Protecting Real Estate Transactions in the Age of Cyberfraud

Spot it. Stop it. Secure it.

National Webinar

Thursday October 23, 2025

FCT

Agenda

Keynote

Protecting Real Estate Transactions in the Age of Cyberfraud

- Claudiu Popa, Certified Canadian Cybersecurity and Privacy Expert

Panel discussion

- Twane Boettinger, Director, Information Security & IT Risk Governance
- John Tracy, Senior Legal Counsel Claims
- Marie Taylor, Director, National Underwriter Legal, Risk and Compliance

Q&A

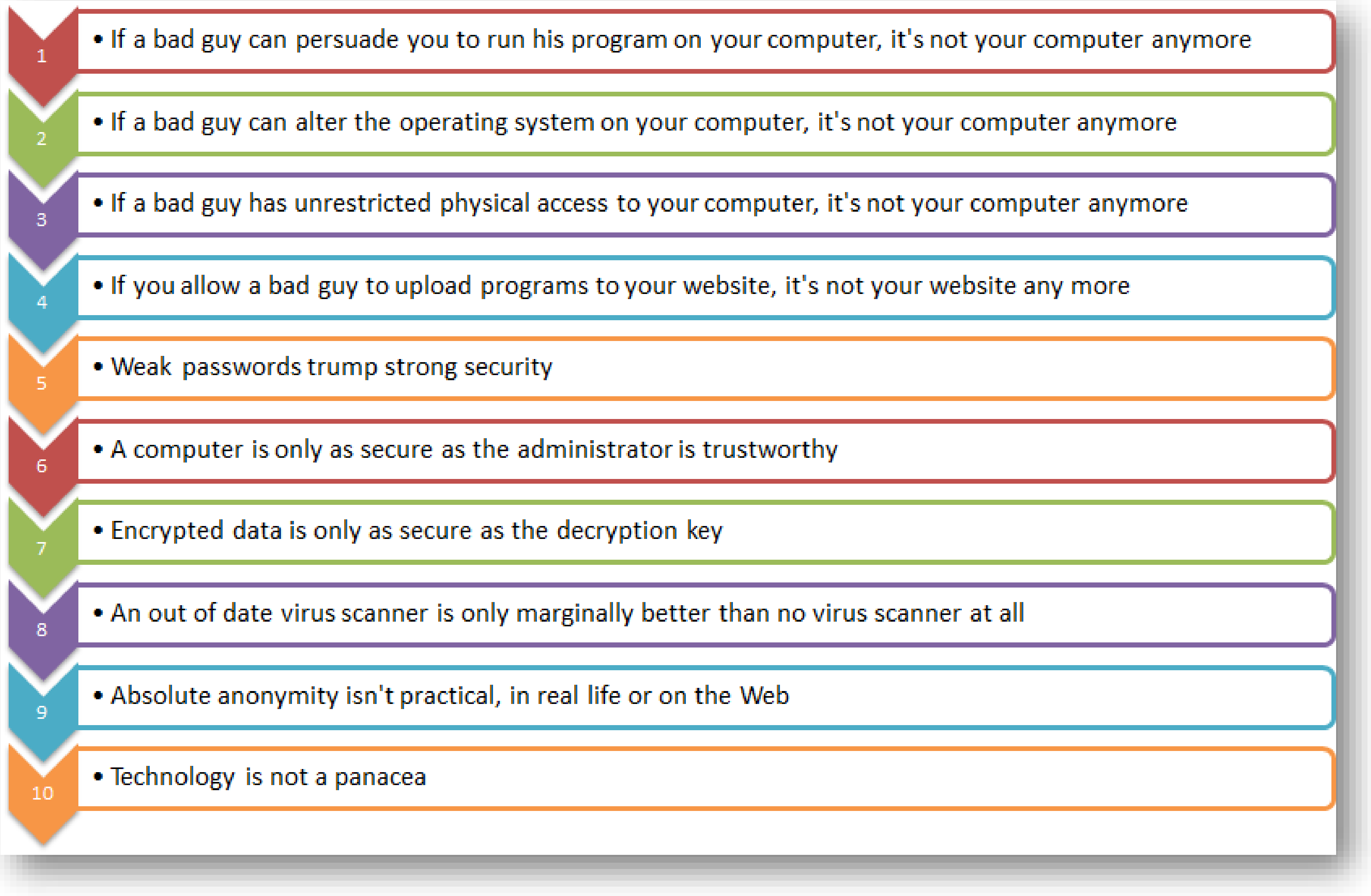
Protecting Real Estate Transactions in the Age of Cyberfraud

Spot it. Stop it. Secure it.

Claudiu Popa

CISSP CISA PMP CRISC CIPP

Let’s get the ground rules out of the way

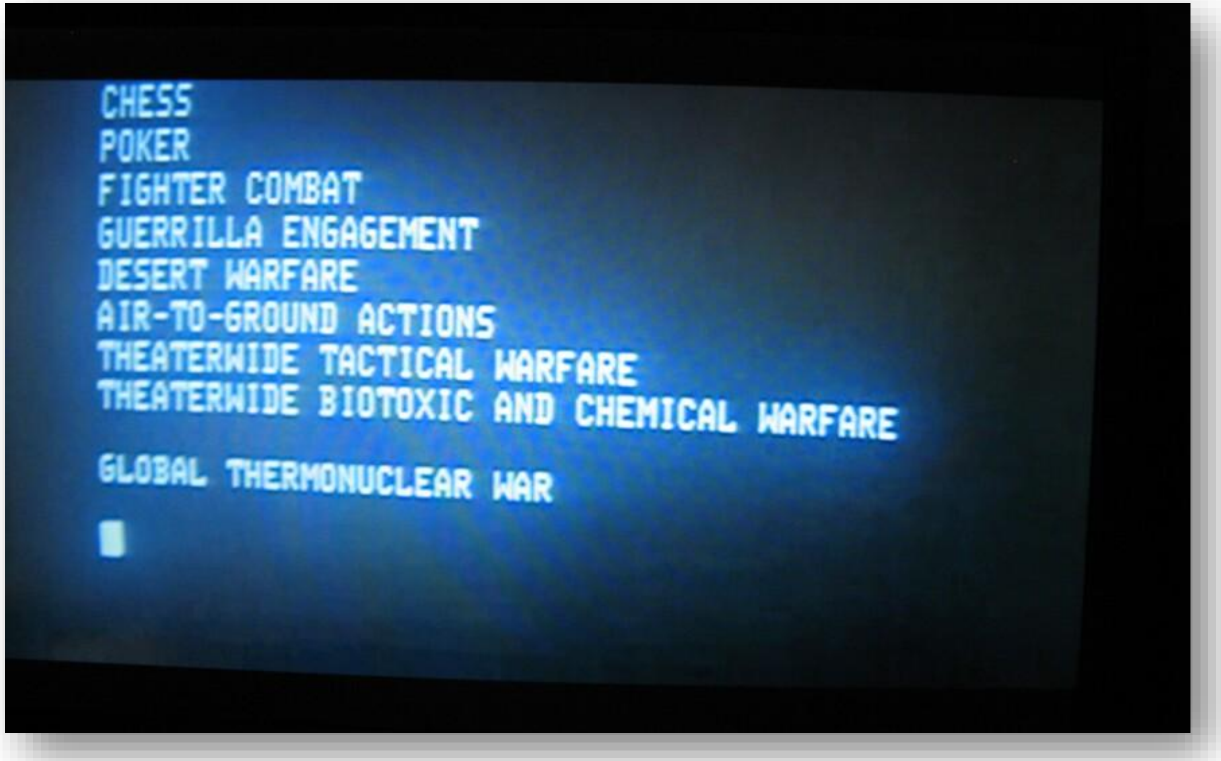


1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
2. If a bad guy can alter the operating system on your computer, it's not your computer anymore
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
4. If you allow a bad guy to upload programs to your website, it's not your website any more
5. Weak passwords trump strong security
6. A computer is only as secure as the administrator is trustworthy
7. Encrypted data is only as secure as the decryption key
8. An out of date virus scanner is only marginally better than no virus scanner at all
9. Absolute anonymity isn't practical, in real life or on the Web
10. Technology is not a panacea

Spot it.

Identify the threat

Who's behind all the cybercrime?

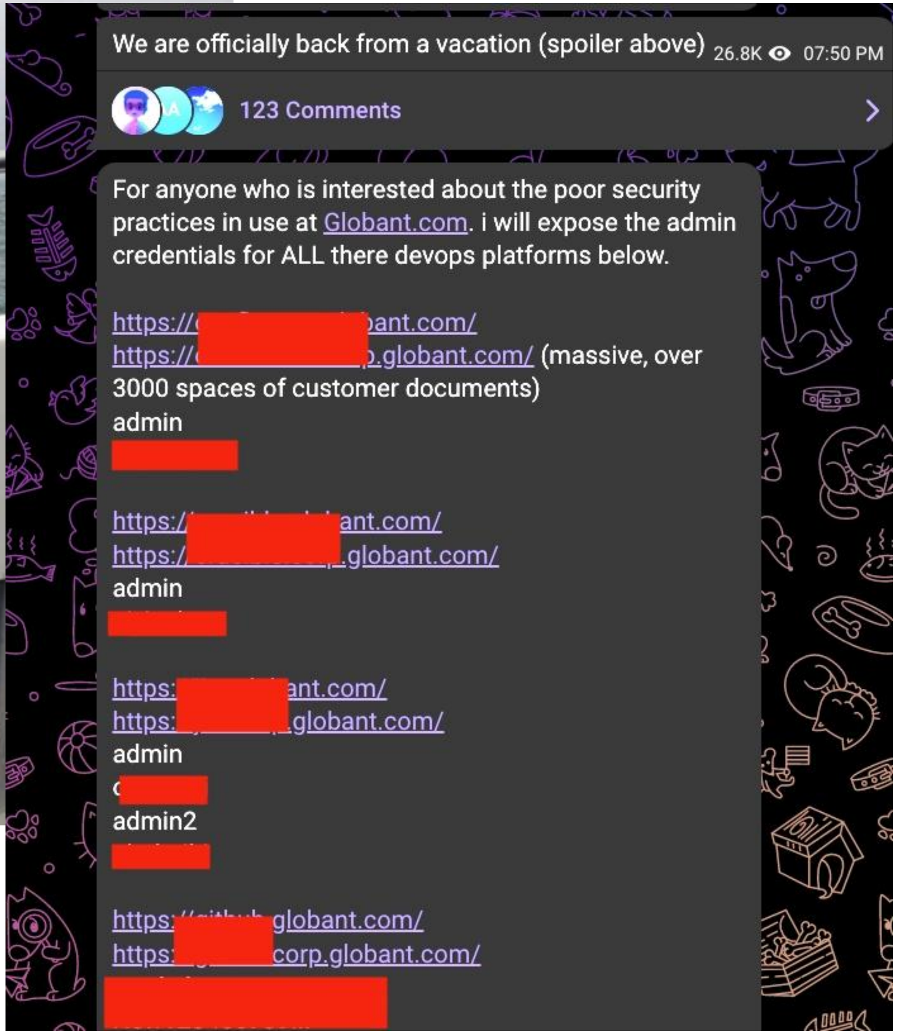


```
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE

GLOBAL THERMONUCLEAR WAR

▮
```

Has cybercrime become child's play?



We are officially back from a vacation (spoiler above) 26.8K 07:50 PM

123 Comments

For anyone who is interested about the poor security practices in use at Globant.com. i will expose the admin credentials for ALL there devops platforms below.

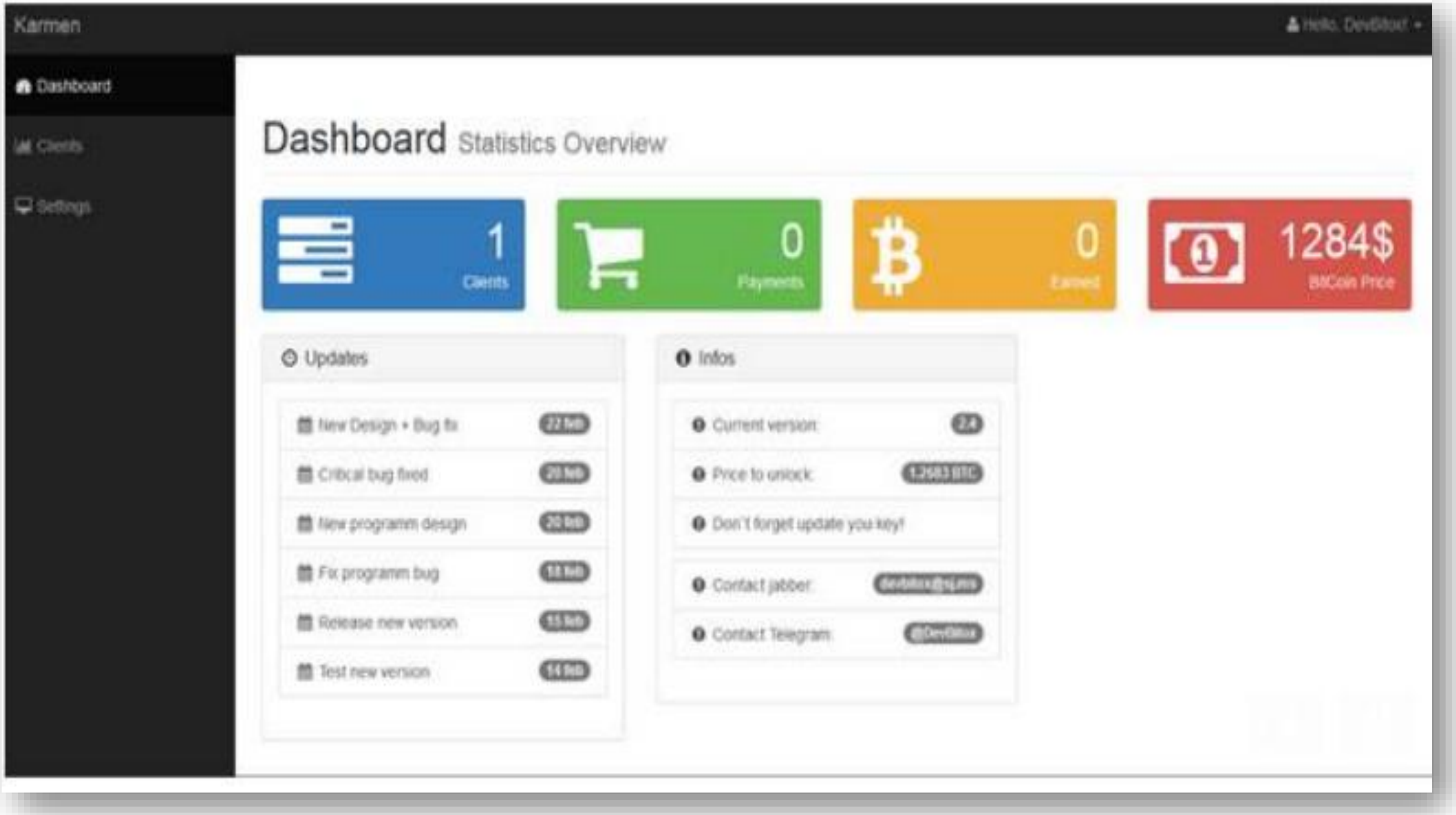
https://[redacted]ant.com/
https://[redacted].globant.com/ (massive, over 3000 spaces of customer documents)
admin
[redacted]

https:/[redacted]ant.com/
https:/[redacted].globant.com/
admin
[redacted]

https:[redacted]ant.com/
https:[redacted].globant.com/
admin
[redacted]
admin2
[redacted]

https:[redacted]globant.com/
https:[redacted]corp.globant.com/
[redacted]

For many, cybercrime is a side hustle



Karmen

Hello, DevBitox! ▾

Dashboard

Clients

Settings

Dashboard Statistics Overview

1	0	0	1284$
Clients	Payments	Earned	BitCoin Price

Updates

New Design + Bug fix	22 feb
Critical bug fixed	20 feb
New programm design	20 feb
Fix programm bug	18 feb
Release new version	15 feb
Test new version	14 feb

Infos

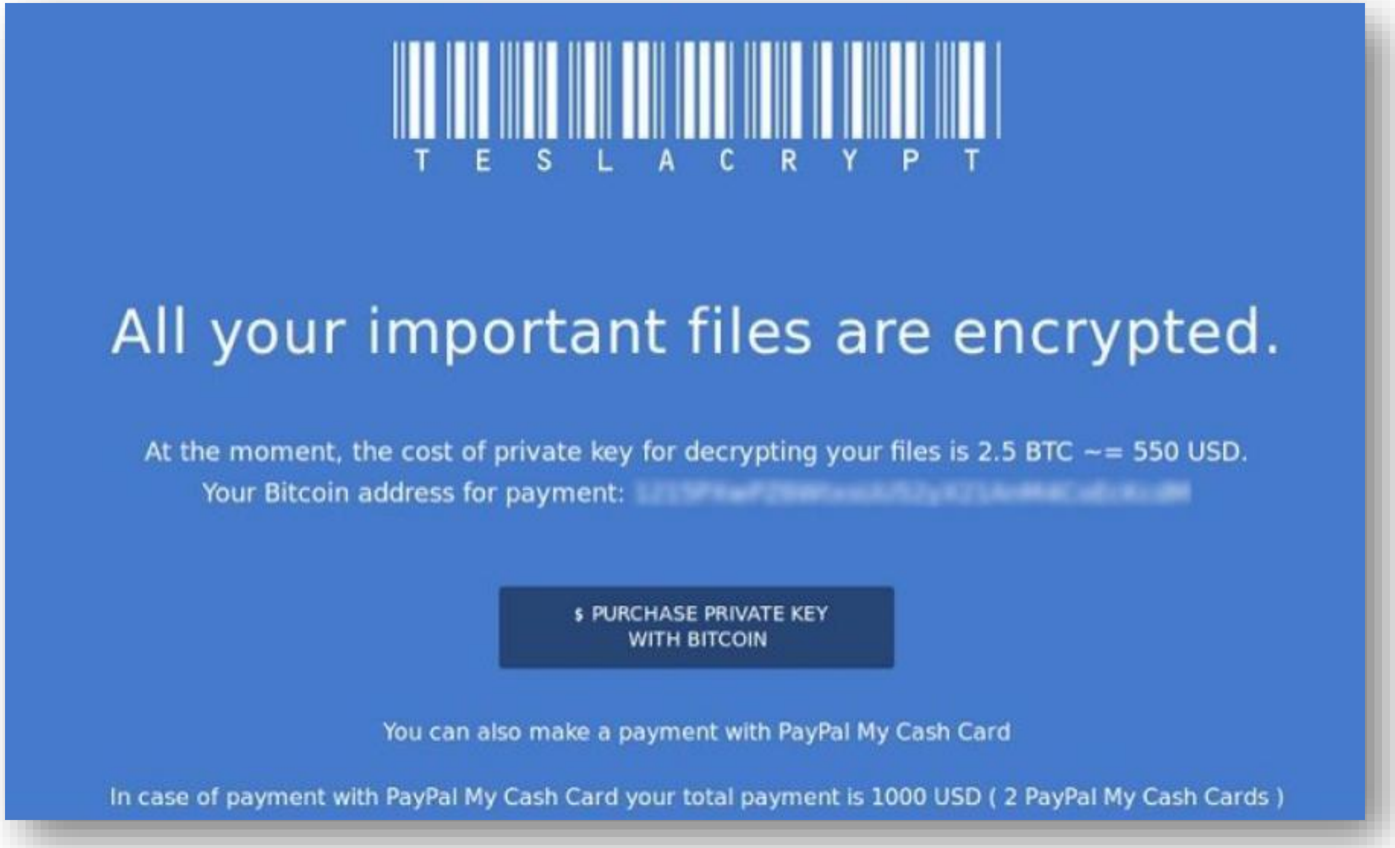
Current version:	2.4
Price to unlock:	1.2683 BTC
Don't forget update you key!	
Contact jabber:	devbitox@sj.ms
Contact Telegram:	@DevBitox

Stop it.

Prevent cybercrime

Ransomware: Canada is the world’s 2nd most targeted country

$US 2 million ransoms are now the norm



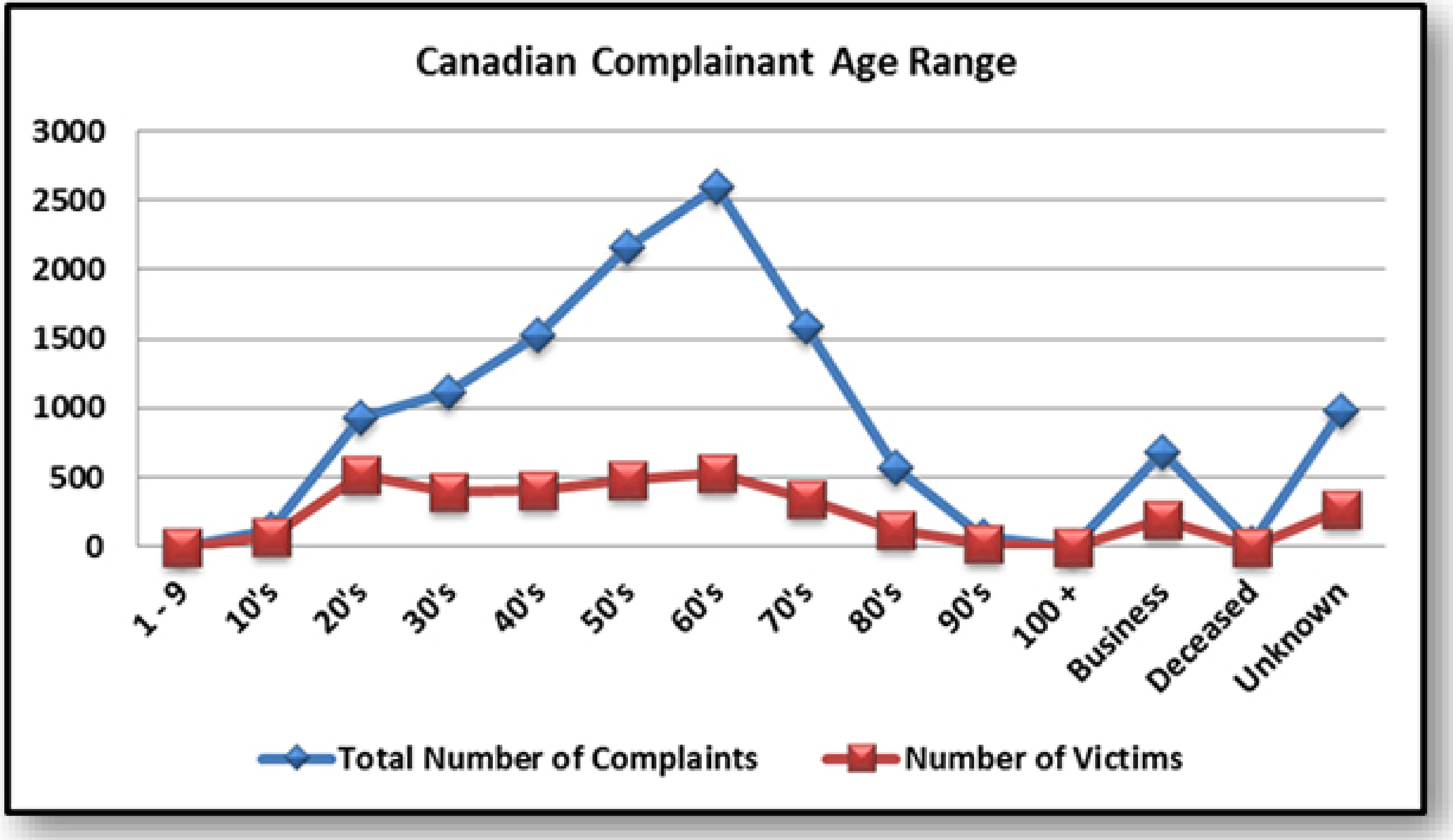
All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [redacted]

You can also make a payment with PayPal My Cash Card

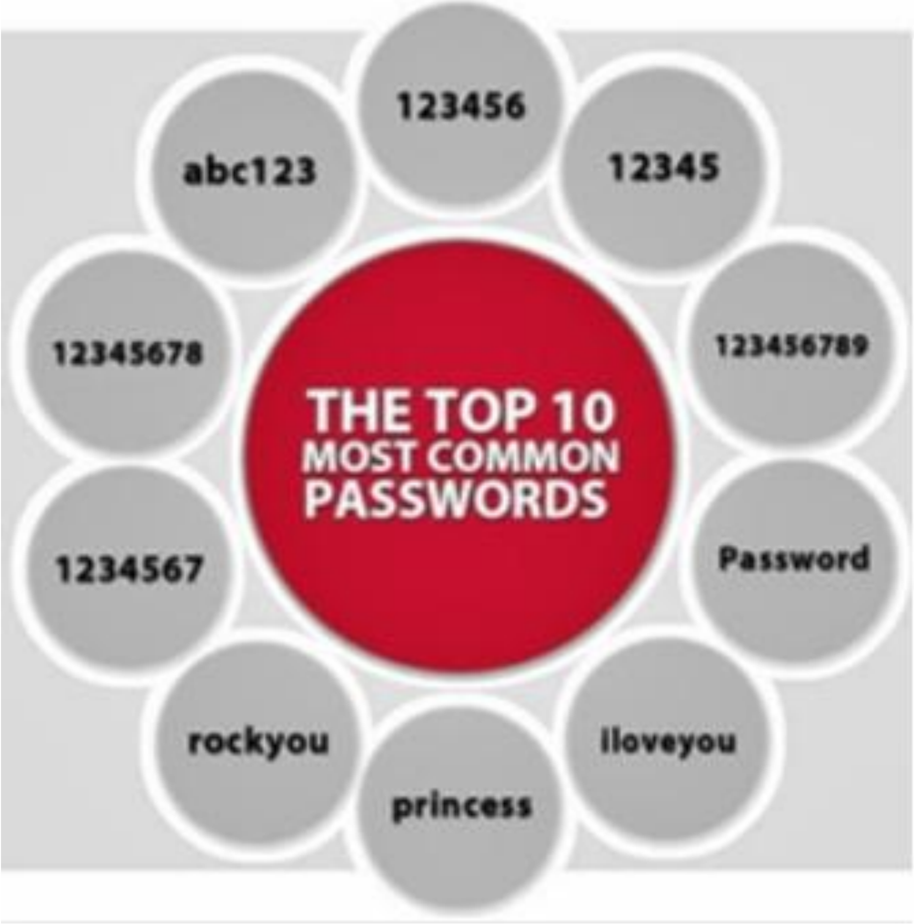
In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

Everyone is equal, but some are more equal than others…



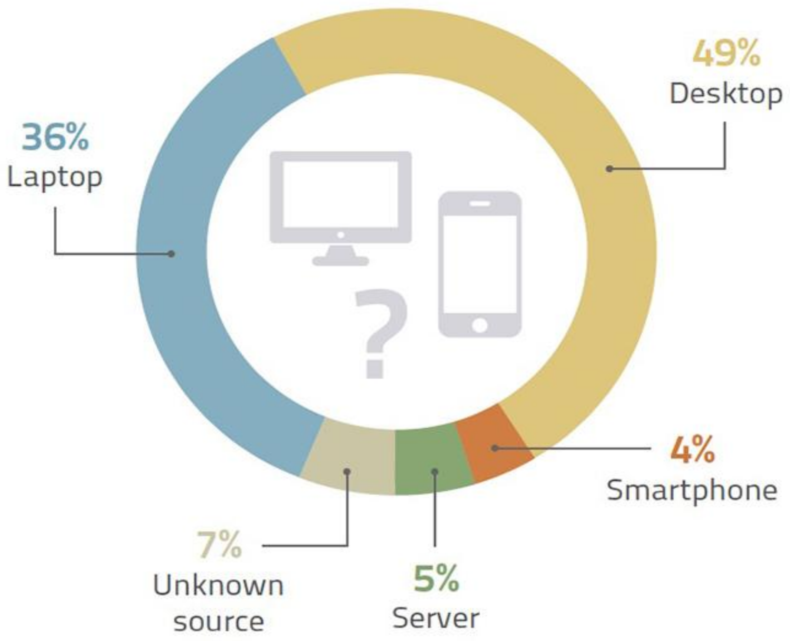
When did it stop being all about the passwords?

- short passwords
- guessable passwords (i.e. pet name)
- simple character pattern
- password reuse between sites
- entering passwords in infected computers
- not being aware of shoulder surfers
- sharing passwords on fake websites
- allowing others to set your password
- not using multifactor when available



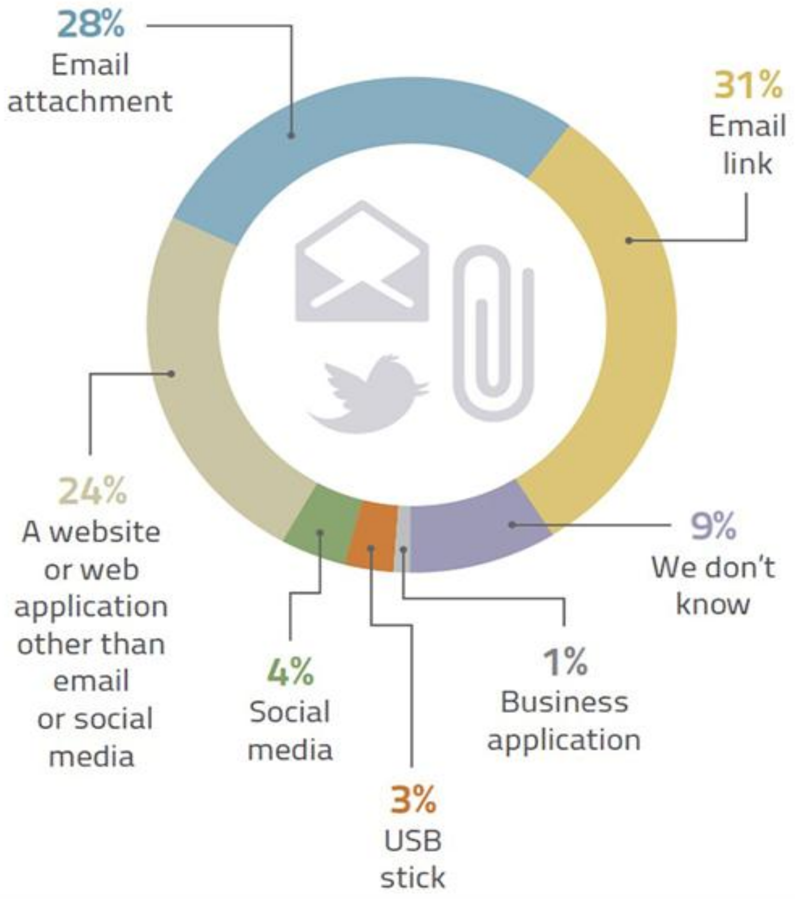
Some things never change

Physical locations in which ransomware entered the organization

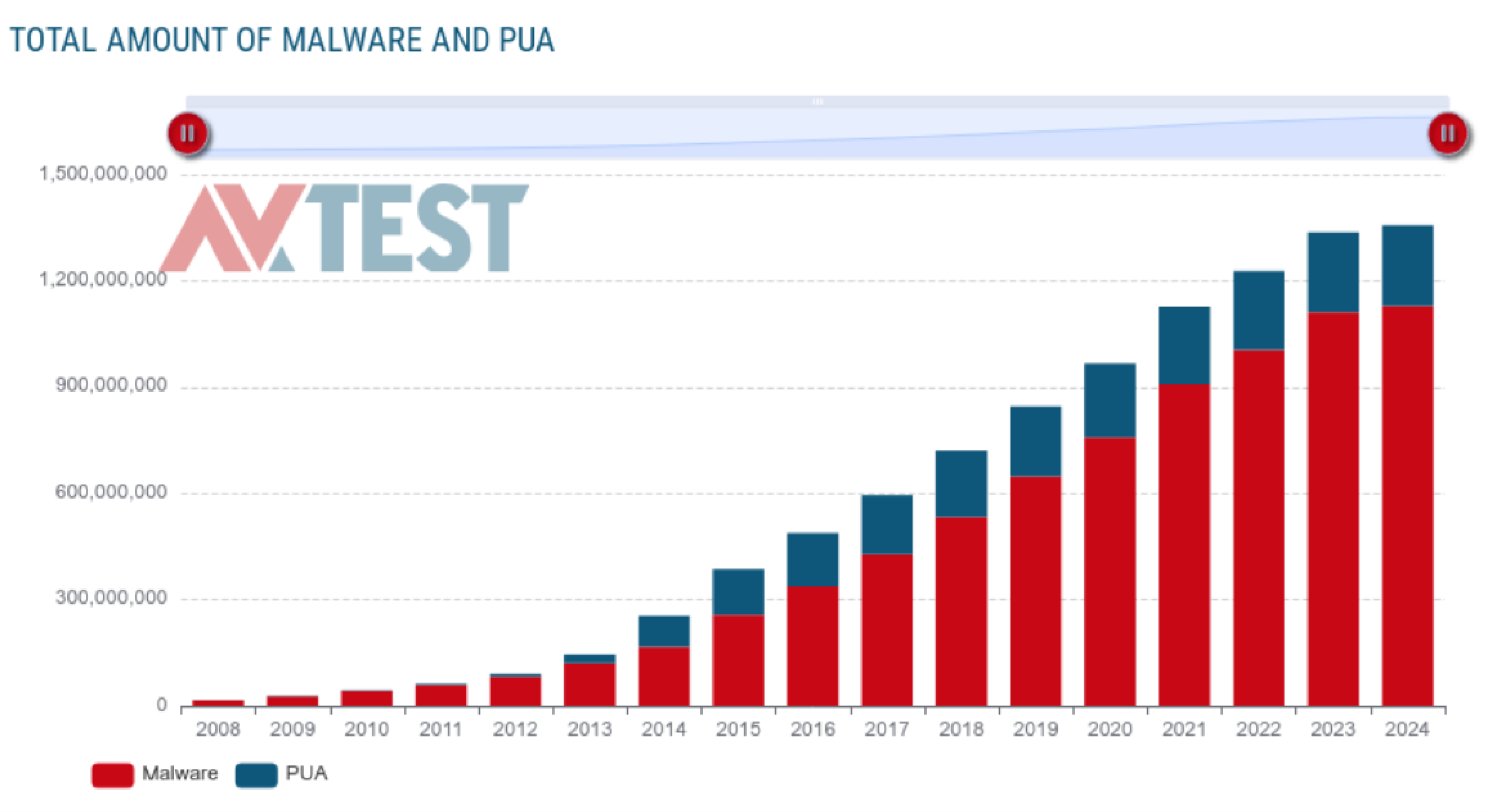


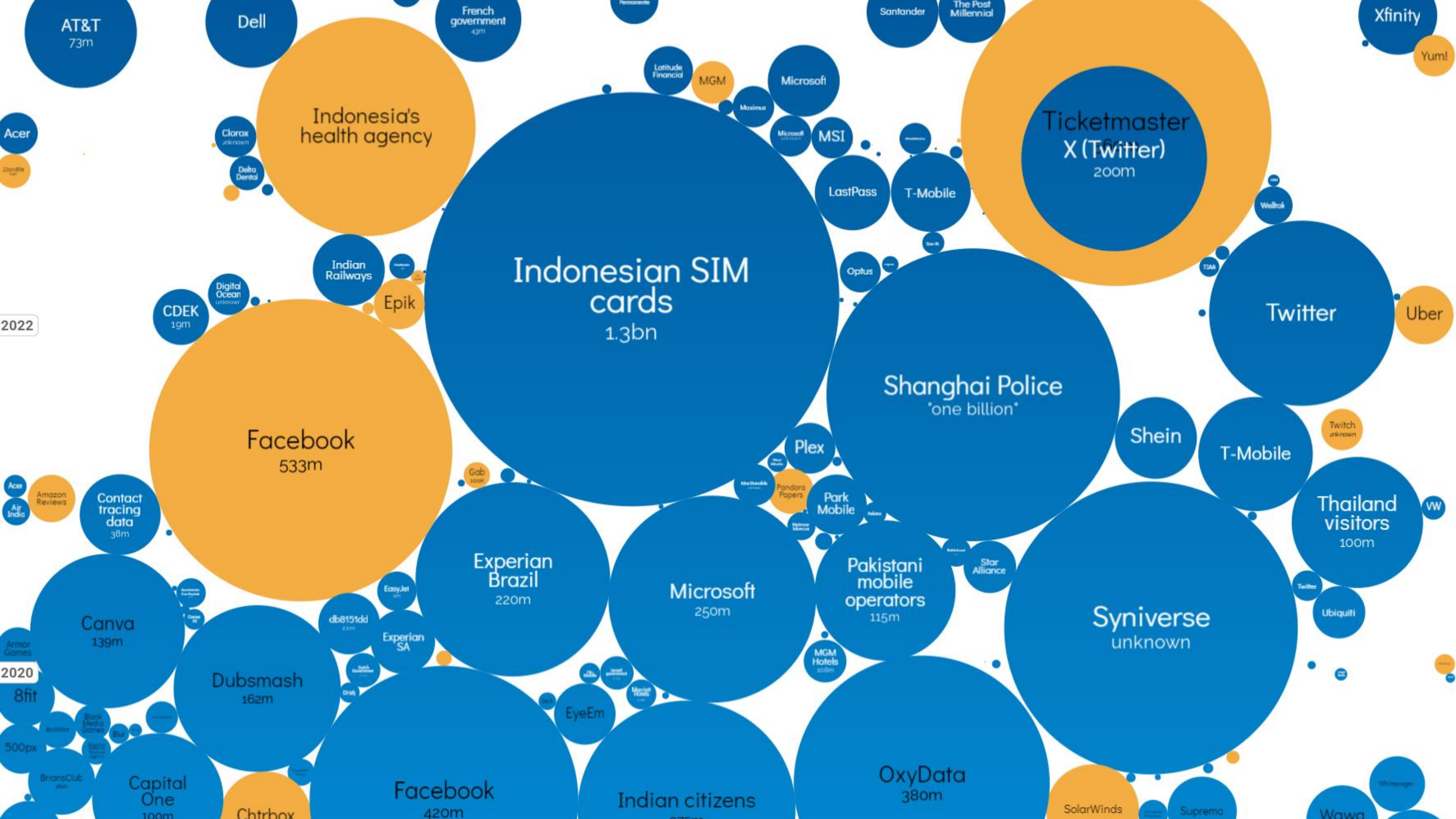
SOURCE: "UNDERSTANDING THE DEPTH OF THE GLOBAL MALWARE PROBLEM," OSTERMAN RESEARCH, AUGUST 2016; TOTAL EQUALS 101%

Applications by which ransomware entered the organization



All indicators pointed to an explosion of malware in 2025




AT&T
73m
Dell
French government
43m
Santander
The Post Millennial
Xfinity
Yum!
Acer
Clorox
unknown
Delta Dental
Indonesia's health agency
Latitude Financial
MGM
Microsoft
Maximus
Microsoft
unknown
MSI
LastPass
T-Mobile
Ticketmaster
X (Twitter)
200m
Wattpad
Indian Railways
Epik
Digital Ocean
unknown
CDEK
19m
2022
Indonesian SIM cards
1.3bn
Optus
TIAA
Twitter
Uber
Shanghai Police
"one billion"
Shein
T-Mobile
Twitch
unknown
Facebook
533m
Gab
100K
Plex
Pandora Papers
Park Mobile
Thailand visitors
100m
VW
Acer
Air India
Amazon Reviews
Contact tracing data
38m
Experian Brazil
220m
Microsoft
250m
Pakistani mobile operators
115m
Star Alliance
Syniverse
unknown
Twitter
Ubiquiti
Canva
139m
EasyJet
9m
db8151dd
22m
Experian SA
Armor Games
2020
8fit
Dubsmash
162m
MGM Hotels
10.6m
EyeEm
Marriott Hotels
Blank Media Games
Blur
500px
BriansClub
26m
Capital One
100m
Chtrbox
Facebook
420m
Indian citizens
OxyData
380m
SolarWinds
Suprema
Whitepages
Wawa

Can companies keep up with risk posture changes?

Key Shift

Attackers use advanced tactics like AI ransomware-as-a-service agents to infiltrate corporate networks.

Global Spike

Cybercrime damages expected to reach **$10.5 trillion annually** by the end of this year despite 13% of IT budgets spent on cybersecurity.

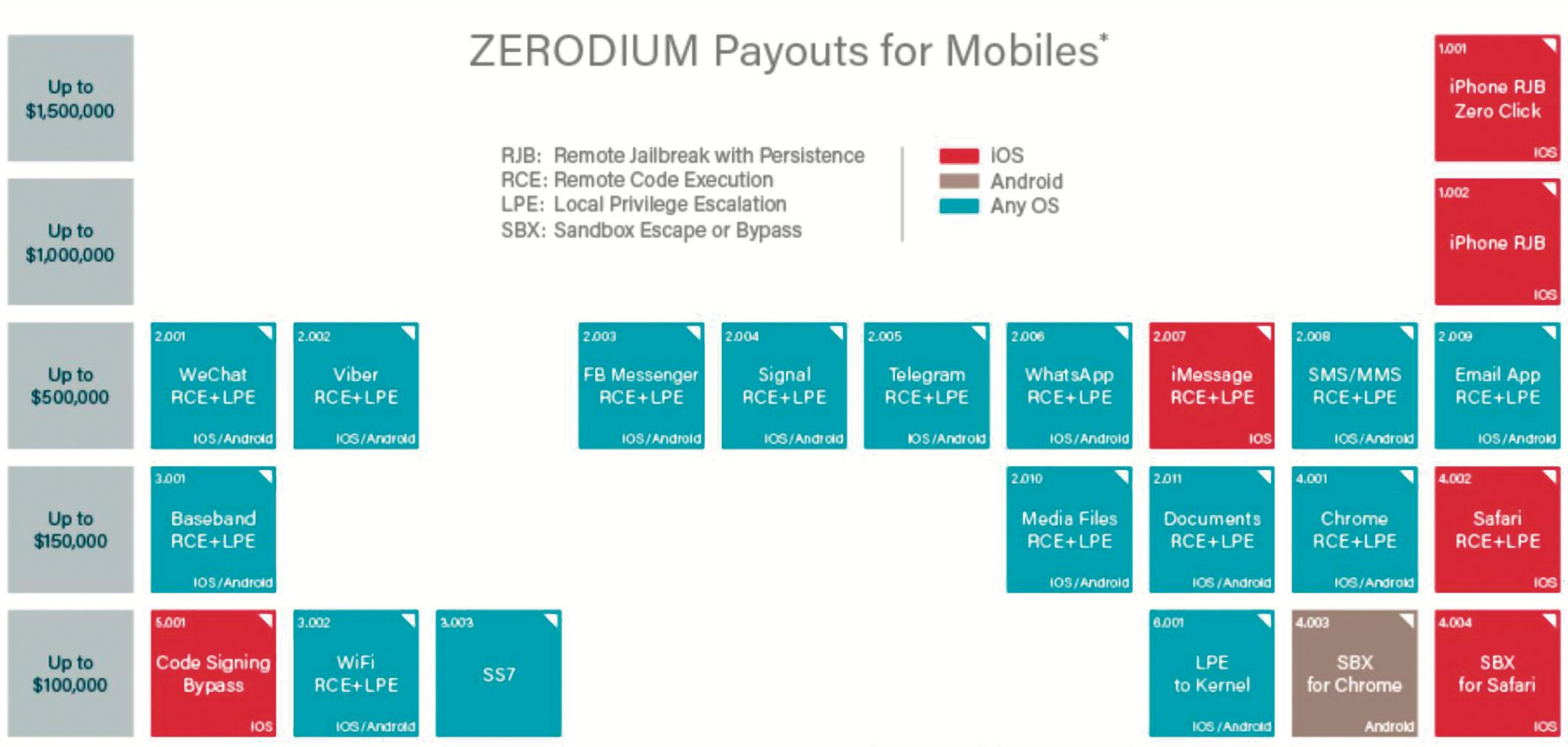
No Longer Theoretical

Governments and major logistics firms faced crippling attacks, halting shipments and causing multi-million-dollar losses.

Imperative Action

Boards must prioritize funding for cybersecurity risk management, preventive controls, detection, and supply chain risk.

How did cybercrime become commoditized?



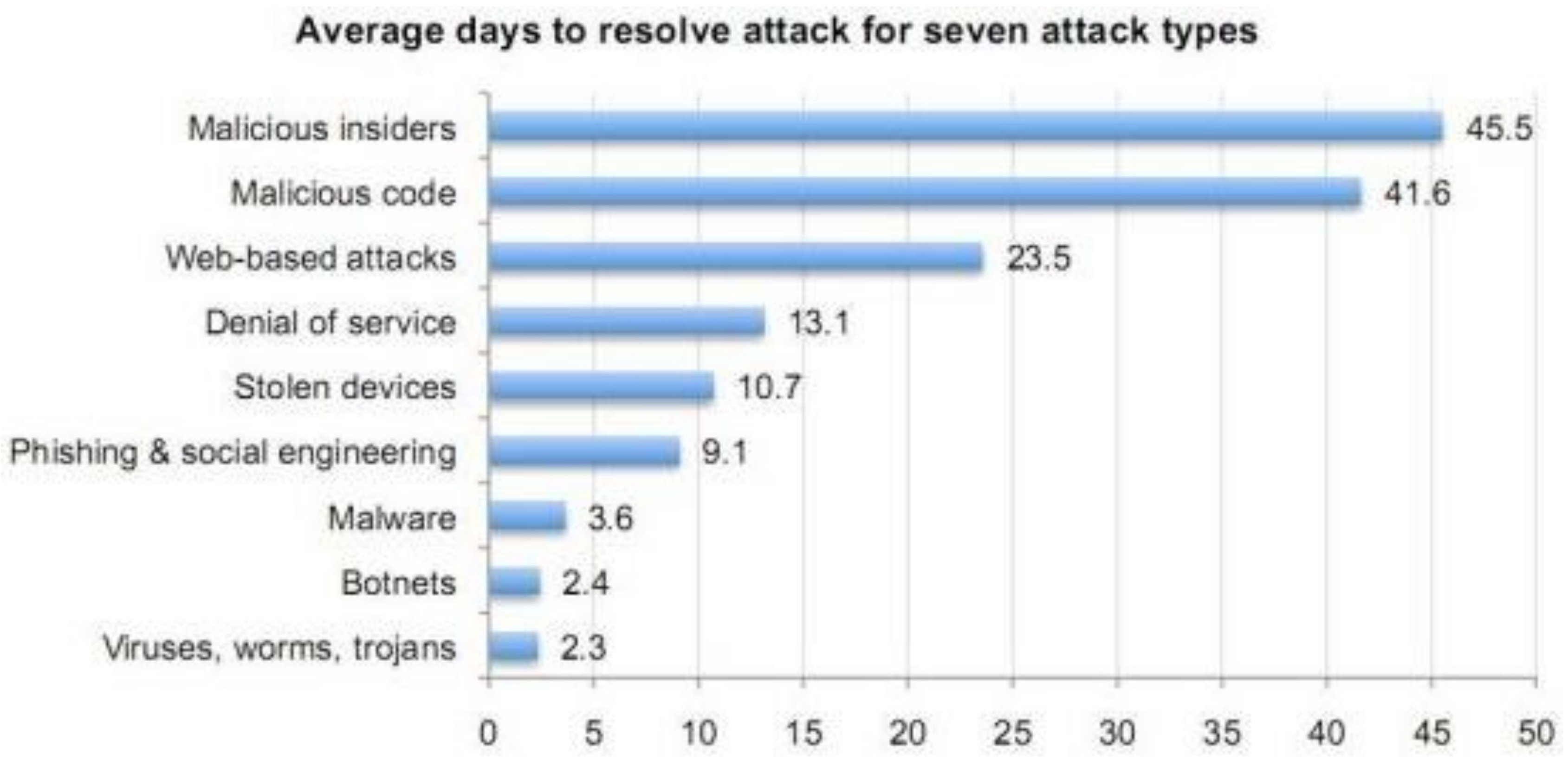
ZERODIUM Payouts for Mobiles*

RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

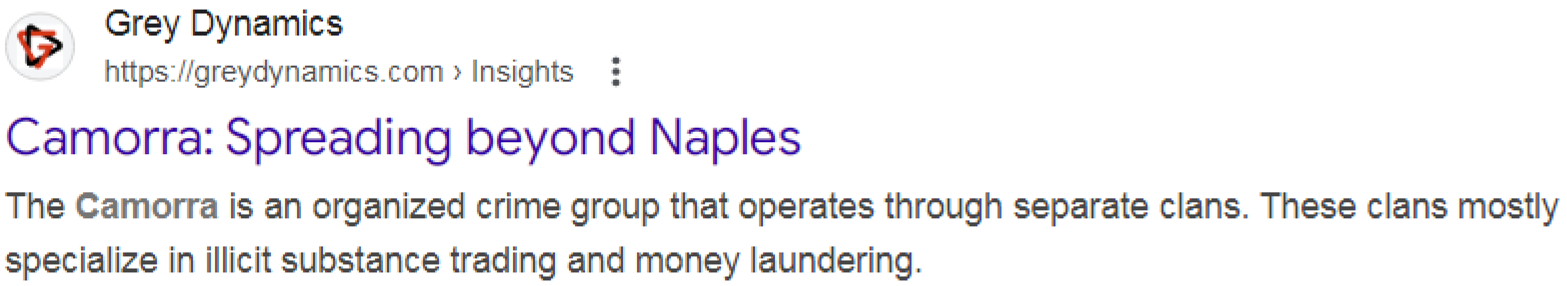
🟥 iOS
🟫 Android
🟦 Any OS

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 $150,000	3.001 Baseband RCE+LPE iOS/Android						2.010 Media Files RCE+LPE iOS/Android	2.011 Documents RCE+LPE iOS/Android	4.001 Chrome RCE+LPE iOS/Android	4.002 Safari RCE+LPE iOS
Up to $100,000	5.001 Code Signing Bypass iOS	3.002 WiFi RCE+LPE iOS/Android	3.003 SS7					6.001 LPE to Kernel iOS/Android	4.003 SBX for Chrome Android	4.004 SBX for Safari iOS

287 days to detect common malware infections … year after year



How does organized cybercrime work?

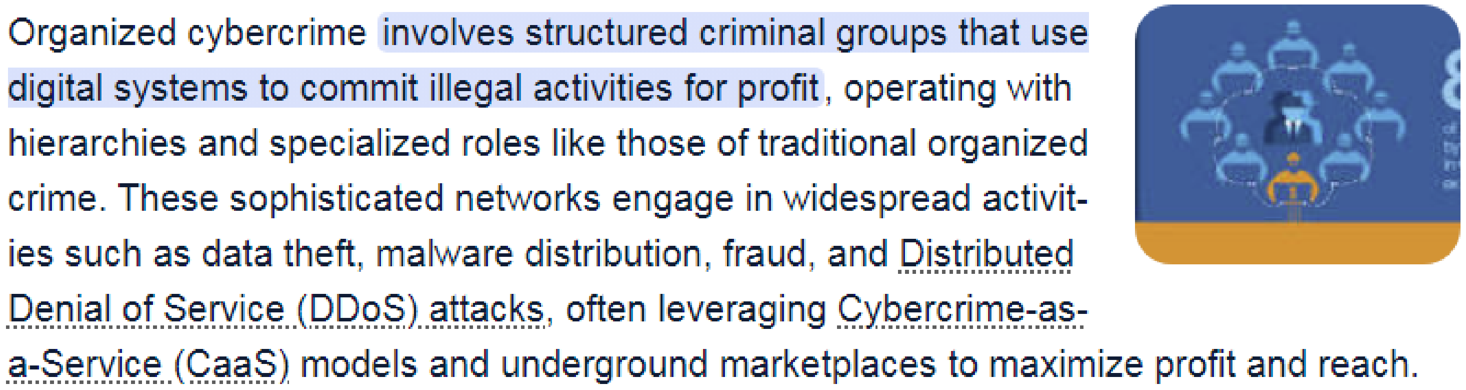


Grey Dynamics

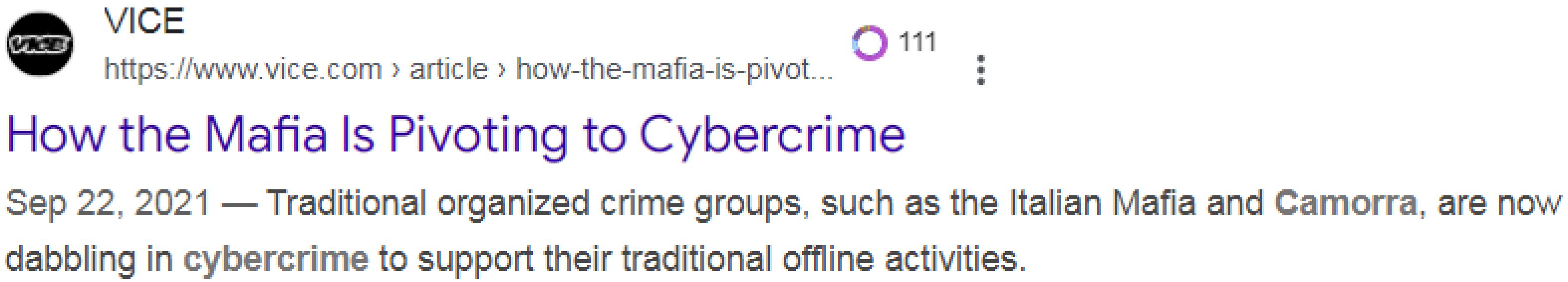
https://greydynamics.com › Insights

Camorra: Spreading beyond Naples

The **Camorra** is an organized crime group that operates through separate clans. These clans mostly specialize in illicit substance trading and money laundering.



Organized cybercrime involves structured criminal groups that use digital systems to commit illegal activities for profit, operating with hierarchies and specialized roles like those of traditional organized crime. These sophisticated networks engage in widespread activities such as data theft, malware distribution, fraud, and Distributed Denial of Service (DDoS) attacks, often leveraging Cybercrime-as-a-Service (CaaS) models and underground marketplaces to maximize profit and reach.



VICE

https://www.vice.com › article › how-the-mafia-is-pivot...

111

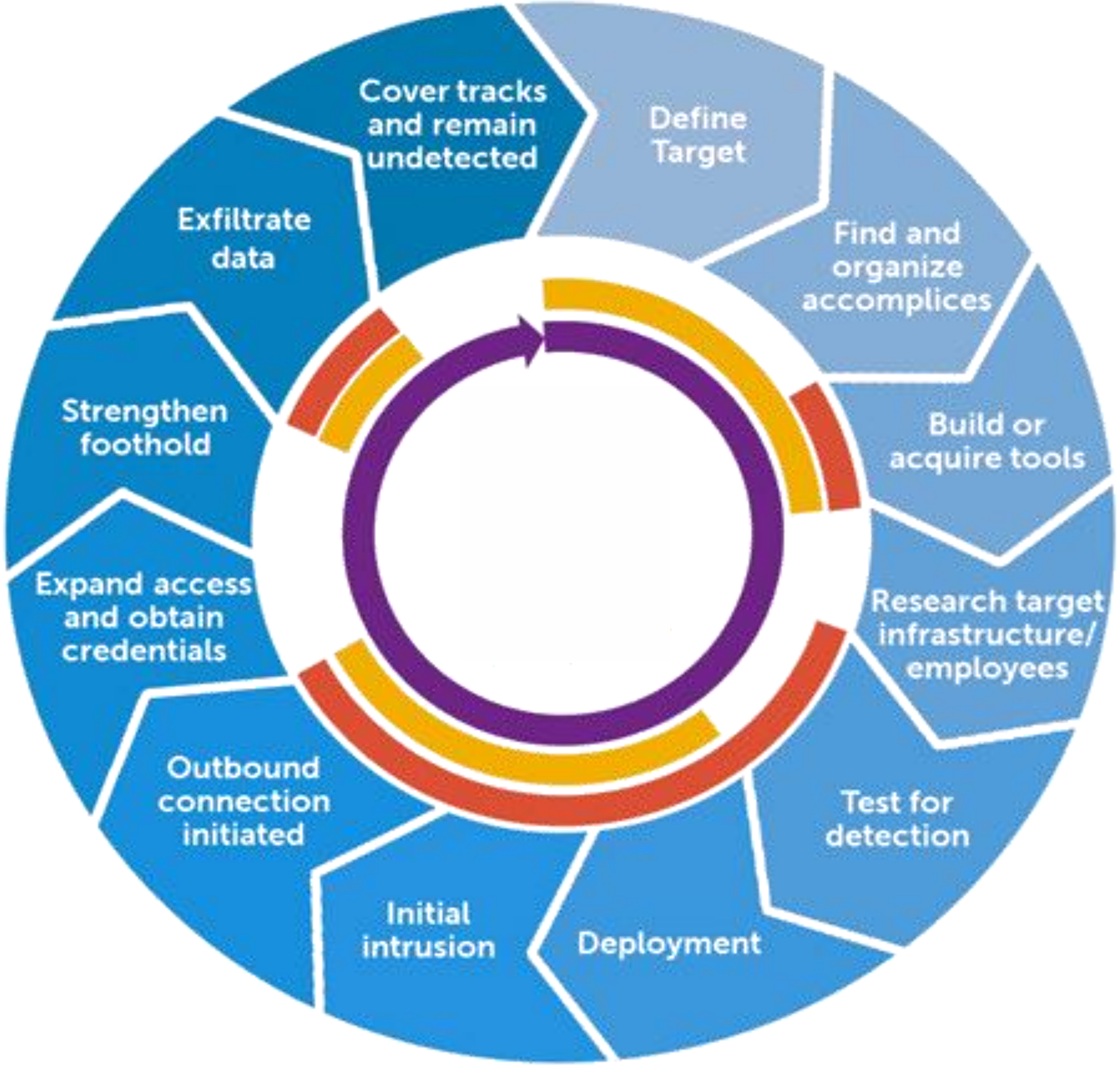
How the Mafia Is Pivoting to Cybercrime

Sep 22, 2021 — Traditional organized crime groups, such as the Italian Mafia and **Camorra**, are now dabbling in **cybercrime** to support their traditional offline activities.

Secure it.

Data protection

Remember the kill chain


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

What would it have taken to prevent multimillion$ breaches?

- Company-wide focus on **privacy compliance**
- **Informed consent** was employed by default
- Data collection had been **limited and minimized**
- Information had been **rigorously deleted**
- **Limited access** to PI and segregation had been enforced
- Safe hygiene and **need-to-know** had been communicated
- **Privacy by design** was the default rather than an ideal
- They had stuck to the 10 Immutable Laws!

Canada Revenue Agency Agence du revenu du Canada

GCKey

EQUIFAX

Desjardins

CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

LifeLabs®

TransUnion®

Data protection & privacy compliance

1

Regulatory wave

GDPR, CCPA, and new international data laws set higher penalties—fines up to 4% of annual global turnover.

2

Competitive advantage

Compliance frameworks (ISO 27001, SOC 2) boost customer trust and brand reputation.

3

Risk vs. reward

Failure to comply can trigger damaging investigations and public scrutiny.

4

Practical tip

Regularly audit data handling processes and train teams on privacy regulations.

Investigations are about innovation, but also practice

Opportunity

AI-driven analytics detect threats in real time, reducing breach impact by up to **40%** (source: Deloitte).

Threat

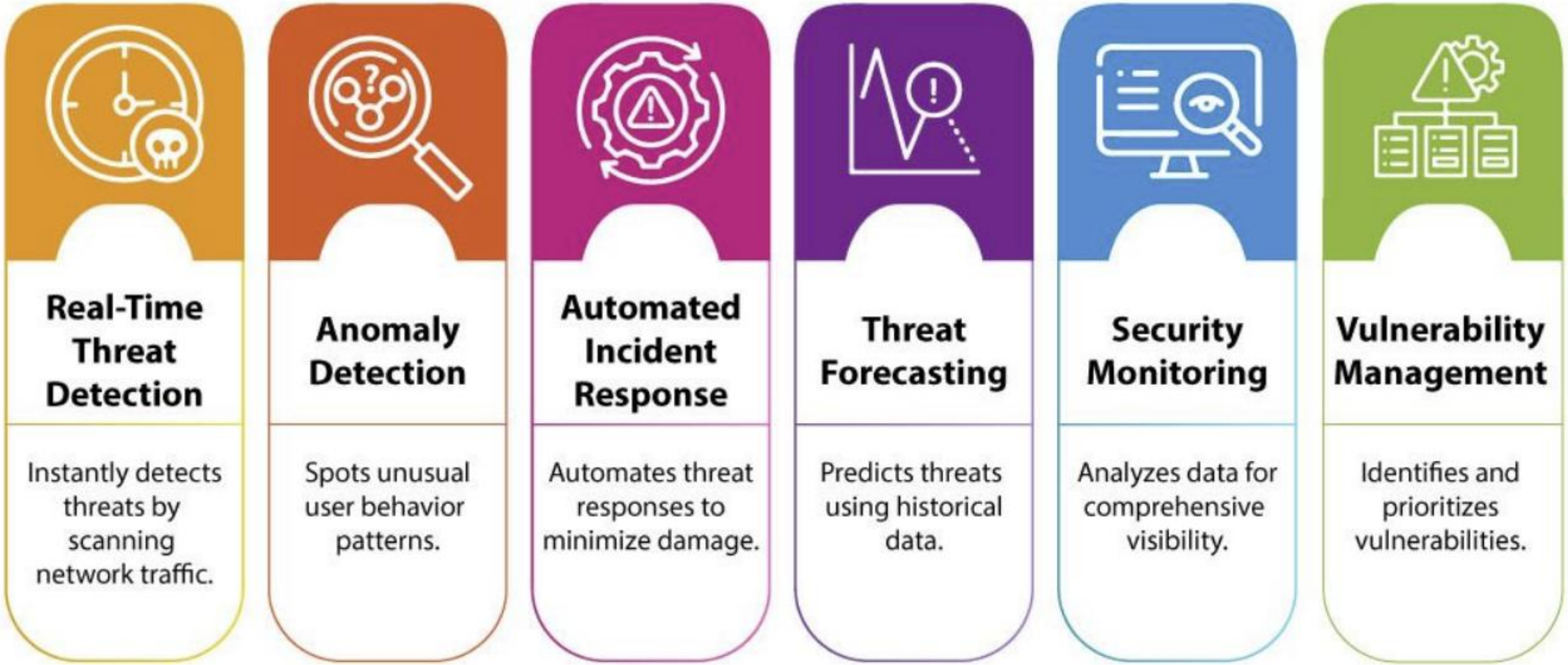
Attackers deploy AI bots to find security gaps and craft sophisticated phishing campaigns.

Leader’s role

Balance innovation with vigilant oversight (e.g., ethical AI usage).

Action item

Establish AI governance policies and continuous monitoring.



Real-Time Threat Detection

Instantly detects threats by scanning network traffic.

Anomaly Detection

Spots unusual user behavior patterns.

Automated Incident Response

Automates threat responses to minimize damage.

Threat Forecasting

Predicts threats using historical data.

Security Monitoring

Analyzes data for comprehensive visibility.

Vulnerability Management

Identifies and prioritizes vulnerabilities.

Next steps: test yourself

Stay curious

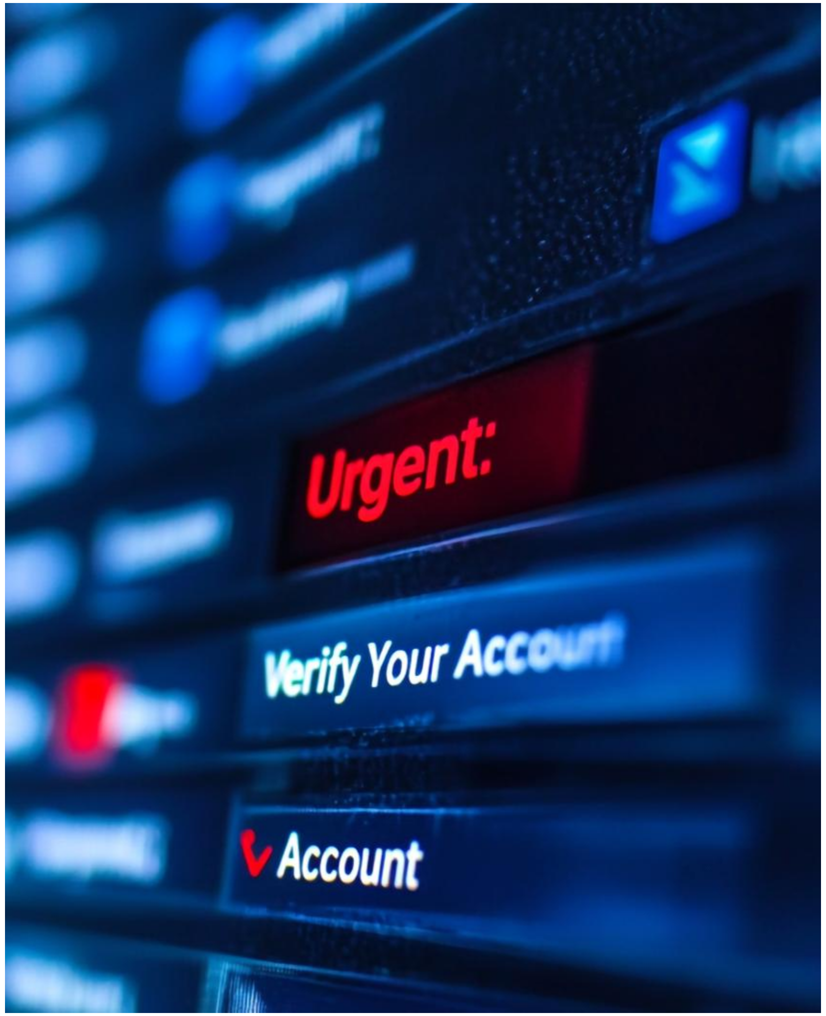
Document and communicate best practices and role-specific tasks

Build upon trust

Build due diligence into your supply chain from the top down

Simulate and investigate

Carry out incident response table-top exercises & data breach tests



2025 DATARISK RESEARCH REPORT

2025 Sector Report on Cyber Security

2025

FCT Cybersecurity Resource Guide

More than a policy

Visit fct.ca/fraud-insights-centre for additional tools and resources.