SBAcademy
SECURITY THROUGH KNOWLEDGE

Webinar powered by:

Swascan

Cyber Security Awareness (ed implicazioni nello Smart Working)

Che cosa rischiamo online... mentre cerchiamo di restare sicuri off-line?

Relatori
Raoul "Nobody" Chiesa
Ing. Selene Giupponi
Moderatore
Piero Iezzi

Disclaimer from the Lecturers

The information contained within this presentation **does not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known local National laws.

The information contained in this presentation is for **educational purposes** and **knowledge information** only; the authors **are not responsible** if you will use this material in order to **damage people, assets, things**.

The authors hold the **intellectual property** and **it's not allowed to use this material for different purposes**.

The Hackers Profiling Project is hold by **UNICRI** and **ISECOM** and was **created by Mr. Raoul Chiesa.**

Quoted trademarks belongs to **registered owners**.

The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **University of Parma**, **Security Brokers, Swascan,** and **its own Associated Partners and Companies**.

Contents of this presentation **may be quoted or reproduced**, provided that the **source of information, and authorship, is acknowledged, mentioned and credited.**

Le informazioni mostrate durante la sessione sono riservate
e ne è vietata la riproduzione e qualsiasi modalità di registrazione/screenshot.

Siamo dotati degli strumenti necessari a rilevare comportamenti scorretti.

Se vi serve qualcosa, chiedetecelo.

Le slide saranno rese disponibili ai partecipanti la prossima settimana.

HACKMAGEDDON

Adesso pensiamo
di avere la vostra attenzione ☺

INDICE

1. Covid-19 vs Telelavoro
2. Scenario e Problematiche
3. Cybercrime: what & why
4. “Cyber Hygiene” & Common Sense
5. Misure da Adottare: alcuni Consigli
6. Cosa fare come azienda?
7. Come vi può aiutare lo Stato
8. Come vi possiamo aiutare noi
9. …and a Special Gift for you all!
10. Q&A session (moderata)

Introductions

Relatori e Moderatore

Raoul “Nobody” Chiesa

Ing. Selene Giupponi

Piero Iezzi

whois Raoul

- Co-founder @ **Swascan**
- President, Founder @ **The Security Brokers**
- Indipendent Special Senior Advisor on Cybercrime @ **UNICRI**
  (*United Nations Interregional Crime & Justice Research Institute*)
- Roster of Experts @ **ITU** (*UN International Telecomunication Union*)
- Former PSG Member, **ENISA** (*Permanent Stakeholders Group @ European Union Network & Information Security Agency*)
- Founder, Former Member, @ **CLUSIT** (*Italian Information Security Association*)
- Steering Committee, **AIP/OPSI** (*Privacy & Security Observatory)*
- Board of Directors, **ISECOM** *(Institute for Security & Open Methodologies)*
- **OSSTMM** Key Contributor *(Open Source Security Testing Methodology Manual)*
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Former Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various Cecurity Communities and Universities**

whois Selene

- **Managing Director Europe, RESecurity**
- **Computer Engineering Degree** + II Level **Master in Computer Forensics & Digital Investigations**
- General Secretary and Member @ **IISFA** (INFORMATION SYSTEM FORENSICS ASSOCIATION, ITALIAN CHAPTER)
- Active Member of the **IT Engineer Commission**, Engineers Association of the Latina Province
- **Digital Forensics Court Trial Witness** on e-crimes and ICT enhanced crimes
- Consultant for multiple **Law Enforcement agencies** around the world
- Advisor @ **European Courage Focus Group** – Cyber Terrorism & Cybercrime
- **ITU** Roster of Experts Official Member
- **HTCC** HIGH TECH CRIME CONSORTIUM Member
- Co-Founder at **The Security Brokers**
- Trainer at **NATO**, **INTERPOL**
- **CIFI** - Certified Information Forensics Investigator
- Certified Trainer for **SPEKTOR** & **UFED**
- **ECSO** Board of Directors Member

COVID-19 & Smart Work

Tutte le relazioni di business si spostano nelle più diverse modalità remote

Sì, io ti sento...
Parla, parla, parla!

Mi senti?
Riesci a sentirmi?

Mi vedi?

Ma che c...!
Io sento benissimo!!

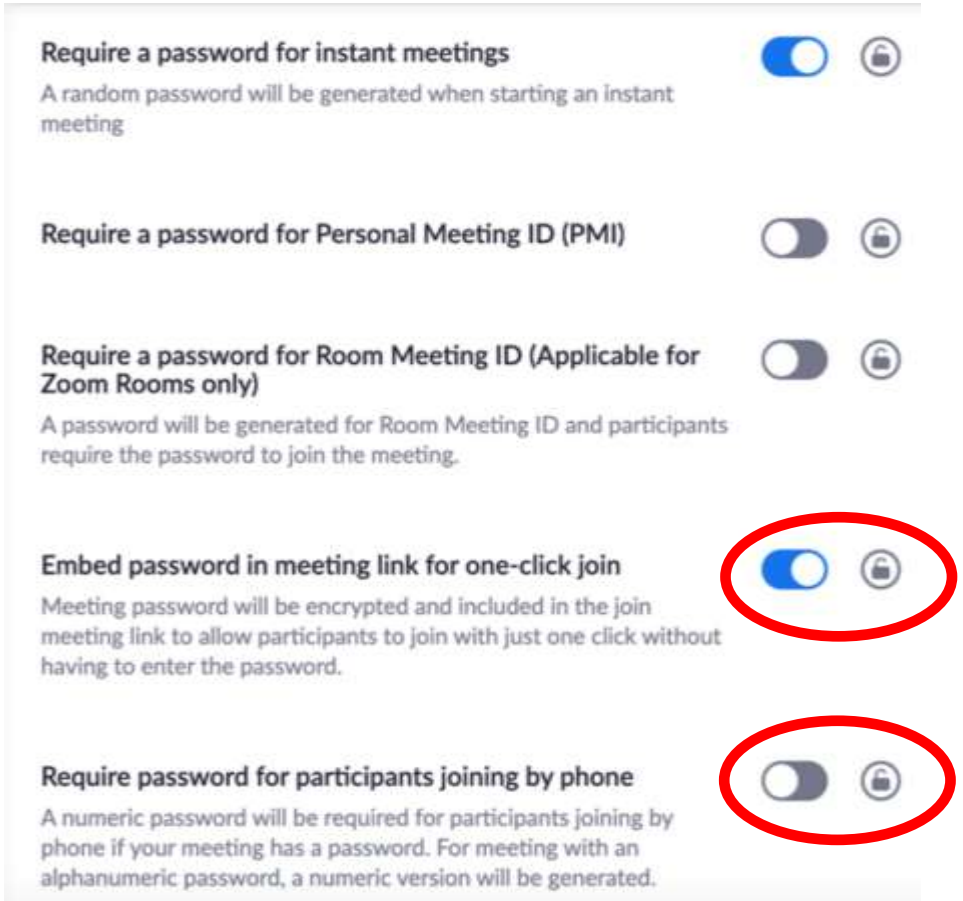
Mi senti?

Attiva il microfono
che io non ti sento

Prima di iniziare: il “caso Zoom”…

… e l'underground digitale

Perché siamo qui?



Un cambio di mindset

- La slide precedente è un esempio emblematico di ciò che vogliamo spiegarvi.
- Le opzioni di sicurezza **ci sono ma non sono impostate di default**: dobbiamo abilitarle noi ☺

Il caso Teams

www.cyberark.com › threat-research-blog › be... ▾ Traduci questa pagina

Beware of the GIF: Account Takeover Vulnerability in Microsoft ...

3 giorni fa - This **vulnerability** would have affected every user who uses the **Teams** desktop or web browser version. CyberArk worked with **Microsoft** Security ...

www.welivesecurity.com › 2020/04/27 › micros... ▾ Traduci questa pagina

Microsoft Teams flaw could let attackers hijack accounts ...

3 giorni fa - CyberArk has now described a possible attack scenario: "We found that by leveraging a sub-domain takeover **vulnerability** in **Microsoft Teams**, ...

www.scmagazine.com › ... › Vulnerabilities ▾ Traduci questa pagina

Microsoft Teams vulnerability patched, could lead to account ...

2 giorni fa - **Microsoft's Teams** collaboration platform contains a **vulnerability** that can be exploited with a malicious GIF enabling an attacker to take over a ...

www.cbronline.com › news › teams-vulnerabilit... ▾ Traduci questa pagina

Microsoft Teams Vulnerability Let Hackers "Take Over Entire ...

3 giorni fa - **Microsoft's** collaboration platform **Teams** contained a **vulnerability** that allowed hackers to send out a GIF that only had to been seen, in order ...

Remote Work VS Smart Work

Differenze dal punto di vista tecnico

- **Remote work**: lavoro che si svolge a distanza rispetto alla sede centrale, da casa o da un luogo decentrato specifico

- **Smart work**: non è obbligatorio legarsi a un luogo fisico fisso in cui lavorare (casa, sede distaccata, ma anche un ristorante, un pub o un parco se presente una connessione Wi-Fi).
- BYOD

Scenario e Problematiche

1. Utilizzo dei PC “di casa” e non di quelli aziendali
2. Assenza o drastica diminuzione degli strumenti di difesa in essere
3. Aumento del rischio di contagi informatici e dell’esposizione degli utenti e degli asset digitali utilizzati
4. Innalzamento dell’interesse del cybercrime e **lancio massivo di campagne di phishing** e **schemi di frode coordinati**

Cybercrime: What & Why

1. Il Cybercrime utilizza **modelli di business molto creativi**

- Servizi **Differenziati**
- "**E' come il maiale**": non si butta via niente (cfr. una delle prossime slide)

2. Il goal finale: utilizzare o rivendere **i vostri dati**

Cybercrime: What

L'esecuzione di crimini, mediante l'ausilio di mezzi informatici e di telecomunicazione, con lo scopo di acquisire illegalmente informazioni e di tramutarle in denaro.

Esempi:

Furto di Identità

- Personal Info

Furto di Credit Identity

- Financial Info: login bancari, CC/CVV, «fullz», etc

Hacking

- verso e-commerce, e-banking, Credit Cards Processing Centers

Industrial Espionage

- Hacking su commissione

Attacchi DDoS

- Blackmail, Hacktivism

Malware

- Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile

Spam

Counterfeiting

- medicinali, luxury, prodotti & servizi

Gambling

- Riciclaggio di denaro
- Finti siti e/o non autorizzati (i.e. Italia -> da AAMS)

Porno generico

- fake sites, etc

Pornografia minorile / infantile

Harassment

- Cyberstalking
- Cyberbullying
- Cybergrooming, ...

Cybercrime: Why

1. **Attori**
- Chi sono? Cfr. Hacker's Profiling Project (HPP)

2. **Motivazione**
- Fama
- Denaro
- Ideali
- Nessuno (?)

3. **Prodotti/Servizi**
- Campagne di affiliation, boosting, advertising, traffic generation, etc…
- Decine di famiglie di servizi e prodotti «impensabili per l'uomo comune»
- Di alcuni faremo cenno nelle prossime slide

4. **Legislazioni**
- Non presenti in tutti i Paesi per tutti i reati: carenze nella cooperazione internazionale
- Cybercrime: profonda presenza in Paesi con problematiche interne (legislazioni, budget, formazione delle Forze dell'Ordine, corruzione)

Questo, semplicemente perché l'**informazione è immediatamente trasformabile** in:

- ✓ **Vantaggio competitivo**
- ✓ **Informazione sensibile/critica**
- ✓ **Denaro**
- ✓ **Ricatto**

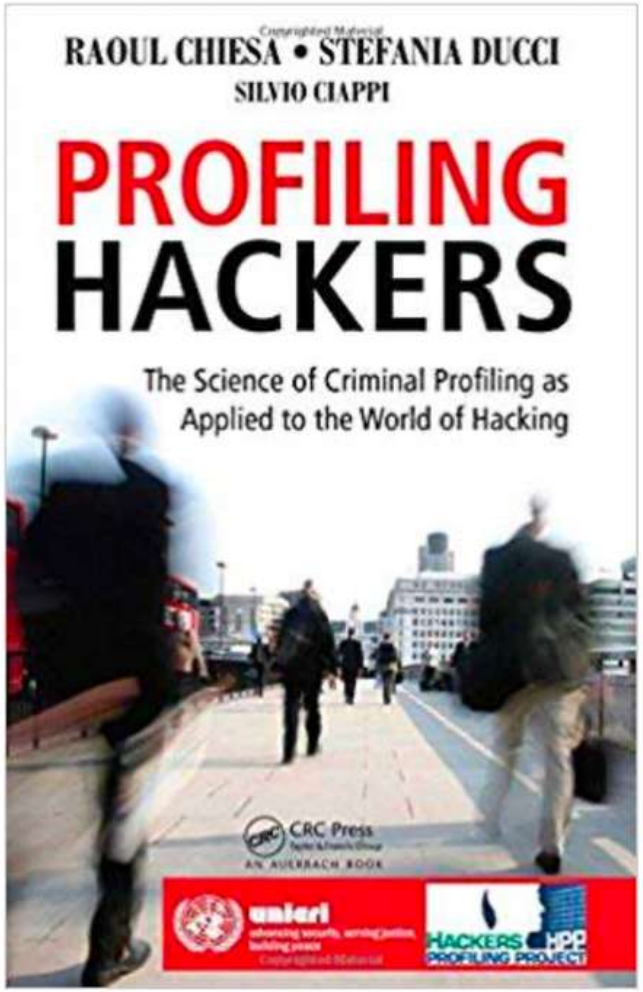
Hacker's Profiling Project (HPP) by UNICRI / ISECOM

unicri
advancing security, serving justice, building peace

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

HACKERS HPP
PROFILING PROJECT

Profiling Hackers

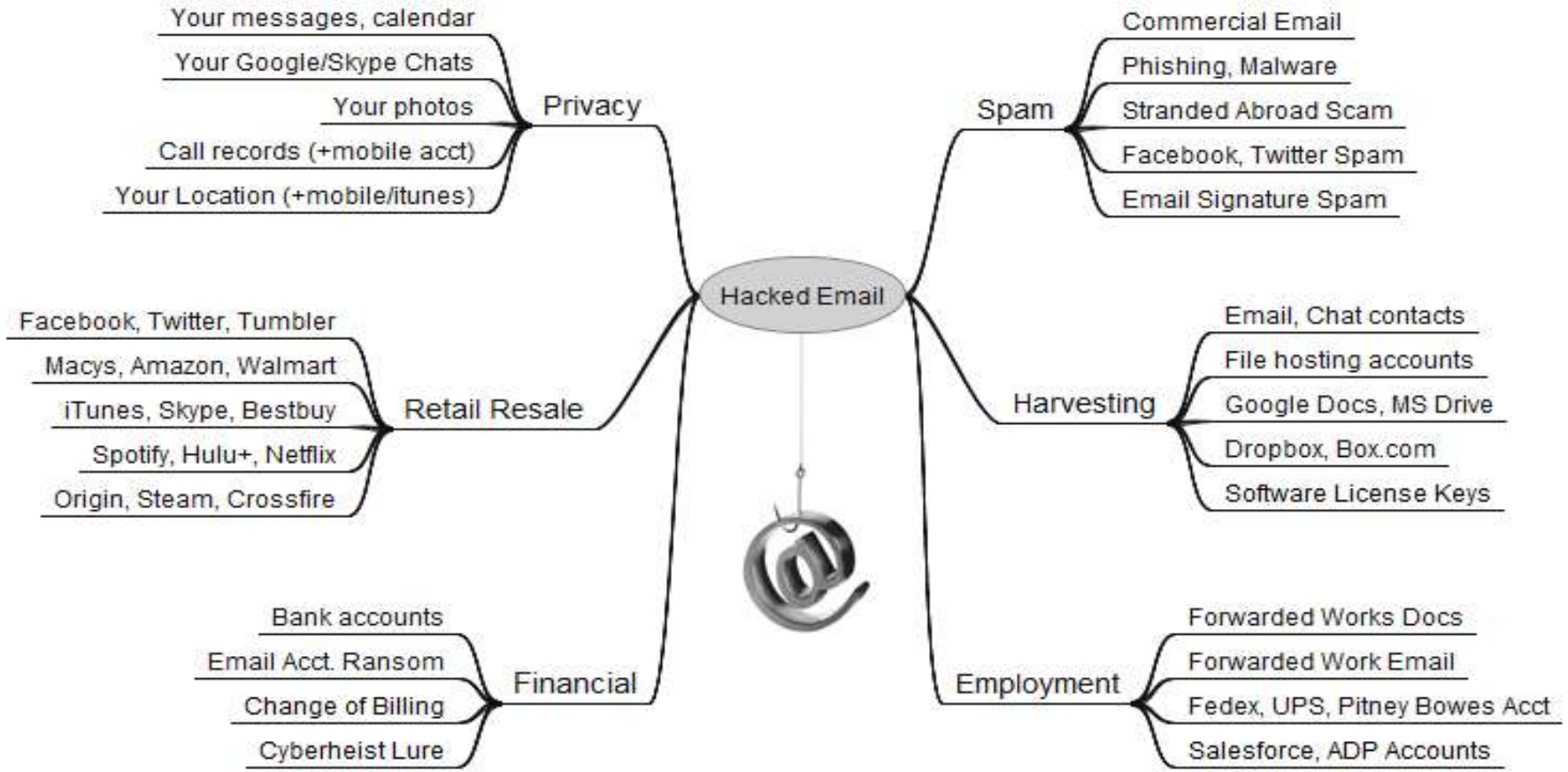


- **Applied Research** Project started back in **2004**
- **Field Research** tasks started in **2006** (still on-going)
- Law Enforcement Officers and Government Agencies **loved our profiling approach!**
- **FBI Academy Library** in Quantico, VA (USA)
- FBI cybercrimes **Special Agents must-read** book
- Italian Intelligence Agency (**DIS**) official Hacker's Profiles
- Translated in **different languages** (Italian, Spanish,French, Russian, Chinese, Arabic, etc..)
- **Cutting-edge milestone** from the previous "Black-hat /White-hat" approach

HPP – Hacker's Profiling Project (UNICRI/ISECOM)

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

Cybercrime: hacked email



“Cyber Hygiene” & Common Sense

7 macro-argomenti per la nostra Cyber Hygiene:

- Backup
- OS Patching
- VPN
- Phishing
- AV
- Endpoint Protection
- PC “dedicato”

+ Buon senso (e consigli)

Backup

Avere un backup aggiornato è la condizione ideale per mitigare possibili danni conseguenti a:

- Rottura dell'hardware
- Sovrascritture incidentali di files
- Contagio da ransomware e malware

BackUP – Fatevi delle domande

- ✓ Quanto tempo fa avete fatto l'ultimo backup?
- ✓ Il backup e' disponibile solo sui server aziendali?
- ✓ Conoscete il concetto di "backup incrementale"?
- ✓ Come organizzate i vostri dati (di lavoro) sui PC di casa?
- ✓ Quali strumenti HW e SW usate per i backup? E da quanto tempo?
- ✓ Cloud e backup: cifratura dei dati ?

OS Patching

Aggiornare sempre il proprio OS (Sistema Operativo) ed il software / le applicazioni installate.

NOTA: Questo vale **anche ed in particolar modo** per i vostri smartphone e tablet, e per i **dispositivi personali**.

VPN (Virtual Private Network)

- ✓ VPN gratuite o a pagamento vs VPN proprietarie (“in-house”)
- ✓ Ottimizzazione dei costi (ad esempio, AV che includa già il servizio di VPN)
- ✓ Aspetti di privacy e cyber security aziendale nell’uso di VPN gratuite

Phishing & Ingegneria Sociale

- ✓ Com’era prevedibile, stiamo assistendo ad un **aumento esponenziale** degli attacchi di **phishing** (email “esca”) e di **molteplici malware** (software malevoli).
- ✓ Queste **truffe usano la scusa del COVID-19**, e di varie parole chiave ad esso correlate, per **invogliare l’utente ad aprire allegati infetti**, o a **cliccare su URL** che a loro volta portano a **siti fake**, o **violati** e **contagiati**.
- ✓ Adesso ne **analizzeremo qualcuna**!

Phishing & Ingegneria Sociale

✓ **Phishing di account personali VS sicurezza aziendale**

- Spesso stessa password, o variante della stessa
- Facilitano attacchi phishing mirati ed usano “leva psicologica”

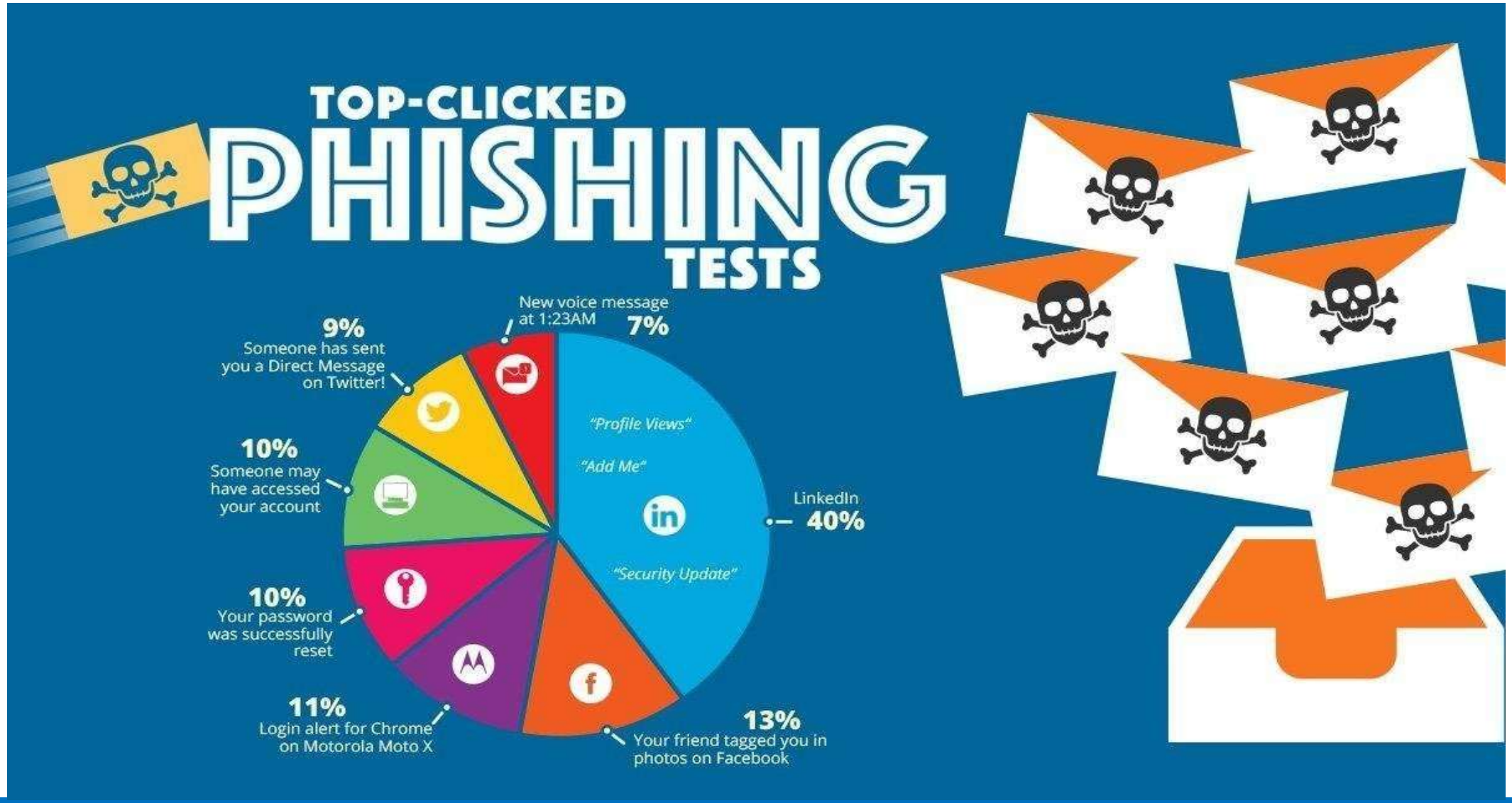
✓ **Credenziali compromesse di terze parti**

- Ad esempio della nostra utenza PEC, il vostro account Netflix, etc…

✓ **Credenziali aziendali compromesse presenti su Dark Web**

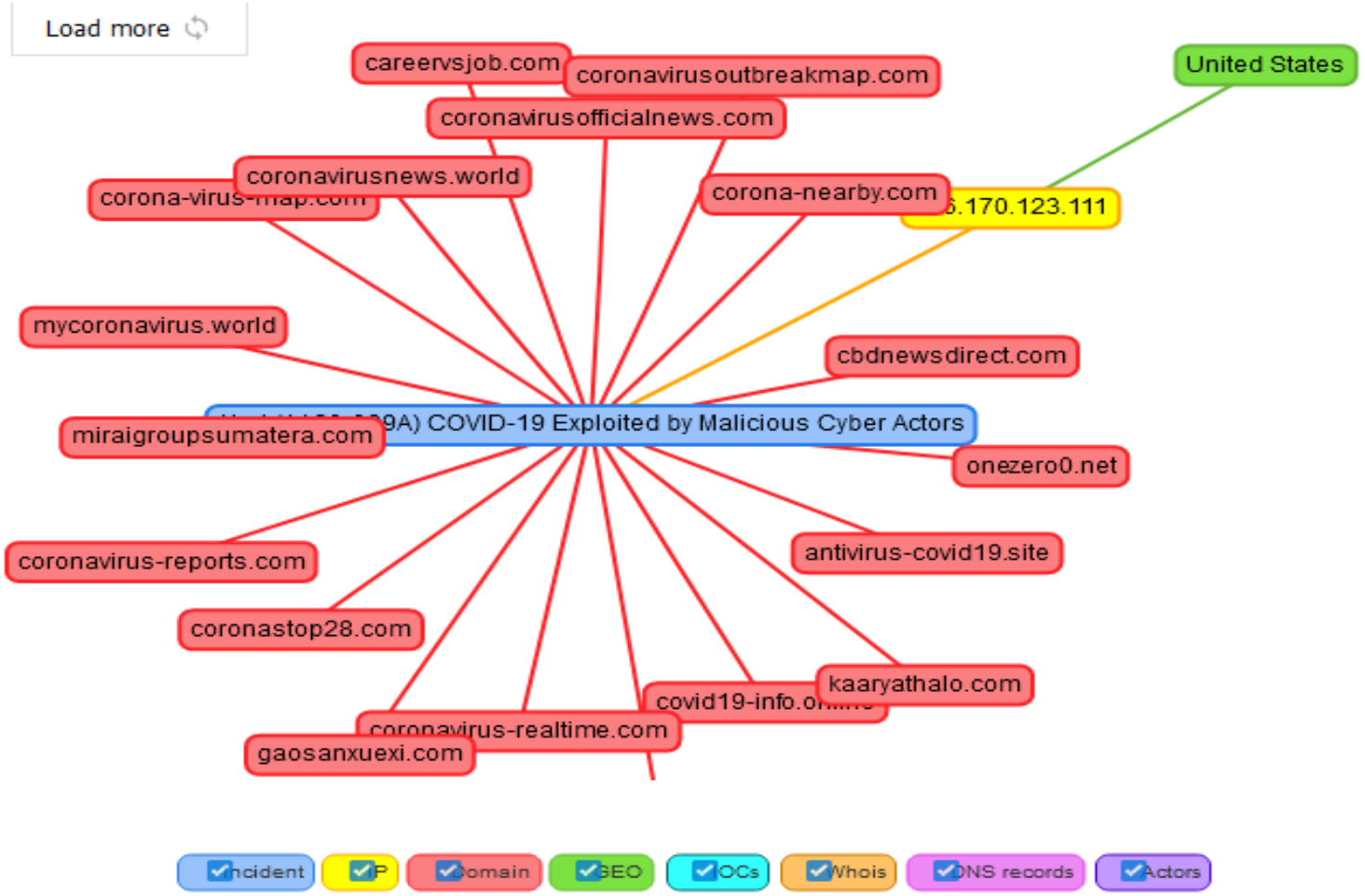
- Poche aziende hanno ad oggi gli strumenti per informarsi in tempo reale
- Impatti lato GDPR e sanzioni economiche

Phishing & Ingegneria Sociale



Phishing & Ingegneria Sociale

Esempio: propagazione del malware del WHO



NOTA: **non** andate sui siti riportati in questo screenshot!

Phishing & Ingegneria Sociale

Rai News

ITALIA

aa

Finta app immuni fa scaricare virus informatico: allarme del governo

Tweet

01 giugno 2020

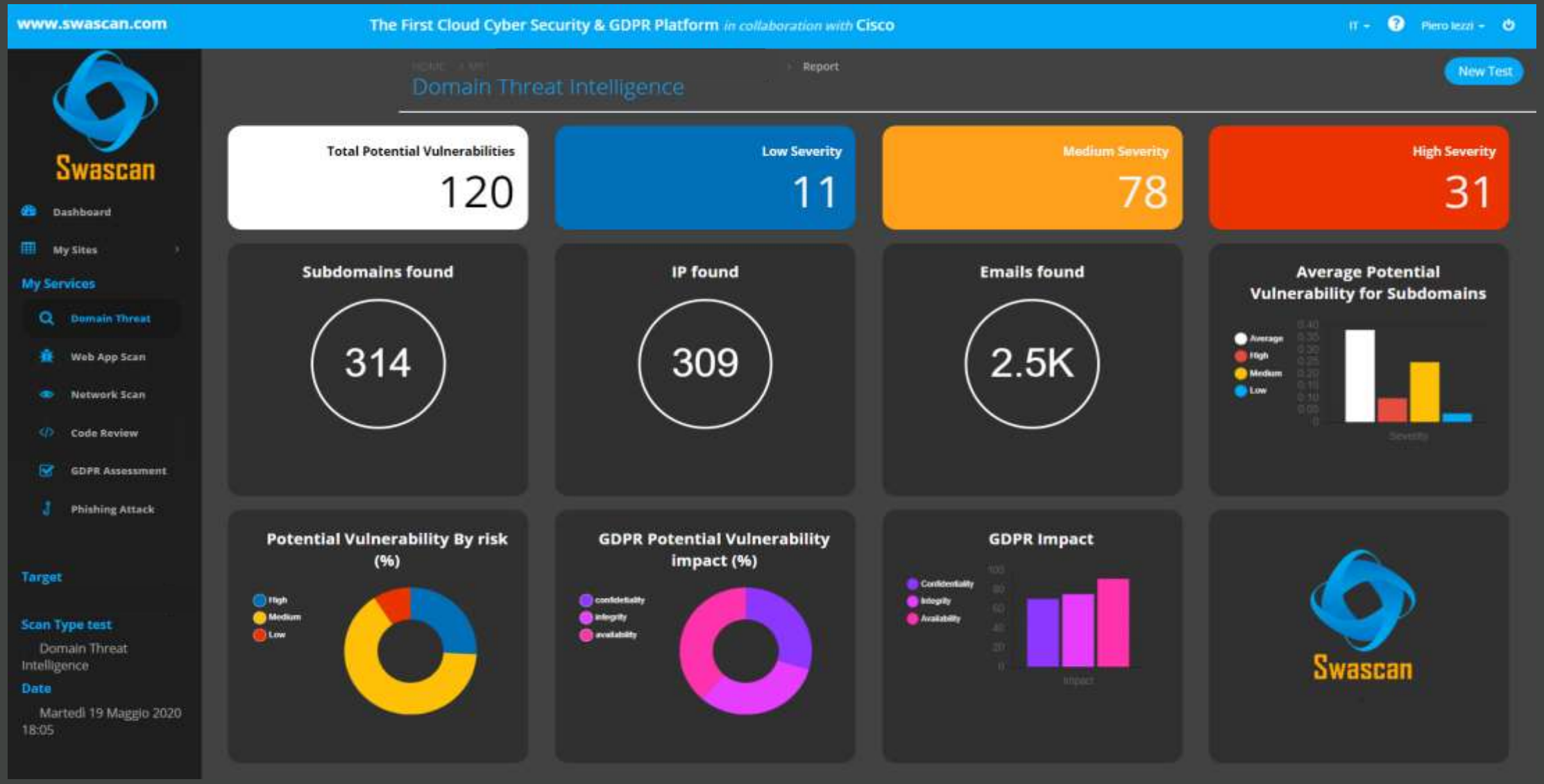
Una campagna di virus informatici investe l'Italia nelle ore in cui sta per essere resa disponibile l'app Immuni. A renderlo noto Agid-Cert, la struttura del governo che si occupa di cybersicurezza. Il virus si chiama FuckUnicorn e diffonde un ransomware (virus che prende in ostaggio i dispositivi e poi chiede un riscatto) con il pretesto di far scaricare un file denominato Immuni. Si

Phishing & Ingegneria Sociale (@pec.it)

IMMAGINE RIMOSSA NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

NOTA: **non** andate sui siti riportati in questo screenshot!

Domain Threat Intelligence



Cyber Threat Intelligence

AV (Anti-Virus)

Oggigiorno gli AV “standard”, purtroppo, non sono più uno strumento efficace al 100% contro le infezioni.

Ad esempio bloccano solo i malware già noti e conosciuti (dei quali esiste un “signature”), ma nulla possono contro vulnerabilità “zero-day’ e, soprattutto, contro quei malware non ancora identificati dal produttore o i file-less attack – ne parleremo tra poco.

AV (Anti-Virus)

Ciò nonostante, avere un antivirus “a bordo” è misura quanto meno obbligatoria (chiamiamola best practice o “buon senso del padre di famiglia”).

- Aggiornare sempre l’antivirus: “signatures” ed “engine”
- Provare ad utilizzare una VM (Virtual Machine) con Windows

Live examples: IOC e AV detection rate

Type some keywords here for search...

Trojan.Downloader.LnK.Gen Additional_CSD_Rebate.pdf.lnk	**Analysis date:** 8 Apr, 2020 **File type:** Windows shortcut **Detection ratio:** 21 / 60 **MD5:** 120e3733e167fcabdfd8194b3c49560b **SHA256:** f8b053e32eed9a5e814c89eec50e743a906f1aadc7a6f58e25f0410863c5ec4a
HEUR:Exploit.MSOffice.Generic .	**Analysis date:** 8 Apr, 2020 **File type:** Rich Text Format **Detection ratio:** 35 / 60 **MD5:** fef12d62a3b2fbf1d3be1f0c71ae393e **SHA256:** 0dd9d9638a59b6fbab792b7781962571b653c44ebae3d9b8351937ec71f0af8b
Trojan-Downloader.BAT.wGet.ah 58954102	**Analysis date:** 8 Apr, 2020 **File type:** Text **Detection ratio:** 17 / 60 **MD5:** adebf3b5cb93645489b332033bc764ad **SHA256:** 19270639537a2241861eae2bbf4b4095fc6e1915e4dee476d2e4f277992733fd
ca73cb1feccd34d651eb2ae5094d8311bfb2bdc29455005d4 50ac9c8ee6bbdef.exe	**Analysis date:** 8 Apr, 2020 **File type:** Win32 EXE **Detection ratio:** 0 / 73 **MD5:** 60b7c0fead45f2066e5b805a91f4f0fc **SHA256:** 80c10ee5f21f92f89cbc293a59d2fd4c01c7958aacad15642558db700943fa22

AV detection rate (esempio: 1/5)

ANTIVIRUS	RESULT	UPDATE
ALYac	(not set)	8 Apr, 2020
APEX	(not set)	7 Apr, 2020
AVG	(not set)	7 Apr, 2020
Acronis	(not set)	15 Mar, 2020
Ad-Aware	(not set)	7 Apr, 2020
AegisLab	(not set)	7 Apr, 2020
AhnLab-V3	(not set)	7 Apr, 2020
Alibaba	(not set)	27 May, 2019
Antiy-AVL	(not set)	8 Apr, 2020
Arcabit	(not set)	7 Apr, 2020
Avast	(not set)	7 Apr, 2020
Avast-Mobile	(not set)	7 Apr, 2020
Avira	(not set)	8 Apr, 2020
Baidu	(not set)	18 Mar, 2019

AV detection rate (esempio: 2/5)

Baidu	(not set)	18 Mar, 2019
BitDefender	(not set)	8 Apr, 2020
BitDefenderTheta	(not set)	7 Apr, 2020
Bkav	(not set)	7 Apr, 2020
CAT-QuickHeal	(not set)	8 Apr, 2020
CMC	(not set)	21 Mar, 2019
ClamAV	(not set)	7 Apr, 2020
Comodo	(not set)	7 Apr, 2020
CrowdStrike	(not set)	2 Jul, 2019
Cybereason	(not set)	16 Jun, 2019
Cylance	(not set)	8 Apr, 2020
Cyren	(not set)	8 Apr, 2020
DrWeb	(not set)	8 Apr, 2020
ESET-NOD32	(not set)	7 Apr, 2020
Emsisoft	(not set)	8 Apr, 2020

AV detection rate (esempio: 3/5)

Endgame	(not set)	26 Feb, 2020
F-Prot	(not set)	7 Apr, 2020
F-Secure	(not set)	7 Apr, 2020
FireEye	(not set)	16 Mar, 2020
Fortinet	(not set)	7 Apr, 2020
GData	(not set)	7 Apr, 2020
Ikarus	(not set)	7 Apr, 2020
Invincea	(not set)	7 Apr, 2020
Jiangmin	(not set)	8 Apr, 2020
K7AntiVirus	(not set)	7 Apr, 2020
K7GW	(not set)	7 Apr, 2020
Kaspersky	(not set)	7 Apr, 2020
Kingsoft	(not set)	8 Apr, 2020
MAX	(not set)	8 Apr, 2020
Malwarebytes	(not set)	7 Apr, 2020

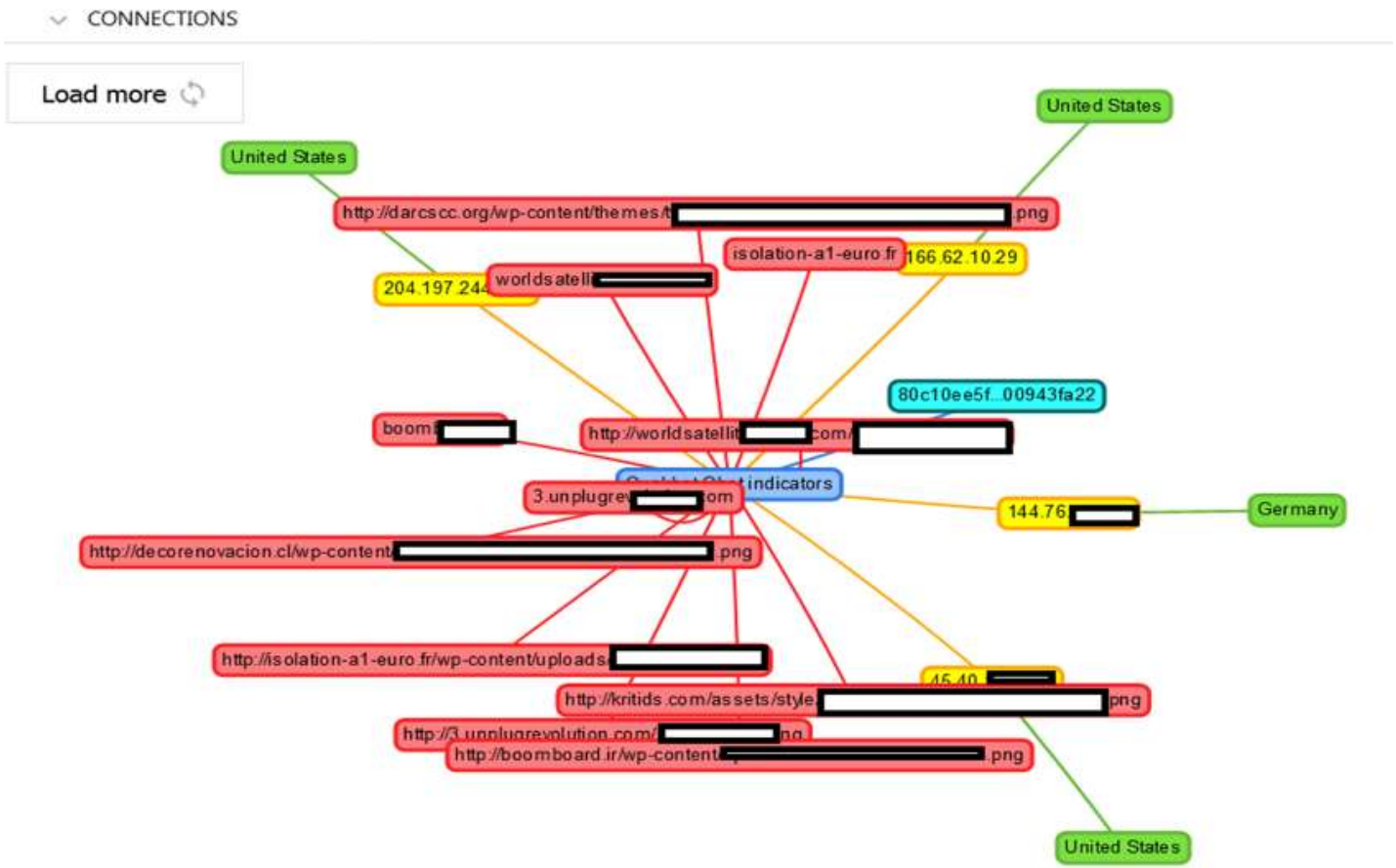
AV detection rate (esempio: 4/5)

ANTIVIRUS	RESULT	UPDATE
ALYac	(not set)	8 Apr, 2020
APEX	(not set)	7 Apr, 2020
AVG	(not set)	7 Apr, 2020
Acronis	(not set)	15 Mar, 2020
Ad-Aware	(not set)	7 Apr, 2020
AegisLab	(not set)	7 Apr, 2020
AhnLab-V3	(not set)	7 Apr, 2020
Alibaba	(not set)	27 May, 2019
Antiy-AVL	(not set)	8 Apr, 2020
Arcabit	(not set)	7 Apr, 2020
Avast	(not set)	7 Apr, 2020
Avast-Mobile	(not set)	7 Apr, 2020
Avira	(not set)	8 Apr, 2020
Baidu	(not set)	18 Mar, 2019

AV detection rate (esempio: 5/5)

SymantecMobileInsight	(not set)	10 Feb, 2020
TACHYON	(not set)	8 Apr, 2020
Tencent	(not set)	8 Apr, 2020
TotalDefense	(not set)	7 Apr, 2020
Trapmine	(not set)	23 Jan, 2020
TrendMicro	(not set)	7 Apr, 2020
TrendMicro-HouseCall	(not set)	8 Apr, 2020
Trustlook	(not set)	8 Apr, 2020
VBA32	(not set)	7 Apr, 2020
VIPRE	(not set)	8 Apr, 2020
ViRobot	(not set)	7 Apr, 2020
Webroot	(not set)	8 Apr, 2020
Yandex	(not set)	7 Apr, 2020
Zillya	(not set)	7 Apr, 2020
ZoneAlarm	(not set)	8 Apr, 2020

Propagazione del malware



Siti infettati
per contagiare

NOTA: **non** andate sui siti riportati in questo screenshot!

EPP (EndPoint Protection)

- **Dotarsi di EPP**
- Far eseguire una **corretta configurazione**, evitando falsi positivi e falsi negativi
- Ricordarsi di **prevedere un periodo iniziale** di “fine tuning delle regole e delle eccezioni” (tipicamente tra i 5 ed i 15 giorni).

Alla fine di questo webinar forniamo link per offrire 40 giorni di utilizzo gratuito della nostra soluzione ad alcune tipologie di aziende

EPP (EndPoint Protection)

La soluzione da noi individuata ha come caratteristica unica di essere dotata di un "NanoOS", ossia un micro-sistema operativo.

Ciò impedisce anche ai malware più invasivi di "disabilitare" il software di EPP, come per altro fanno spesso i malware con gli AV.

Semplicemente, li "spengono".

Pros&Cons dell'utilizzo di un PC Dedicato

Non tutte le aziende sono pronte o possono permettersi di fornire un PC dedicato allo smart worker.

- Problematiche di costi e di logistica
- Sicurezza dei dati in transito e conseguenti responsabilità

Ad oggi la maggior parte delle piccole e medie aziende ha chiesto al dipendente di utilizzare il PC di casa.

Pros&Cons dell'utilizzo di un PC Dedicato /2

Questo può causare indirettamente diverse problematiche di sicurezza… i motivi sono molto semplici e quasi ovvi:

- Utilizzo del PC da parte degli altri membri della famiglia: la moglie su Facebook, la figlia su Instagram, il figlio con il gaming on-line, il marito su… XXX ☺

- Battute a parte, ogni utilizzatore si espone a molteplici rischi, in differenti contesti, scenari e piattaforme, derivanti da un gran numero di "Vettori di Attacco".

I rischi ai quali siamo esposti

Privo di adeguati strumenti di difesa ed a causa degli utilizzi ludici mischiati a quelli professionali, il PC si espone principalmente a:

- Contagio attraverso il browser a causa di siti e pagine infette
- Diventare vittime di phishing e campagne mirate
- Furto credenziali e-banking
- Furto login e password intranet e/o accesso VPN aziendale
- Installazione non autorizzata di keylogger
- Botnet con esfiltrazione dei dati
- Botnet per azioni criminose (ad esempio, attacchi DDoS) e conseguenti responsabilità legali

Esempi di utenti già colpiti.../1

Files **gia' esfiltrati** dalla botnet

Date

13 Mar 2020, 17:40pm

IP 151.53.xxx.xx Bot

Country **Italy**

Machine ID 6ade8f7c-f0cf-41c3-ab7e-4aexxxxxxxxx

Hostname **DESKTOP-MNXXYY (aless)**

Botnet **plist_202003_arkei**

Address **Italy,Naples,IT**

Request Type **Browser history**

Software **GoogleChrome**

Telegram/D877F783D5D3EF8C013 Mar 2020, 17:40pm

Files/desctop.zip13

Mar 2020, 17:40pm Telegram/map113 Mar 2020, 17:40pm

Cookies/Google Chrome_Default.txt

13 Mar 2020, 17:40pm

Esempi di utenti già colpiti.../2

History/Google Chrome_Default.txt

https://**postepay.poste.it/gamma/carte-postepay.html Carte** Postepay
https://www.skidrowcodex.net/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
https://www.skidrowcodex.net/page/2/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
https://www.skidrowcodex.net/page/3/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
https://www.filecrypt.cc/pax/iox.html Redirect
https://**it.usenet.nl/registrazione**/?utm_source=AF%5FTA%5F103197&utm_medium=AFNE&utm_campaign=438993&utm_content=0%5F1
https://sofifa.com/ Giocatori FIFA 20 3 mar 2020 SoFIFA
https://www.hidemyass.com/it-it/proxy Proxy Web gratuito | Navigazione online anonima | Hide My Ass!
https://www.hidemyass-freeproxy.com/process/it-it GamesTorrents | Descargar Juegos Torrent Gratis
https://www.likevisibility.com/ **Comprare Follower Instagram, Fan Facebook LikeVisibility**
https://postepay.poste.it/ppay/private/pages/index.html Accedi o Registrati
http://**gmail.com/ Posta in arrivo (4.186)** - xxxxxxxxxxxxxxxx@gmail.com - Gmail

Esempi di utenti già colpiti.../3

Informazioni esfiltrate dalla botnet

Date:	Fri Mar 13 17:40:12 2020
MachineID:	6ade8f7c-f0cf-41c3-ab7e-4ae80923ad90
GUID:	{705680a4-aa51-11e9-9ffc-806e6f6e6963}
Path:	**C:\Users\aless\AppData\Local\Temp\xhE6axAk.exe**
Work Dir:	C:\ProgramData\I7M1LBMXQ1AH5JN18WWL5LPBV
Windows:	Windows 10 Home [x64]
Computer Name:	**DESKTOP-MNXXXXX**
User Name:	**aless**
Display Resolution:	**1920x1080**
Display Language:	it-IT
Keyboard Languages:	Italiano (**Italia**) / Inglese (Stati Uniti d'America)
Local Time:	13/3/2020 17:40:12
TimeZone:	UTC1
[Hardware]	
Processor:	AMD Ryzen 5 2400G with Radeon Vega Graphics
CPU Count:	8
RAM:	7092 MB
VideoCard:	AMD Radeon(TM) RX Vega 11 Graphics
[Network]	
IP:	**151.53.xxx.xx**
Country:	Italy (IT)
City:	**Ercolano (Campania)**
ZIP:	80056
Coordinates:	40.8112,14.3528
ISP:	INFOSTRADA (WIND Telecomunicazioni S.p.A)

Esempi di utenti già colpiti.../4

"Lo studente"

- https://web.**whatsapp.com**/ https://web.whatsapp.com/
- https://www.**subito.it**/ Subito: compra e vendi vicino a te - Annunci gratuiti
- https://www.**zooplus.it/checkout**/overview Alimenti e accessori per cani, gatti e animali domestici | zooplus
- https://www.**iliad.it**/account/ iliad - Benvenuto in iliad
- https://www.samsung.com/it/ Samsung **Italia** | Smartphone | Elettrodomestici | TV
- https://**iostudio.pubblica.istruzione.it/voucher MIUR** - Ministero dell'Istruzione, dell'Università e della Ricerca
- https://iam.pubblica.istruzione.it/iam-ssum/sso/l**ogin?goto=**https%3A%2F%2Fiostudio.pubblica.istruzione.it%3A443%2Fvoucher MIUR - Ministero dell'Istruzione, dell'Università e della Ricerca
- https://www.google.com/search?q=**minecraft**+server&oq=minecraft+server&aqs=chrome..69i57j0l5.22155j0j7&sourceid=chrome&ie=UTF-8 minecraft server - Cerca con Google
- https://www.minecraft.net/it-it/download/server/ **Download server for Minecraft** | Minecrafta

Esempi di utenti già colpiti.../5

Browsers/AutoComplete/MozillaFireFox_pip323o3.default-1485616945327-1556918316871.txt

(funzionalità “autocomplete”)

email_address hxxxxxx@googlemail.com
username MxxxxiMxxxx
vb_login_username isac
if false
emailconfirm hxxxxx@googlemail.com
ev Microdata
log x1337
id 673040592830731
LOGIN_USER **admin**
cd[Schema.org] []
phone 011711212786
ips_username x1234x
email antonia-x-xxxx@web.de

Date	18 May 2019, 9:54am
IP	**91.192.xxx.xx**
Bot Country	Switzerland
Machine ID	a21b684-ef82f2e6-65ae38f1
Hostname	M44xx(matzereh)
Botnet	**logs08092019/LogsOtrabotka**
Address	Switzerland,CH
Request Type	**Browser autocomplete**
Software	MozillaFirefox

email Jennifer Villegas
btcinput 0.00271428
email jennifervillegas
subject password is
btcinput 0.00267608
website @x1337xx
btcinput 0.00338736

Finta Email da Apple

II tuo lD AppIe e stato utilizzato per accedere a i..

Mittente Apple Data 2020-01-26 17:48

Per proteggere la tua privacy, le immagini remote di questo messaggio sono state bloccate.
Visualizza immagini

Gentile Cliente,

il tuo ID Apple è stato utilizzato per accedere a iCloud da un browser web.

Data e ora: **26 gennaio 2020, 17:36 PDT**

Indirizio IP , Luogo: **178.213.13.136, Russia - Moscow**

Se recententemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recententemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro

Finta Email da Apple

Corpo del Messaggio

Gentile Cliente,

il tuo ID Apple è stato utilizzato per accedere a iCloud da un browser web.

Data e ora: **26 gennaio 2020, 17:36 PDT**

Indirizio IP , Luogo: **178.213.13.136, Russia - Moscow**

Se recentemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recentemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro possa aver eseguito l'accesso al tuo account, clicca sul link seguente per riavviare il informazioni Il mio ID Apple.

Cordiali saluti,

Supporto Apple

Finta Email da Apple

Ma in realtà...

Return-Path: <app@rep.com>
X-Original-To: selene@giupponis.it
Delivered-To: selene@giupponis.it
X-No-Auth: unauthenticated sender
Received: from lipik (localhost.localdomain [127.0.0.1])
by lipik.liponet.sk (Postfix) with SMTP id A91D829BBA
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:03 +0100 (CET)
X-No-Auth: unauthenticated sender
Received: from lipik.liponet.sk (www.liponet.sk [195.168.209.56])
by in-6.smtp.seeweb.it (Postfix) with ESMTP id 73B49140114C
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:04 +0100 (CET)
Received: from lipik (localhost.localdomain [127.0.0.1])
by lipik.liponet.sk (Postfix) with SMTP id A91D829BBA
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:03 +0100 (CET)
Subject: II tuo lD AppIe e stato utilizzato per accedere a iCloud da un browser web
Date: Sun, 26 Jan 2020 17:48:03 +0100
Mime-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
To: selene@giupponis.it
Content-Transfer-Encoding: quoted-printable
From: Apple<app@rep.com>
Message-Id: <20200126164803.A91D829BBA@lipik.liponet.sk>
X-Virus-Scanned: clamav-milter 0.99.2 at in-6.smtp.seeweb.it
X-Virus-Status: Clean
X-Spam-Status: No, score=2.5 required=7.0 tests=GB_GOOGLE_OBFUR,
GOOG_REDIR_HTML_ONLY,HTML_MESSAGE,HTML_MIME_NO_HTML_TAG,
HTML_TEXT_INVISIBLE_FONT,MIME_HTML_ONLY,PDS_DBL_URL_TNB_RUNON,SPF_HELO_NONE,
SPF_NONE autolearn=disabled version=3.4.0
X-Spam-Level: **
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on in-6.smtp.seeweb.it

Fatevi delle domande, dateci delle risposte

Quanto ritiene probabile il rischio di poter essere vittima di una frode o un raggiro tramite Internet (cyber attack)?
- Molto probabile
- Abbastanza probabile
- Non molto probabile
- Molto improbabile
- Non lo so / nessuna risposta

Per quale ragione?
- Ritengo di avere attuato le opportune precauzioni
- Ritengo che i servizi a cui accedo siano ragionevolmente protetti
- Non ritengo di essere un possibile obiettivo di un cyber attack
- Non ritengo che il cyber attack sia una minaccia concreta
- Non lo so / nessuna risposta

Le è capitato di subire un tentativo di frode tramite telefono o messaggio negli ultimi 12 mesi?
- Si
- No

Pensi all'ultima volta in cui ha ricevuto un'email di phishing, come si è comportato?
- L'ho immediatamente riconosciuta e cancellata
- Ho cliccato sul link dell'email
- Ho cliccato sul link e dopo ho inserito I dati richiesti
- Niente, non ho fatto nulla
- Non so / non ricordo

Sui suoi dispositivi informatici (PC, smartphone, tablet…) utilizza sistemi di protezione contro virus o attacchi hacker?
- Si, su tutti i miei dispositivi e ne verifico il costante aggiornamento
- Si, su tutti i miei dispositivi ma non ne verifico il costante aggiornamento
- Si, ma non su tutti i miei dispositivi
- No, non li utilizzo
- Non so / nessuna risposta

Quando riceve un allegato non atteso tramite e-mail da un familiare, conoscente o amico, come si comporta?
- Non apro mai allegati inattesi e verifico con il mittente
- Verifico che l'allegato non contenga virus, quindi lo apro
- Apro l'allegato solo se non mi sembra sospetto
- Apro sempre gli allegati se ne conosco il mittente
- Non so / nessuna risposta

Quando accede a reti Wi-Fi pubbliche (es. ufficio, comune, bar, sala d'attesa…) come si comporta?
- Non accedo mai a reti Wi-Fi pubbliche per evitare rischi
- Accedo solo a reti Wi-Fi protette da password
- Accedo a reti Wi-Fi solo se conosciute
- Accedo a reti Wi-Fi e non mi assicuro mai dell'affidabilità
- Non so / nessuna risposta

Consigli per il SysAdm e gli User (e gli studenti!)

- **Se e dove possibile..**

Ad esempio, laddove l'azienda abbia già dotato il dipendente di laptop o desktop dedicato, imporre con i dovuti strumenti le **restrizioni necessarie** (ad esempio: **login come User** e non come Administrator, **hardening** della macchina, etc.)

- **In alternativa:**

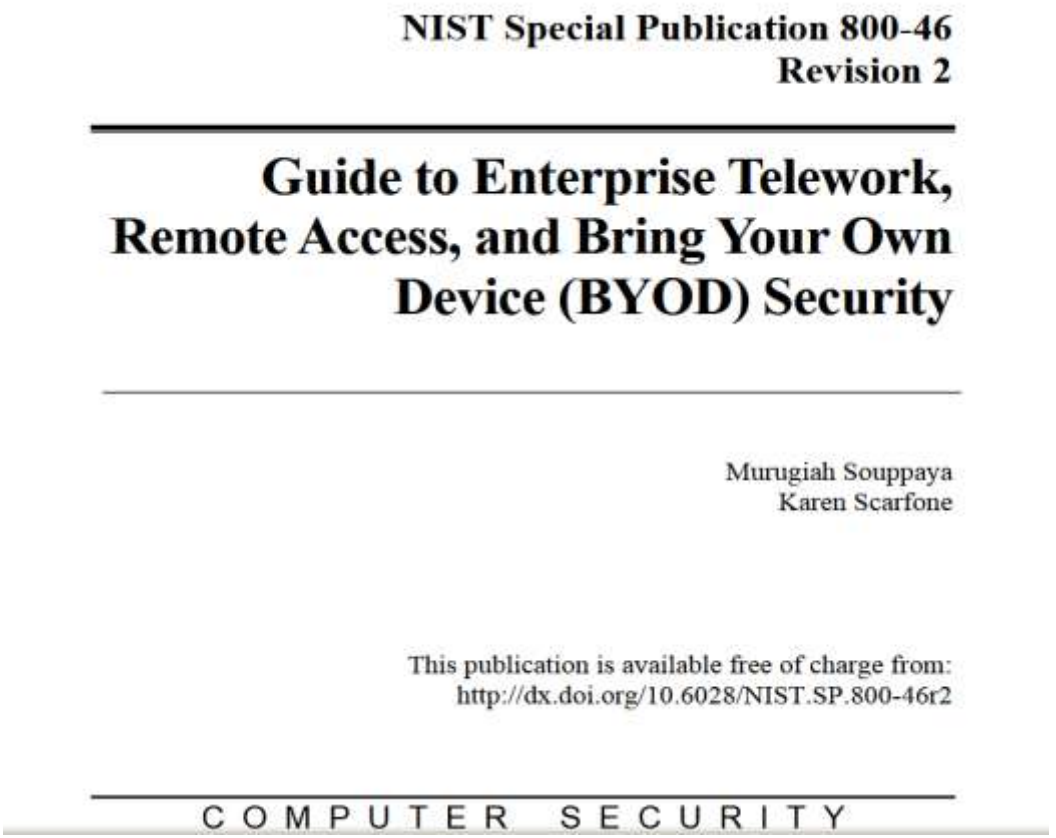
Operare da un **ambiente virtuale**: installazione di una Virtual Machine (per esempio VirtualBox) per **contenere** / **mitigare** / **abbassare** / **evitare** il rischio, ed eventuali **incidenti di sicurezza**

Che Fare Come Azienda

- Necessità **penetration testing** al portale aziendale, ai CRM critici, alla rete interna
  - Il presidio in questo periodo è stato alquanto sguarnito (e lo e' ancora!)… ed il cybercrime ne è moooolto **consapevole**!
- Necessità di **VPN dedicate** (e ben configurate)
- Necessità **Endpoint Protection** VS Antivirus
- Necessità **review accordi privacy** e proprietà intellettuale con i dipendenti

Che Fare Come Azienda

- Risulta pero' abbastanza inutile dare consigli "a **spizzichi e bocconi**".
- Stavamo per scrivere una **guida dedicata**, ma prima ci siamo guardati in giro.....
- Nella **moltitudine di pubblicazioni**, piu' o meno belle, spicca la SP 80-46 del **mitico NIST**:
  - Inutile reinventare la ruota: tutto il resto non serve.
  - Impossibile scrivere qualcosa di piu' bello e completo!



NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-46r2

COMPUTER SECURITY

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Che Fare Come Azienda

- Necessità di rafforzare l'ottavo strato della sicurezza: **il fattore umano**

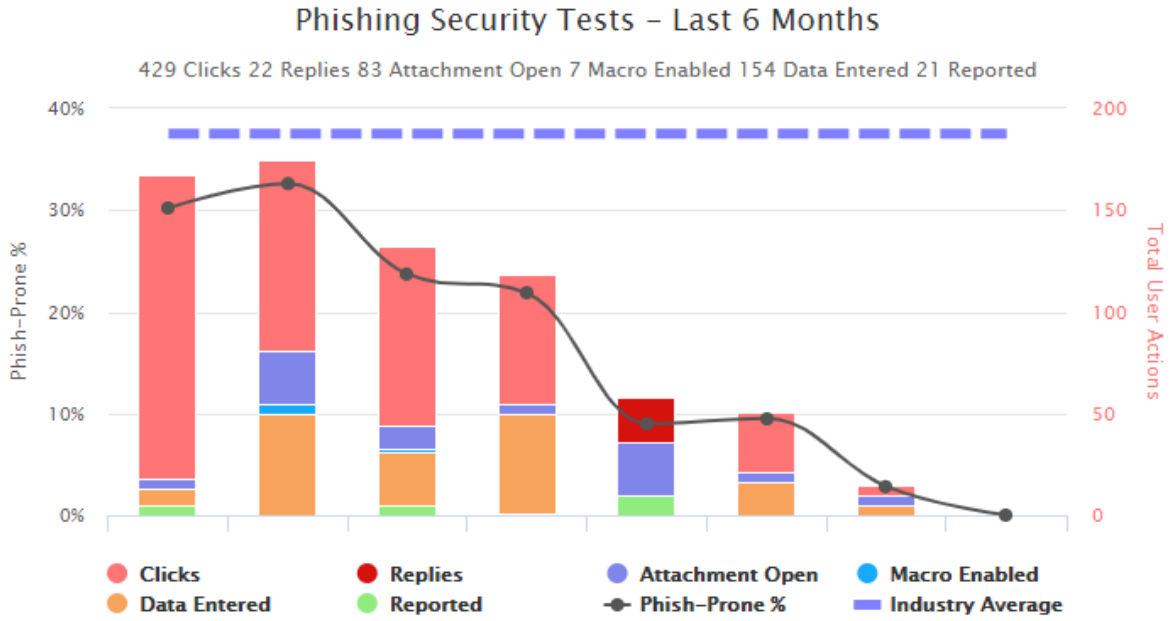
- Il Sistema Operativo 'Uomo' ha bisogno della stessa manutenzione dedicata agli altri sistemi di sicurezza, e cioè:
  - Aggiornamenti/patch continui nel corso dell'anno, e nel corso degli anni

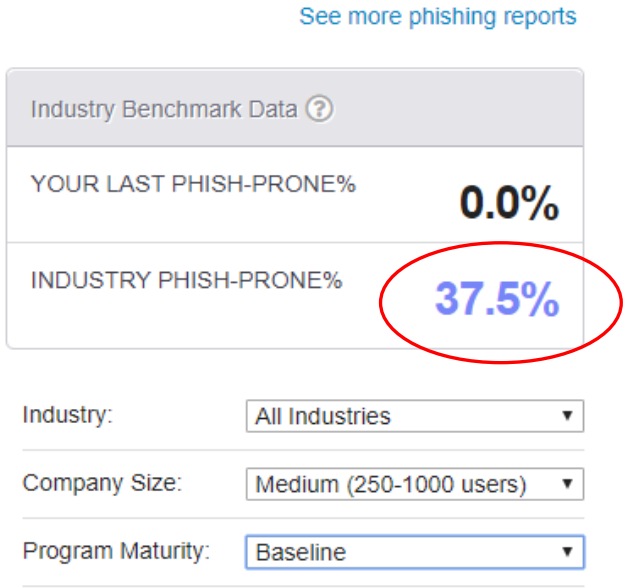
- Solo così quello che oggi è il nostro punto debole potrà diventare la nostra estrema linea di difesa!

Noi abbiamo scelto il sistema di phishing awareness ideato da Kevin Mitnick.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Che Fare Come Azienda

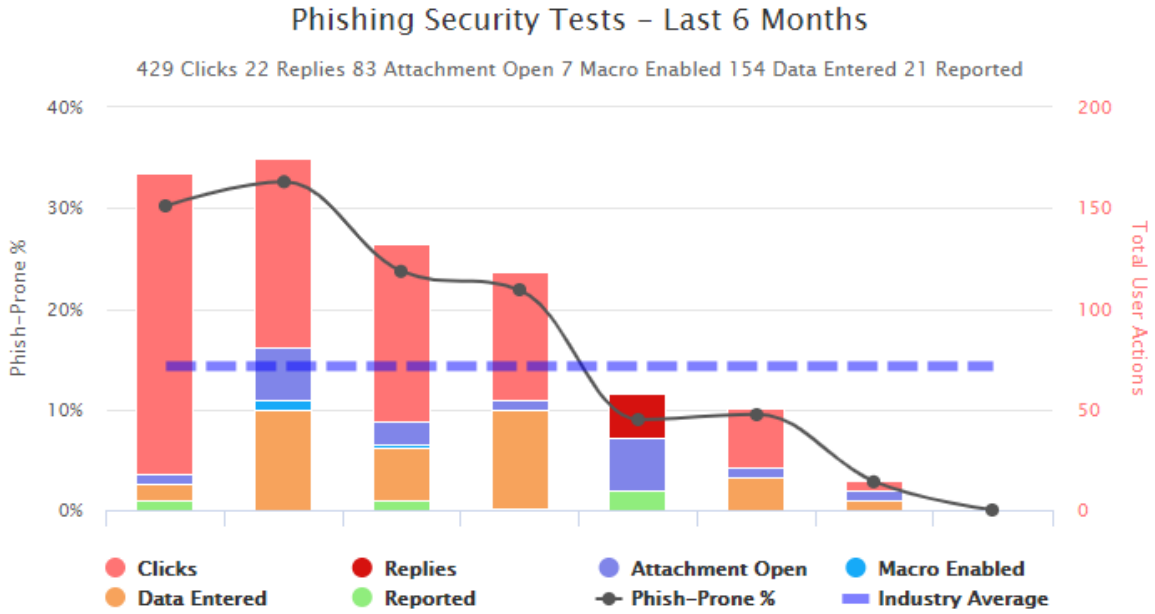


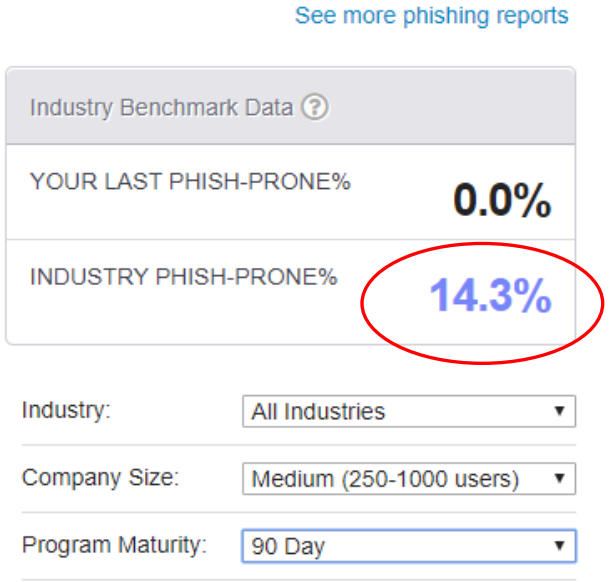


Blind test giorno zero vs il tuo benchmark

Campione: oltre 10 milioni di utenti

Che Fare Come Azienda

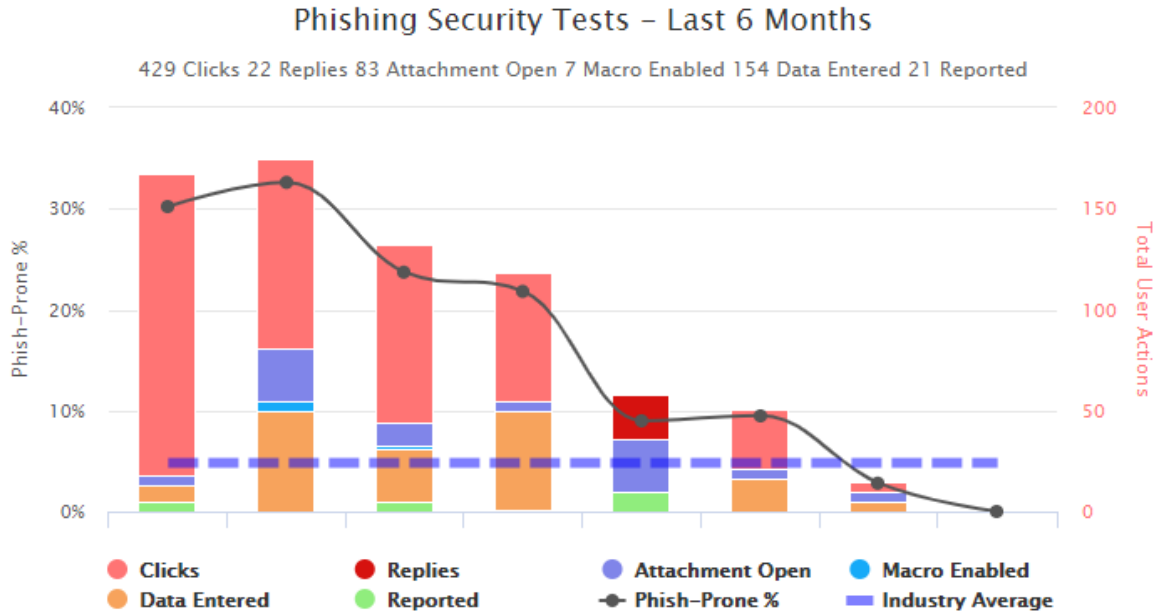


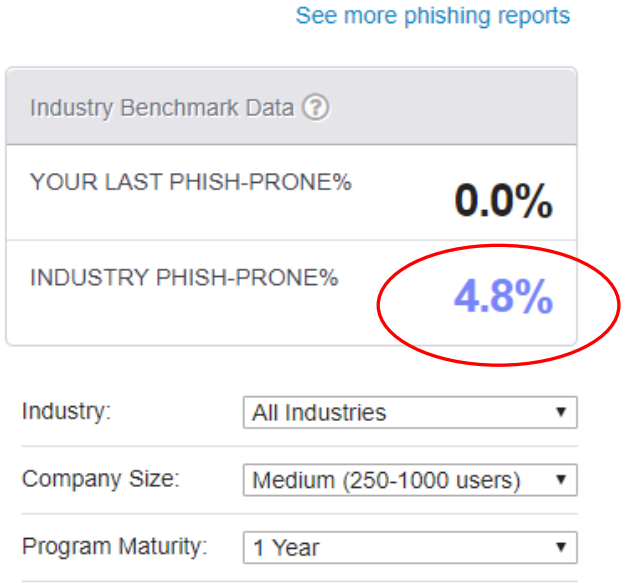


Test dopo 90 giorni vs il tuo benchmark

Campione: oltre 10 milioni di utenti

Che Fare Come Azienda





Test dopo 1 anno vs il tuo benchmark

Campione: oltre 10 milioni di utenti

Come Vi Può Aiutare Lo Stato

Credito d'imposta formazione 4.0

A cosa serve

La misura è volta a stimolare gli investimenti delle imprese nella formazione del personale sulle materie aventi ad oggetto le tecnologie rilevanti per la **trasformazione tecnologica e digitale** delle imprese.

https://www.mise.gov.it/index.php/it/incentivi/impresa/credito-d-imposta-formazione

Come Vi Possiamo Aiutare Noi

Cyber Emergency Kit

Il progetto #unitiperinformare

Un progetto:

- Tutto italiano
- Interdisciplinare
- Slegato da brand o prodotti
- Su base volontaria
- Nasce come GdL “Milano 4 COVID”
- Sviluppato durante la Fase 1 del lockdown

MULTIDISCIPLINA E INFORMAZIONE CONTRO IL COVID19

MILANO FOR COVID

UNITI PER INFORMARE

https://www.unitiperinformare.it/index.php/consensus-report/

Come Vi Possiamo Aiutare noi /1

SLIDE RIMOSSA NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

CONTATTARE I DOCENTI PER AVERE I DETTAGLI, SE VI SERVONO

Come Vi Possiamo Aiutare noi /2

Set di Test per verificare…. (Domain Spoof Test, Weak Password Test, Free Phishing Alert Button)

TESTO RIMOSSO NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

CONTATTARE DIRETTAMENTE I DOCENTI PER AVERE I DETTAGLI, SE VI SERVONO

Come Vi Possiamo Aiutare noi /3

- **EPP per i vostri asset digitali**

TESTO RIMOSSO NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

CONTATTARE DIRETTAMENTE I DOCENTI PER AVERE I DETTAGLI, SE VI SERVONO

Recap del “buon senso” /1

✓ **Non esistono** “fortune immediate”: eredita’ di parenti lontani e deceduti, lotterie, etc.

✓ **Esaminate con cura** il MITTENTE delle email sospette (ed anche di quelle “strane” come richieste, sebbene non “sospette a prima vista”)

✓ **Leggete** sempre **con attenzione** il TESTO delle email che vi arrivano: lingua, forma, contenuto e richieste

✓ **Non fornite mai** Utenza e Password **in risposta ad una email**

✓ Nel **dubbio**, **alzate il telefono** e **richiamate** il “mittente” **a voce**

✓ **Non fornite password, PIN o altre informazioni al telefono** se vi chiamano per chiedervele (appendete e **richiamate voi al numero che gia’ conoscete ed usate abitualmente**)

✓ **Non aprite allegati email** se siete dubbiosi: **contattate l’IT e/o inoltrate loro l’email sospetta**

✓ Per i CFO: **verificate sempre che la parte iniziale** (Country) **dell’IBAN** sia “IT”, o comunque **che corrisponda all’IBAN al quale effettuate bonifici abitualmente** (frode “BEC” o “Man in the Mail”)

Recap del “buon senso” /2

- Raccomandazione: se dovete per forza **utilizzare condivisioni (strumenti di file sharing in Cloud), limitatele**, avendo almeno cura di **impostare una scadenza al link di sharing.**

- **Ribadiamo** ancora una volta le **criticità degli smartphone** dove **tipicamente**, **almeno la posta elettronica aziendale è presente.**

- **Imparate il concetto di “separazione” dei dati aziendali da quelli personali sugli smartphone.**

La tecnologia è bella:

basta usare la testa!

…and a special gift for you all!

Alcuni consigli anti-phishing e “anti-scam” di Kevin Mitnick, l’hacker più famoso del mondo nonché amico storico di Raoul, ed altre risorse gratuite per…

#staysafeonline&offline!

https://www.digitree.it/covid-19-awareness-resource-kit

Q&A session

Stay in Touch (but Stay Safe)!

Raoul “Nobody” Chiesa

Ing. Selene Giupponi

Piero Iezzi

Grazie!

#andratuttobene
#distantimasicuri

SBAcademy
SECURITY THROUGH KNOWLEDGE

Webinar powered by:

Swascan

Cyber Security Awareness (ed implicazioni nello Smart Working)

Che cosa rischiamo online... mentre cerchiamo di restare sicuri off-line?

Relatori
Raoul "Nobody" Chiesa
Ing. Selene Giupponi
Moderatore
Piero Iezzi