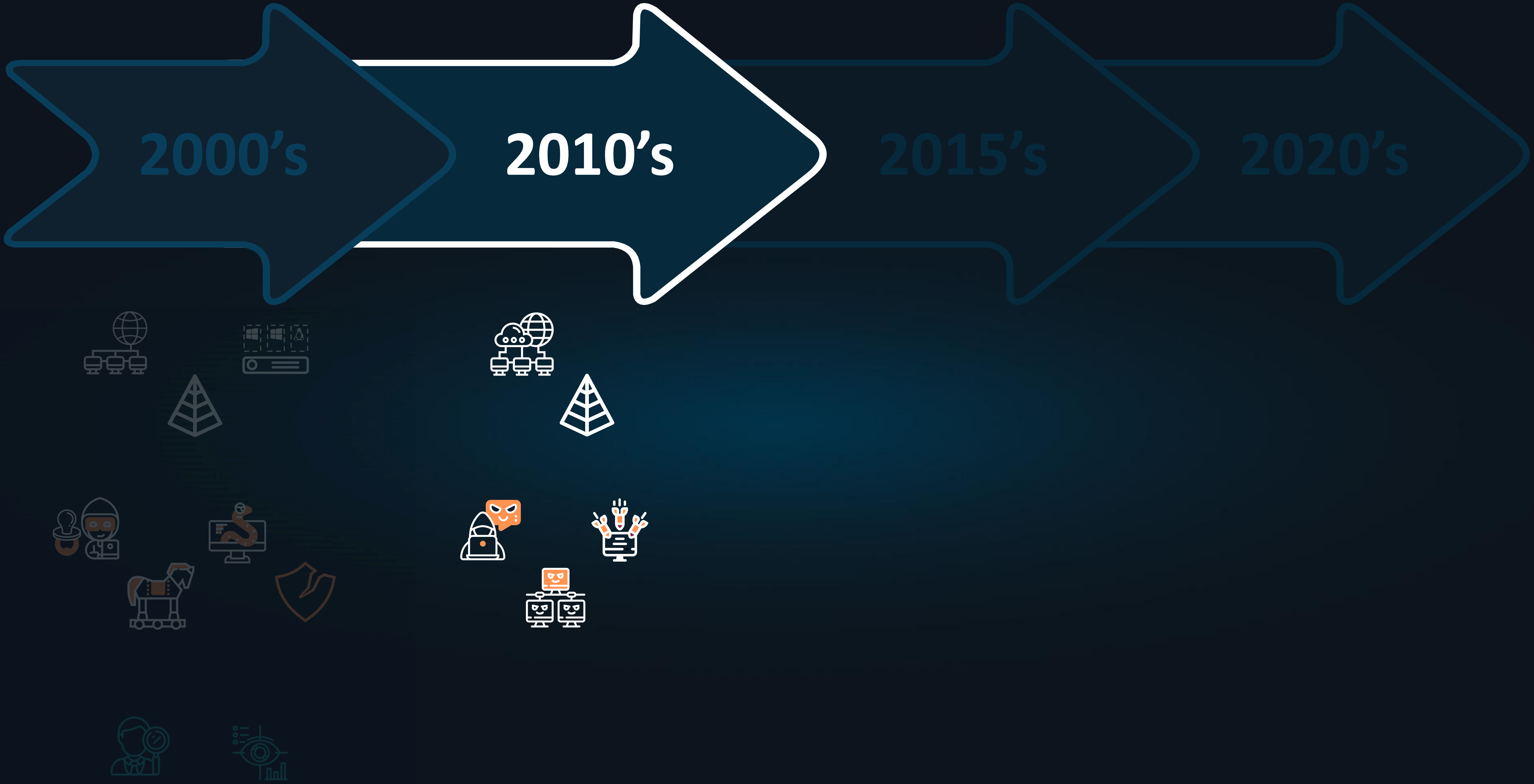
Volume Entree journalier MS1102P1

ms1102p1.int[redacted]

12 Nov 2008 00:00 to 12 Nov 2008 23:59 (GMT +0100) — Data in time range: 100.0 % complete

Incoming Mail Summary

Message Category	%	Messages
🟦 Stopped by Reputation Filtering	82.9%	81.8k
🟦 Stopped as Invalid Recipients	2.2%	2,141
🟨 Spam Detected	1.6%	1,579
🟧 Virus Detected	0.0%	5
🟨 Stopped by Content Filter	0.1%	62
Total Threat Messages:	**86.7%**	**85.6k**
□ Clean Messages	13.3%	13.1k
Total Attempted Messages:		**98.7k**

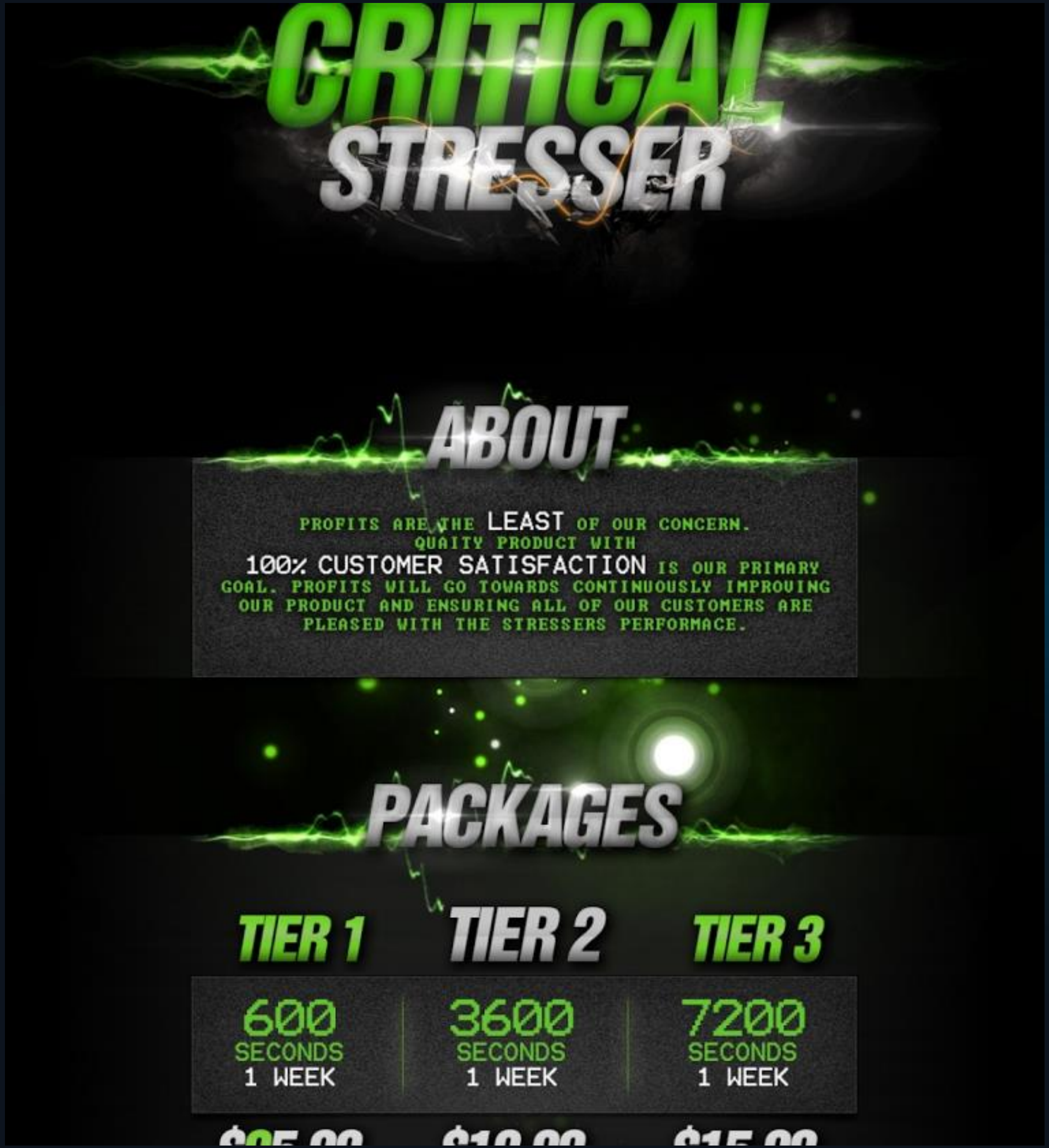


2000's

2010's

2015's

2020's



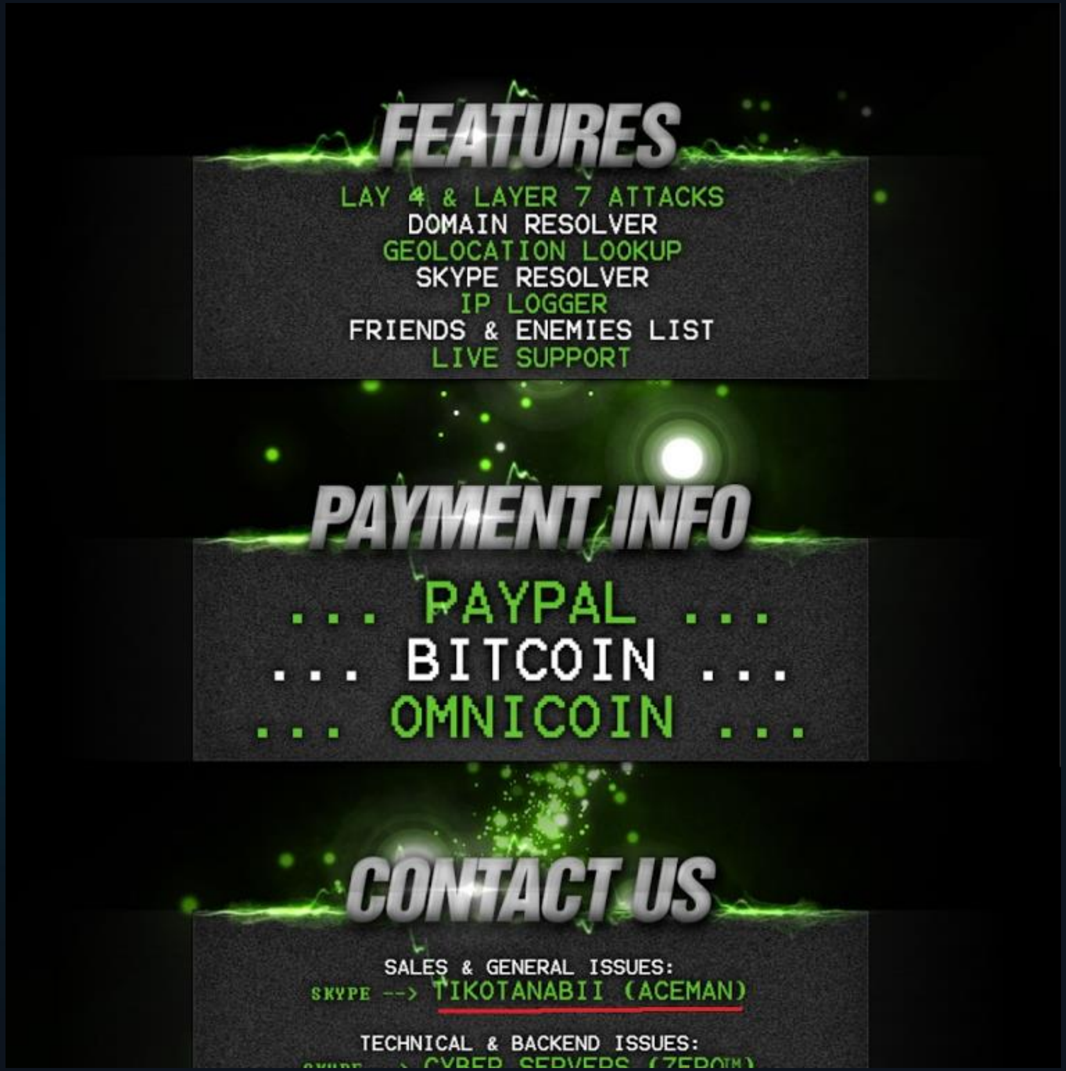
CRITICAL STRESSER

ABOUT

PROFITS ARE THE LEAST OF OUR CONCERN.
QUAITY PRODUCT WITH
100% CUSTOMER SATISFACTION IS OUR PRIMARY GOAL. PROFITS WILL GO TOWARDS CONTINUOUSLY IMPROUING OUR PRODUCT AND ENSURING ALL OF OUR CUSTOMERS ARE PLEASED WITH THE STRESSERS PERFORMACE.

PACKAGES

TIER 1	TIER 2	TIER 3
600 SECONDS 1 WEEK	3600 SECONDS 1 WEEK	7200 SECONDS 1 WEEK
$05.00	$10.00	$15.00



FEATURES

LAY 4 & LAYER 7 ATTACKS
DOMAIN RESOLVER
GEOLOCATION LOOKUP
SKYPE RESOLVER
IP LOGGER
FRIENDS & ENEMIES LIST
LIVE SUPPORT

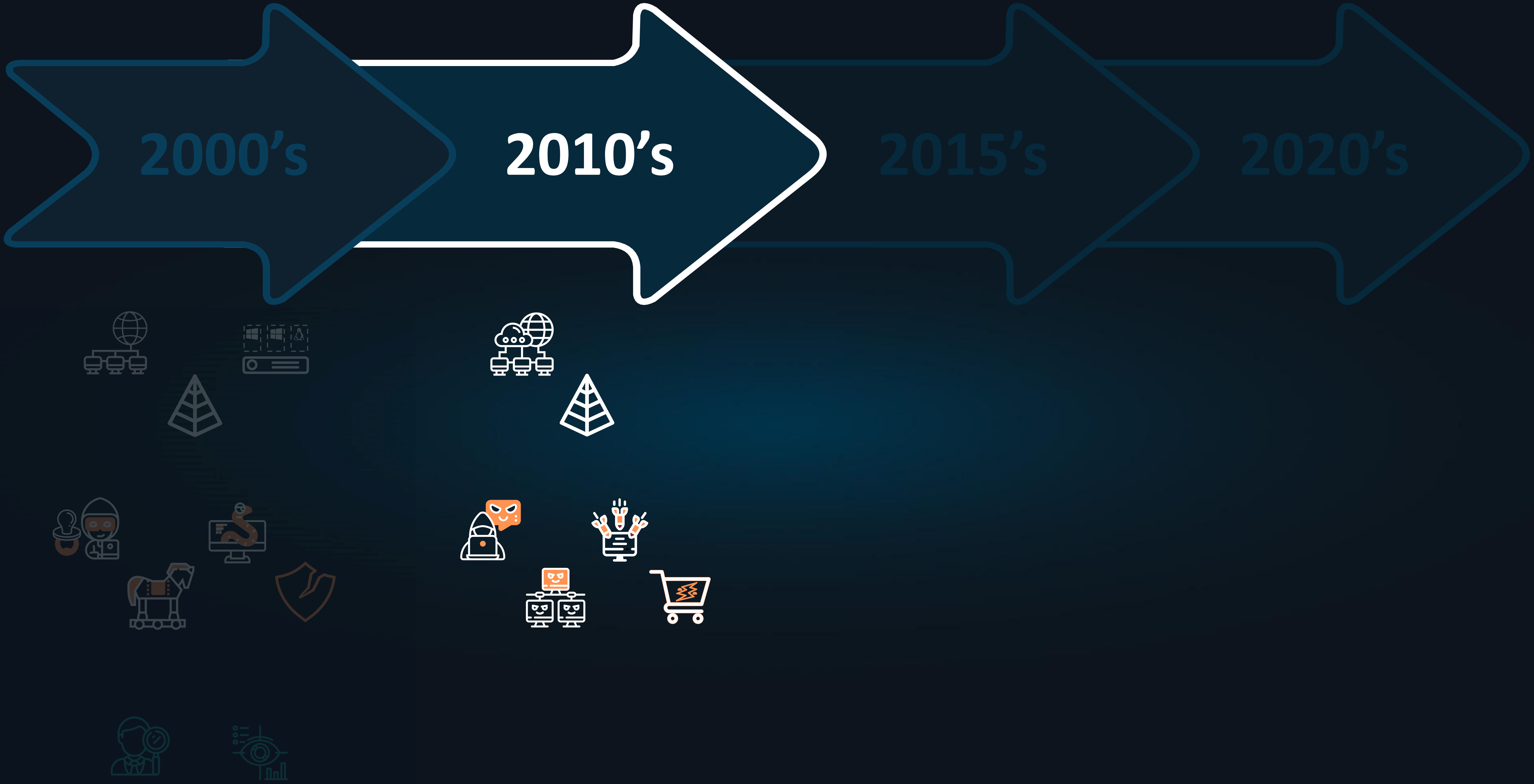
PAYMENT INFO

... PAYPAL ...
... BITCOIN ...
... OMNICOIN ...

CONTACT US

SALES & GENERAL ISSUES:
SKYPE --> TIKOTANABII (ACEMAN)

TECHNICAL & BACKEND ISSUES:
SKYPE --> CYBER SERVERS (ZERO™)

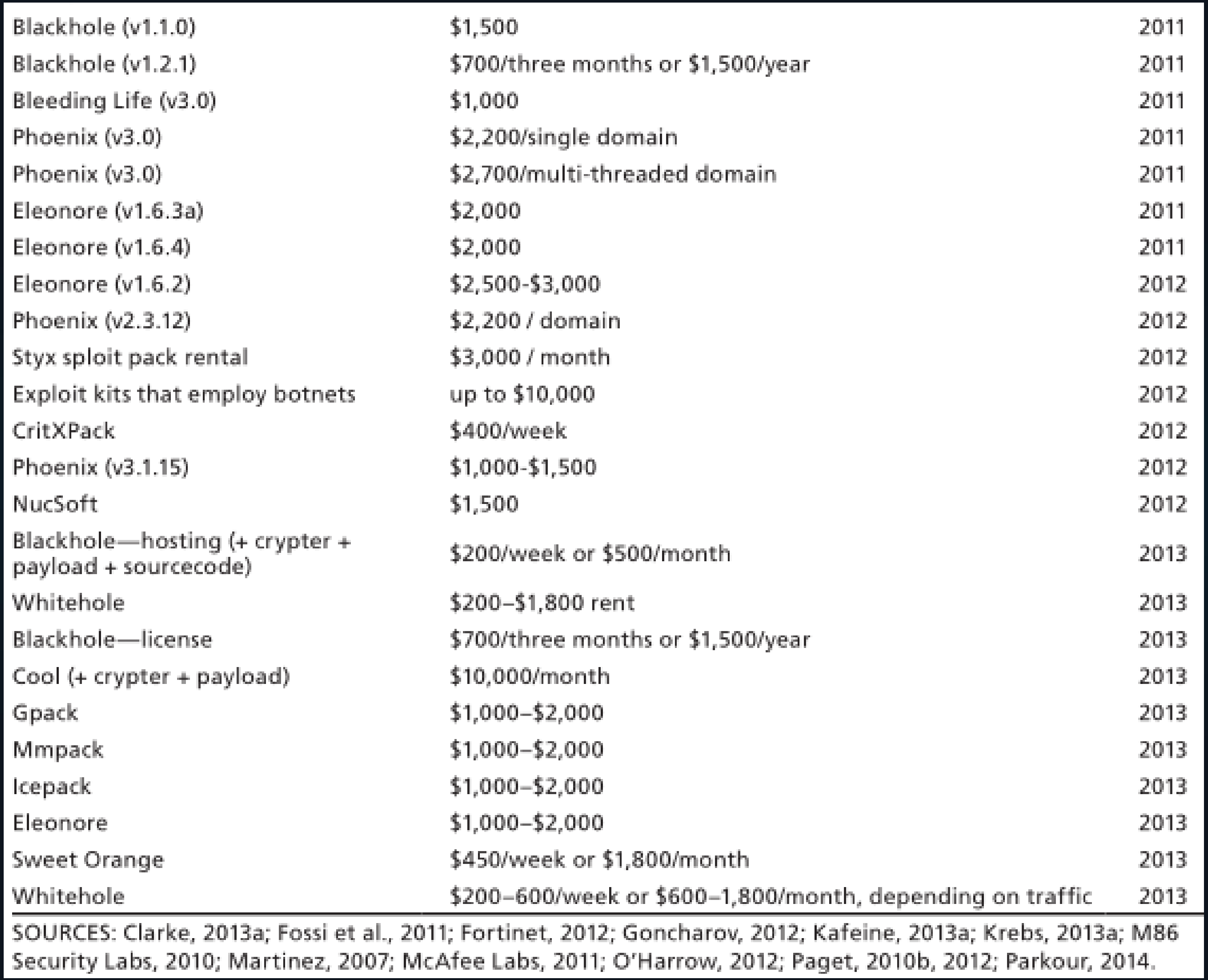


2000's

2010's

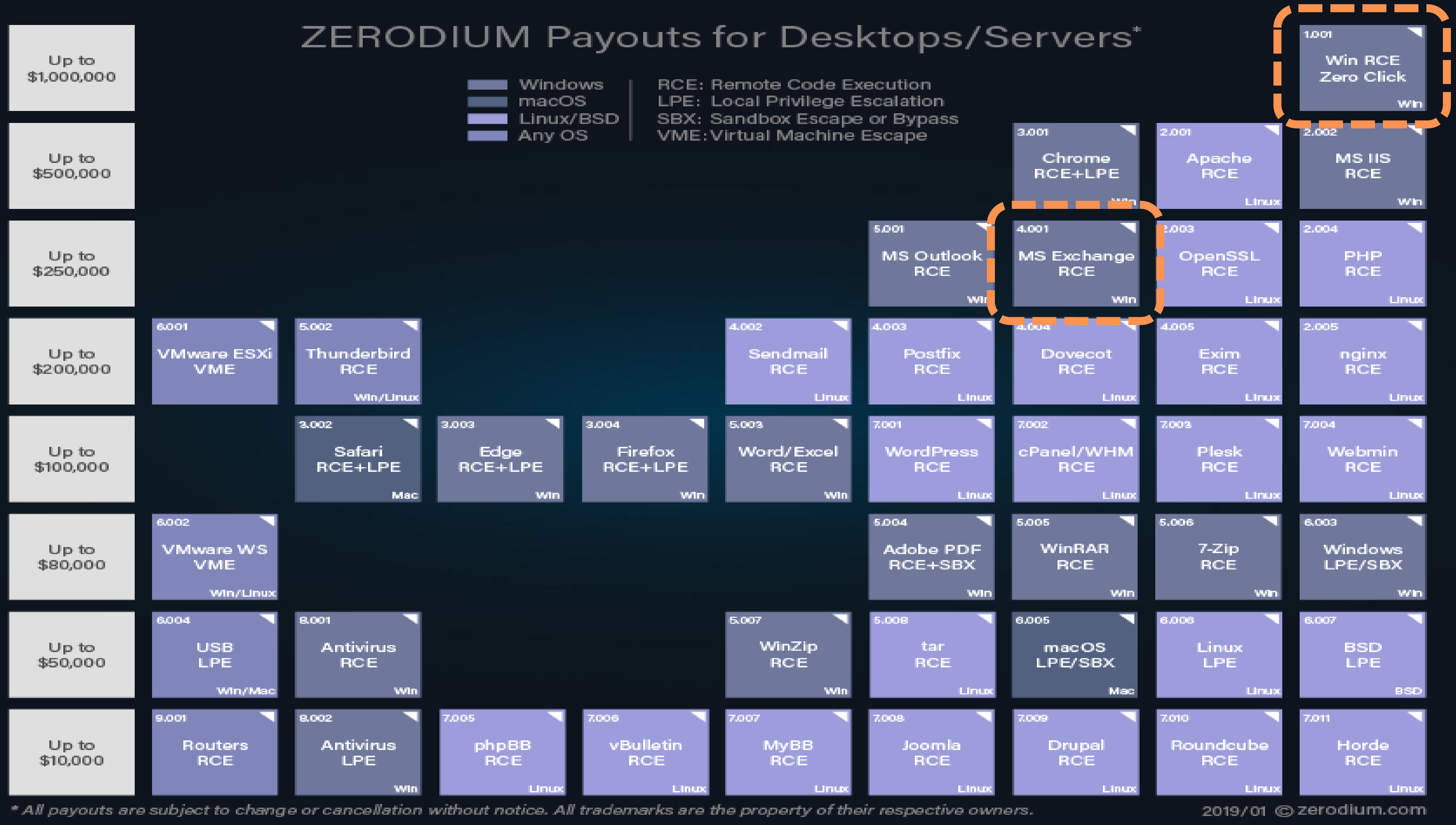
2015's

2020's



Blackhole (v1.1.0)	$1,500	2011
Blackhole (v1.2.1)	$700/three months or $1,500/year	2011
Bleeding Life (v3.0)	$1,000	2011
Phoenix (v3.0)	$2,200/single domain	2011
Phoenix (v3.0)	$2,700/multi-threaded domain	2011
Eleonore (v1.6.3a)	$2,000	2011
Eleonore (v1.6.4)	$2,000	2011
Eleonore (v1.6.2)	$2,500-$3,000	2012
Phoenix (v2.3.12)	$2,200 / domain	2012
Styx sploit pack rental	$3,000 / month	2012
Exploit kits that employ botnets	up to $10,000	2012
CritXPack	$400/week	2012
Phoenix (v3.1.15)	$1,000-$1,500	2012
NucSoft	$1,500	2012
Blackhole—hosting (+ crypter + payload + sourcecode)	$200/week or $500/month	2013
Whitehole	$200–$1,800 rent	2013
Blackhole—license	$700/three months or $1,500/year	2013
Cool (+ crypter + payload)	$10,000/month	2013
Gpack	$1,000–$2,000	2013
Mmpack	$1,000–$2,000	2013
Icepack	$1,000–$2,000	2013
Eleonore	$1,000–$2,000	2013
Sweet Orange	$450/week or $1,800/month	2013
Whitehole	$200–600/week or $600–1,800/month, depending on traffic	2013

SOURCES: Clarke, 2013a; Fossi et al., 2011; Fortinet, 2012; Goncharov, 2012; Kafeine, 2013a; Krebs, 2013a; M86 Security Labs, 2010; Martinez, 2007; McAfee Labs, 2011; O'Harrow, 2012; Paget, 2010b, 2012; Parkour, 2014.



ZERODIUM Payouts for Desktops/Servers*

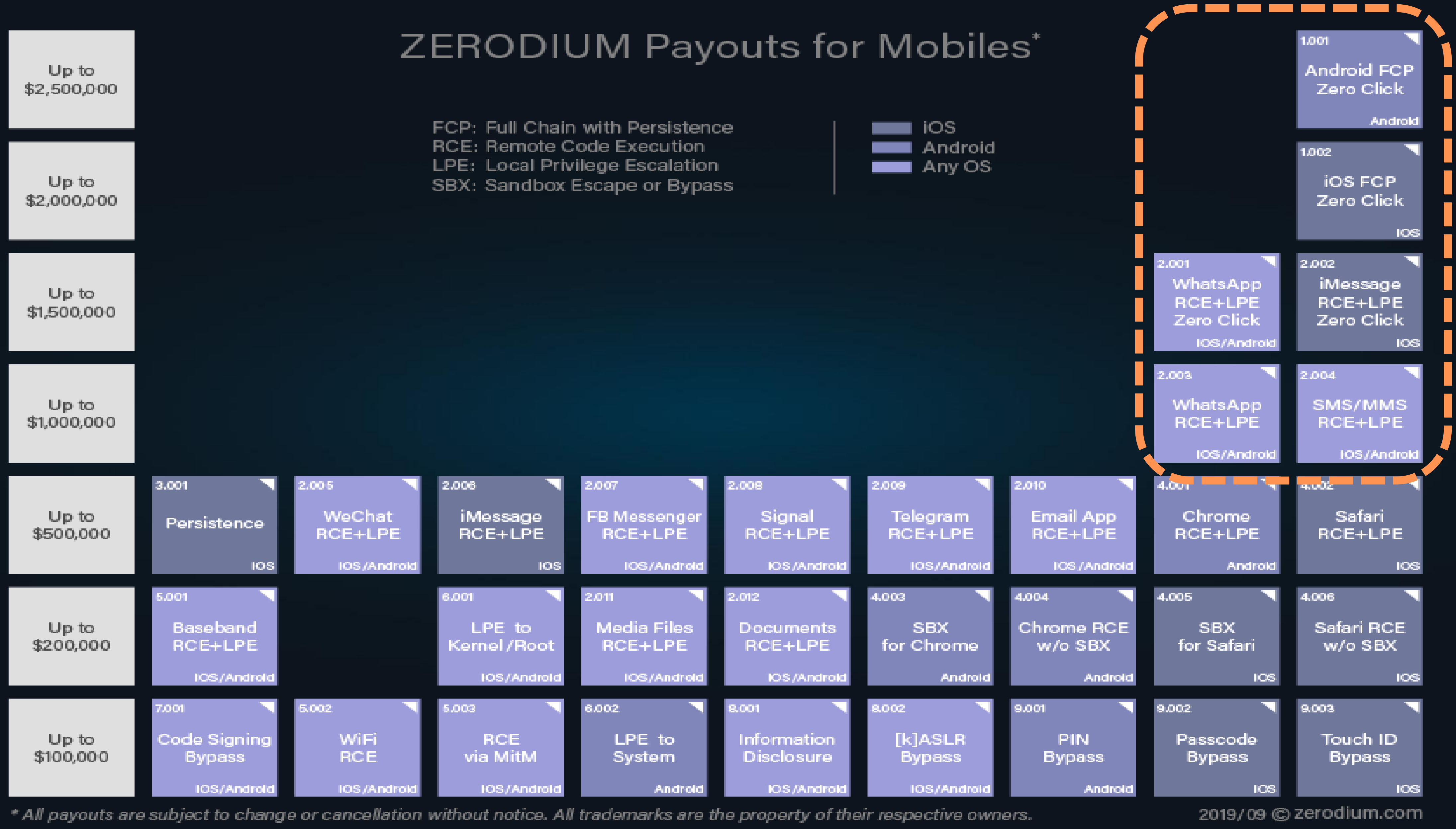
- ▬ Windows
- ▬ macOS
- ▬ Linux/BSD
- ▬ Any OS

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		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 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	9.001 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.*

2019/01 © zerodium.com



ZERODIUM Payouts for Mobiles*

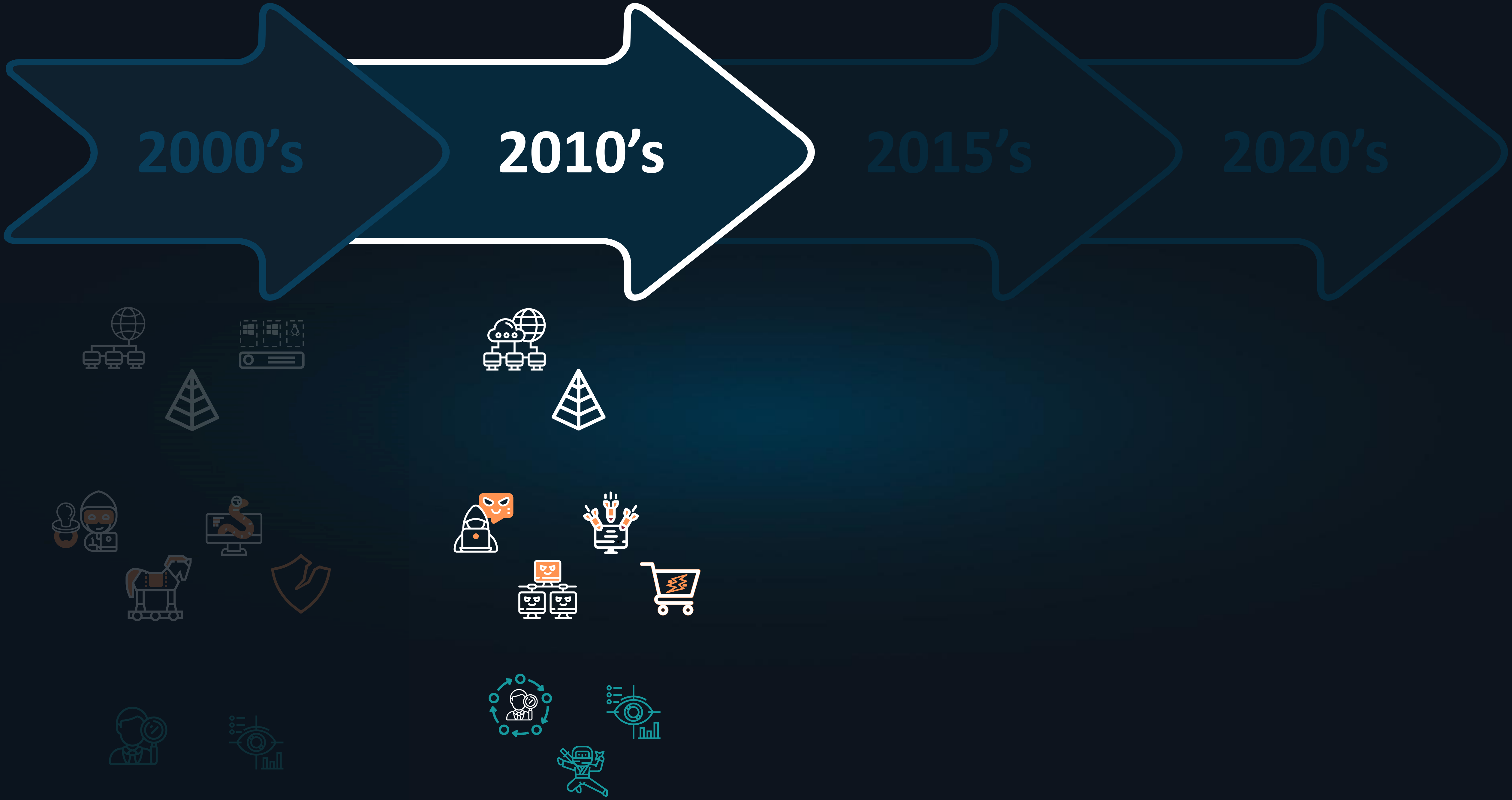
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

▨ iOS
▨ Android
▨ Any OS

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE 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 $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

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

2019/09 © zerodium.com



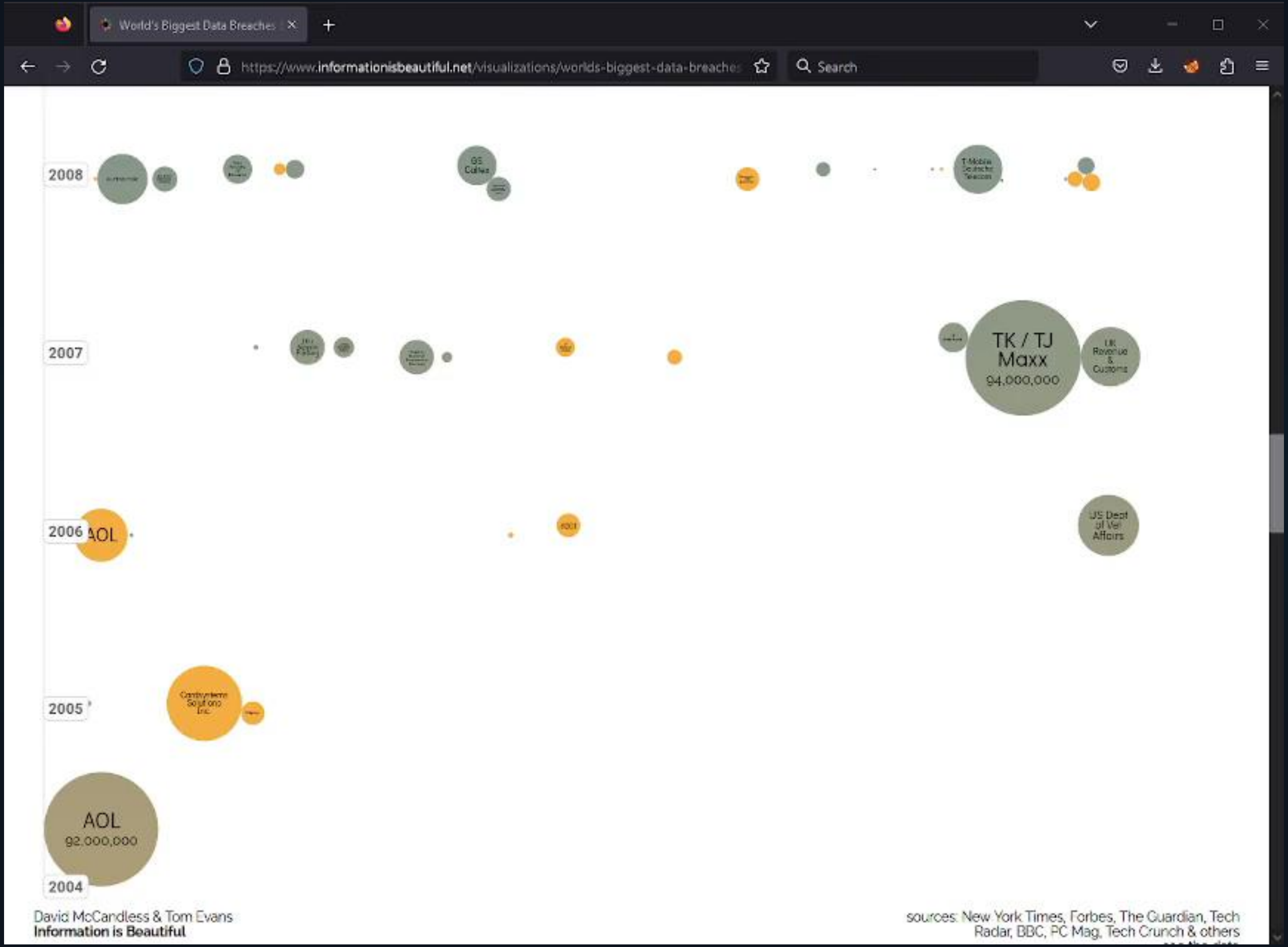
2000's

2010's

2015's

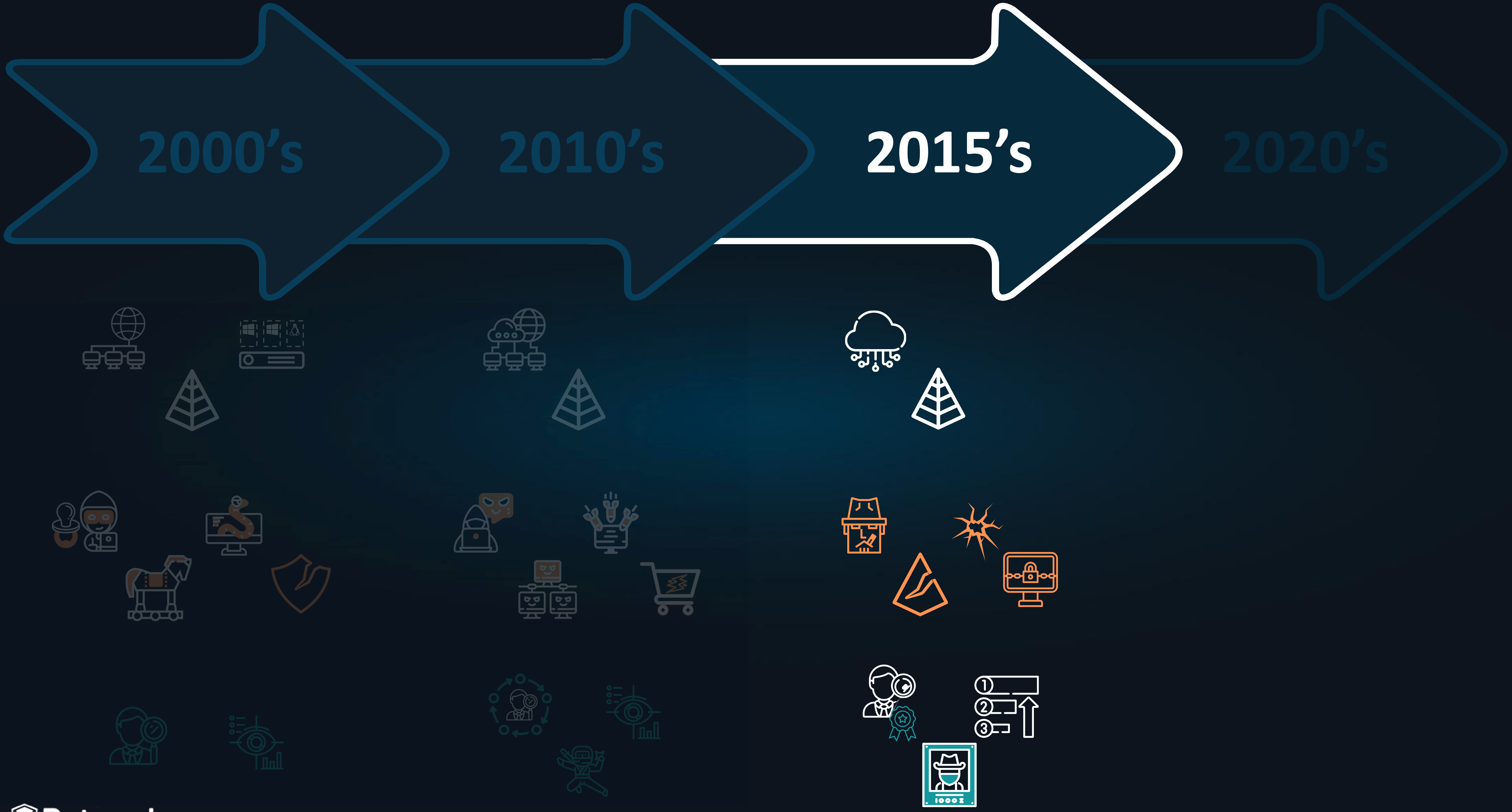
2020's

2000's
2010's
2015's
2020's


World's Biggest Data Breaches
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches
Search
2008
GS Caltex
T-Mobile Deutsche Telecom
2007
TK / TJ Maxx
94,000,000
UK Revenue & Customs
2006
AOL
US Dept of Vet Affairs
2005
CardSystems Solutions Inc.
AOL
92,000,000
2004

David McCandless & Tom Evans
Information is Beautiful

sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others



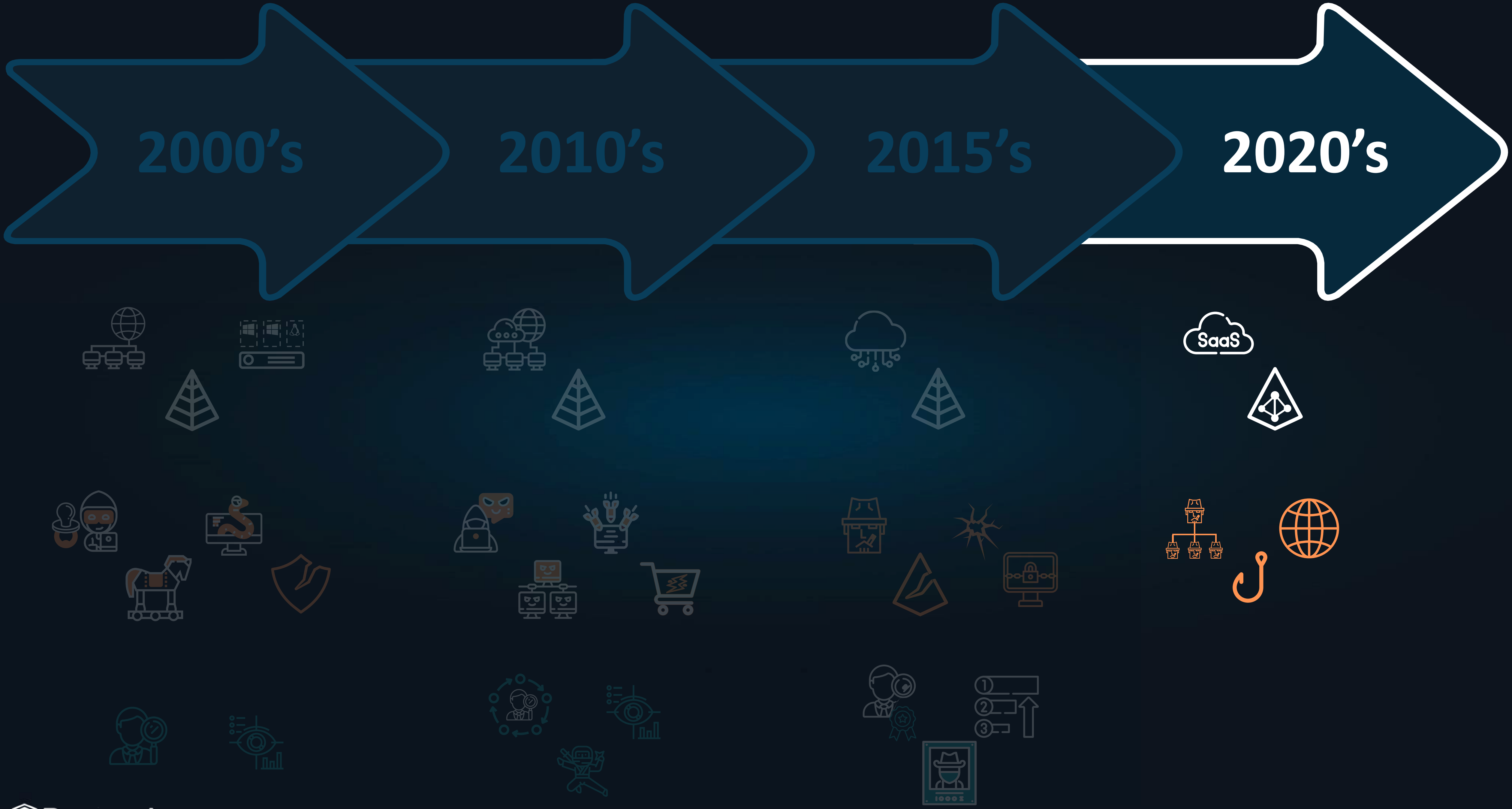
2000’s

2010’s

2015’s

2020’s

	Vulnerability management		Offensive Cybersecurity			
	Vulnerability Scanner	Vulnerability management tool	Pentest	BugBounty		
Attack Surface	◐	○	◐	◐		
Continuous watch	○	○	○	◐		
Qualification of vulnerabilities	○	◐	●	●		
Prioritizing and contextualizing	◐	●	●	○		
Remediation plan	○	◐	●	●		
Remediation follow-up	○	◐	○	○		
Re-test	○	○	◐	◐		
Available for non-expert	○	○	○	○		



2000’s

2010’s

2015’s

2020’s

2020

Solarwinds
Curveball *(CVE-2020-0601)*
RCE Apple Mail *(CVE-2020-9818)*
SMBleed *(CVE-2020-1206)*
ZeroLogon *(CVE-2020-1459)*
BadNeighbour, local IPv6 DoS on Windows *(CVE-2020-1459)*

01/01/2021 : << Hold my beer >>

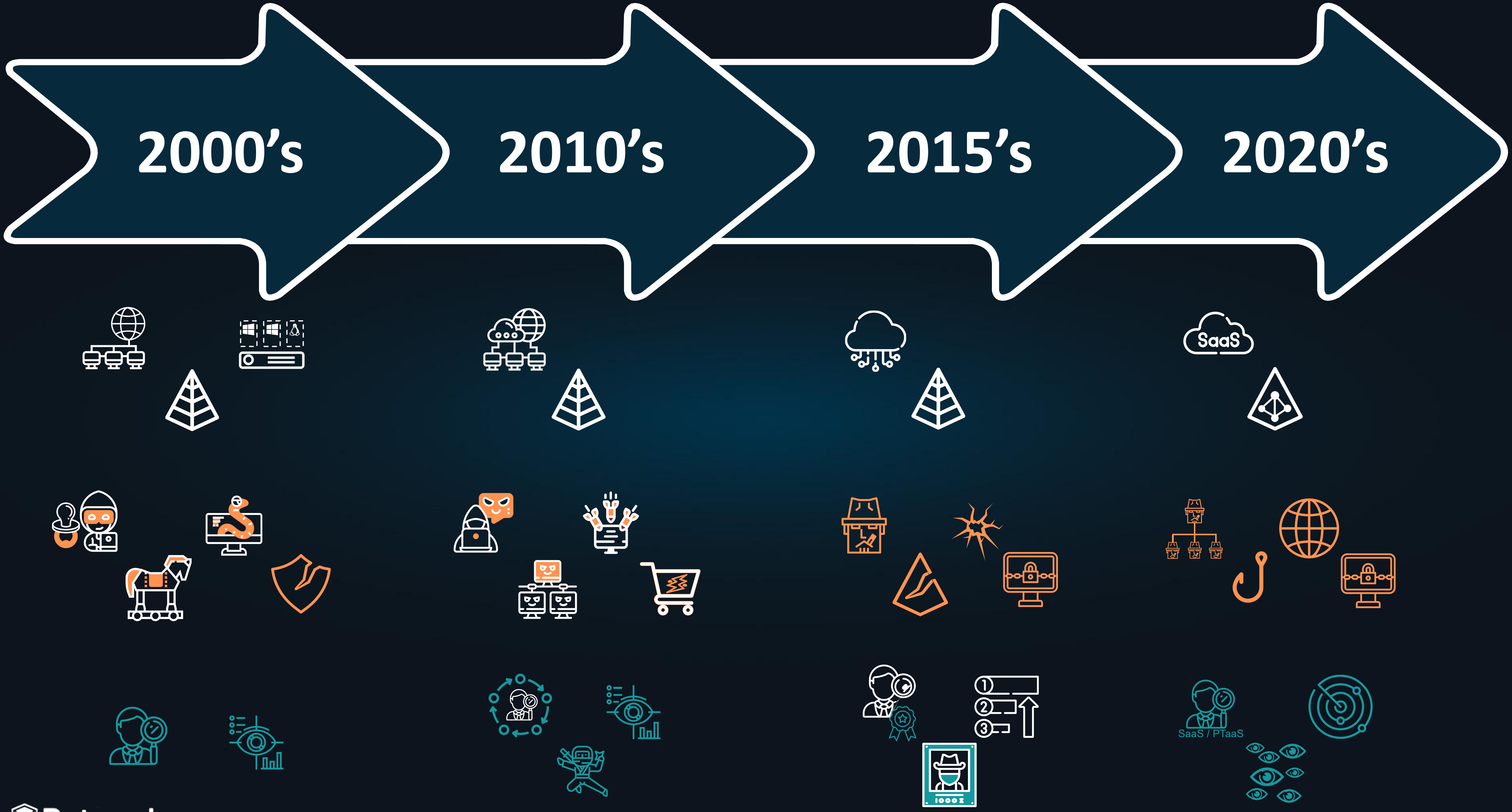
2021 Q1

Immunity Canvas leak -> Spectre exploit *(CVE-2017-5753, CVE-2017-5715)*
ProxyLogon, Exchange OWA pre-auth RCE *(CVE-2021-26855,...)*
pwn2own, 3 x Exchange OWA pre-auth RCE
Routable IPv6 DoS on Windows *(CVE-2021-24086)*
VMWare vSphere Client pre-auth RCE *(CVE-2021-21972)*
Fortinet, pre-auth RCE *(CVE-2020-29016, CVE-2020-29019...)*
F5 pre-auth Remote Command Injection *(CVE-2021-22986)*
Cisco small business, pre-auth RCE *(CVE-2021-1459)*
BleedingTooth, pre-auth RCE on Bluetooth *(CVE-2020-12352, CVE-2020-12351)*
Dedalus data leak of 500 000 french
Facebook data leak of 533 millions users
Linkedin data leak of 1 billion users

2000’s
2010’s
2015’s
2020’s
SaaS
SaaS / PTaaS

Patrowl

	Vulnerability management		Offensive Cybersecurity				
	Vulnerability Scanner	Vulnerability management tool	Pentest	BugBounty	Pentest as a Service (PTaaS)	External Attack Surface Management (EASM)	External Posture Management
Attack Surface	◐	○	◐	◐	○	◐	🟢
Continuous watch	○	○	○	◐	◐	◐	🟢
Qualification of vulnerabilities	○	◐	●	●	🟢	○	🟢
Prioritizing and contextualizing	◐	●	●	○	🟢	◐	🟢
Remediation plan	○	◐	●	●	🟢	◐	🟢
Remediation follow-up	○	◐	○	○	◐	◐	🟢
Re-test	○	○	◐	◐	◐	◐	🟢
Available for non-expert	○	○	○	○	○	○	🟢



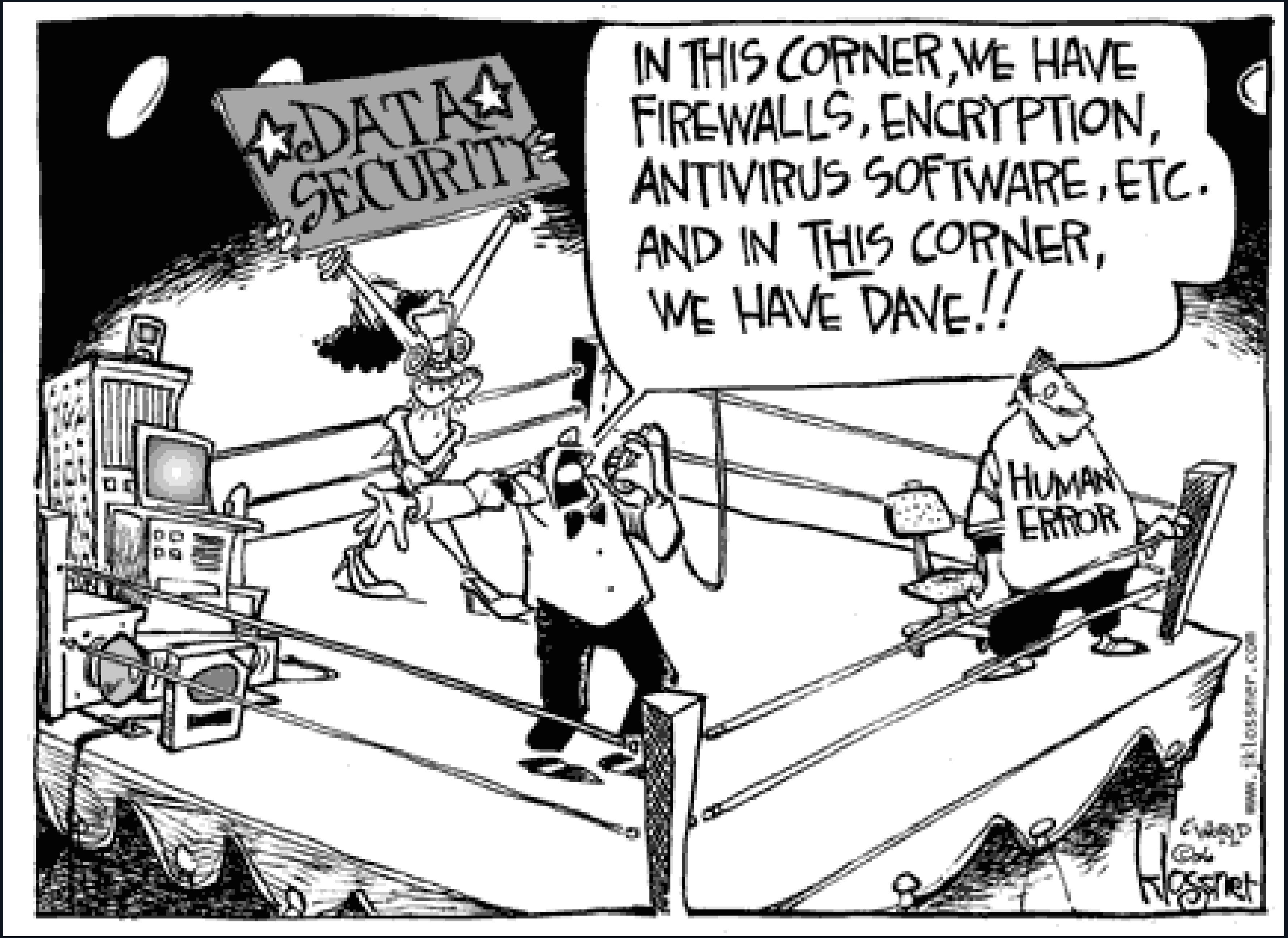
2000’s

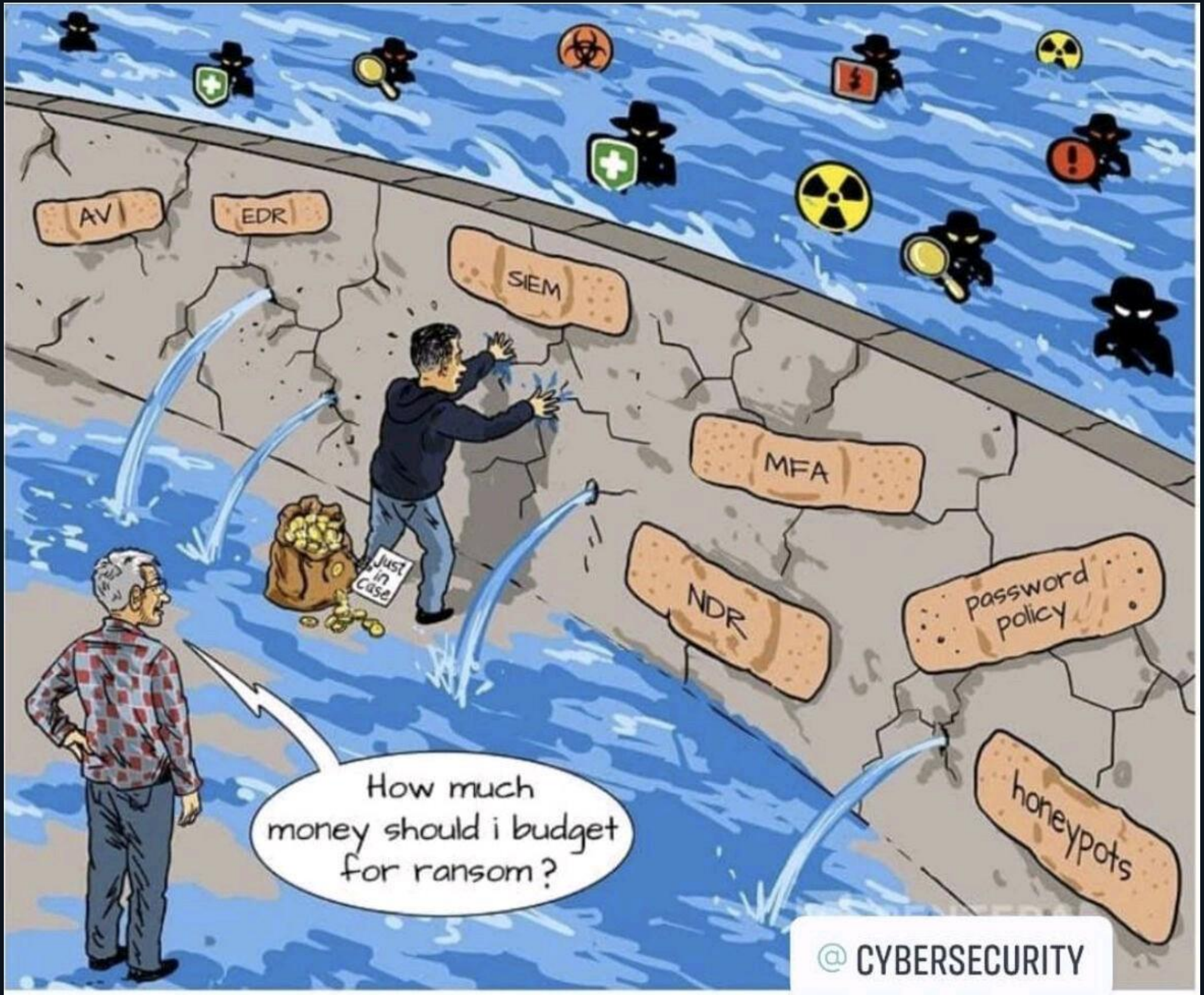
2010’s

2015’s

2020’s

Patrowl


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner



AV
EDR
SIEM
MFA
NDR
password policy
honeypots
Just in Case
How much money should i budget for ransom?
@ CYBERSECURITY

Thanks!