Universitá degli Studi di Milano, Dipartimento di Informatica
Via Celoria 18, 20135 Milano (Italy)
Room 6017 (sixth floor), +39 0250316362
x.com/lab_laser

andrea.monzani@unimi.it, marzio.decorato@unimi.it, matteo.zoia@unimi.it

Area di ricerca

- Binary Analysis/Reverse Engineering
- **Protections mechanisms for embedded systems, IoT and firmware**
- Java language security
- **Sandboxing and windows kernel drivers**
- **Virtualization security**
- Windows authentication protocol UAC
- Android Security
- Support systems to threat intelligence

Attivitá del laboratorio

- **Embedwatch, security on IoT (CISCO University Research Program, PNRR, KCL, UCL)**
- RemOTA, device remote attestation (SERICS, RUB)
- **VS-TEE, a Framework for Virtualizing TEEs in ARM Cloud Contexts**
- New state-dependent fuzzing techniques (EURECOM)
- **Windows sandbox for vulnerable driver behaviors (EURECOM)**
- ECC vulnerabilities on IoT using ML (Security Pattern)
- LLM studies on phishing generation and detection and malware detection with logs
- Android privacy assessment through automatic guided feedback techniques
- **Browser Introspection (TU)**

TU - Technische Universität Wien, Austria
UCL – University College London, UK
KCL – King's College London, UK
RUB - Ruhr University Bochum, Germany
SERICS – Data Governance and Protection (PNRR)
MUSA - Multilayred Urban Sustainability Action (PNRR)
SERICS - Risk management for future cyber-physical ecosystems (EcoCyber) (PNRR)

Partners

Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CYTRIX

REAQTA

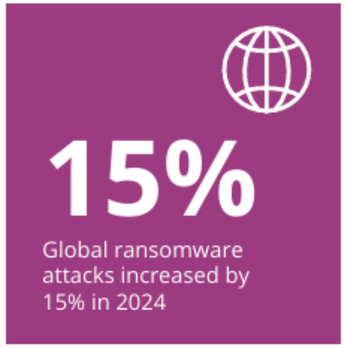
CYBER CHALLENGE.IT

SECURITY PATTERN

Malware vs. EDR: una guerra senza esclusione di colpi

Andrea Monzani | PhD Student @ Unimi

Statistiche su attacchi ransomware



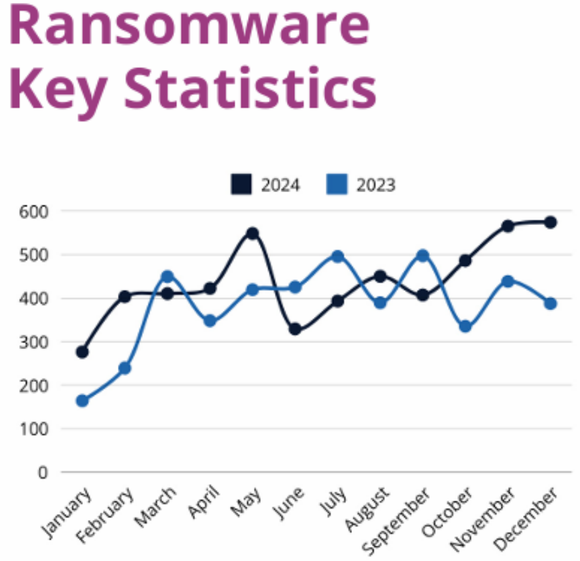


Figure 1 Number of Ransomware Attacks 2023 vs 2024

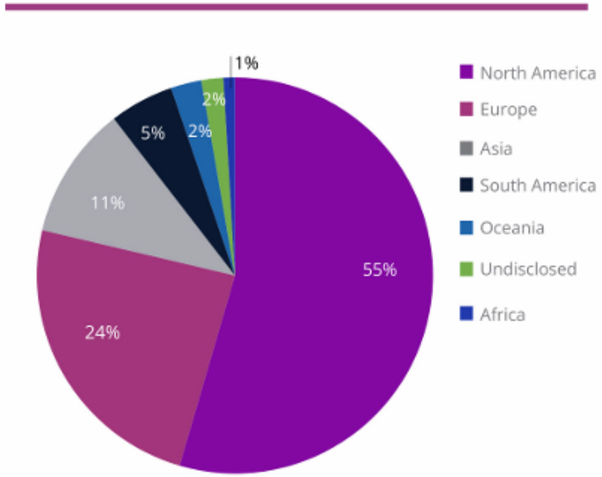
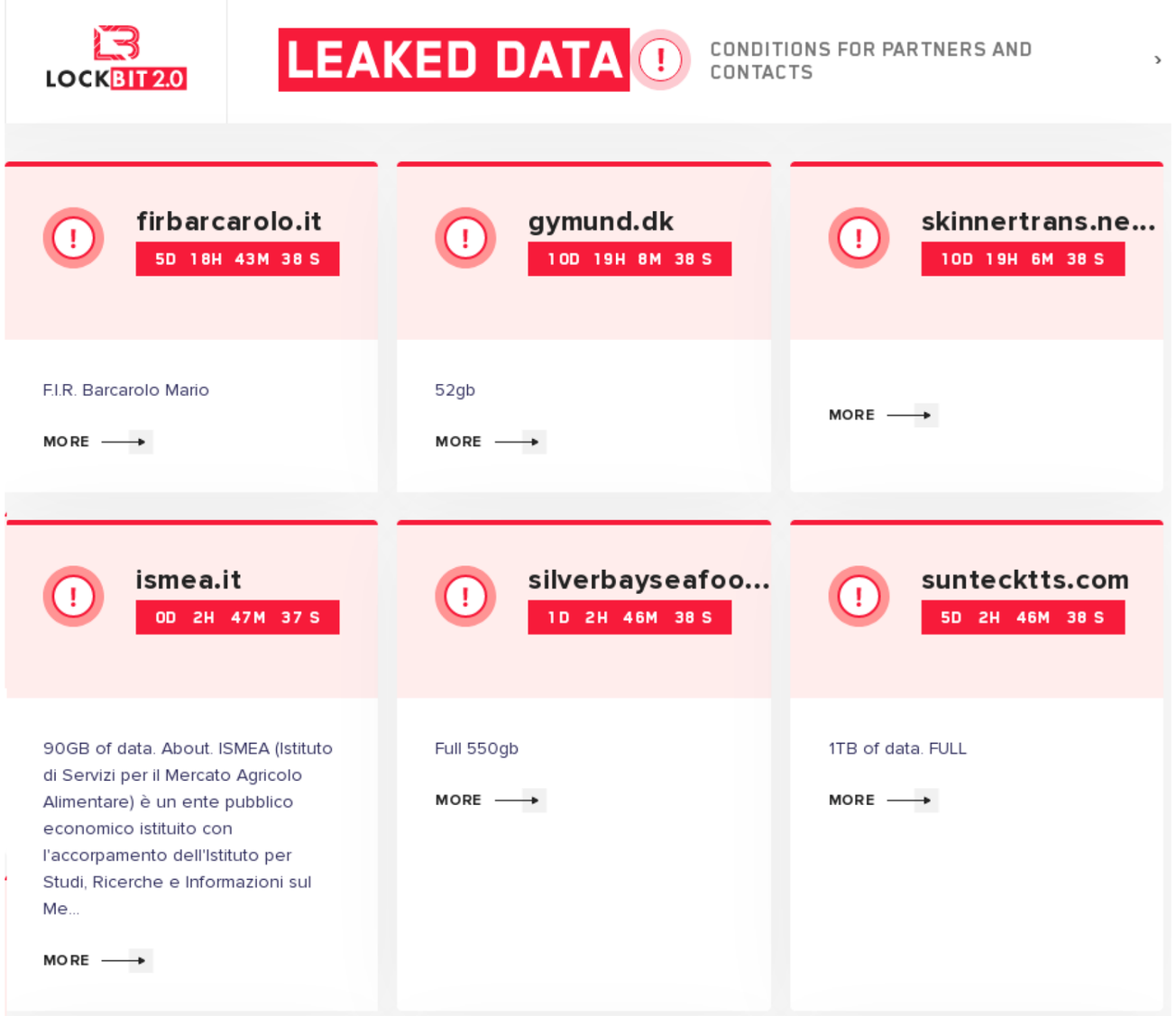


Figure 2 Number of Ransomware Attacks by Region 2024

- Tra gli attacchi più comuni perpetrati a danni di aziende o singoli individui troviamo i ransomware; l' obiettivo è solitamente l' estorsione di denaro
- Gli attaccanti, attraverso un malware, *esfiltrano* tutti i dati presenti sulla macchina compromessa e successivamente ne *cifrano* il contenuto rendendoli illeggibili
- A fronte di un pagamento, gli attaccanti «promettono» di non pubblicare i dati rubati e di fornire una chiave per decifrare i file
- Secondo il Cyber Threat Monitor Report 2024 del nccgroup, 5263 attacchi ransomware sono stati registrati nel 2024, il 15% in più rispetto a quelli del 2023

(Immagine presa dal Cyber Threat Monitor Report 2024, nccgroup)

(Immagine presa da https://www.cynet.com/attack-techniques-hands-on/malware-evolution-analyzing-lockbit-2-0/)



(Immagine adattata da https://unit42.paloaltonetworks.com/lockbit-2-ransomware/)

Come ci difendiamo?

- Antivirus, Endpoint Detection and Response (EDR), eXtended Detection and Response (XDR)
- Diverse aziende producono software di difesa
- Microsoft mette a disposizione la versione base di Defender in tutte le installazioni di Windows

CrowdStrike Achieves 100% Detection, 100% Protection, 100% Accuracy in 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

https://www.crowdstrike.com/en-us/press-releases/crowdstrike-achievement-2024-se-labs-enterprise-advanced-security-edr-ransomware-test/

Microsoft Defender

Come gli attaccanti rispondono?

SentinelOne
https://it.sentinelone.com › resources › sentinelone-vs-te...

SentinelOne VS Terminator EDR Killer (Spyboy)

SentinelOne VS Terminator **EDR Killer** (Spyboy) | Preventing a Windows BYOVD Attack (ZamguardDriver) · Scopri la piattaforma di sicurezza informatica più avanzata ...

Logpoint
https://www.logpoint.com › blog · Traduci questa pagina

EDR Killers: After All, EDRs Are Not Invincible

5 feb 2025 — **EDR** Killers are a growing cybersecurity threat in 2025 - Read our report and find out how Logpoint helps you detect those sinister tools and ...

Broadcom
https://www.broadcom.com › ... · Traduci questa pagina

Protection Highlight: Impairing Defense using AV/EDR Killers

17 dic 2024 — Attackers implant a vulnerable driver into a system, then exploit it to kill or disable security applications in order to execute their ...

Sophos News
https://news.sophos.com › it-it › 2024/08/14 › gli-aggre...

Gli aggressori ransomware introducono un nuovo EDR ...

14 ago 2024 — Gli analisti di Sophos si sono recentemente imbattuti in una nuova utility **EDR-killer** distribuita da un gruppo criminale che stava cercando ...

Cyber Security 360
https://www.cybersecurity360.it › news › soluzioni-edr-...

EDR nel mirino degli attacchi BYOVD

13 gen 2023 — La tecnica BYOVD coinvolge gli hacker usando un driver kernel-mode, noto per essere vulnerabile agli exploit. Oltre che ad attacchi in grado di ...

ExtraHop
https://www.extrahop.com › D... · Traduci questa pagina

Black Market for EDR Killers on the Dark Web

15 ago 2024 — Another **EDR** bypass tool popular with threat actors is 'spyboy's Terminator kit. A 2023 YouTube video produced by CrowdStrike evaluated this tool ...

Trend Micro
https://www.trendmicro.com › h... · Traduci questa pagina

How Ransomhub Ransomware Uses EDRKillShifter to ...

20 set 2024 — Trend Micro tracked this group as Water Bakunawa, behind the RansomHub ransomware, employs various anti-**EDR** techniques to play a high-stakes ...

Sophos News
https://news.sophos.com › it-it › tag › edr-killer

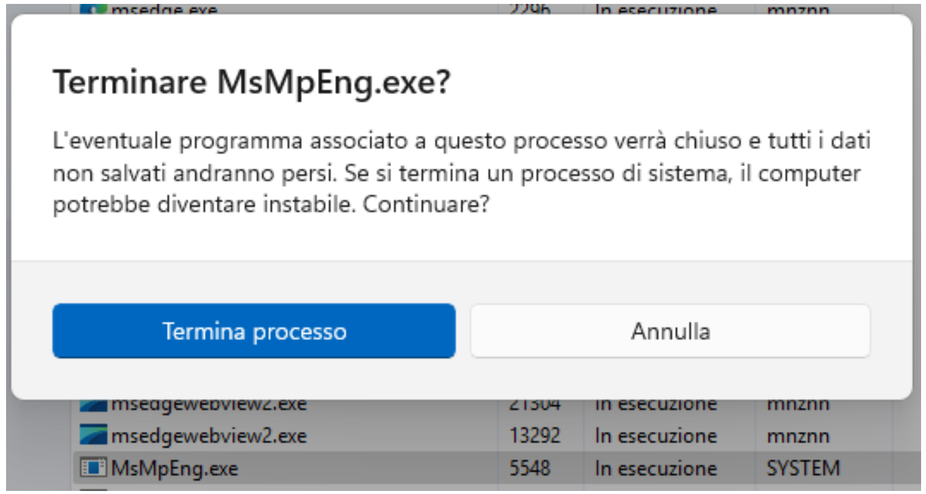
EDR killer

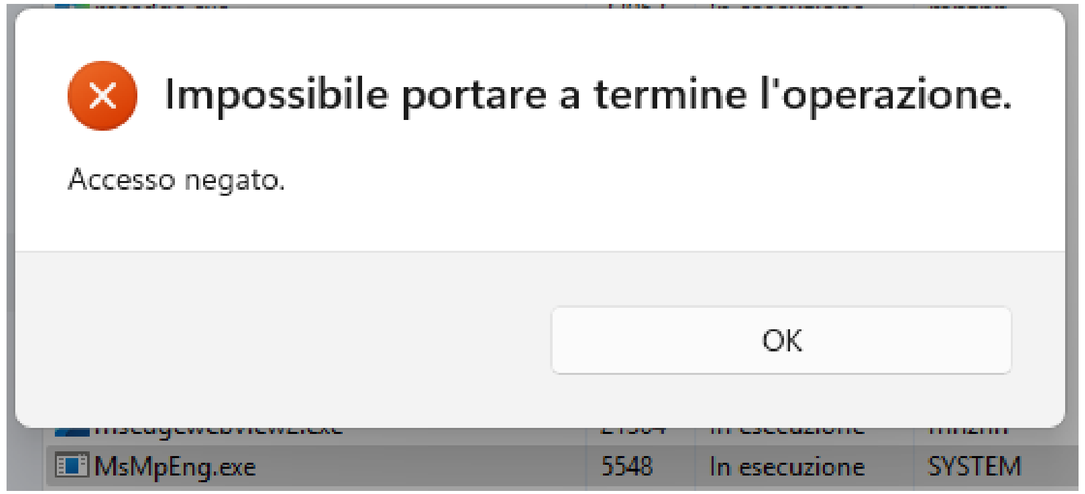
L'aggiornamento di uno strumento di attacco compromette i computer Windows · Gli aggressori ransomware introducono un nuovo **EDR killer** nel loro arsenale.

EDRKiller & BYOVD

- Un antivirus, EDR, XDR o qualsiasi altro software di protezione da malware non è molto diverso da un programma generico: finche è in esecuzione può continuare a proteggere il computer, altrimenti viene meno la sua capacità di rilevare potenziali minacce

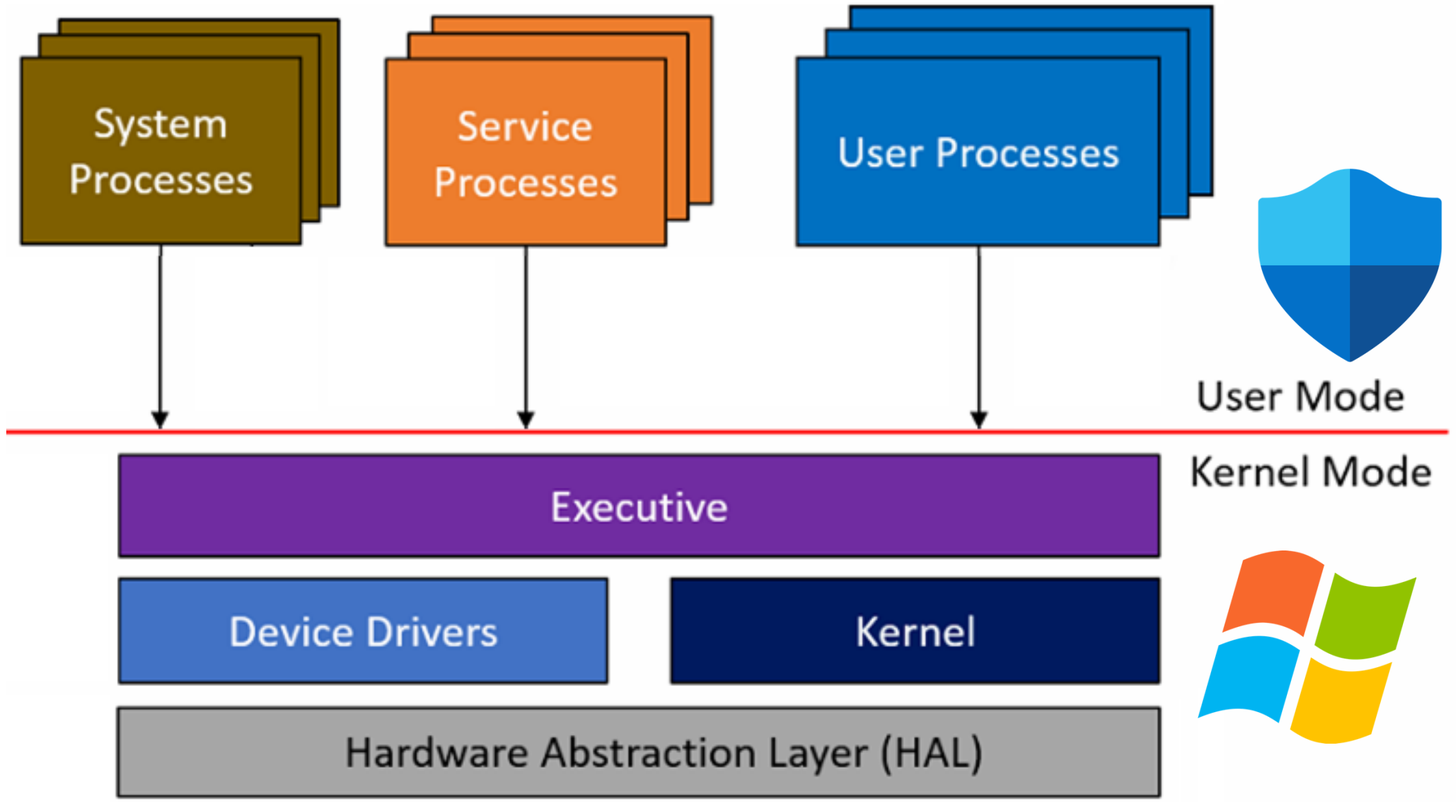
- Windows implementa specifiche protezioni per impedire che gli antivirus possano essere «terminati» da un altro programma una volta avviati





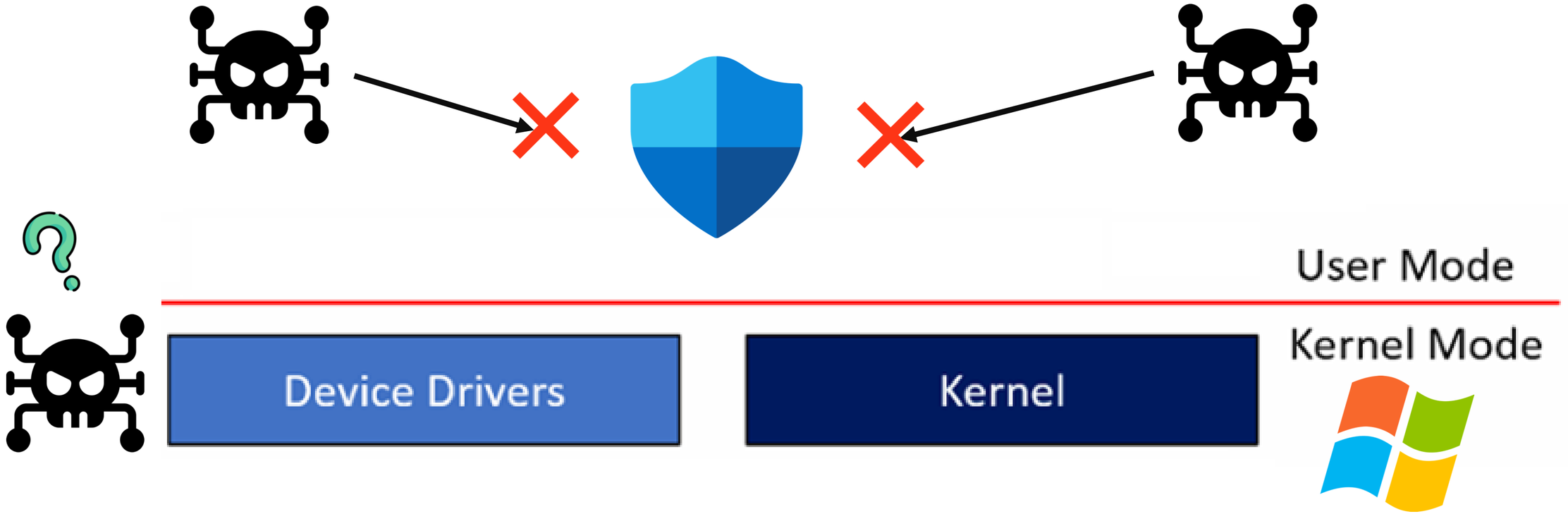
Architettura di Windows

- Due livelli di privilegi: il kernel (il sistema operativo) controlla lo user mode (le applicazioni)
- Il corpo principale di un antivirus fa parte dello user-mode
- Il kernel protegge un antivirus impedendo a componenti dello user-mode di terminarlo



(Immagine adattata da Windows 10 System Programming, Part 1 di Pavel Yosifovich)

Possibilità di attacco



r/crowdstrike • 2 anni fa
Andrew-CS Autore top 1%

2023-05-31 // SITUATIONAL AWARENESS // Spyboy Defense Evasion Tool Advertised Online

Emerging

What happened?

On May 21, 2023, an online persona named *spyboy* began advertising an endpoint defense evasion tool for the Windows operating system via the Russian-language forum Ramp. The author claims that the software — seen in a demonstration video as being titled "Terminator" — can bypass twenty three (23) EDR and AV controls. At time of writing, *spyboy* is pricing the software from $300 USD (single bypass) to $3,000 USD (all-in-one bypass).

Technical Details

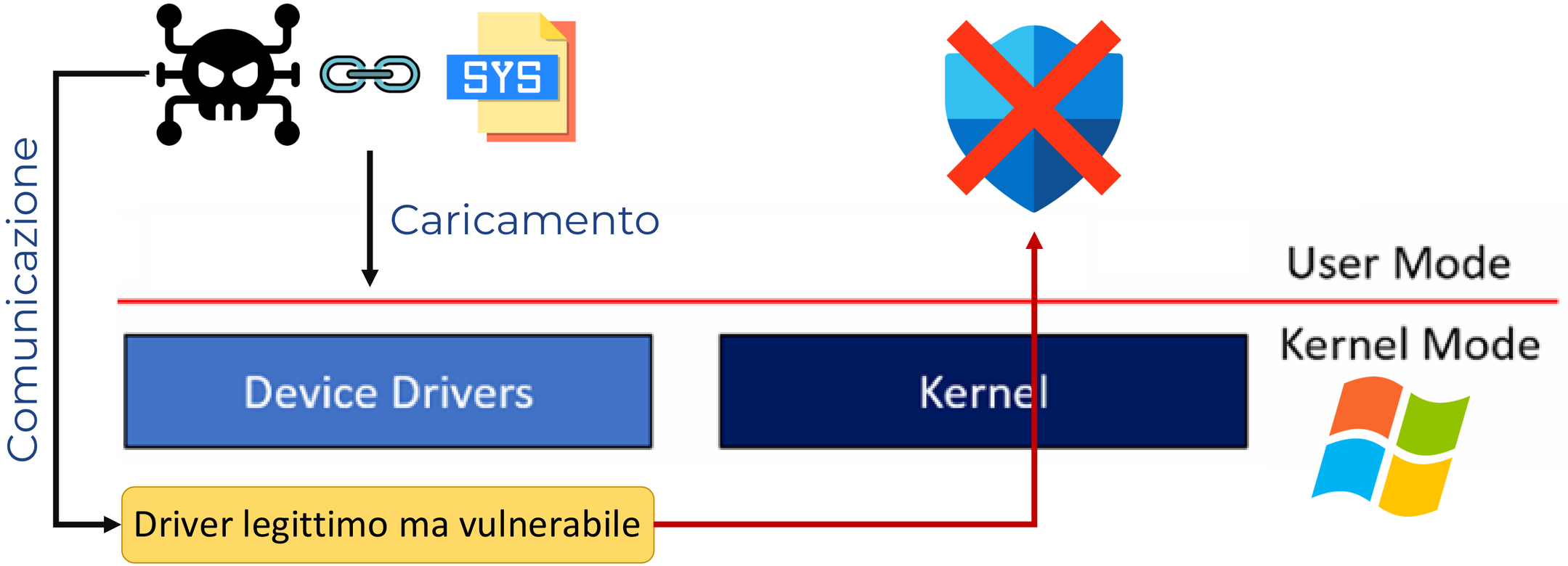
At time of writing, the Terminator software requires administrative privileges and User Account Controls (UAC) acceptance to properly function. Once executed with the proper level of privilege, the binary will write a legitimate, signed driver file — Zemana Anti-Malware — to the `C:\Windows\System32\drivers\` folder. The driver file is given a random name between 4 and 10 characters. An example of this driver file can be found on VirusTotal here.

This technique is similar to other Bring Your Own Driver (BYOD) campaigns observed being used by threat actors over the past several years.

Under normal circumstances, the driver would be named `zamguard64.sys` or `zam64.sys`. The driver is signed by "Zemana Ltd." and has the following thumbprint: `96A7749D856CB49DE32005BCDD8621F38E2B4C05`.

Once written to disk, the software loads the driver and has been observed terminating the user-mode processes of AV and EDR software.

EDR Killer


SYS
Caricamento
Comunicazione
User Mode
Kernel Mode
Device Drivers
Kernel
Driver legittimo ma vulnerabile

Il nostro progetto

- Modificare una sandbox esistente (drakvuf) sviluppando un plugin in grado di rilevare comportamenti considerati pericolosi messi in atto da un certo programma sfruttando uno o più driver caricati nel sistema

- In collaborazione con Antonio Parata (PhD Student @ LaSER) & EURECOM

Il nostro progetto

Host principale

Plugin + software analisi

Drakvuf

Macchina virtuale Windows 10 isolata dal resto del sistema

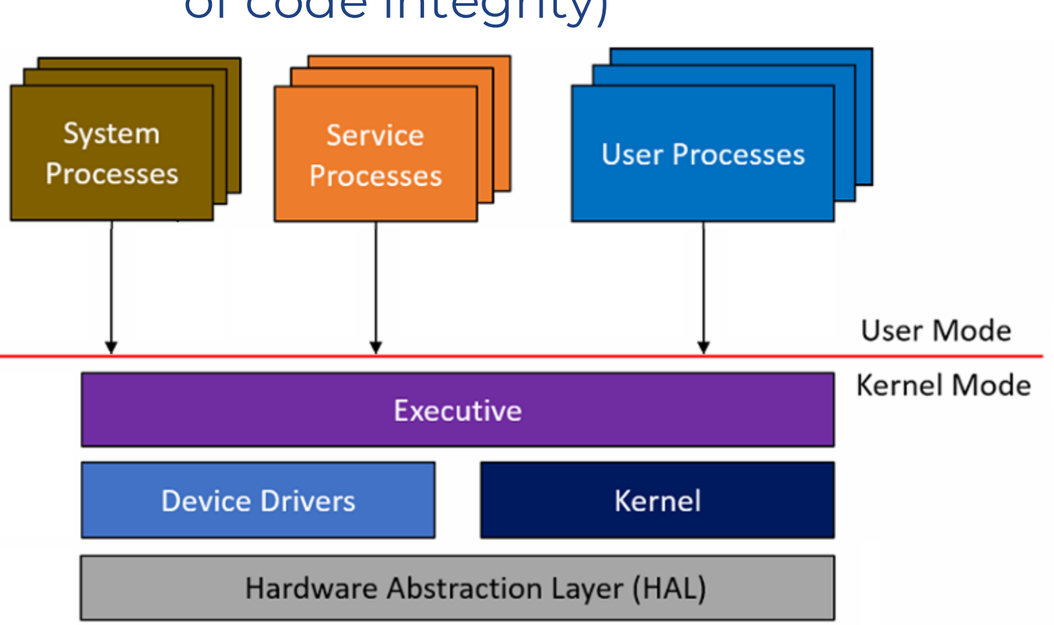
Layer di virtualizzazione (Xen Hypervisor)

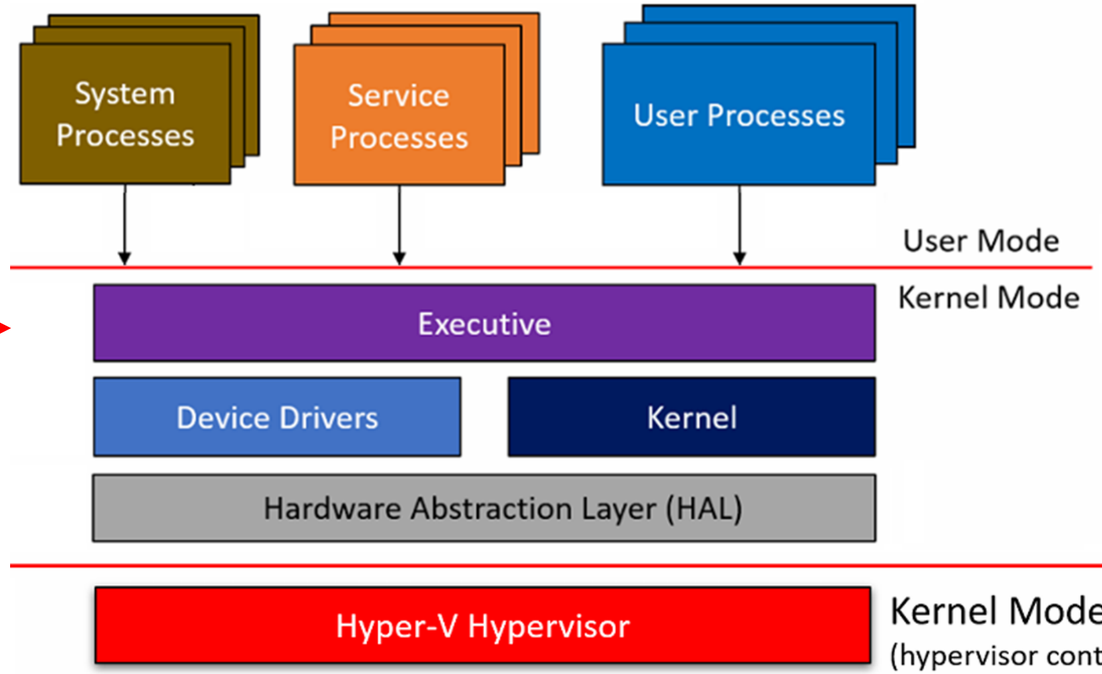
Macchina fisica

Accenno a misure di sicurezza

- Attraverso Windows 11, Microsoft sta tendando di apportare diverse modifiche alle misure di sicurezza in ambiente Windows

- Protezione dell' integrità del codice tramite virtualizzazione (Virtualization-based protection of code integrity)





Accenno a misure di sicurezza

Microsoft vulnerable driver blocklist

With Windows 11 2022 update, the vulnerable driver blocklist is enabled by default for all devices, and can be turned on or off via the Windows Security app. Except on Windows Server 2016, the vulnerable driver blocklist is also enforced when either memory integrity (also known as hypervisor-protected code integrity or HVCI), Smart App Control, or S mode is active. Users can opt in to HVCI using the Windows Security app, and HVCI is on by-default for most new Windows 11 devices.

Living Off The Land Drivers

Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

Analisi sullo stato della cybersecurity negli enti pubblici

Marzio De Corato | Fellow researcher @ Unimi
Matteo Zoia | PhD Student @ Unimi

Scopo del progetto

- Tra gli scopi del progetto MUSA spoke 4 vi è quello di valutare lo **stato della transizione digitale della pubblica amministrazione italiana.**

- Valutazione del livello di maturità delle amministrazioni locali rispetto a tre tematiche emergenti nel mondo digitale: **la cybersecurity, l'adozione di tecniche di Intelligenza Artificiale e il ricorso ai Big data/tecniche di Data Analysis.**

- Perché iniziare con la **Cybersecurity ? E' il fattore abilitante per lo sviluppo di una qualunque strategia di digitalizzazione** che un ente volesse mettere in atto.

Come valutare la cybersecurity ?

- Non ci siamo basati sulle percentuali di enti che hanno o meno adottato particolare tecnologie o metodologie

- Abbiamo cercato di capire quale fosse **il livello culturale sul tema della cybersecurity** presente nei nostri enti locali ed **il loro livello di preparazione** per affrontare sfide imminenti come quella del passaggio al cloud.

- Abbiamo scelto **i comuni perché sono una delle componenti più importanti della Pubblica Amministrazione**, nonché quella più capillare e che maggiormente si interfaccia con i cittadini.

- Il collaboratore naturale era **ANCI/ANCILAB**

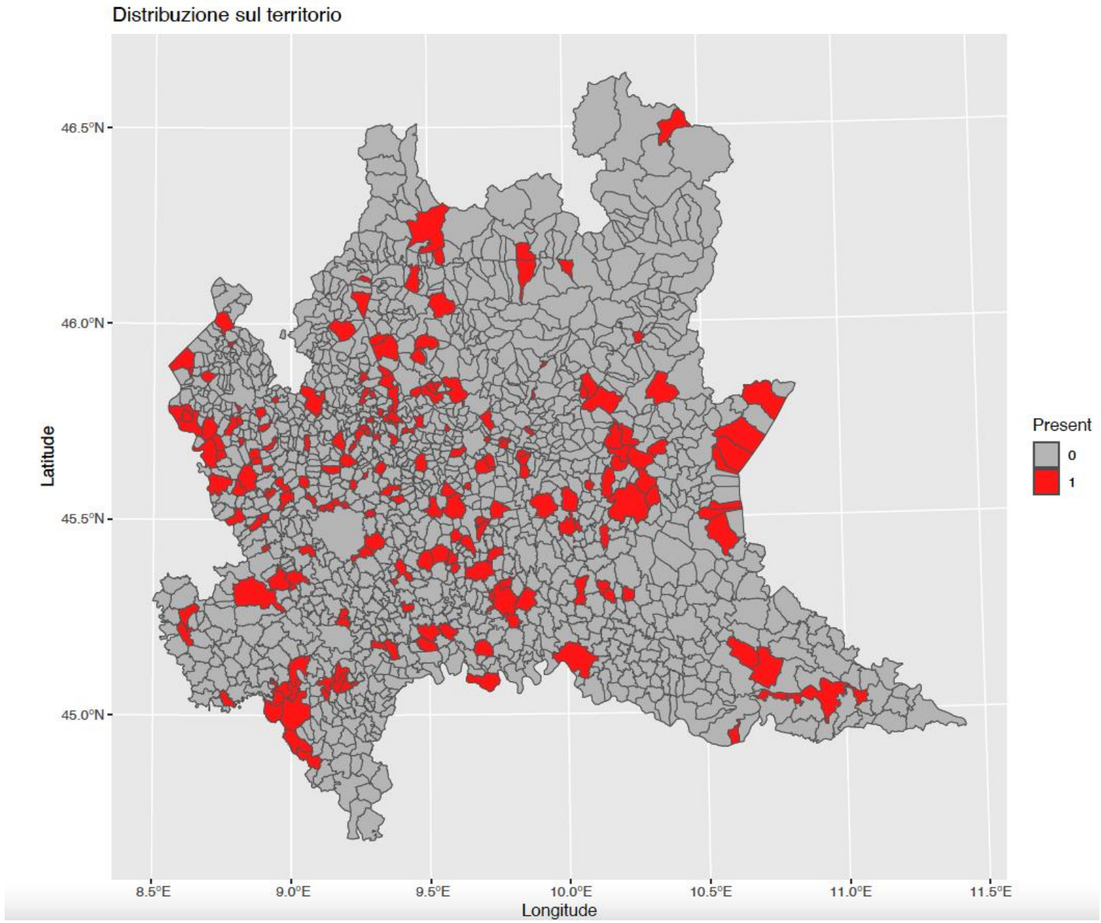
Come valutare la cybersecurity ?

- Componente soggettiva: preparazione e consapevolezza del personale dei comuni (tecnico IT/amministrativo/politico → **focus groups e sondaggio on-line**)
- Componente oggettiva: **vulnerability assessment** (black-box) e **campagna di phishing**

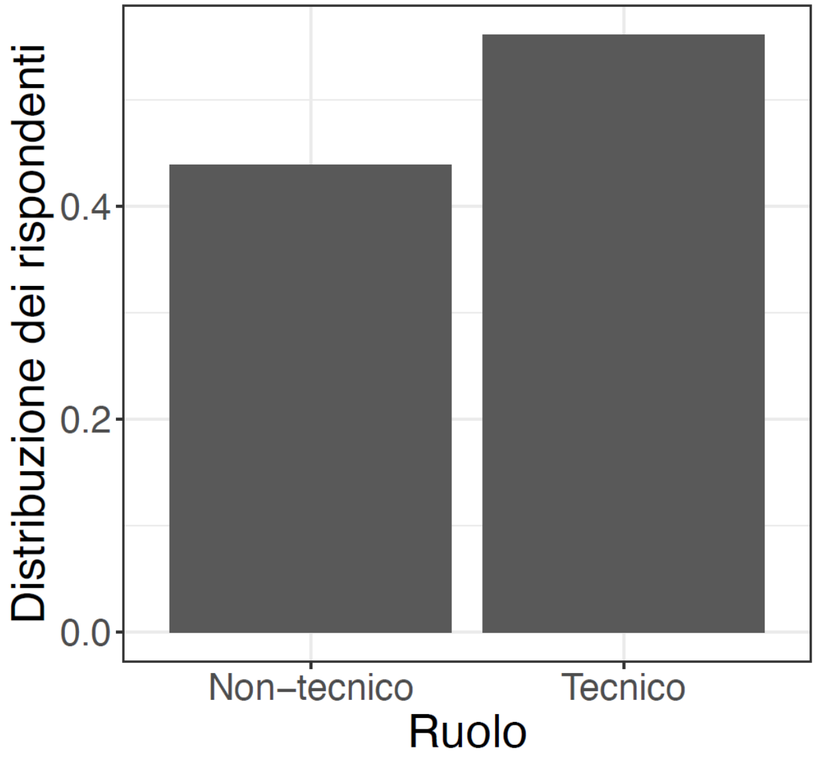
Componente soggettiva

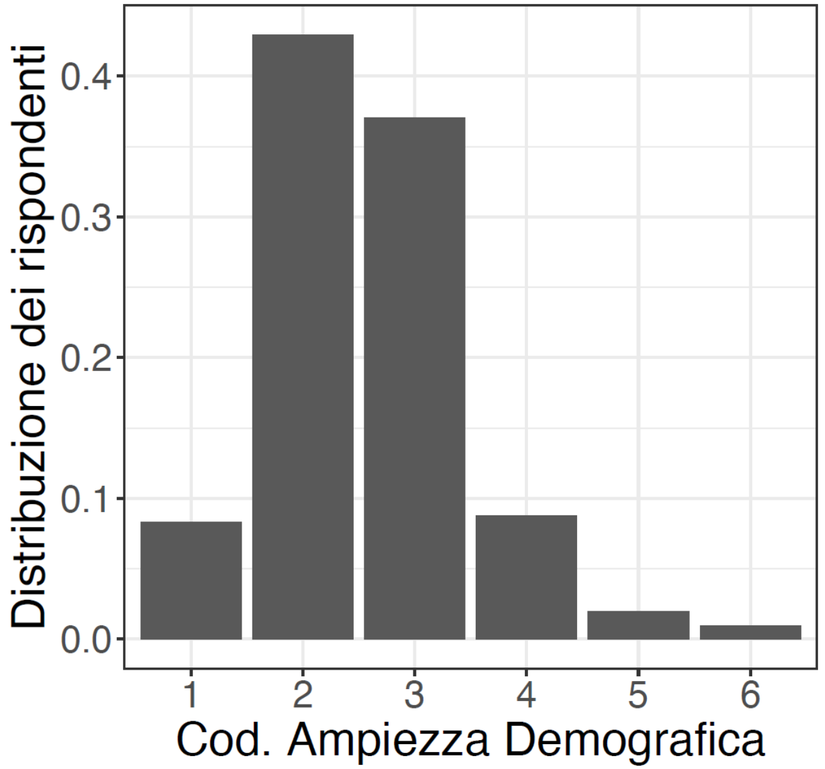
- Personale politico/dirigente (gruppo governance G)
- Personale amministrativo che deve svolgere anche compiti IT (competenze IT base) (Gruppo tecnico base T)
- Personale tecnico (anche esterno) specializzato in compiti IT (competenze IT avanzate) (Gruppo tecnico avanzato TA)
- Per ciascuno di questi gruppi è stato organizzato un focus group.
- Sulla base dell'esperienza dei focus group è stato predisposto **un sondaggio on-line indirizzato, tramite ANCILAB, a tutti i comuni della Lombardia.** Le domande poste sono state le stesse dei focus group, le possibili risposte sono state scelte tra le key word proposte dai partecipanti

Componente soggettiva – distribuzione dei rispondenti



Componente soggettiva – distribuzione dei rispondenti



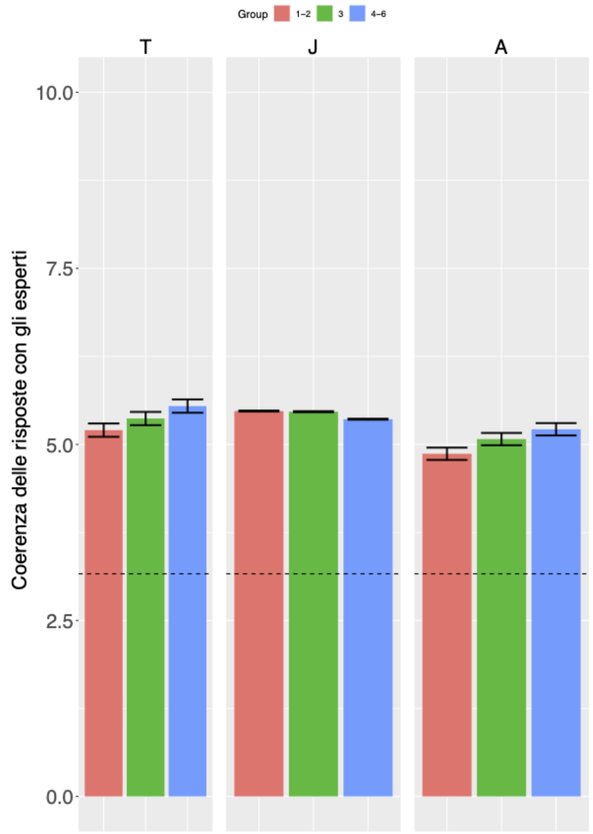


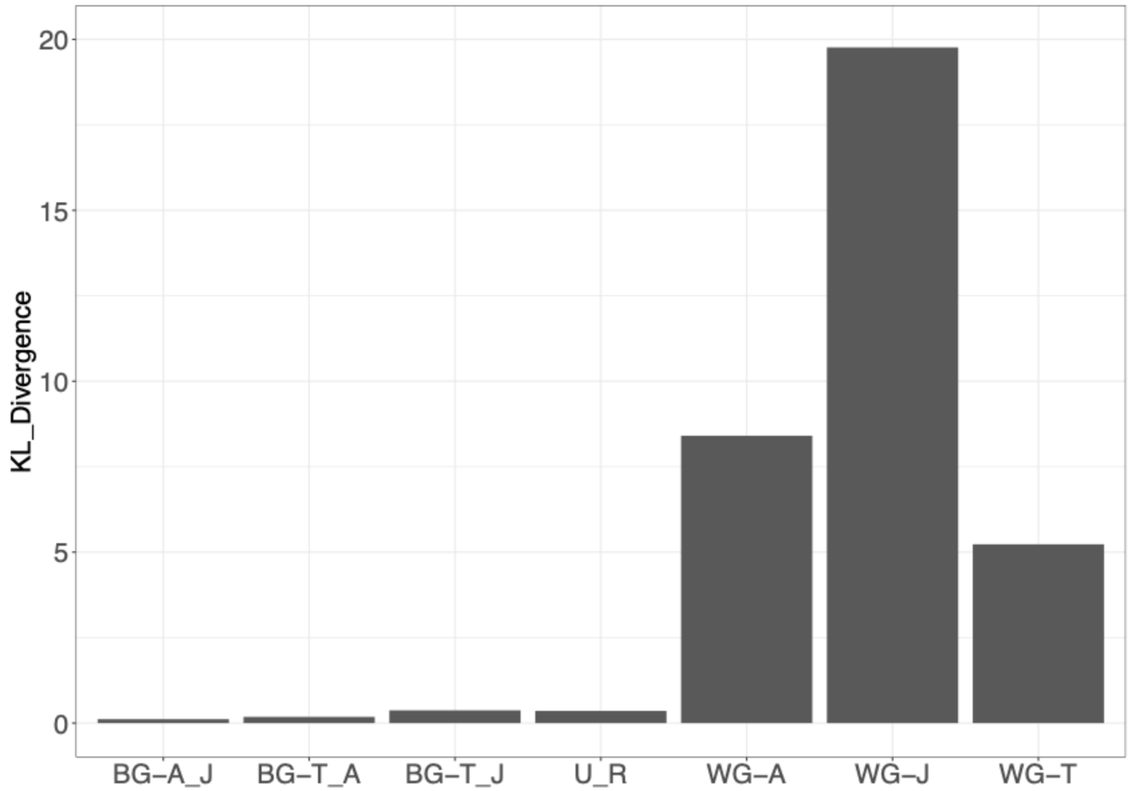
Classe Dem	Popolazione (2020)
1	fino a 999 abitanti
2	1000-4999
3	5000-19999
4	20000-59999
5	60000-99999
6	100000+

Componente soggettiva

- La sicurezza informatica coinvolge tre aree di competenza: **tecnico-informatica (T), giuridica (J), e manageriale (A)**.
- Per ciascuna delle tre, **sono stati selezionati degli esperti** a cui è stato sottoposto il questionario somministrato al personale dei comuni. Si è inoltre valutata la divergenza di opinione dei tecnici.
- La valutazione delle risposte è stata fatta valutando la **coerenza delle risposte fornite dal personale dei comuni con quella degli esperti**
- Al fine di avere un termine di confronto si anche selezionato un **gruppo di persone privo di competenze specifiche** in ciascuna delle tre aree di competenza.

Componente soggettiva - valutazione



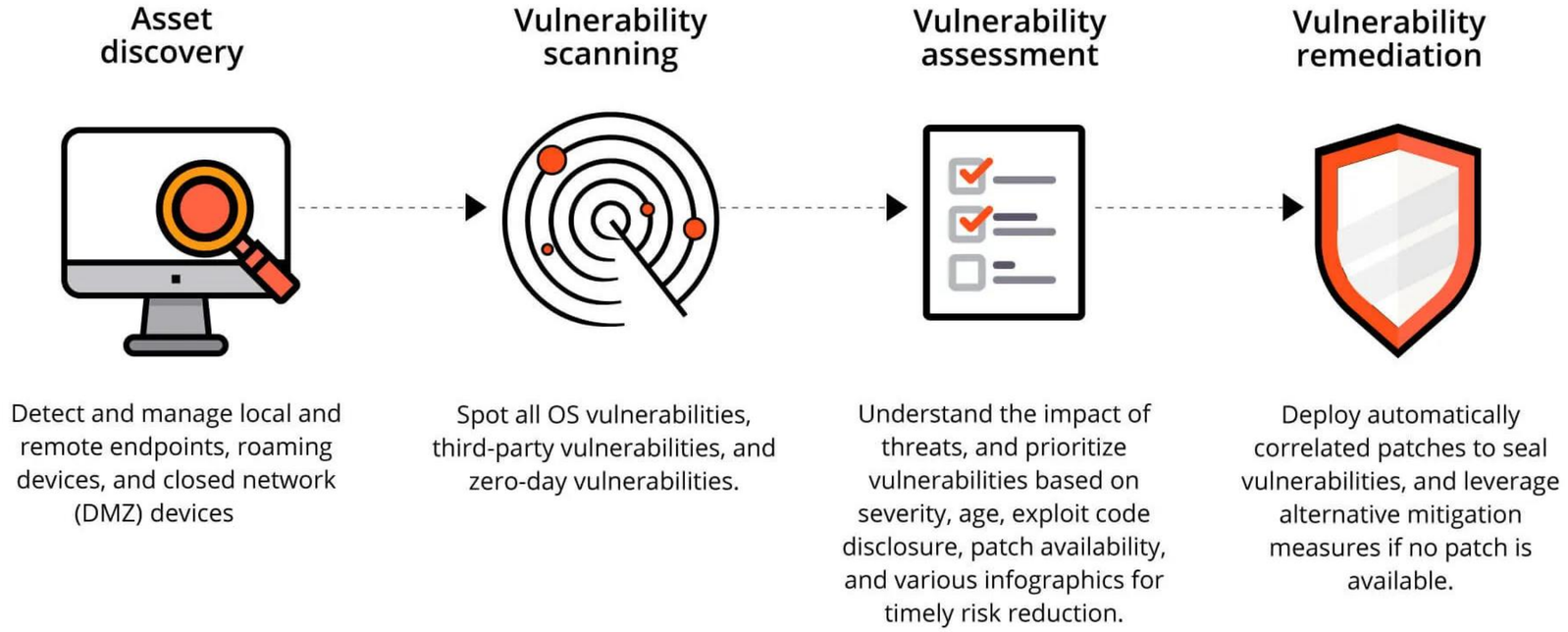


Componente soggettiva – esito

- **Prevalgono negli enti competenze di tipo tecnico**, quelle tipicamente che trovano applicazione immediata e che possono essere testate sul campo.
- Sono **molto rare le competenze di tipo manageriale** di più difficile reperimento, ma anche non così immediatamente applicabili nel contesto di un comune medio/piccolo.
- Il risultato è la presenza di **personale con competenze in grado di risolvere le urgenze**, un po' meno elaborare un piano a medio - lungo termine.

Vulnerability Assessment

Il VA è un processo che mira ad identificare le vulnerabilità in un sistema informatico, una rete o un'applicazione software.
Una vulnerabilità è una debolezza o un difetto che potrebbe essere sfruttato da un attaccante per compromettere la sicurezza del sistema.



Vulnerability Assessment

- Partecipanti: 20 Comuni
- Provenienza: Lombardia
- Dimensione: 3K-200K abitanti
- Eseguito da Luglio 2023 ad Agosto 2023

Vulnerability

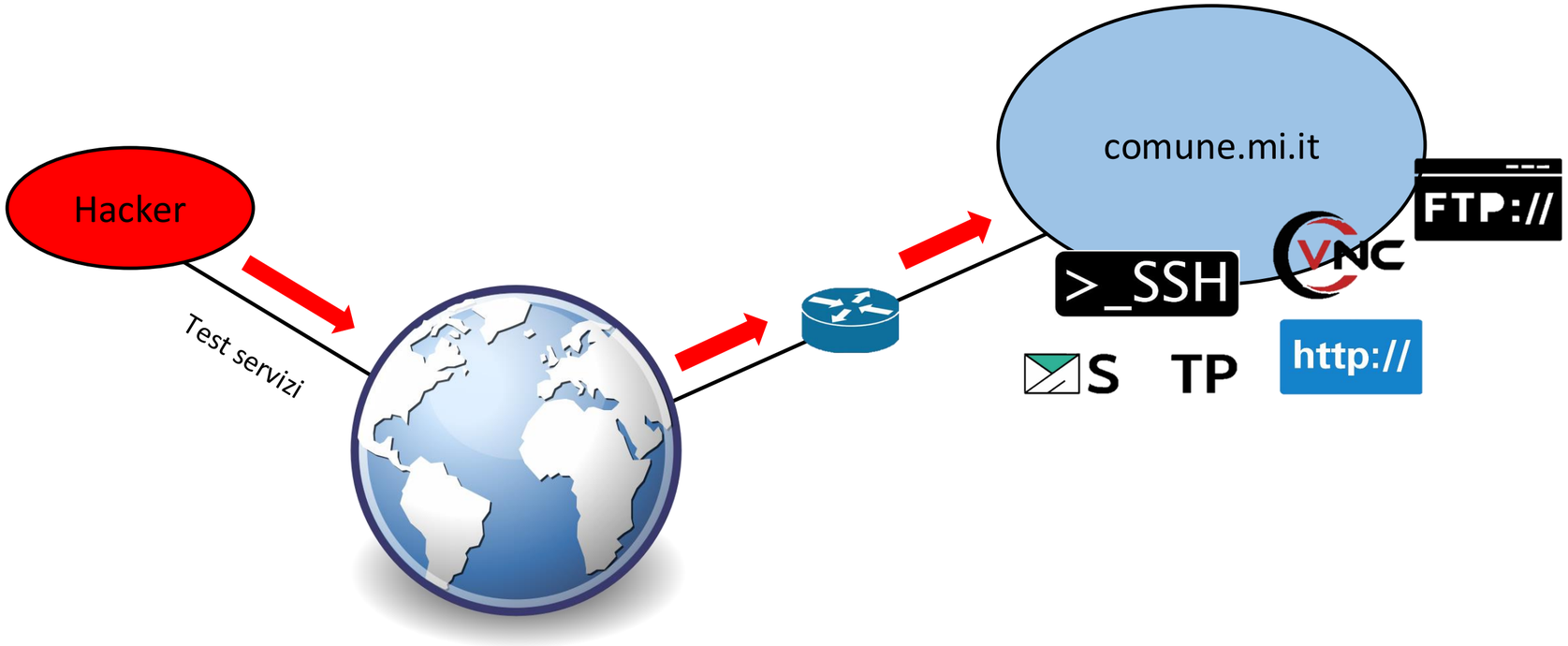
- DNS enumeration
- Port scanning
- Threat intelligence
- SQLi su webapp
- XSS su webapp
- Check certificati

https://gitlab.com/laser_unimi/vyper

+

Analisi manuale

Attack schema



Phishing

Il phishing è una forma di attacco informatico mirato ad ottenere informazioni sensibili, come **username**, **password** e **dettagli finanziari**, simulando l'identità di una fonte affidabile.
Gli attaccanti cercano di ingannare le vittime facendo loro credere che la comunicazione provenga da una fonte legittima, come una banca, un'azienda o un servizio online.

Gmail

Cerca nella posta

Scrivi

Posta in arrivo

Etiche

SMS

Viaggio

Altro

14 di 12.106

Il tuo ordine 406-4551649-6636331 che include "Stampante HP P8060.." Posta in arrivo ×

4 giorni fa)

Accedi

Email (nome utente o telefono cellulare)

email

Password **Password dimenticata?**

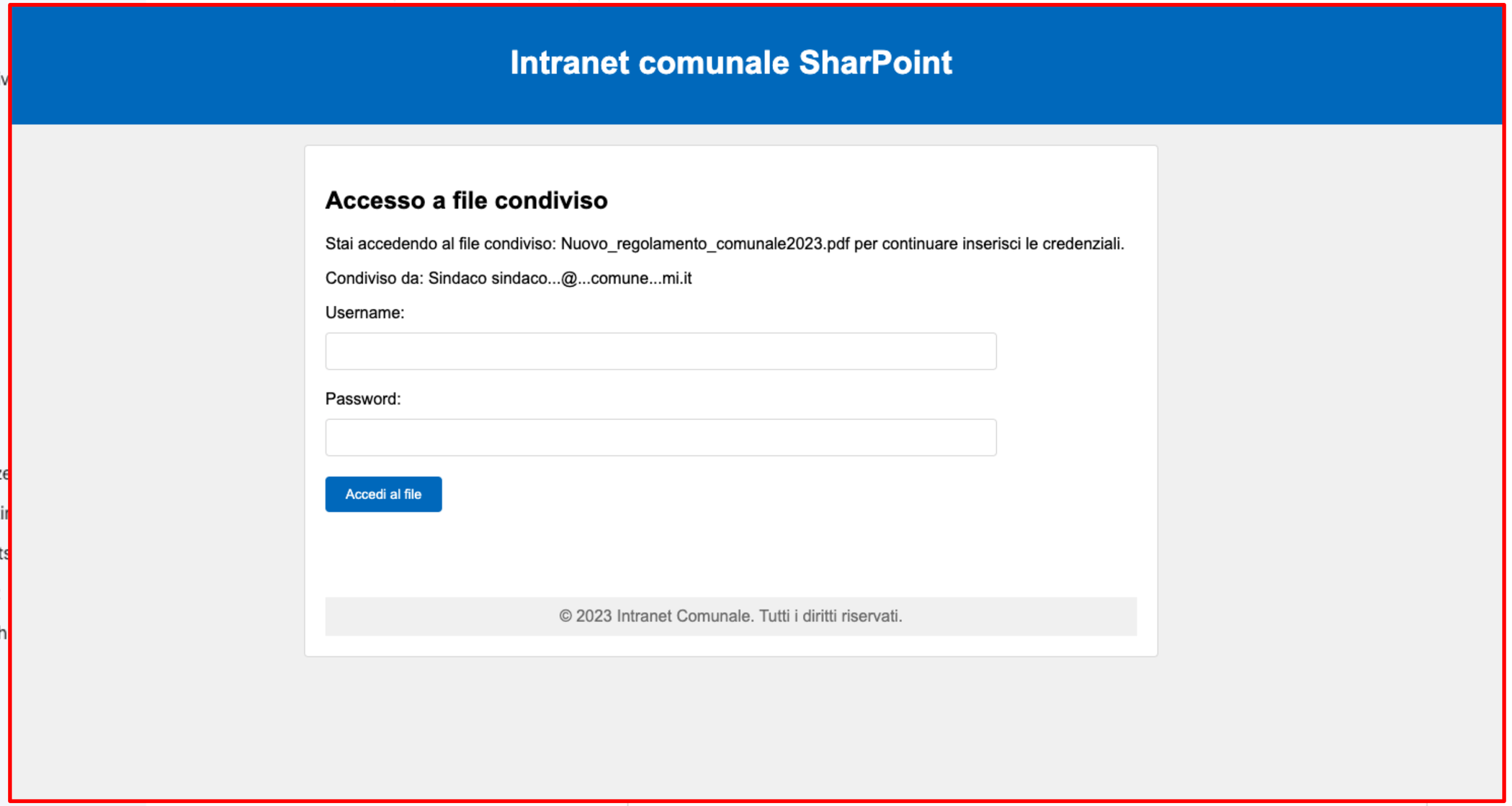
password

Accedi

Crea nuovo account

Conditions of Use Privacy Notice Help

Venduto da ARA3D EU
Gestito da Logistica di Amazon



Intranet comunale SharPoint

Accesso a file condiviso

Stai accedendo al file condiviso: Nuovo_regolamento_comunale2023.pdf per continuare inserisci le credenziali.

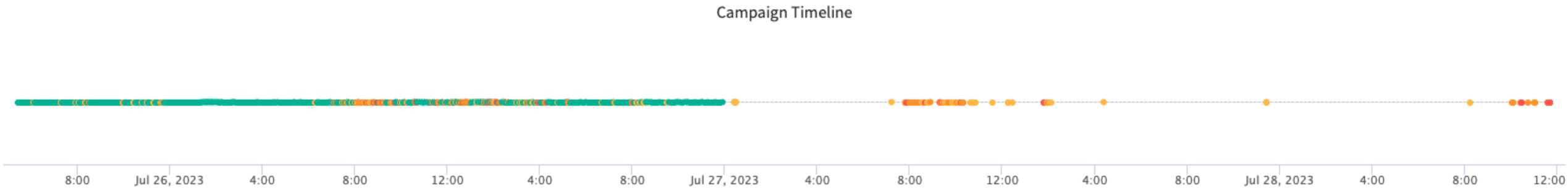
Condiviso da: Sindaco sindaco...@...comune...mi.it

Username:

Password:

Accedi al file

Phishing campaign



Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
394	135	102	37	0

Clicked Link
- Windows (OS Version: 10)
- Firefox (Version: 115.0)

Clicked Link
- Android (OS Version: 10)
- Chrome (Version: 114.0.0.0)

Clicked Link
- Samsung SM-A405FN (OS Version: 11)
- Samsung Browser (Version: 22.0)

Clicked Link
- Apple iPhone (OS Version: 16.5.1)
- Safari (Version: 16.5.2)

Polizia Locale Comando plcomando@[redacted] Submitted Data

Timeline for Polizia Locale Comando

Email: plcomando@[redacted]
Result ID: y3lX2MY

- Campaign Created — *July 25th 2023 5:26:58 pm*
- Email Sent — *July 26th 2023 12:26:25 pm*
- Clicked Link — *July 26th 2023 12:54:47 pm*
  - Windows (OS Version: 10)
  - Firefox (Version: 85.0)
- Email Opened — *July 26th 2023 12:55:02 pm*
- Submitted Data — *July 26th 2023 12:55:13 pm*
  - Windows (OS Version: 10)
  - Firefox (Version: 85.0)

Replay Credentials

View Details

Parameter	Value(s)
username	[redacted].it

Mail personale del dipendente

Mozilla

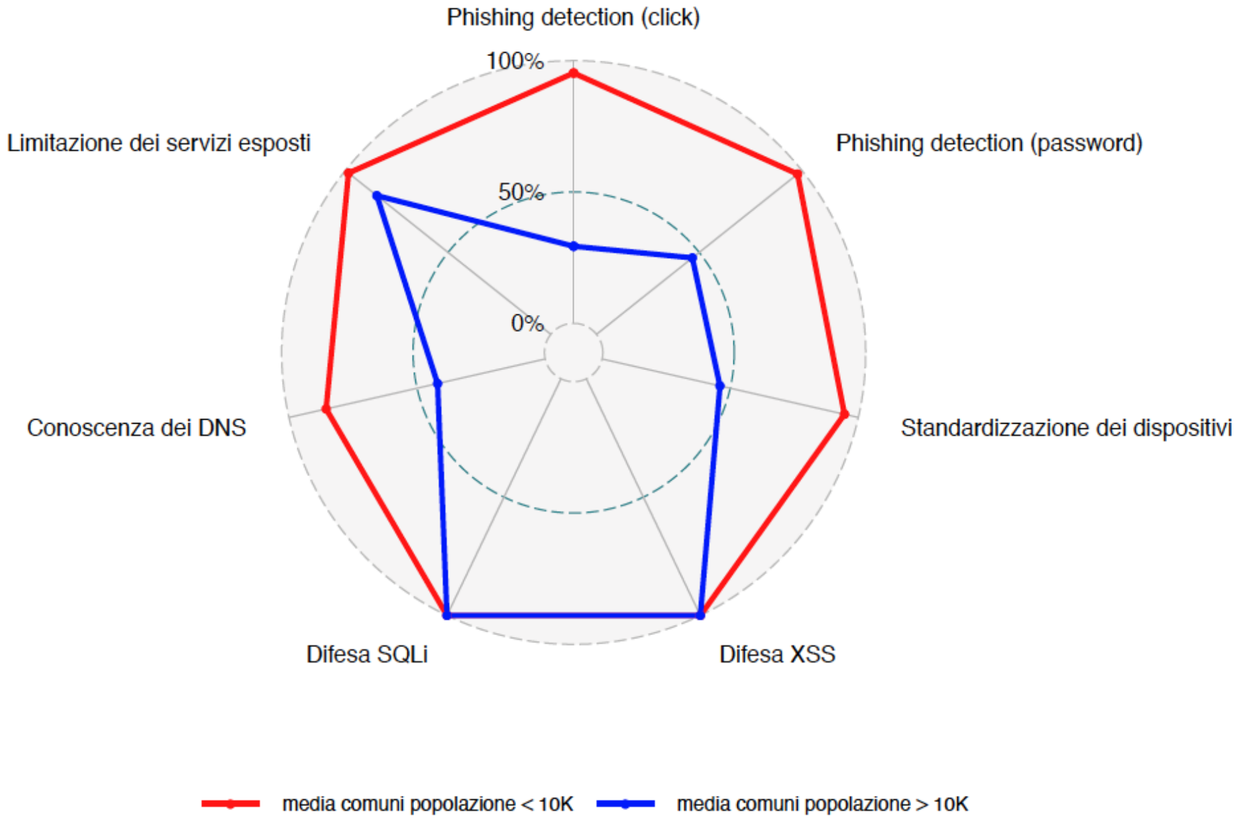
85.0

Firefox Release
January 26, 2021

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2015	72	2	2	78	15
2016	55	6	6	71	11
2017	1	0	0	1	0
2018	3	0	7	4	40
2019	0	3	6	5	4
2020	1	1	1	2	6
2021	0	0	0	0	0
2022	0	0	1	2	0
2023	2	0	0	1	0
2024	1	0	0	2	0
2025	0	0	1	0	0
Total	135	12	24	166	76

Componente oggettiva- Esito complessivo



Conclusioni

- Il quadro generale che emerge è quello di un sistema (quello dei comuni) in cui esiste la consapevolezza del problema cybersecurity, ma anche il rammarico di non avere gli strumenti necessari per poterlo affrontare come si deve.

- La formazione è de facto il problema più critico che emerge dalla nostra analisi, una formazione che i comuni si sono fatti da soli per affrontare i problemi del day by day ma che ora che le sfide ed i problemi diventano più grossi non basta più.

- I comuni ne sono consapevoli e sono disponibili a porvi rimedio, sembra però mancare l'interlocutore.

Versione completa del report

creative commons

Q&A

Universitá degli Studi di Milano, Dipartimento di Informatica
Via Celoria 18, 20135 Milano (Italy)
Room 6017 (sixth floor), +39 0250316362
x.com/lab_laser

andrea.monzani@unimi.it, marzio.decorato@unimi.it, matteo.zoia@unimi.it