Cybersecurity

Come si protegge la propria azienda?

Data
mercoledì, 19 aprile 2023 ore 09:00

Luogo
Camera di commercio di Bolzano, 3° piano

Costo
gratuito

CAMERA DI COMMERCIO,
INDUSTRIA, ARTIGIANATO
E AGRICOLTURA DI BOLZANO

PMI e cybersecurity

Igor Falcomatà

Il vostro relatore..

- attività professionale (~25 years)
  - analisi delle vulnerabilità
  - simulazioni di attacco
  - consulenza
  - formazione
- vita privata:
  - fondatore sikurezza.org
  - Attivo in vari Linux User Group

NETWORK enforcer SECURITY

Igor Falcomatà

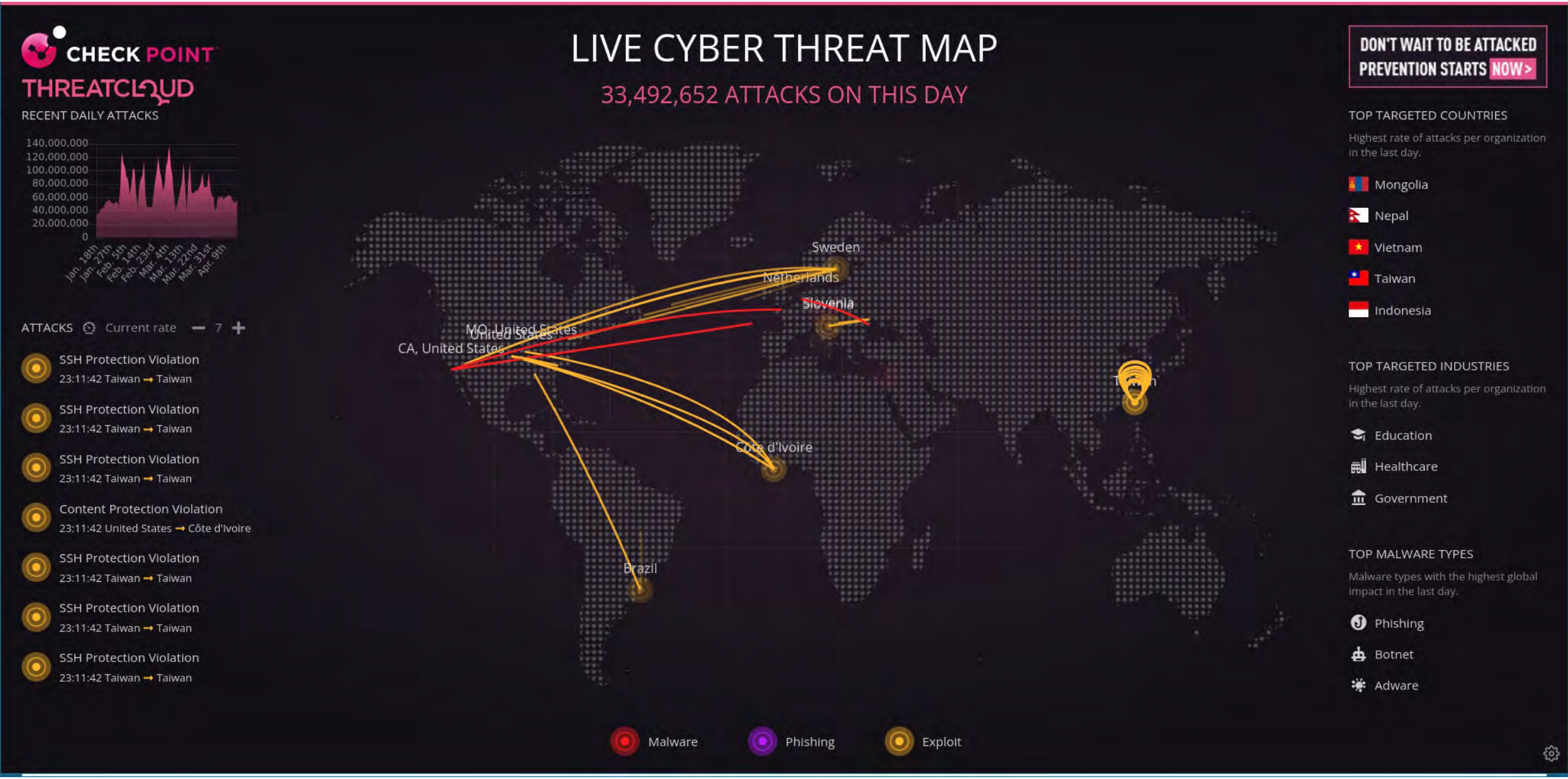
CEO & founder

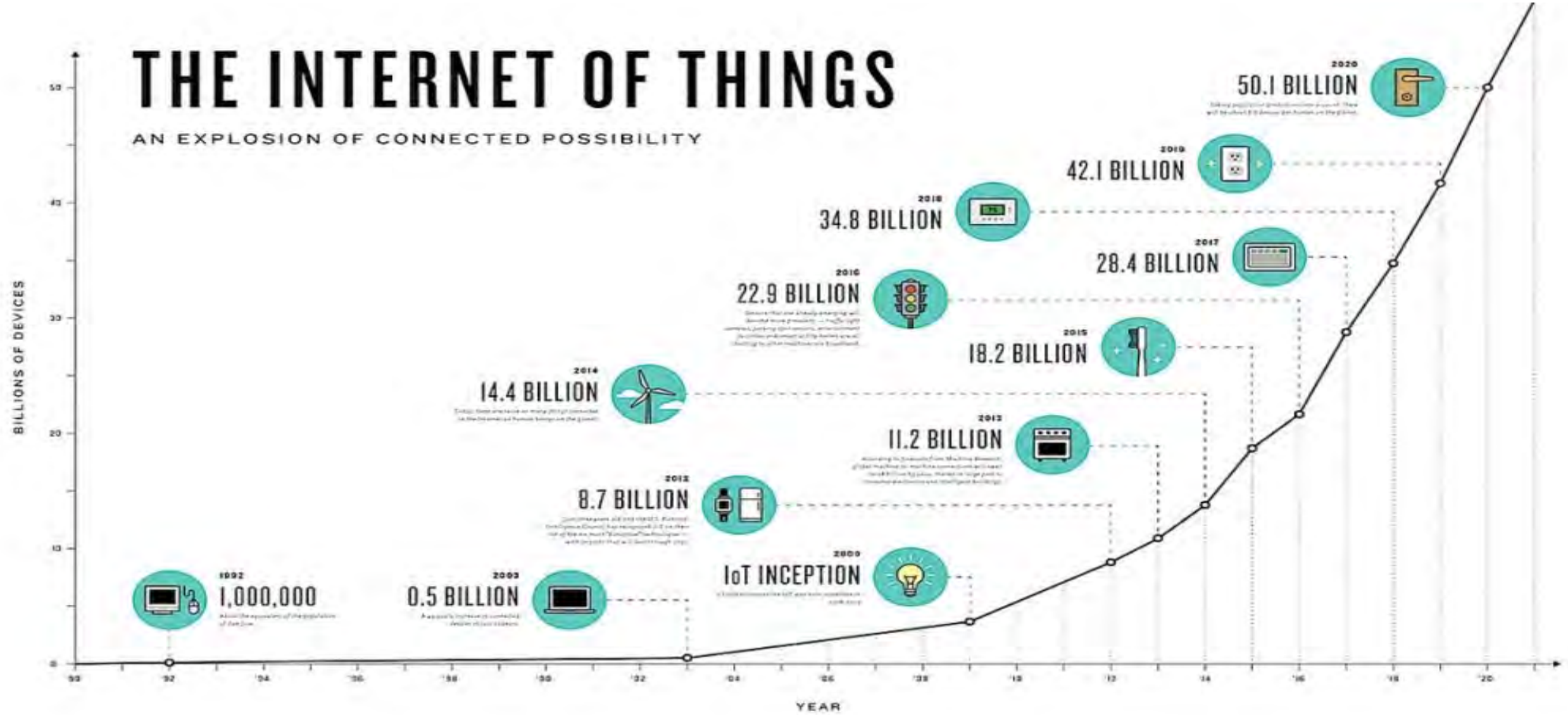
ifalcomata@enforcer.it

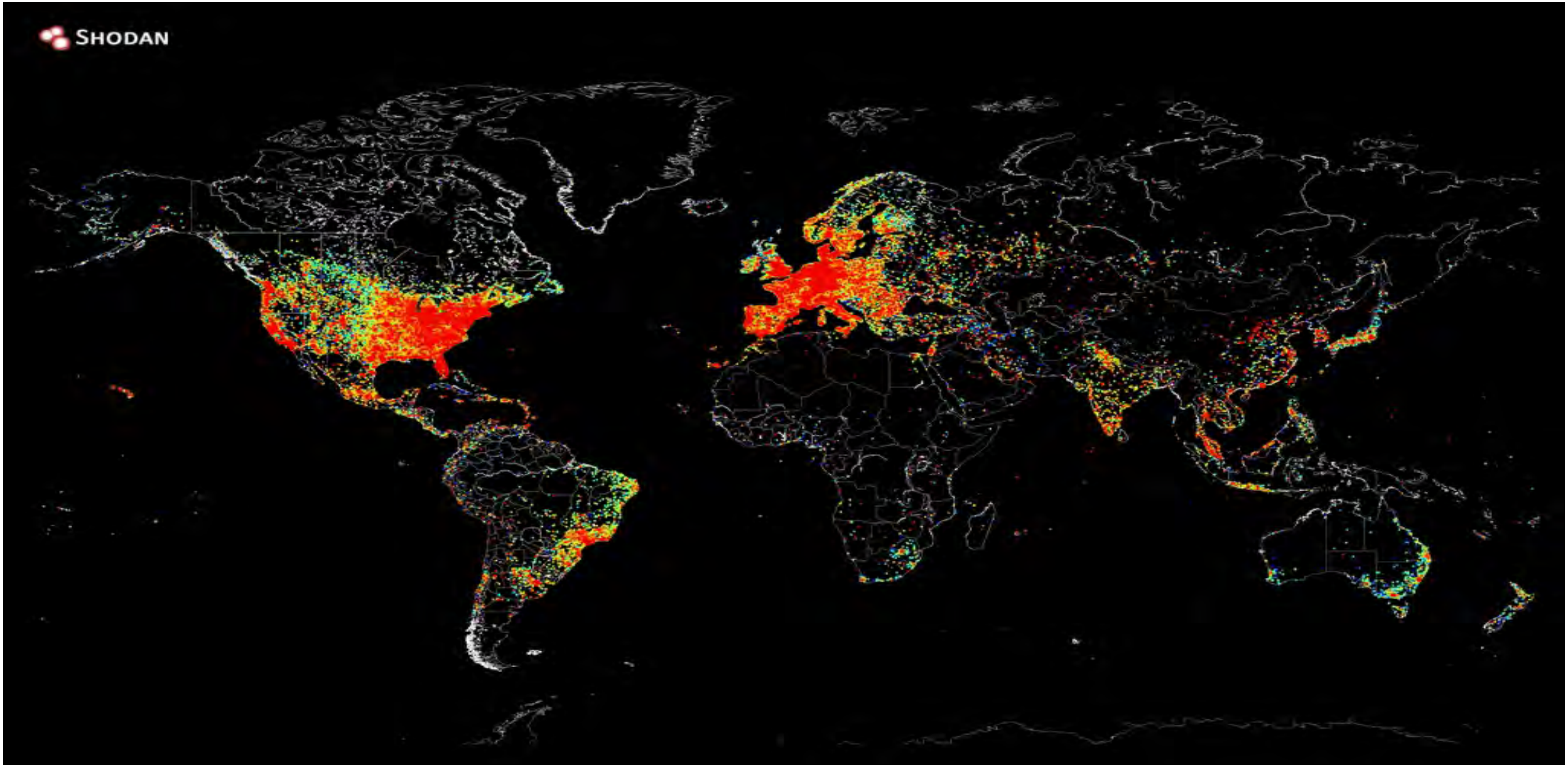
Di cosa parleremo..

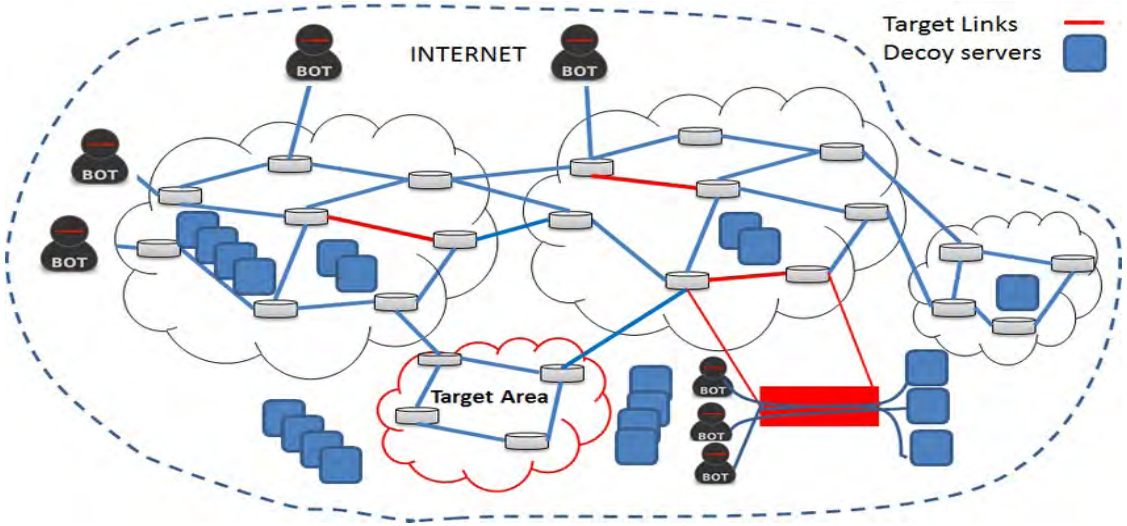
- Perché proprio a me?
- Perché le PMI?
- Fondamenta insicure
- Principali minacce
- Come approntare una corretta strategia di difesa?

Perché proprio a me?

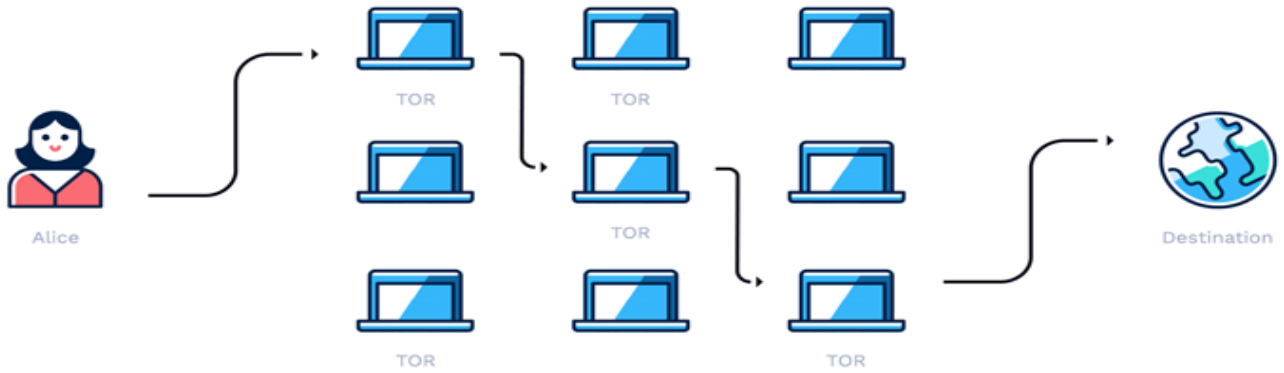

CHECK POINT
THREATCLOUD
RECENT DAILY ATTACKS
140,000,000
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
Jan. 18th
Jan. 27th
Feb. 5th
Feb. 14th
Feb. 23rd
Mar. 4th
Mar. 13th
Mar. 22nd
Mar. 31st
Apr. 9th
ATTACKS
Current rate
7
SSH Protection Violation
23:11:42 Taiwan → Taiwan
SSH Protection Violation
23:11:42 Taiwan → Taiwan
SSH Protection Violation
23:11:42 Taiwan → Taiwan
Content Protection Violation
23:11:42 United States → Côte d'Ivoire
SSH Protection Violation
23:11:42 Taiwan → Taiwan
SSH Protection Violation
23:11:42 Taiwan → Taiwan
SSH Protection Violation
23:11:42 Taiwan → Taiwan
LIVE CYBER THREAT MAP
33,492,652 ATTACKS ON THIS DAY
Sweden
Netherlands
Slovenia
MO, United States
United States
CA, United States
Côte d'Ivoire
Brazil
Malware
Phishing
Exploit
DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>
TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.
Mongolia
Nepal
Vietnam
Taiwan
Indonesia
TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.
Education
Healthcare
Government
TOP MALWARE TYPES
Malware types with the highest global impact in the last day.
Phishing
Botnet
Adware

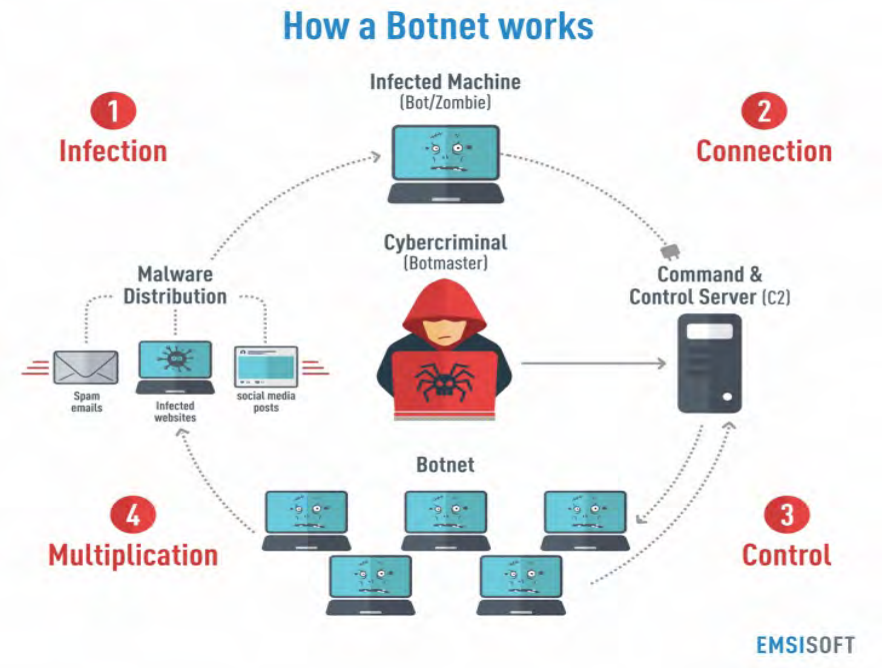

THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
1992
1,000,000
2003
0.5 BILLION
2009
IoT INCEPTION
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION
BILLIONS OF DEVICES
YEAR


SHODAN


INTERNET
Target Links
Decoy servers
BOT
Target Area


FREE Wi-Fi


Alice
TOR
TOR
TOR
TOR
TOR
Destination


How a Botnet works
1
Infection
Infected Machine
(Bot/Zombie)
2
Connection
Cybercriminal
(Botmaster)
Malware
Distribution
Command &
Control Server (C2)
Spam
emails
Infected
websites
social media
posts
Botnet
4
Multiplication
3
Control
EMSISOFT

LOCAL NEWS ›

Lasell University student bought Tesla after stealing $547,000 in credit card scam, police say

WBZ NEWS

BY WBZ-NEWS STAFF

UPDATED ON: MARCH 10, 2023 / 6:07 AM / CBS BOSTON

Gestisci i Cookie

Now Playing

Cybercriminals

Cybercriminals make extensive use of cryptocurrencies that consequently have to be laundered, invested or cashed out. Proceeds from cybercrime activities normally do not require a conversion as they are often already in cryptocurrencies. Cybercriminals extensively use obfuscation techniques and services to hinder transactions traceability.

CASE EXAMPLE

Money laundering network for cybercriminals

A complex investigation involving 20 countries resulted in the dismantling of a criminal network laundering tens of millions of euros in stolen funds that was advertising its services in online forums. Against the payment of a transaction fee (up to the 50% of the transaction), the network opened and maintained hundreds of corporate and personal bank accounts worldwide to receive and transfer money from cybercriminals who stole it from accounts of victims. Laundered funds were then returned to their cybercriminal clientele.

Source: Europol 2020, 20 arrests in QQAAZZ multi-million money laundering case

Le truffe online sono in continua evoluzione. Sempre più spesso, i malfattori chiedono aiuto ai titolari di un conto bancario che, ignari di commettere un reato e dei pericoli che corrono, si trasformano in "money mule". Se qualcuno ti chiede di trasferire del denaro utilizzando il tuo conto corrente in cambio di contanti, allora ti sta chiedendo di essere un money mule (mulo di denaro). In tal caso, sarai complice di un reato finanziario senza neanche saperlo.

Financial and cybercrimes top global police concerns, says new INTERPOL report

19 October 2022

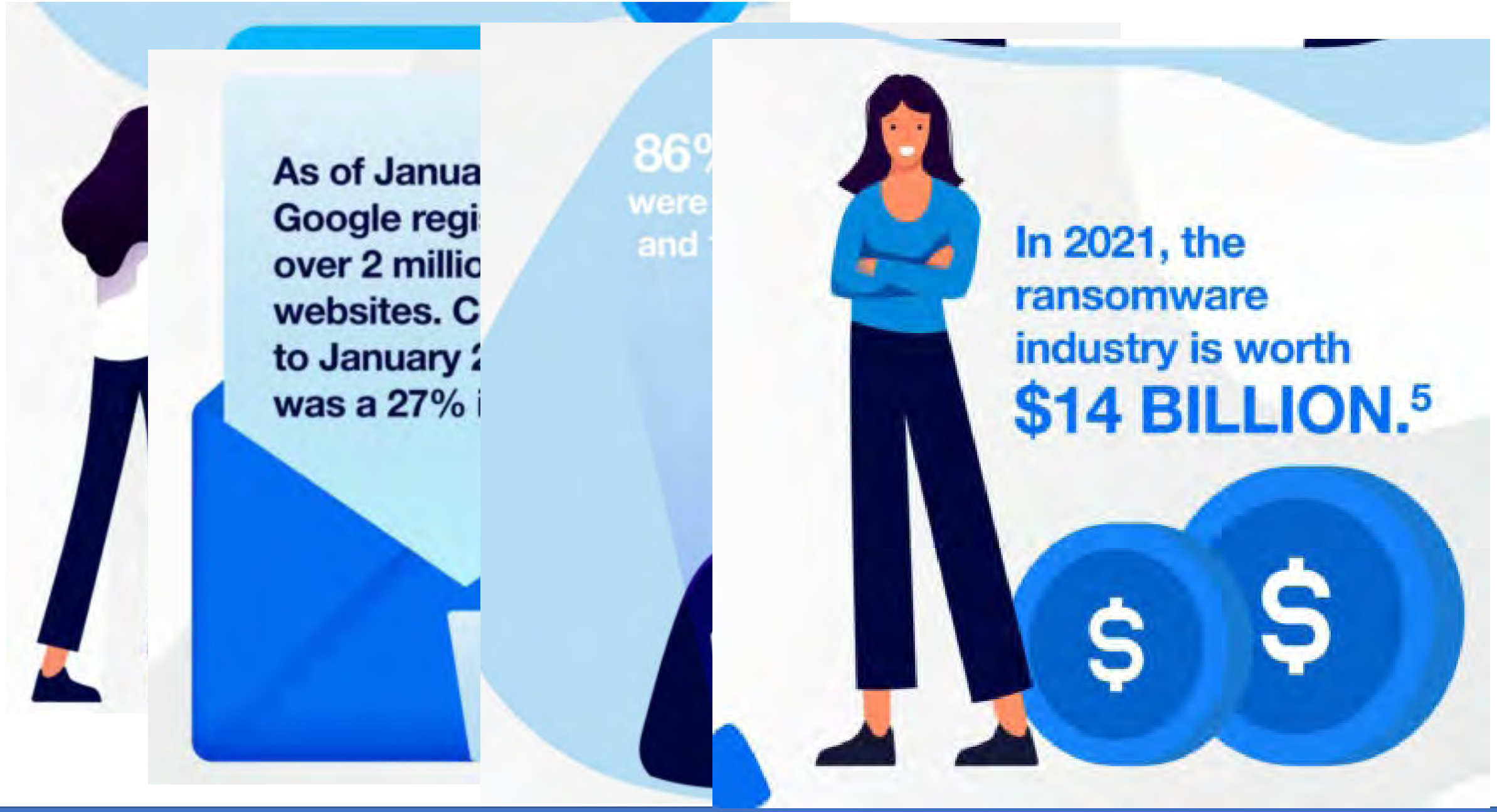
INTERPOL's inaugural Global Crime Trend report leverages data from the organization's 195-country membership to map out current and emerging threats worldwide.


CYBERSECURITY
STATISTICS
IN 2022


95%
of cybersecurity breaches are made possible by human error.²


As of January 2021, Google registered over 2 million phishing websites. Compared to January 2020, this was a 27% increase.[4]


As of Janua
Google regi
over 2 millio
websites. C
to January 2
was a 27% i
In 2020,
86% of breaches
were financially motivated
and 10% were motivated
by espionage.[3]


As of Janua
Google regi
over 2 millio
websites. C
to January 2
was a 27% i
86%
were
and
In 2021, the
ransomware
industry is worth
$14 BILLION.[5]

..attacchi “semplici”..

(non “spie”, CIA, Mission Impossible..)

'Tox' Offers Free build-your-own Ransomware Malware Toolkit - Mozilla Firefox

'Tox' Offers Free build-yo

https://thehackernews.com/2015/05/ransomware-creator.html

120%

'Tox' Offers Free build-your-own Ransomware Malware Toolkit

May 29, 2015 Swati Khandelwal

SHARE

"**Ransomware**" threat is on the rise, but the bad news is that Ransomware campaigns are easier to run, and now a Ransomware kit is being offered by hackers for free for anyone to download and distribute the threat.

Ransomware is a type of computer virus that infects a target computer, encrypts their sensitive documents and files, and locks the out until the victim pays a ransom amount, most often in Bitcoins.

Sometimes even the best security experts aren't able to unlock them and end up paying off ransom to

Popular This Week

NSA: Ransomware Gangs Are Getting Rich Enough to Buy Zero-Day Exploits

NSA Director of Cybersecurity Rob Joyce also doubles down on the agency's findings that sanctions on Russia have made life harder for ransomware hackers.

By Michael Kan June 9, 2022

(Photo by Nicolas Armer/picture alliance via Getty Images)

The US National Security Agency (NSA) is highlighting a disturbing trend of ransomware gangs using their profits to buy zero-day exploits and to fund research into software vulnerabilities they can use to hack more targets.

Perché le PMI?

- Minori difese (e budget)
- Awareness carente (board, utenti, ..)
- Debito tecnologico
  - aziende manufacturing (non IT, non finance, ..)
  - staff IT sottodimensionato
  - scarse/nessuna competenza specifica cybersecurity
  - dipendenza totale da fornitori (spesso “verticali”)

Fondamenta insicure

Fondamenta insicure

- Ethernet (1982)
- TCP/IP (1983, 1987)
- SMTP (1983, 1995)
- DNS (1985)
- FTP (1971)
- HTTP (1991, 1997)

Presidente della Repubblica → me

sei stato nominato senatore a vita

Buongiorno Igor,

volevo comunicarti che ho deciso di nominarti Senatore a Vita.
Quando hai tempo passa da me per un caffé al quirinale, così vediamo come organizzare la cerimonia.

Cordiali saluti,
Presidente della Repubblica

Palazzo del Quirinale, 00187 Roma - Piazza del Quirinale -
Tel. 06.46991; Fax 06.46993125
Ind. internet: www.quirinale.it

Fondamenta insicure

- Ethernet (1982)

- FTP (1971)
- HTTP (1991, 1997)

Principali minacce

Top Cybersecurity Threats in 2022

Ransomware

This form of cyberattack has been around for decades, and hackers continue to evolve their delivery methods.

Supply Chain Attacks

Hackers use this infiltration method to access source codes, build codes, and other infrastructure components of benign software apps.

Cloud-Based Threats

With so many businesses using the cloud and cloud networks becoming more intricate, their infrastructure has become "low-hanging fruit" for digital threat actors.

Social Engineering

Essentially, any hacking technique that plays on a user's human nature or emotion can fall under the umbrella of social engineering.

Insider Threats

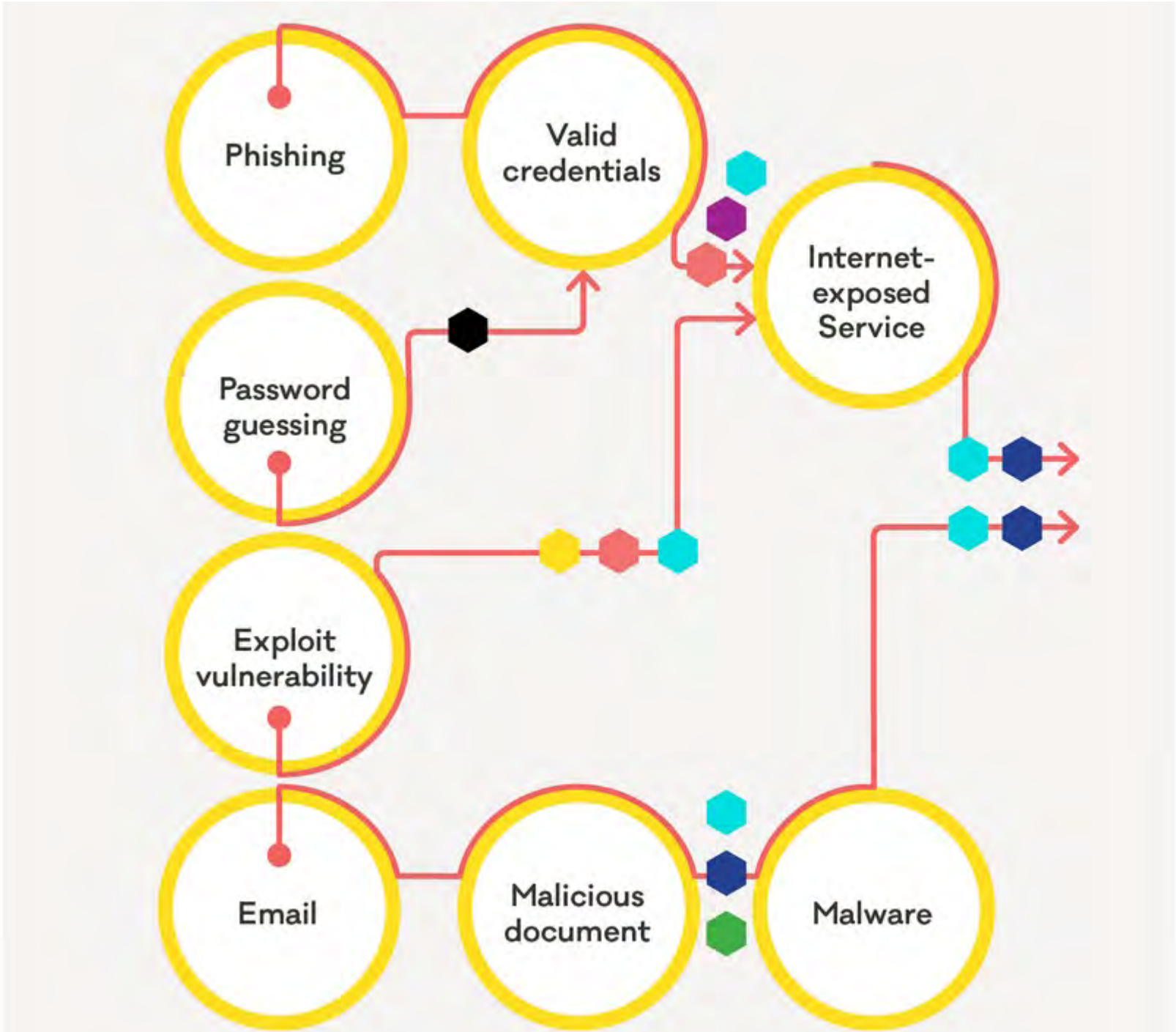
Once internal system users are compromised, they can become an even greater threat to the system than external attackers.

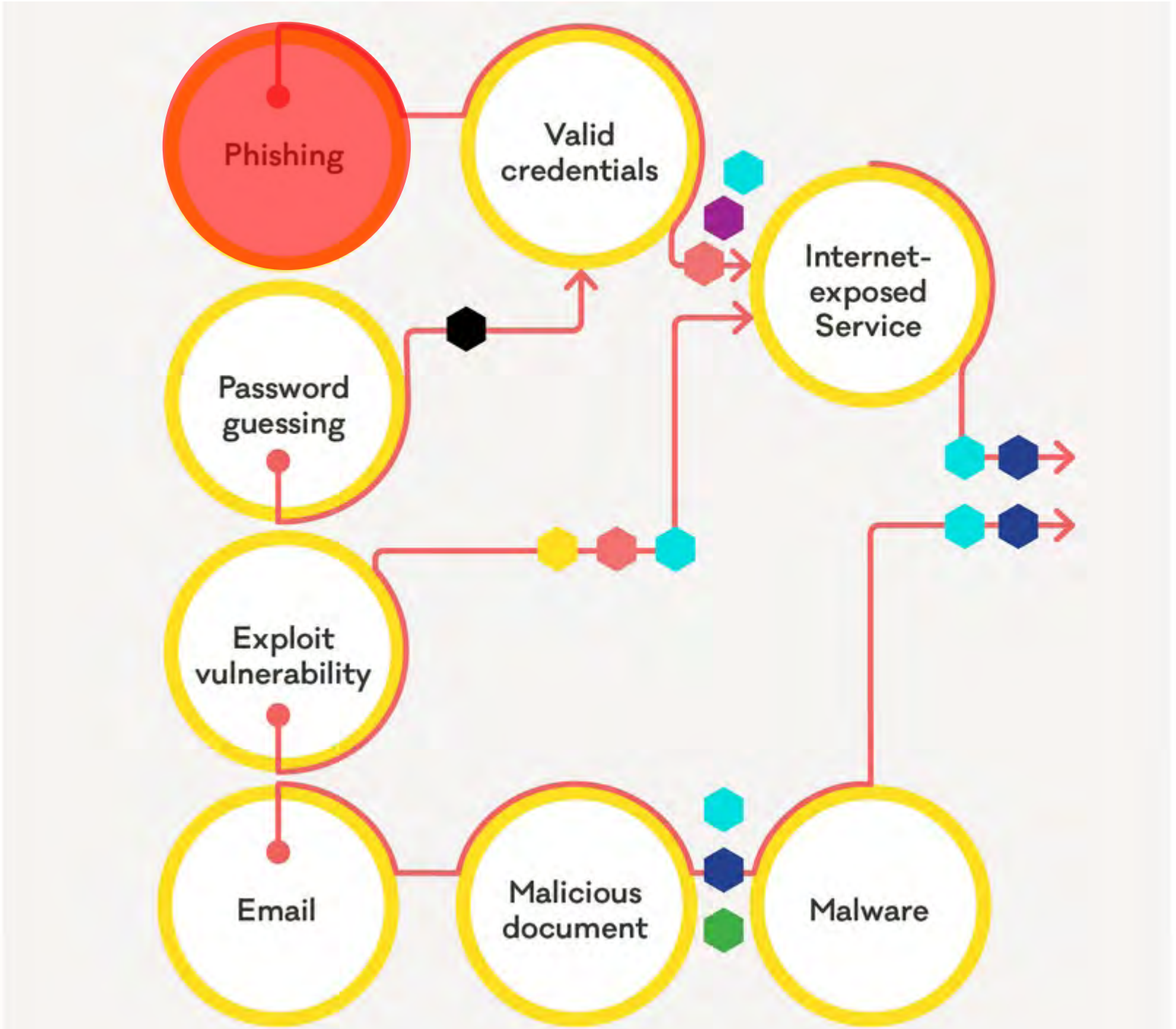
Mobile Devices

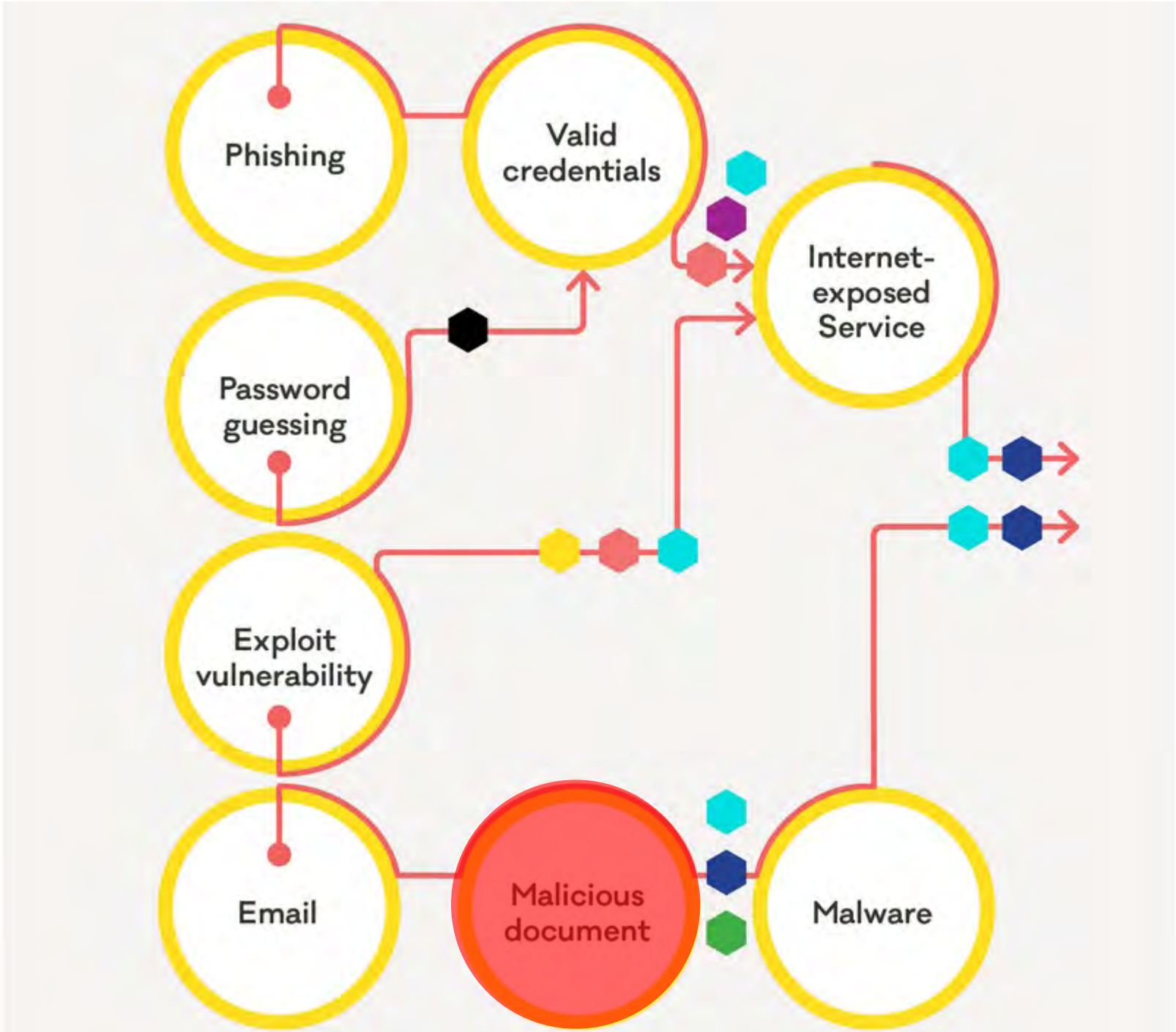
Since employees are now working from home and accessing sensitive company platforms and data from multiple scattered endpoints, hackers are presented with many more infiltration opportunities than ever before.

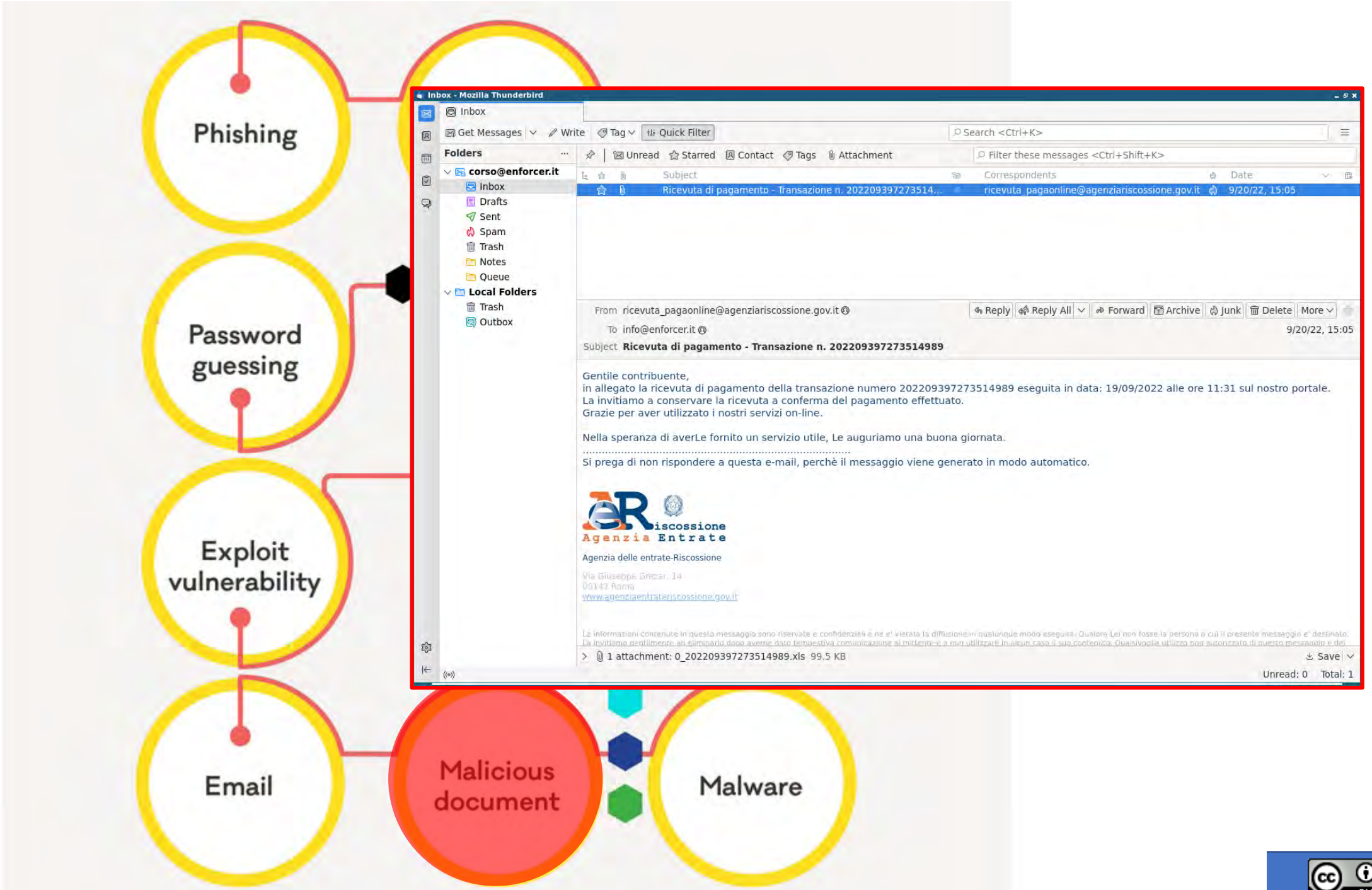
Poor Post-Attack Practices

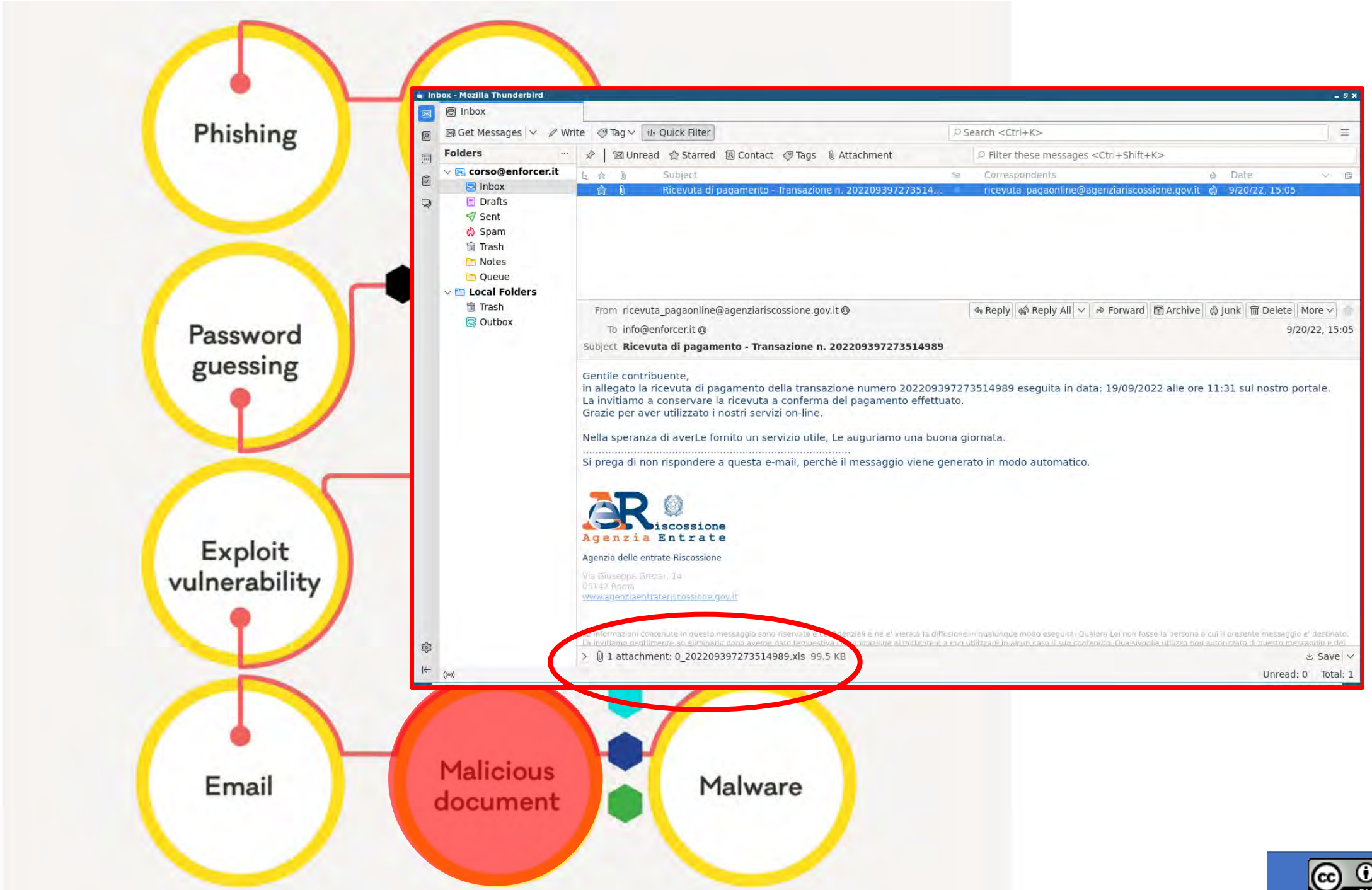
Collecting the right data and following the right post-attack procedure can help you extract the most intel from each attack.

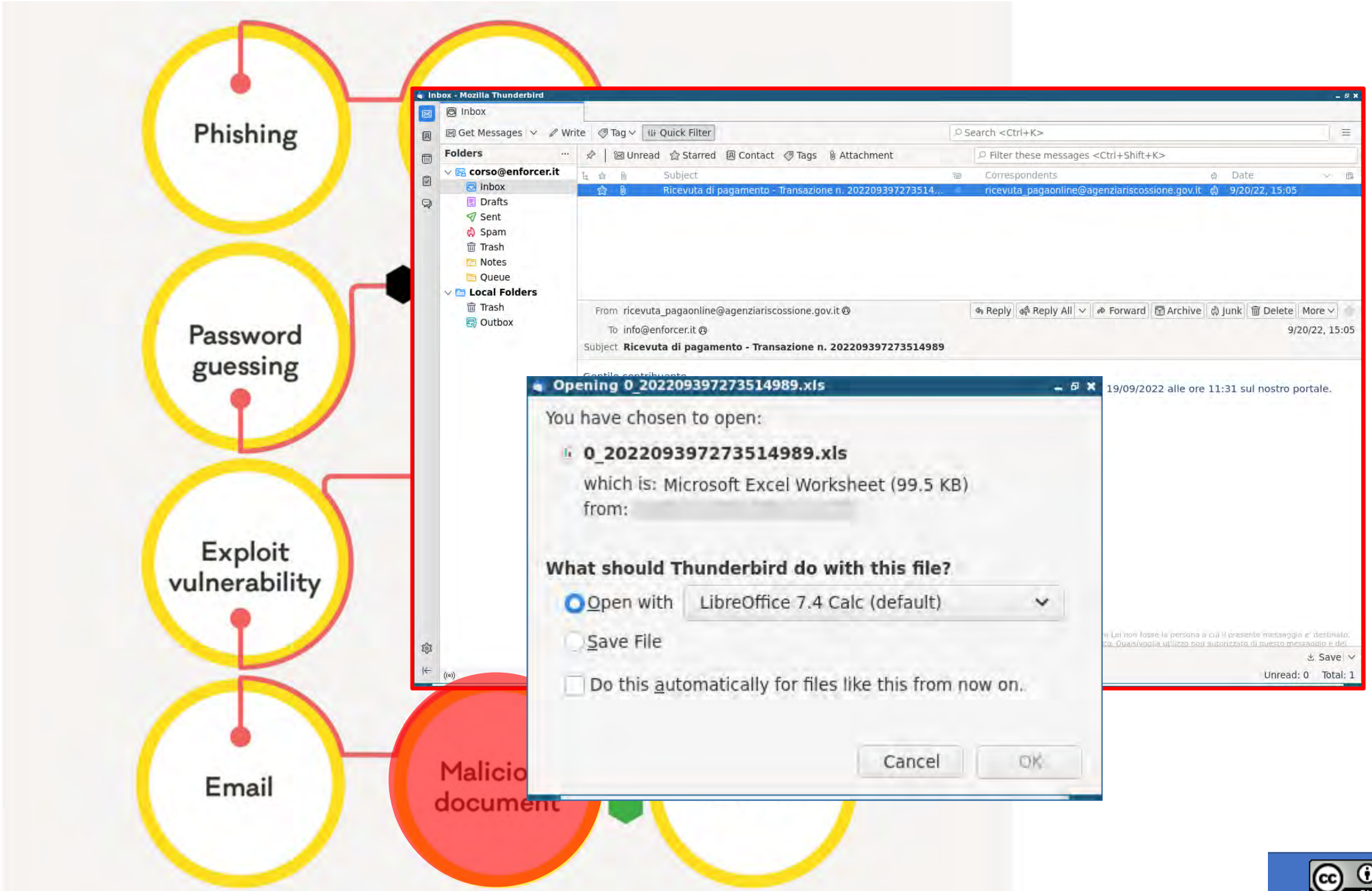

Phishing
Valid credentials
Internet-exposed Service
Password guessing
Exploit vulnerability
Email
Malicious document
Malware

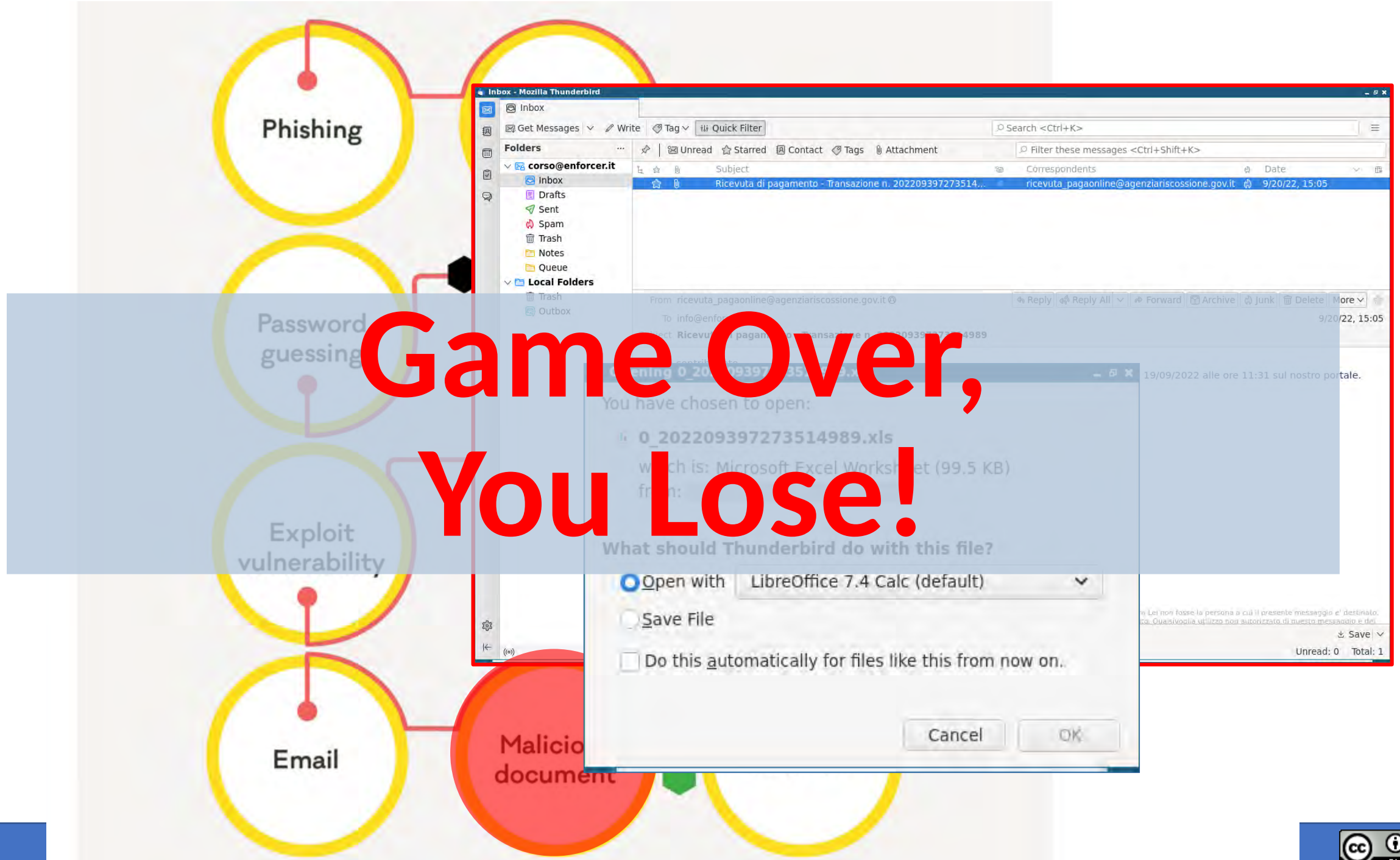

Phishing
Valid credentials
Internet-exposed Service
Password guessing
Exploit vulnerability
Email
Malicious document
Malware


Phishing
Valid credentials
Internet-exposed Service
Password guessing
Exploit vulnerability
Email
Malicious document
Malware


Phishing
Password guessing
Exploit vulnerability
Email
Malicious document
Malware
Inbox - Mozilla Thunderbird
Inbox
Get Messages
Write
Tag
Quick Filter
Search <Ctrl+K>
Folders
corso@enforcer.it
Inbox
Drafts
Sent
Spam
Trash
Notes
Queue
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
Ricevuta di pagamento - Transazione n. 202209397273514..
ricevuta_pagaonline@agenziariscossione.gov.it
9/20/22, 15:05
From ricevuta_pagaonline@agenziariscossione.gov.it
Reply
Reply All
Forward
Archive
Junk
Delete
More
To info@enforcer.it
9/20/22, 15:05
Subject Ricevuta di pagamento - Transazione n. 202209397273514989
Gentile contribuente,
in allegato la ricevuta di pagamento della transazione numero 202209397273514989 eseguita in data: 19/09/2022 alle ore 11:31 sul nostro portale.
La invitiamo a conservare la ricevuta a conferma del pagamento effettuato.
Grazie per aver utilizzato i nostri servizi on-line.
Nella speranza di averLe fornito un servizio utile, Le auguriamo una buona giornata.
Si prega di non rispondere a questa e-mail, perchè il messaggio viene generato in modo automatico.
Agenzia delle entrate-Riscossione
1 attachment: 0_202209397273514989.xls 99.5 KB
Save
Unread: 0
Total: 1


Phishing
Password guessing
Exploit vulnerability
Email
Malicious document
Malware
Inbox - Mozilla Thunderbird
Inbox
Get Messages
Write
Tag
Quick Filter
Search <Ctrl+K>
Folders
corso@enforcer.it
Inbox
Drafts
Sent
Spam
Trash
Notes
Queue
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
Ricevuta di pagamento - Transazione n. 202209397273514..
ricevuta_pagaonline@agenziariscossione.gov.it
9/20/22, 15:05
From ricevuta_pagaonline@agenziariscossione.gov.it
Reply
Reply All
Forward
Archive
Junk
Delete
More
To info@enforcer.it
9/20/22, 15:05
Subject Ricevuta di pagamento - Transazione n. 202209397273514989
Gentile contribuente,
in allegato la ricevuta di pagamento della transazione numero 202209397273514989 eseguita in data: 19/09/2022 alle ore 11:31 sul nostro portale.
La invitiamo a conservare la ricevuta a conferma del pagamento effettuato.
Grazie per aver utilizzato i nostri servizi on-line.
Nella speranza di averLe fornito un servizio utile, Le auguriamo una buona giornata.
Si prega di non rispondere a questa e-mail, perchè il messaggio viene generato in modo automatico.
Agenzia delle entrate-Riscossione
1 attachment: 0_202209397273514989.xls 99.5 KB
Save
Unread: 0
Total: 1


Phishing
Password guessing
Exploit vulnerability
Email
Malicio
document
Inbox - Mozilla Thunderbird
Inbox
Get Messages
Write
Tag
Quick Filter
Search <Ctrl+K>
Folders
corso@enforcer.it
Inbox
Drafts
Sent
Spam
Trash
Notes
Queue
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
Ricevuta di pagamento - Transazione n. 202209397273514..
ricevuta_pagaonline@agenziariscossione.gov.it
9/20/22, 15:05
From ricevuta_pagaonline@agenziariscossione.gov.it
Reply
Reply All
Forward
Archive
Junk
Delete
More
To info@enforcer.it
9/20/22, 15:05
Subject Ricevuta di pagamento - Transazione n. 202209397273514989
19/09/2022 alle ore 11:31 sul nostro portale.
Save
Unread: 0
Total: 1
Opening 0_202209397273514989.xls
You have chosen to open:
0_202209397273514989.xls
which is: Microsoft Excel Worksheet (99.5 KB)
from:
What should Thunderbird do with this file?
Open with
LibreOffice 7.4 Calc (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK


Phishing
Password guessing
Exploit vulnerability
Email
Malicio document
Inbox - Mozilla Thunderbird
Inbox
Get Messages
Write
Tag
Quick Filter
Search <Ctrl+K>
Folders
corso@enforcer.it
Inbox
Drafts
Sent
Spam
Trash
Notes
Queue
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
Ricevuta di pagamento - Transazione n. 202209397273514..
ricevuta_pagaonline@agenziariscossione.gov.it
9/20/22, 15:05
From ricevuta_pagaonline@agenziariscossione.gov.it
Reply
Reply All
Forward
Archive
Junk
Delete
More
9/20/22, 15:05
19/09/2022 alle ore 11:31 sul nostro portale.
You have chosen to open:
0_202209397273514989.xls
What should Thunderbird do with this file?
Open with
LibreOffice 7.4 Calc (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK
Save
Unread: 0
Total: 1
Game Over,
You Lose!

Human-operated ransomware | Microsoft Docs — Mozilla Firefox

Human-operated ranson ×

https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

Filter by title

- Microsoft Security Best Practices
- Introduction
- Governance, risk, and compliance
- Security operations
- Identity and access management
- Network security & containment
- Privileged administration
- Ransomware and extortion
  - Human operated ransomware
  - Rapidly protect against ransomware and extortion
  - Backup and restore plan for ransomware
- Information protection and storage
- Applications and services

Download PDF

Human-operated ransomware

10/15/2021 • 2 minutes to read •

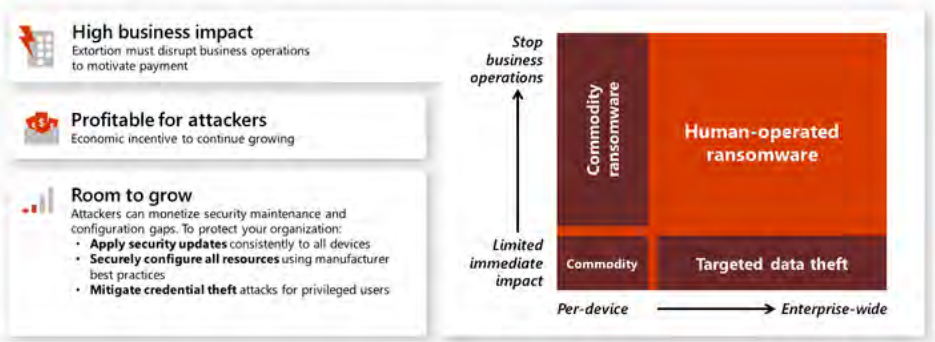
Human-operated ransomware is a large and growing attack trend that represents a threat to organizations in every industry.

Human-operated ransomware is different than commodity ransomware. These "hands-on-keyboard" attacks target an organization rather than a single device and leverage human attackers' knowledge of common system and security misconfigurations to infiltrate the organization, navigate the enterprise network, and adapt to the environment and its weaknesses as they go.

Hallmarks of these human-operated ransomware attacks typically include credential theft and lateral movement and can result in deployment of a ransomware payload to high business impact resources the attackers choose.

These attacks can be catastrophic to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike commodity ransomware that only requires malware remediation, human-operated ransomware will continue to threaten your business operations after the initial encounter.

This figure shows how this extortion-based attack that uses maintenance and security configuration gaps and privileged access is growing in impact and likelihood.



Protect your organization against ransomware and extortion

Is this page helpful?

Yes No

In this article

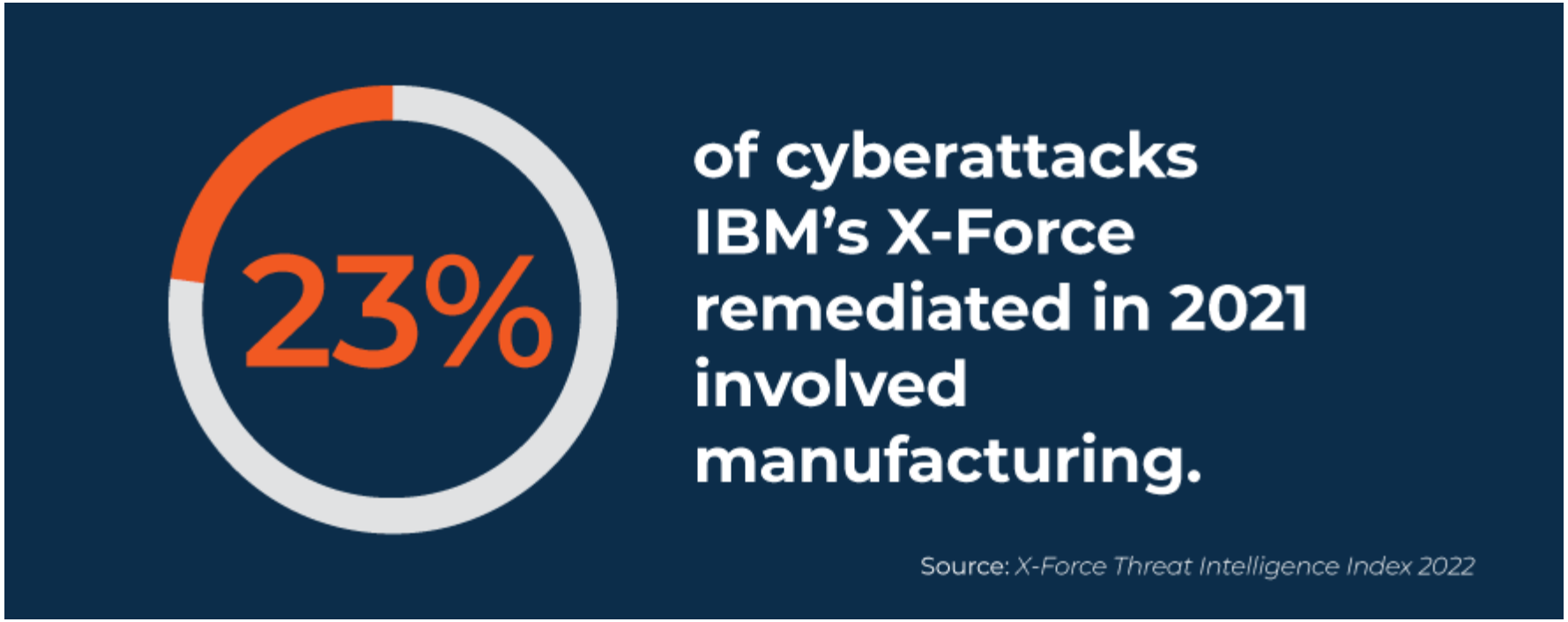
- Protect your organization against ransomware and extortion
- Additional ransomware resources

ANDY GREENBERG SECURITY 02.03.2020 04:56 PM

Mysterious New Ransomware Targets Industrial Control Systems

EKANS appears to be the work of cybercriminals, rather than nation-state hackers—a worrying development, if so.

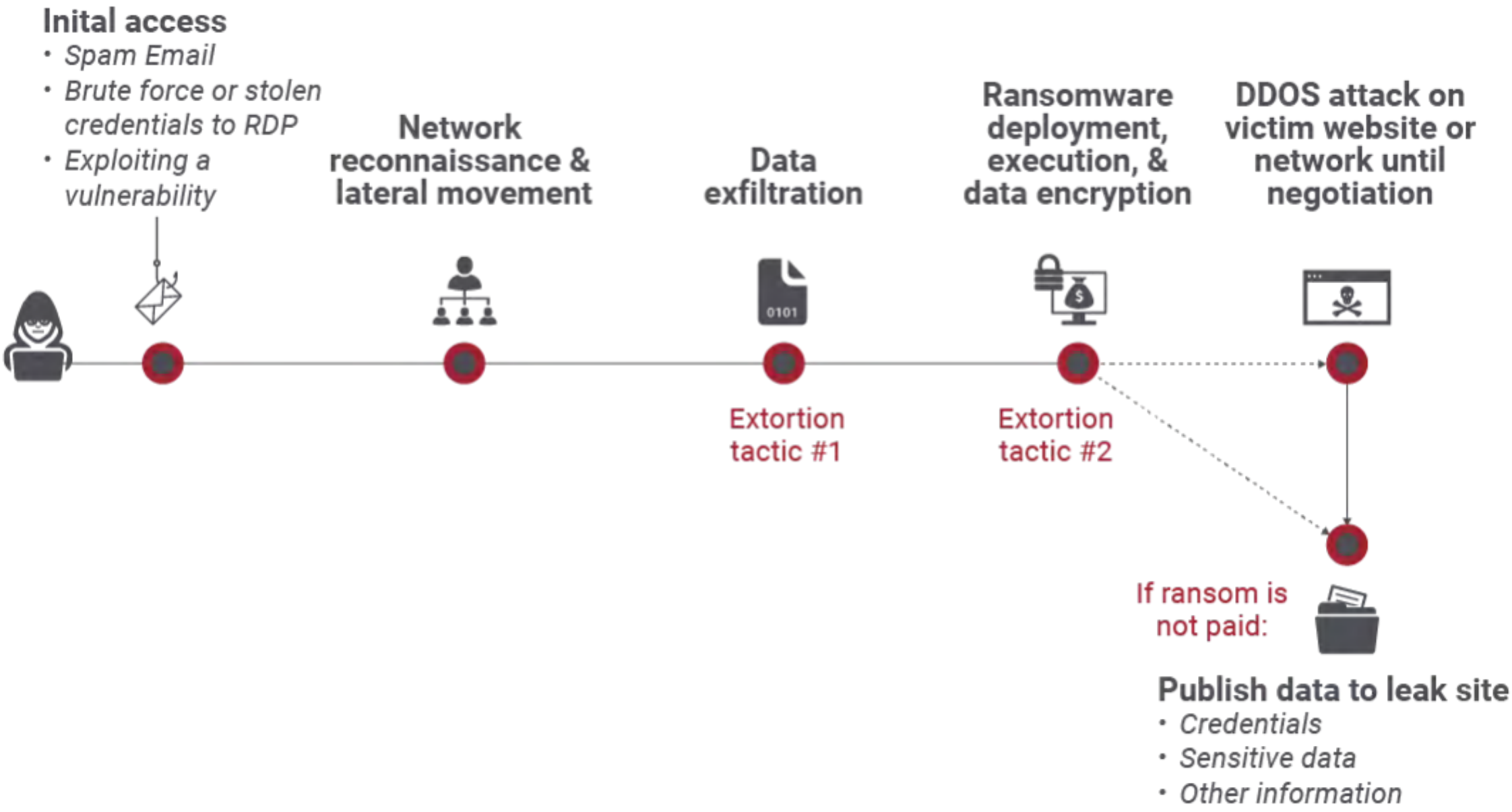
PHOTOGRAPH: GETTY IMAGES


23%
of cyberattacks IBM's X-Force remediated in 2021 involved manufacturing.
Source: X-Force Threat Intelligence Index 2022


61%
of incidents at operational technology (OT)-connected organizations in 2021 were in manufacturing.

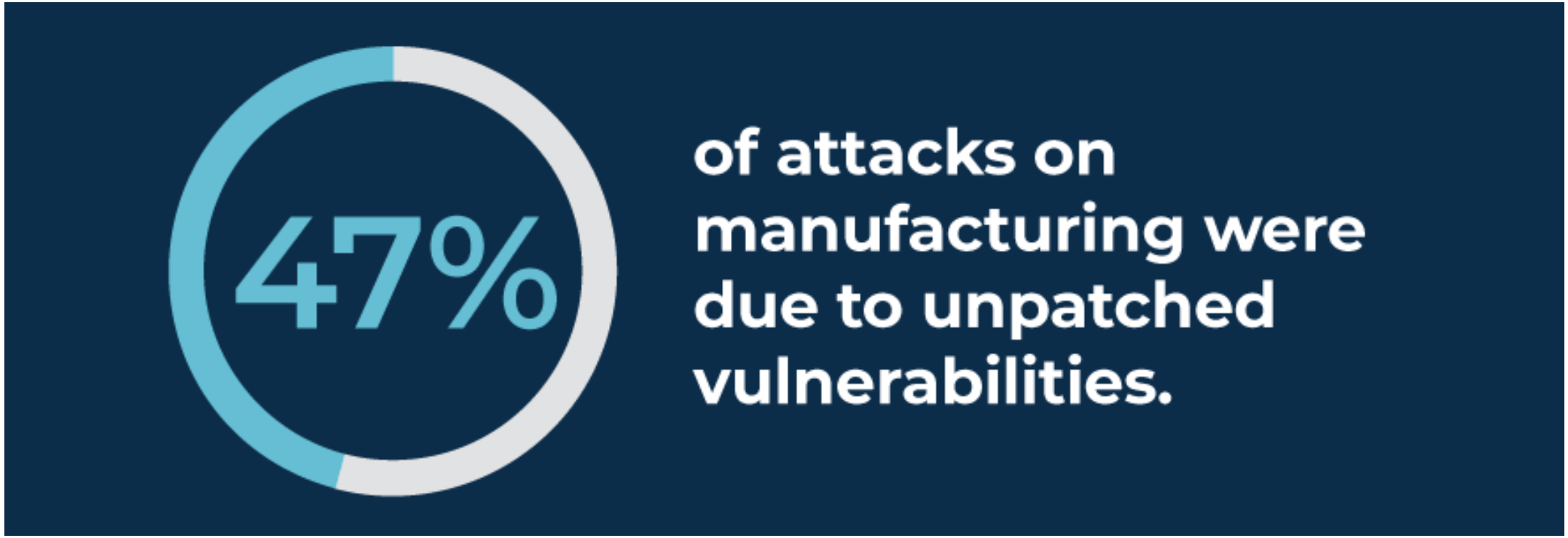

36%
of attacks on
OT-connected
organizations were
ransomware incidents.

#ransomware #double-extortion



75% of cyber attacks committed in 2020 exploited vulnerabilities that had been **discovered at least two years prior** but went unaddressed.

Source: Check Point Software, Cyber Security Report 2021


47%
of attacks on manufacturing were due to unpatched vulnerabilities.

Major Data Breaches

September 2022 Timeline

A data breach is a cybersecurity incident in which an unauthorized party steals or exposes protected information. This visual highlights the major data breaches of September 2022.

September 20: American Airlines

The airline has notified that attackers compromised an undisclosed number of email accounts in July, the company secured the impacted accounts, hired a cybersecurity forensic firm to investigate, and offered affected customers free 2-year membership of Experian's IdentityWorks.

September 19: Kiwi Farms

Kiwi Farms – a forum accused of harassment campaigns targeting trans and non-binary people – confirmed to all its users that their passwords, emails, and device IPs may have been compromised due to someone hacking its proxy service and website. Each node on the forum was deleted.

September 19: Revolut

Revolut confirmed an unauthorized party obtained access to the personal data of 0.16% of their users (tens of thousands of customers), the company discovered the malicious access on September 10 and isolated the attack

563	11,596,113,394	114,135	207,750,231
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

228,102	Thingiverse accounts
50,538	Playbook accounts
66,479	Fantasy Football Hub accounts
72,596	Republican Party of Texas accounts
125,698,496	LinkedIn Scraped Data accounts
266,399	Ajarn accounts
15,003,961	Epik accounts
20,154,583	IndiaMART accounts
878,209	Imavex accounts
6,137,666	SubaGames accounts

Italian insurance Companies (17 GB Data + 950MB Database) (900 Rows Sample) | RaidForums — Mozilla Firefox

RF Italian insurance Compar ×

https://rfmirror.com/Thread-SELLING-Italian-insurance-Companies-17-GB-Data-950MB-Database-900-Rows-Sample?__cf_c

RaidForums Active Mirror, domain issues.

SELLING Italian insurance Companies (17 GB Data + 950MB Database) (900 Rows Sample)

by injection - October 09, 2021 at 03:18 AM

Pages (2): 1 2 Next »

injection

Injection of work

GOD

Posts	87
Threads	22
Joined	Aug 2020
Reputation	752

1 YEAR OF SERVICE

October 09, 2021 at 03:18 AM This post was last modified: 11 hours ago by injection. Edited 30 times in total. #1

Hi Guys
(0_0)

Telegram ID: @injectionRF

"Due to the negligence of the server owner, all server information is sold. The last data date is today"

900 Rows

Sample of customers

updated

Download :::: >>>

Hidden Content

You must register or login to view this content.

Password: injectionRF

Source:Companies

==========

GENERALI ITALIA
Reale Group
VITTORIA ASSICURAZIONI
Genertel
HELVETIA ASSICURAZIONI

Hackers Targeting Tech Supply Chains Spur Security Startup Boom

A growing number of startups are emerging to tackle one of the industry's hardest problems: cyberattacks on the digital supply chain.

Bloomberg News | Oct 19, 2022

(Bloomberg) -- Cyberattacks on the digital supply chain have become increasingly common, as hackers seek out weak links among makers of computer code and equipment to breach organizations that depend on the technologies.

In 2020, for example, hackers suspected of working for Russia's intelligence services used tampered updates from software maker SolarWinds Corp. to infiltrate nine US government agencies. Last year, hundreds of businesses were compromised with ransomware after the breach of another software provider, Kaseya Ltd. And several months later,

Come difendersi?

"Security is a process non a product"

(Bruce Schneier, 1999)

Cybersecurity non è IT

- Definizione di un piano strategico
- Budget, staff, ruoli (CSO, CISO, ..)
- Assessment dei rischi (sul processo produttivo)
- Definizione di un piano operativo
- Formazione per IT, OT e tech
- Awarness per utenti
- Framework e processi continui
- Assicurazione del rischio residuo

“What Every CEO Needs to Know About Cybersecurity” (2015)

Five questions every CEO should ask about cybersecurity:

1. *Is your board of directors fully engaged in cybersecurity?*
2. *When did you and your board review your last risk assessment?*
3. *What makes you a target for attacks?*
4. *What data is leaving your company and is it secure?*
5. *Have I provided my security organization all the tools and resources they need to help prevent a security breach?*

src https://www.business.att.com/content/dam/attbusiness/reports/decodingtheadversary.pdf

Riferimenti 1/2 (perdonate l'autoreferenzialità..)

- OT Security: sicurezza (informatica) negli impianti industriali
  https://www.youtube.com/watch?v=X-TZLuKuIF4 (video)
  https://www.enforcer.it/dl/MIP-OT-Security_Falcomata_Giu2020.pdf (slide)

- Smartworking & Cybersecurity
  https://www.youtube.com/watch?v=gC0h86Ki0BY (video)
  https://www.enforcer.it/dl/MIP-Smartworking_Falcomata_Mag2020.pdf (slide)

- ESC18T16 IOT utile di sicuro. Ma sicuro?
  https://www.youtube.com/watch?v=FoTrXRgvKj0 (video)
  https://www.enforcer.it/dl/ESC_2k18_IOT-Security.pdf (slide)

- RAI Report "Voglio piangere":
  https://www.rai.it/programmi/report/inchieste/Voglio-piangere-2ceb55e0-37ff-4a7e-966f-8842231defbe.html

- RAI Presadiretta "La guerra informatica"
  https://www.raiplay.it/video/2022/10/La-guerra-informatica---Presa-Diretta---Puntata-del-24102022-8291cbad-b764-42b6-8c2b-950da072bd9d.html

Riferimenti 2/2

- Framework Nazionale per la Cybersecurity e la Data Protection
  https://www.cybersecurityframework.it/
- European Cybersecurity Skills Framework (ECSF)
  https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
- Cybersecurity Awareness Raising: The ENISA -Do-It-Yourself Toolbox
  https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box
- ISO/IEC 27001:2013 (e 27xxx)
  https://www.iso.org/standard/54534.html
- CIS Critical Security Controls
  https://www.sans.org/critical-security-controls
- The OWASP® Foundation:
  https://owasp.org/projects/
- Communication network dependencies for ICS/SCADA Systems (ENISA)
  https://www.enisa.europa.eu/publications/ics-scada-dependencies
- Guide to Industrial Control Systems (ICS) Security (NIST, SP-800-82 r2
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Securing Industrial Control Systems-2017 (SANS Institute)
  https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860