The Never-ending Zero-Day

Webinar — January 2022

Tony Anscombe

Chief Security Evangelist

tony.anscombe@eset.com

Agenda

- Vulnerabilities, reporting, & trends
- What is a zero-day?
- The trade of zero-day
- Mitigating zero-day attacks
- Questions

Cybercrime is big business

2025 : US$10.5 Trillion

2020 : US$6 Trillion

2018 : US$1.5 Trillion

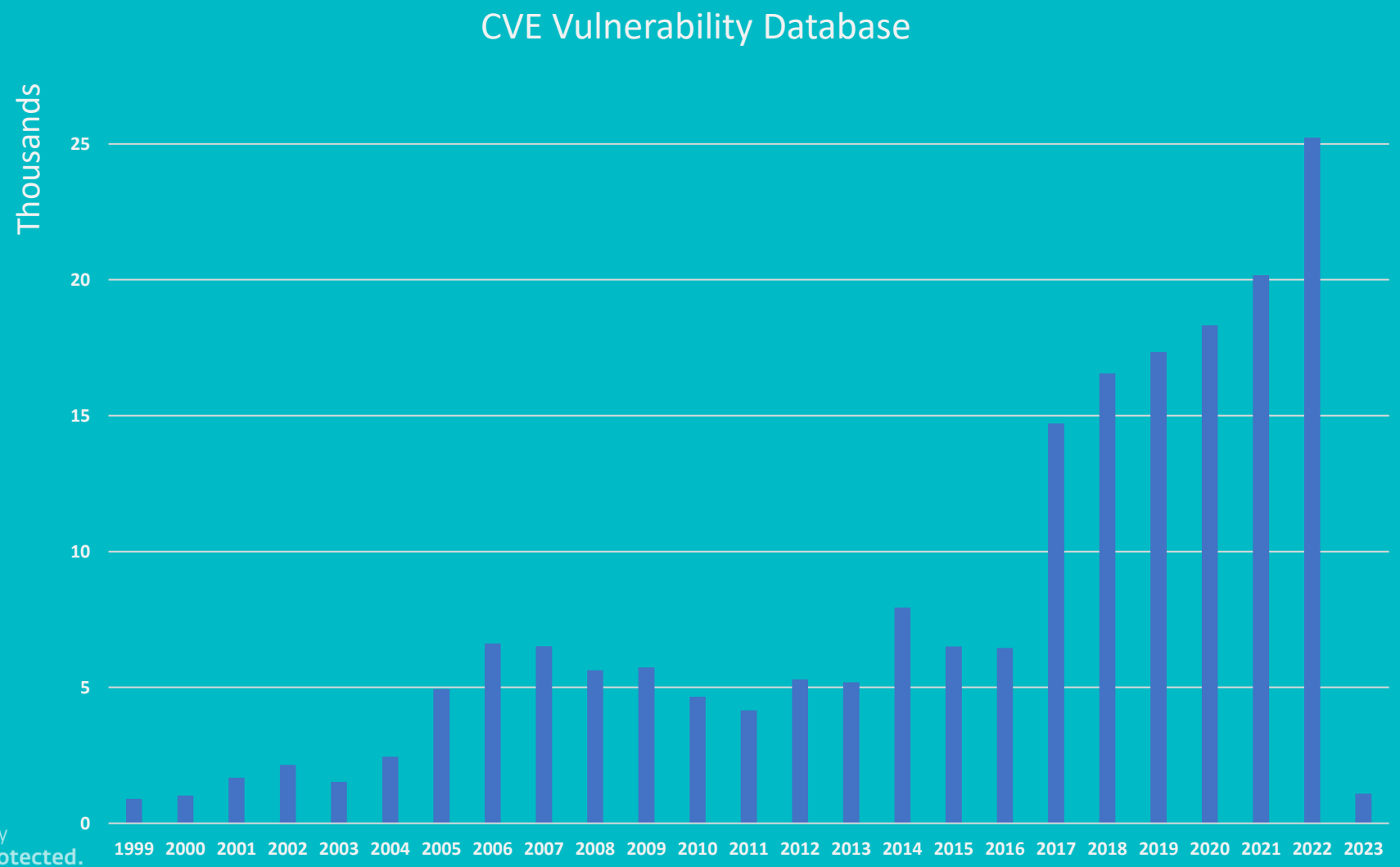
A vulnerability is…

A weakness in software and/or hardware that when exploited results in a negative impact to confidentiality, integrity, or availability.

Mitigation of vulnerabilities typically involves coding changes, but could also include specification changes.

The mission of the CVE® program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Disclosed vulnerability trend



What is a zero-day?

A **zero-day** is a computer software vulnerability previously unknown to those who should be interested in its mitigation, such as the vendor of the target software.

BLEEPINGCOMPUTER

Cisco discloses high-severity IP phone zero-day with exploit code

By Sergiu Gatlan

December 8, 2022 02:24 PM 0

The Hacker News

Google Rolls Out New Chrome Browser Update to Patch Yet Another Zero-Day Vulnerability

Dec 03, 2022 Ravie Lakshmanan

TC

Security

NSA says Chinese hackers are exploiting a zero-day bug in popular networking gear

Comment

Carly Page @carlypage_ / 6:16 AM PST • December 14, 2022

The Hacker News

New Actively Exploited Zero-Day Vulnerability Discovered in Apple Products

Dec 14, 2022 Ravie Lakshmanan

BLEEPINGCOMPUTER

December 2022 security updates fix 81 vulnerabilities

December 6, 2022 11:36 AM

The Hacker News

Microsoft Issues January 2023 Patch Tuesday Updates, Warns of Zero-Day Exploit

Jan 11, 2023 Ravie Lakshmanan

(Some) famous zero-day attacks

Can a CVE assigned vulnerability be a **zero-day?**

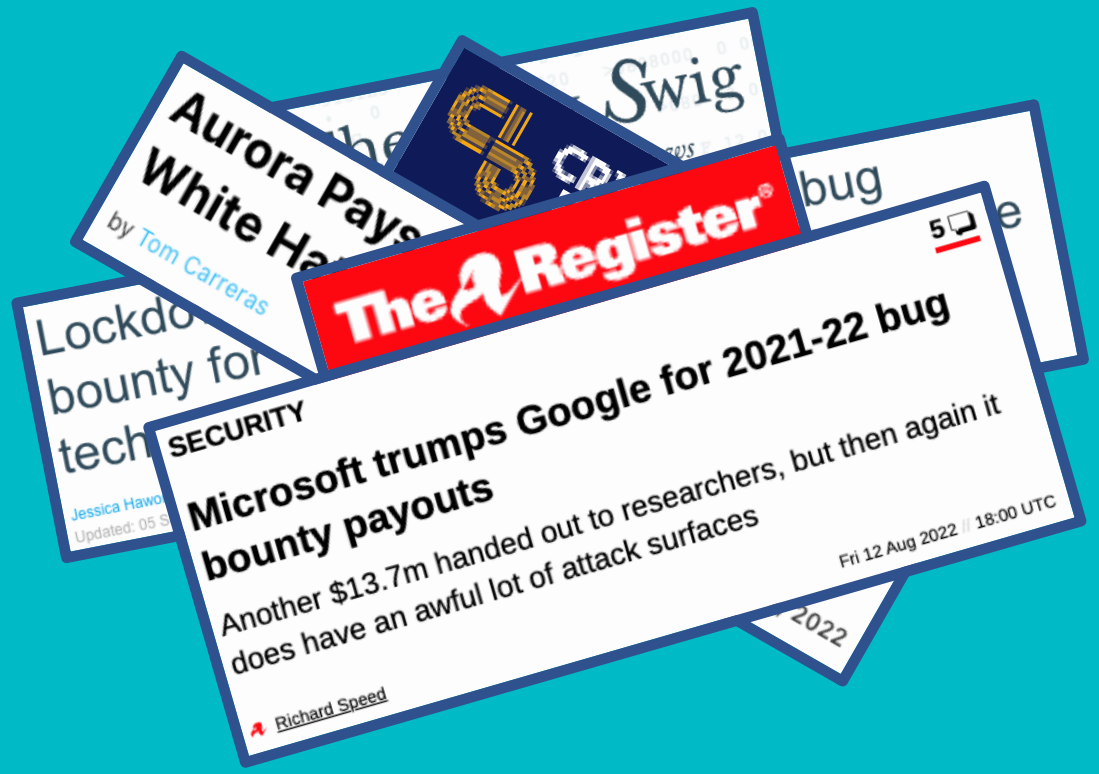
What would you do if you discovered a vulnerability?

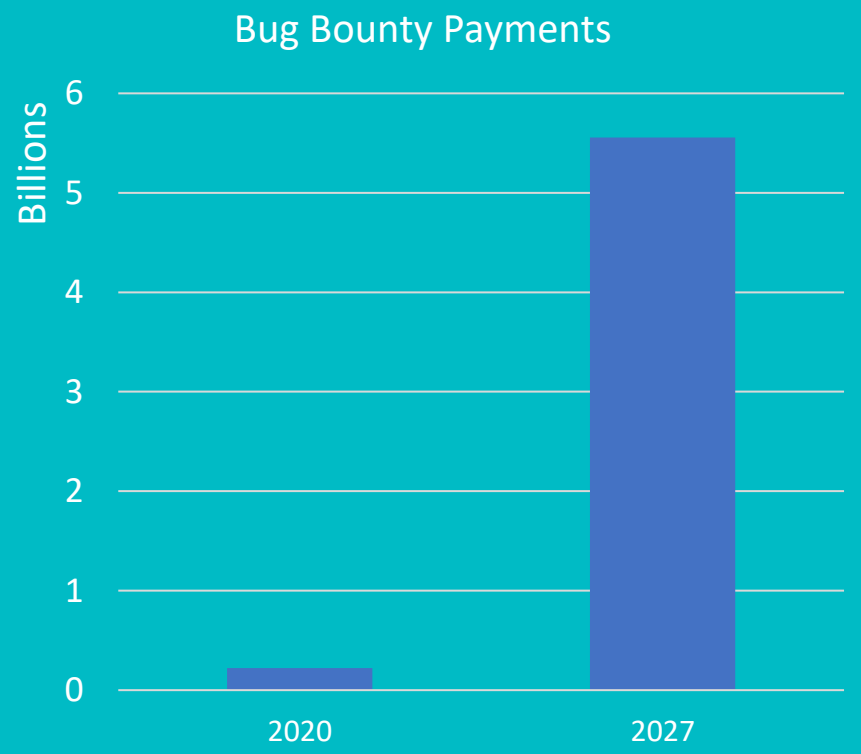
Sell it as a zero-day or disclose it?

The zero-day marketplace

- White market

Bug Bounty Payments





https://www.tanium.com/blog/why-bug-bounty-hunters-are-earning-huge-payouts/

What is coordinated disclosure?

Coordinated disclosure guidelines allow vendors 60 to 120 business days to patch a vulnerability. Often, vendors negotiate with researchers to modify the schedule to allow more time to fix difficult flaws.

Coordinated disclosure — Krook

- Vulnerability in commonly used chipset
- January 2019 – Amazon notified
- August 2019 – CVE-2019-151256
- February 2020 – Public disclosure

The zero-day marketplace

- White market
- Black market

Zero-day black market

- Criminals buy in the black market
- Rewards are usually 10–100 times higher
- Governments
  - Requirements are not met in the grey market
  - Impediments to acquire due to international regulations
- Hacking Team stated they did not sell to blacklisted countries

The zero-day marketplace

- White market
- Black market
- Grey market

Brokers trade in zero-day(s)

”Bounties for eligible zero-day exploits range from $2,500 to $2,500,000 per submission. The amounts paid by Zerodium to researchers to acquire their original zero-day exploits depend on the popularity and security level of the affected software/system, as well as the quality of the submitted exploit (full or partial chain, supported versions/systems/architectures, reliability, bypassed exploit mitigations, default vs. non-default components, process continuation, etc.).”

Source: https://zerodium.com/program.html

Who are the customers?

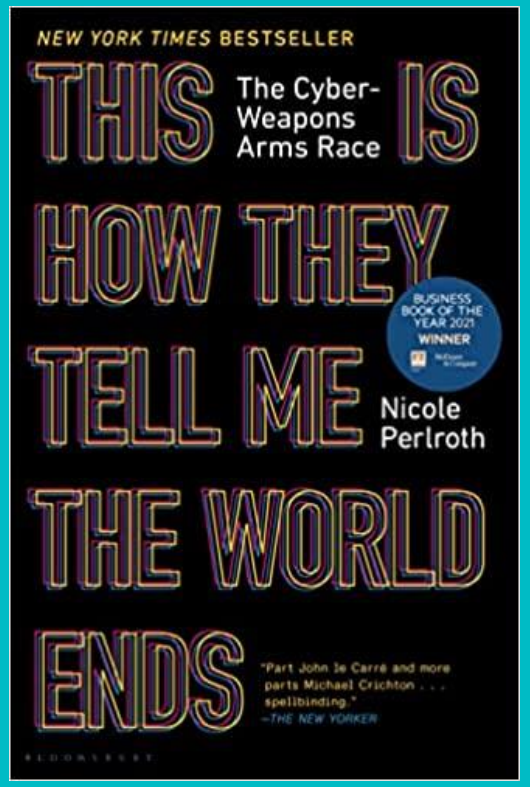
“Zerodium customers are government institutions (mainly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.”

https://zerodium.com/faq.html

Irresponsible non-disclosure

- EternalBlue
- NSA developed
- Held for 5 years
- Microsoft unaware of vulnerability
- Exploit leaked by “shadow brokers”
- Result
  - – WannaCry ransomware attack
  - – NotPetya – the most costly cyberattack

Further reading…



- Published: February 9, 2021
- Publisher: Bloomsbury Publishing
- ISBN-10: 1635576059
- ISBN-13: 978-1635576054

What would you do if you discovered a vulnerability?

Did your answer just change?

Can a zero-day circumvent cybersecurity solutions?

Protecting against zero-day attacks

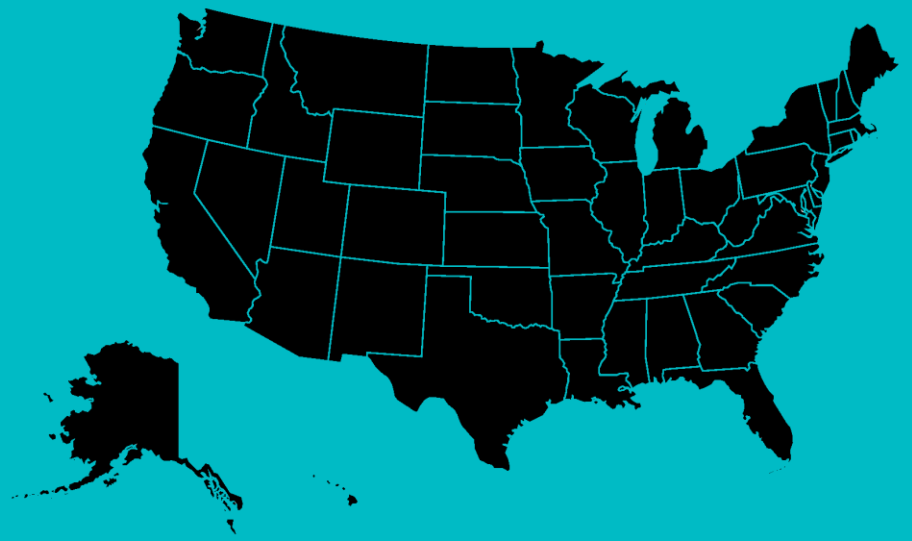
- Control of the environment
- Web application firewall
- Endpoint anti-malware security
- Endpoint detection and response
- Vulnerability management
- Patch management
- Threat intelligence

RSAConference™2023

What happens to the decommissioned hardware at your company?

IT asset disposition

- Global market $24.5 Billion by 2026



- US market $6.4 Billion in 2022

How the research began

- 1 - The starting point
- 17 - More acquired
  - 5 Clean
  - A mirrored pair
  - 2 Protected
  - 9 contained data

56% of devices compromised

Compromised information

- Customer data
  - Internal storage locations
  - External storage locations
  - Customer information

22%

Consequences of a customer data breach

Compromised information

- Third-party data
  - Business partners
  - Connected businesses

33%

Compromised information

- Trusted parties
  - Certificates
  - Cryptographic tokens

44%

- Router to router authentications keys

89%

Compromised information

- Specific applications
  - Cloud based apps
  - On-premises apps

89%

Consequences of an app list

APP 1

2022 – 3 CVEs

Max Severity 4.9

APP 2

2023 - 9 CVEs

2022 – 18 CVEs

Max Severity 8.3

APP 3

2023 - 6 CVEs

2022 – 28 CVEs

Max Severity 9

Difficulties contacting the companies

- Notification fatigue
- They don’t want to hear it
- There is no assigned point person
- No policy exists
- Everyone is trying to sell something
- They thought we were scamming them

The original owners

Vertical	Business	Employees	Revenue (USD, M)
Light manufacturing /supplier	Products/subassemblies integrated in larger companies' products	5-50	5-25
Legal	Nationwide (US) law firm	50-100	5-25
Creative	Services multiple tier one, household brand companies	100-500	25-100
Data center	Direct data services, as well as managed MSP services for region	100-500	25-100
MSP	Manages fintech companies	100-500	25-100
Open-source software	Has over 100 million users, worldwide	100-500	500-1,000
Events	Operates tradeshows and equipment rentals	1,000-5,000	25-100
Multinational technology company	Global data company	1,000+	1,000+
Telecoms	This was CPE (Customer Premises Equipment) for a transportation company	10,000+	1,000+

The value of network access

Network Access Sales in Q3 2022
(KELA Cybercrime Prevention)

- 570 network access listings for sale
- $4 million
  - Average price for access $2,800
  - Average sale time 1.6 days
  - Most common types of access – RDP & VPN

Source: https://ke-la.com/wp-content/uploads/2022/10/KELA-RESEARCH_Ransomware-Victims-and-Network-Access-Sales-in-Q3-2022.pdf

NIST 800-88r1

Networking devices	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to factory default settings.
Purge:	See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator
Notes:	For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure. Network devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.

NIST 800.88r1

- Outsourcing media sanitization and destruction
  - Reasonable option to maintain confidentiality
  - Due diligence when entering into an agreement
    - Independent audit of operations and processes
    - Compliance with applicable rules
    - References from reliable sources
    - Trade association certifications

NIST 800.88r1

- Decommissioning/destruction documentation
  - Manufacturer
  - Model
  - Serial number
  - Organization asset tag
  - Media type
  - Media source
  - Pre-sanitization confidentiality categorization
  - Sanitization description
  - Method used
  - Tool used
  - Verification method

  - Post sanitization confidentiality categorization
  - Post-sanitization destination
  - For both sanitization and verification
    - Name of person
    - Position/title of person
    - Date
    - Location
    - Phone or other contact information
    - Signature
  - Optional
    - Data backup

What happens to the decommissioned hardware in your company?

Please go find out!

What to do if you discover data

- Document everything
- Disconnect the device from any network(s)
- Store and secure the device
- Contact a CISA regional office (if you are in the USA)
  - https://www.cisa.gov/about/contact-us

About ESET

- **Number one** EU cybersecurity company for business
- **1Bn+** internet users protected by our technology
- **400K+** business customers
- **110M** users

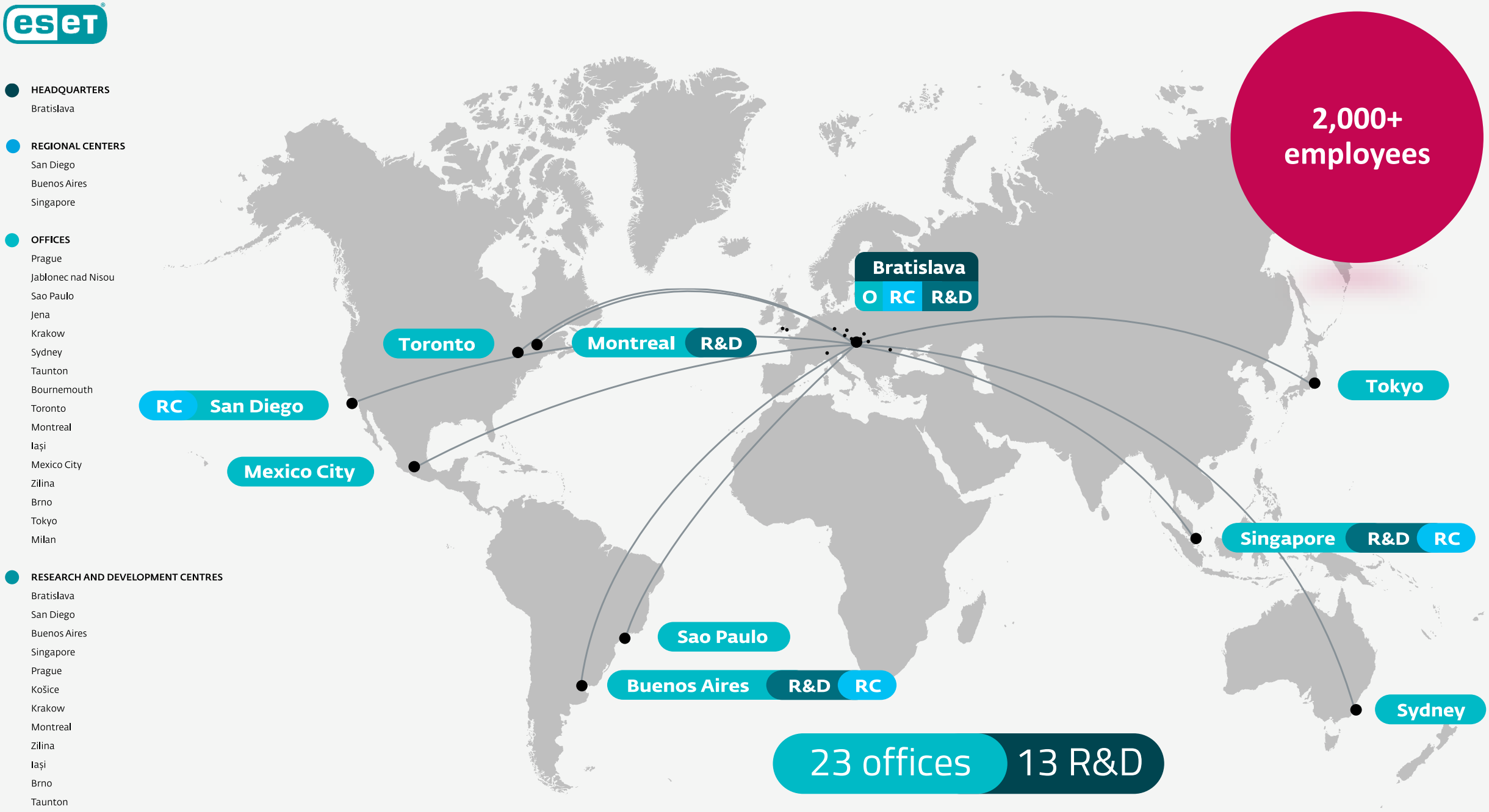
Trusted by Enterprise customers worldwide:

MITSUBISHI MOTORS
Drive your Ambition

Allianz Suisse

Canon
Canon Marketing Japan Group

T


HEADQUARTERS
Bratislava
REGIONAL CENTERS
San Diego
Buenos Aires
Singapore
OFFICES
Prague
Jablonec nad Nisou
Sao Paulo
Jena
Krakow
Sydney
Taunton
Bournemouth
Toronto
Montreal
Iași
Mexico City
Zilina
Brno
Tokyo
Milan
RESEARCH AND DEVELOPMENT CENTRES
Bratislava
San Diego
Buenos Aires
Singapore
Prague
Košice
Krakow
Montreal
Zilina
Iași
Brno
Taunton
2,000+ employees
Bratislava
O RC R&D
Toronto
Montreal R&D
RC San Diego
Tokyo
Mexico City
Singapore R&D RC
Sao Paulo
Buenos Aires R&D RC
Sydney
23 offices
13 R&D

welivesecurity™ BY ESET

POLONIUM targets Israel with Creepy malware

You never walk alone: The SideWalk backdoor gets a Linux variant

ESET Threat Report T2 2022

“Give in to the cybercriminal and you breed more cybercrime.”

Questions by email

Tony Anscombe

tony.anscombe@eset.com