AGID | Agenzia per l'Italia Digitale

FormezPA

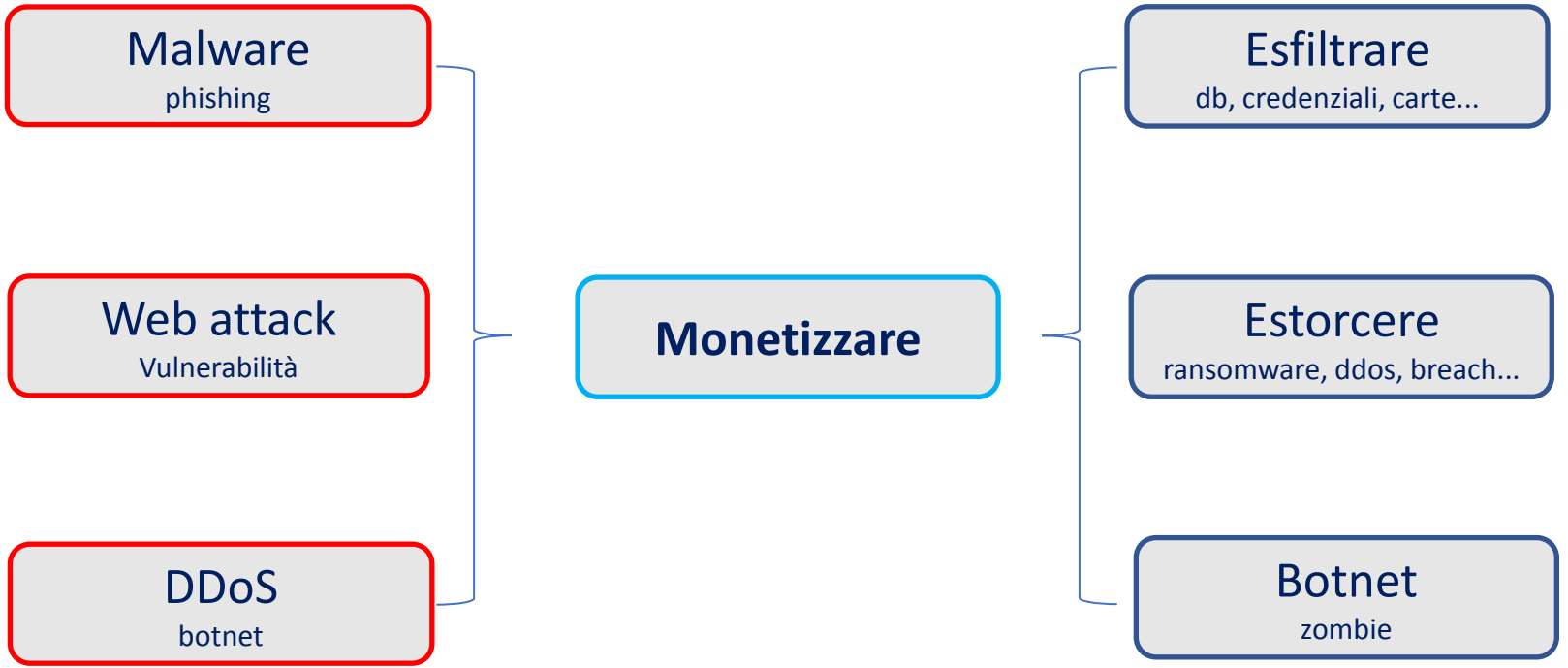
Tipologie di attacchi informatici verso la PP. AA

Gianni Amato, AgID

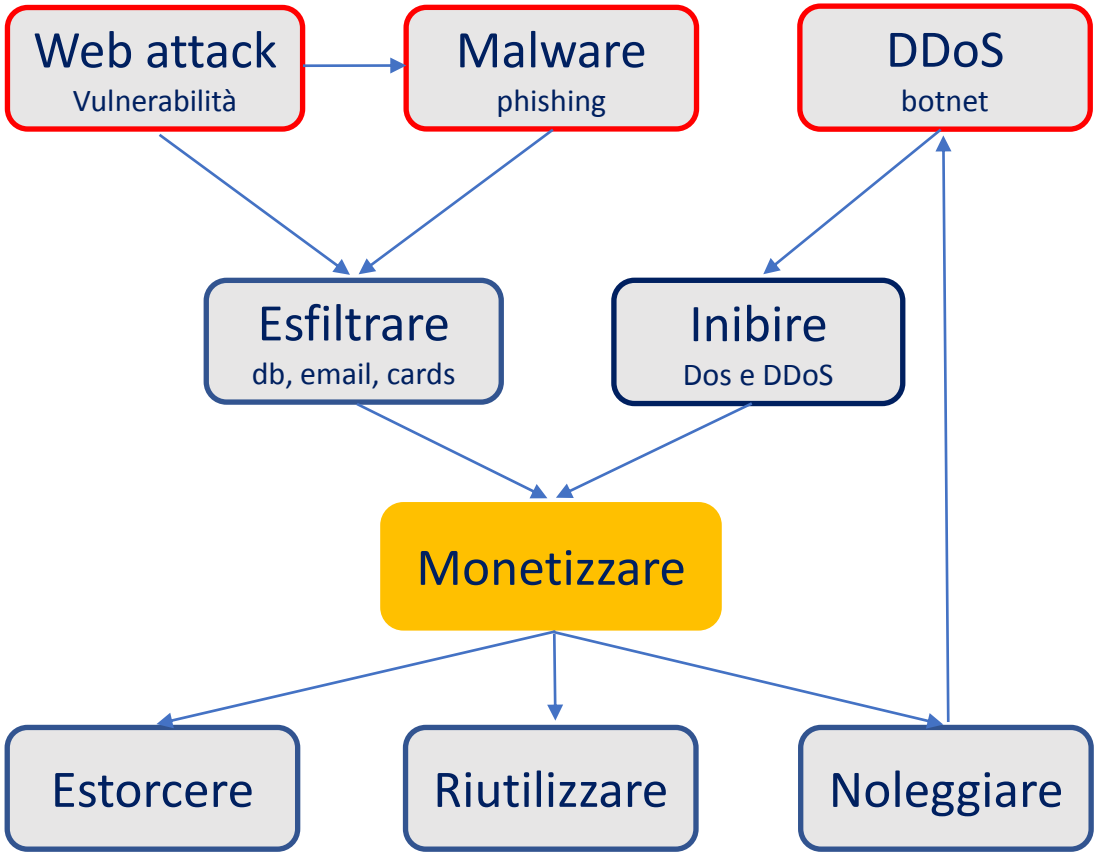
Gli attacchi informatici

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

Panorama delle minacce principali



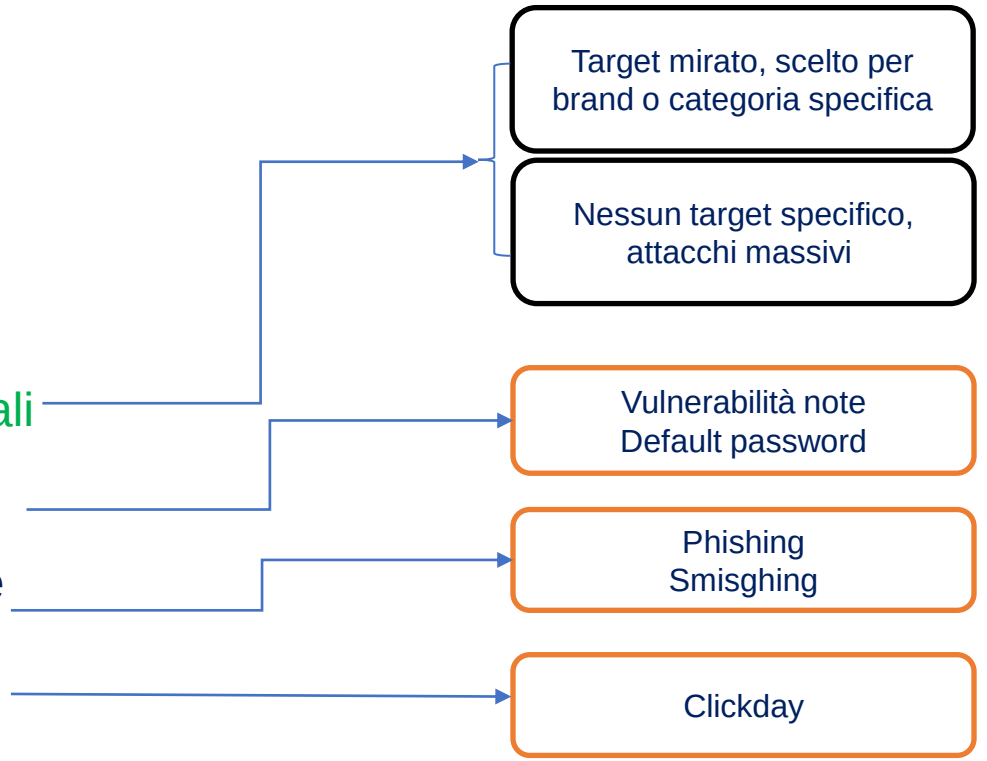
Flusso della minaccia in dettaglio



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



Gli attori: Gli attaccanti

- Criminali di strada → Assoldati o in autonomia
Singoli o in gruppo

- Hacktivisti
- Terroristi
- Paesi (ostili?)

→ con lo scopo di → Sabotare / Spiare / Sorvegliare

- Anarchici
- Ambientalisti

→ Proteste / Sit-in / Mailbombing

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 schiesto 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

La Società della Cura
Fuori dall'economia del profitto.

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 diseguaglianze, 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 diseguaglianze 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 SUCCEDENDO

Da lunedì 10 maggio nel parlamento italiano sarà discussa la co
ripresa delle attività economiche e sociali nel rispetto delle esi
"**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 vaccin
livello globale, con una segnaletica sanitaria modificabile (vacc
il suo enorme potere coercitivo sui non vaccinati. Come in Isra
accedere a strutture e usufruire dei principali servizi essenzia
Covid, saranno sostanzialmente esclusi dalla maggior parte de

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

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

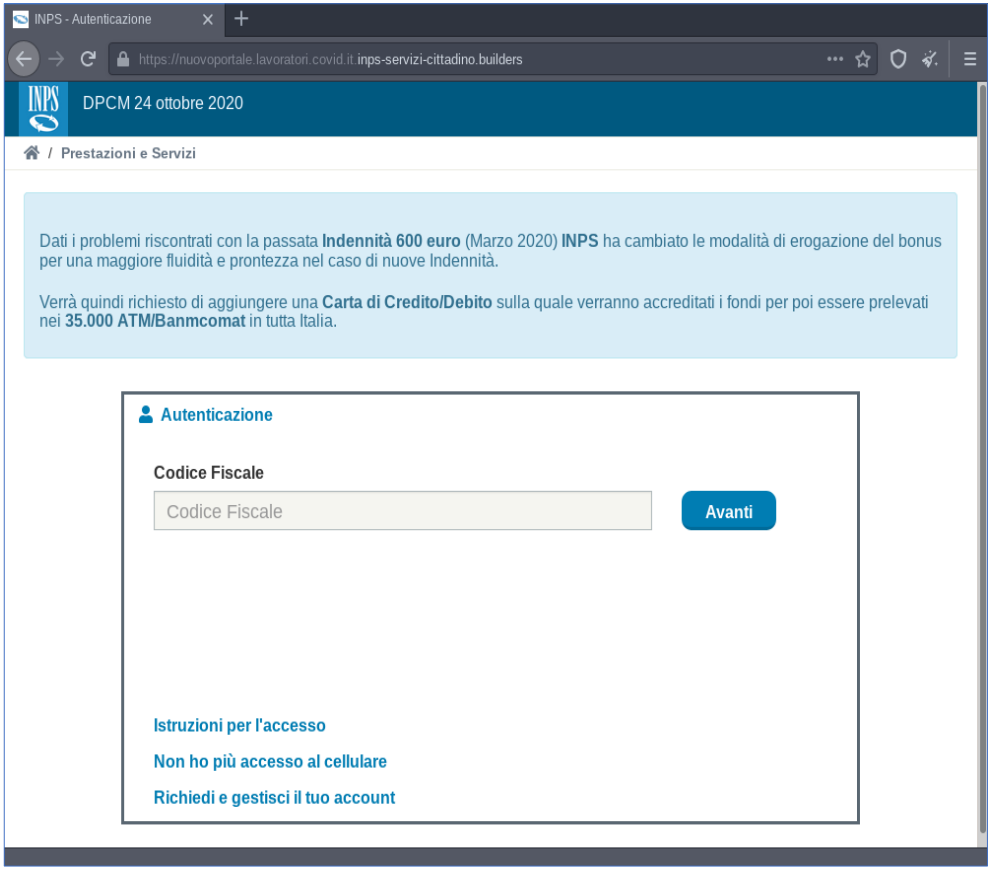
Attraverso questa iniziativa si vuole esercitare una **pressione c**
modificare il loro voto e impedire cosi che possa essere approv

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

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

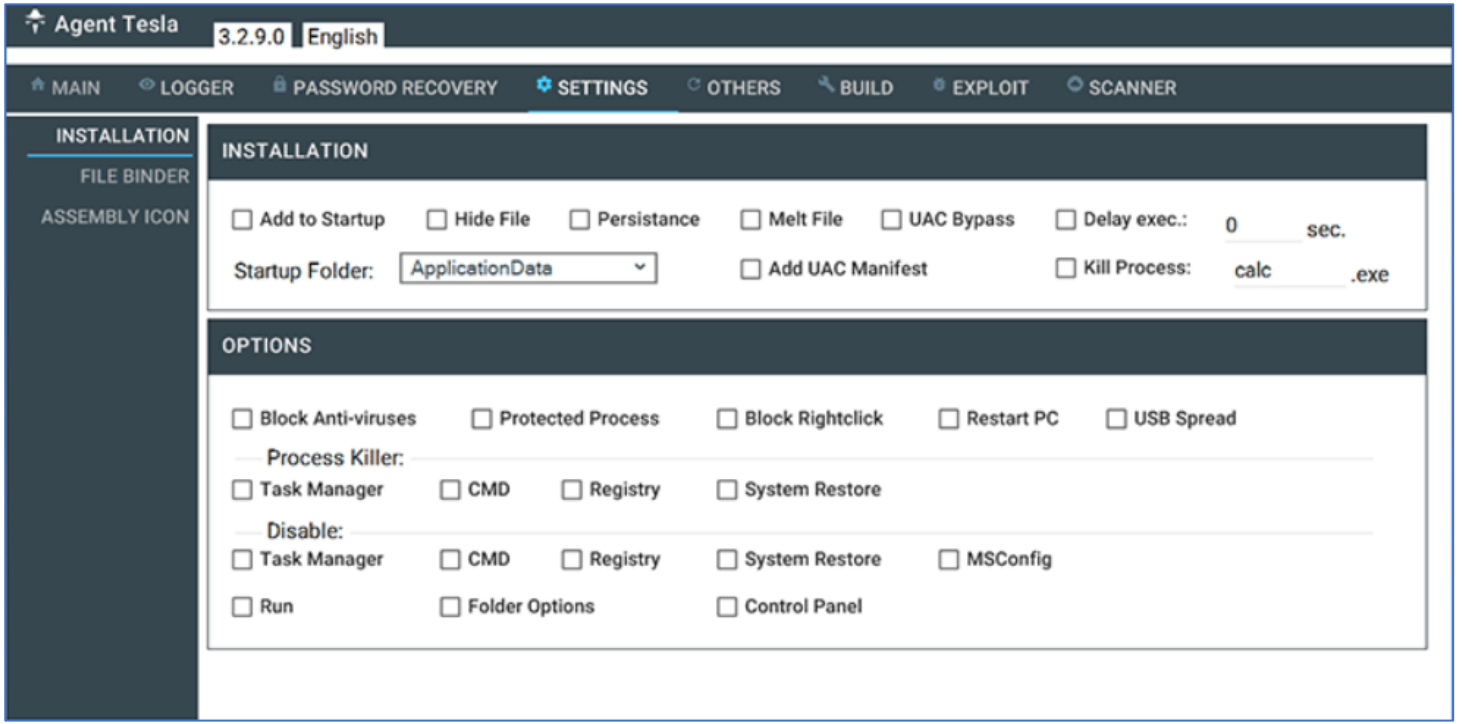
URL:[redacted].it
Username:[redacted]
Password:[redacted]
Application:Firefox

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

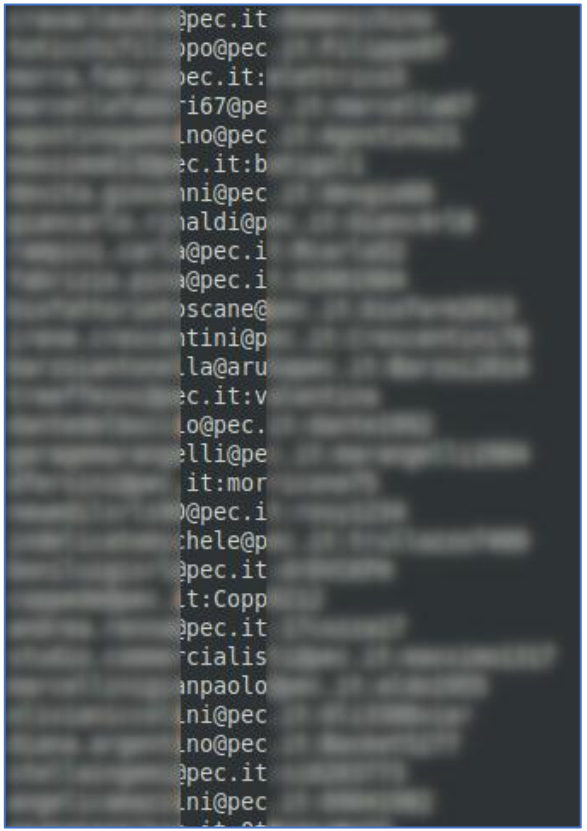
URL:[redacted].istruzione.it
Username:[redacted]
Password:[redacted]
Application:Firefox

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

URL:[redacted].istruzione.it
Username:[redacted]
Password:[redacted]



Posta Elettronica Certificata (e compromessa)



Da [redacted] ☆

Oggetto [redacted] 30/05/21, 23:37

A [redacted] ☆

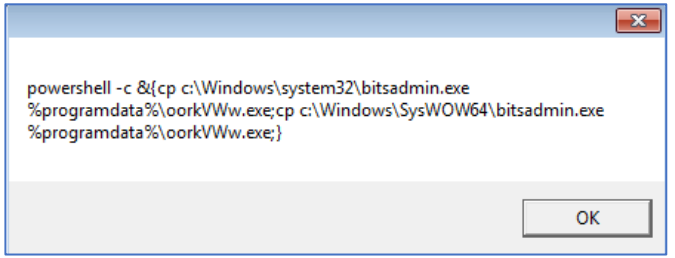
Rispondi | Rispondi a tutti | Inoltra | Altro

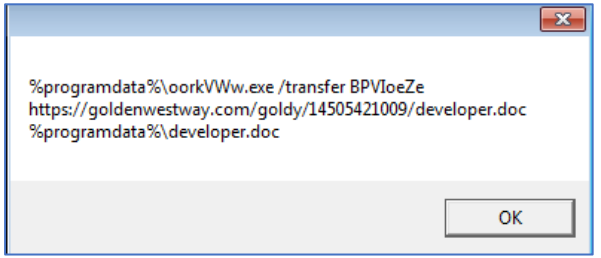
[redacted]

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





Campagne malware via PEC (sLoad)

‹ All dates | January 2021 | February 2021 | March 2021 | May 2021

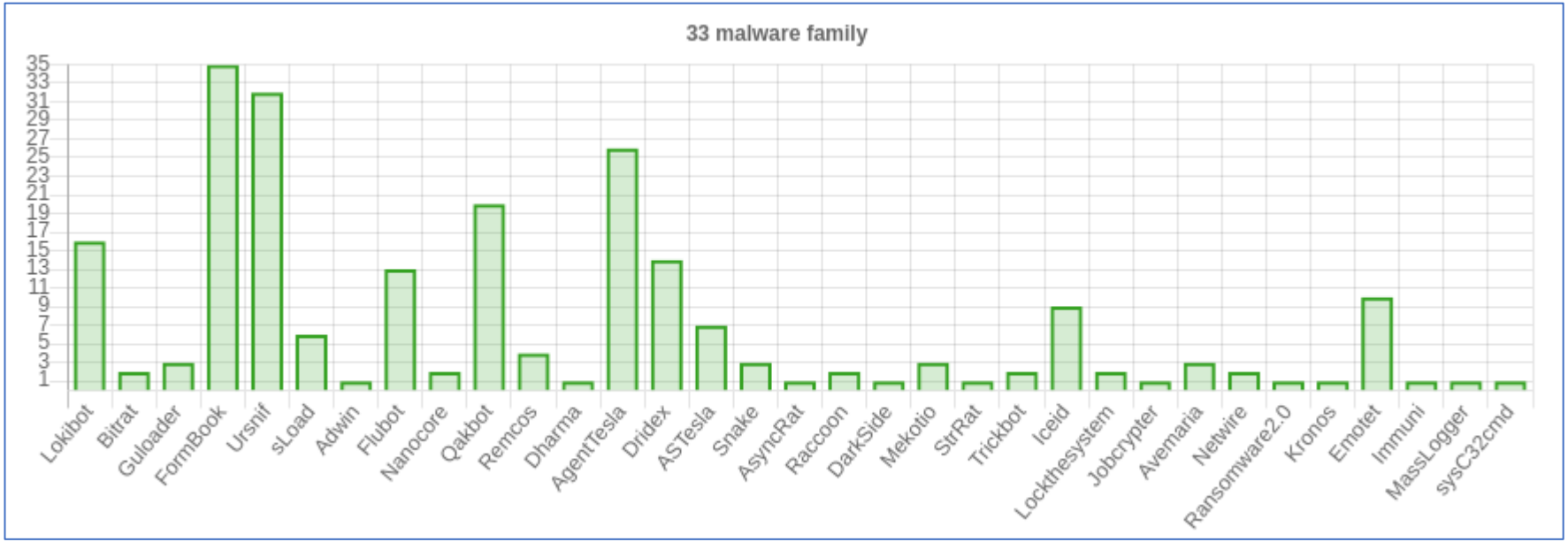
Action: -------- Go 0 of 6 selected

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

6 campaigns

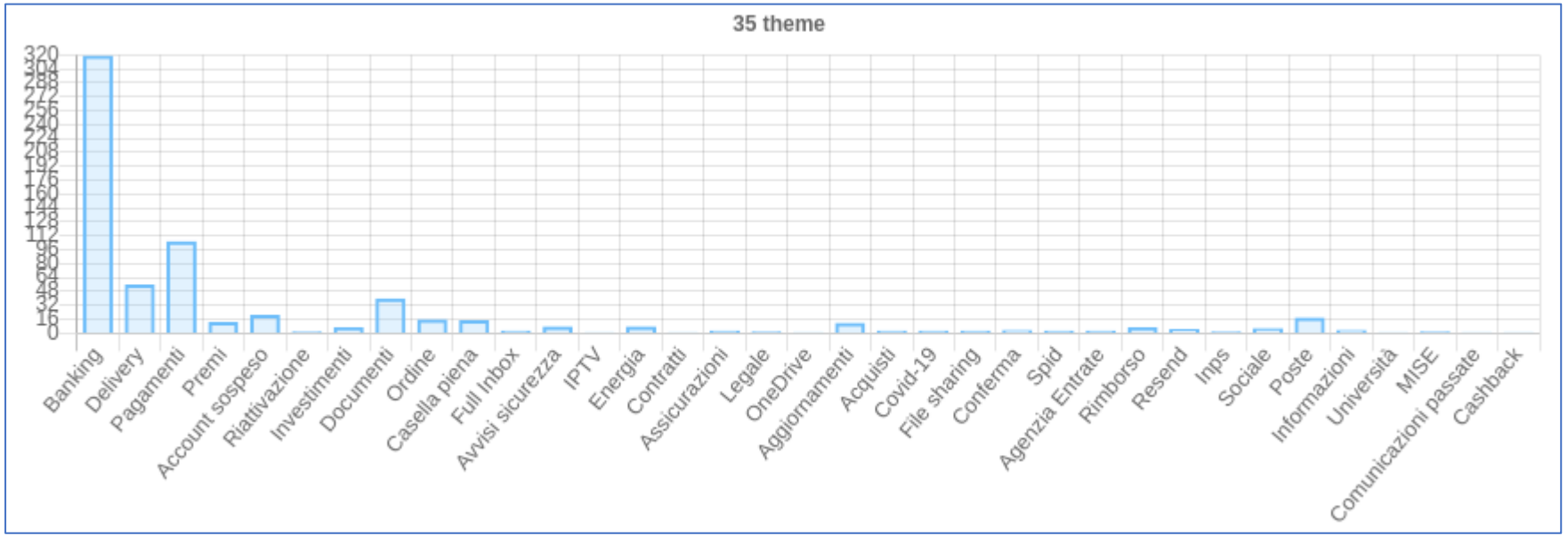
- 6 campagne PEC negli ultimi 6 mesi (2021), unico malware: **sLoad** (https://cert-agid.gov.it/tag/sload/)
- Dal 2019 al 2021 il numero complessivo delle campagne malware veicolate via PEC è **sceso del 90%**
- AGID mette a disposizione una istanza per la **condivisione di IoC tra Gestori** per le campagne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

Malware veicolato in Italia
Gennaio - Giugno 2021

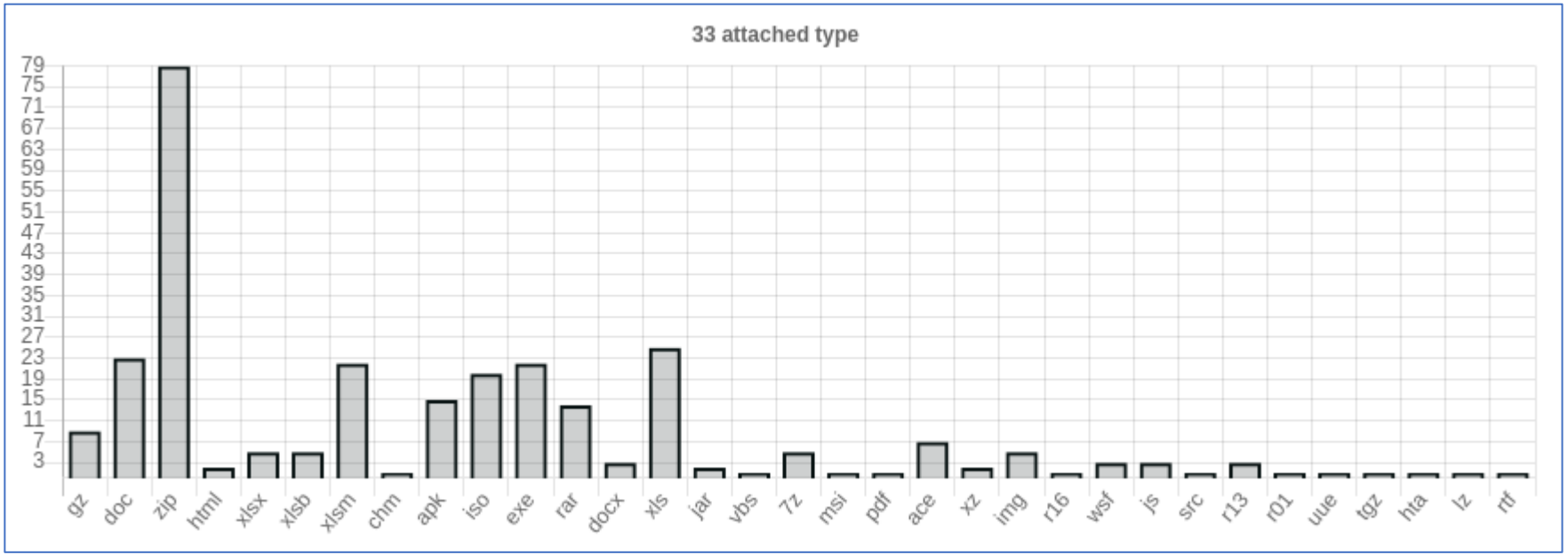


- **706** campagne malevole gestite
- **7803** IoC condivisi

Temi sfruttati nelle campagne malevole
Gennaio – Giguno 2021



Allegati utilizzati nelle campagne malevole
Gennaio – Giguno 2021



Data Breach e/o Data Leak?

Data breach

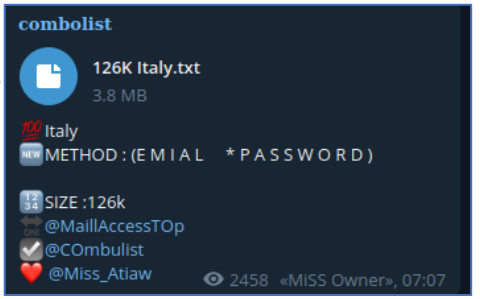
Attacco mirato ad ottenere i dati privati di una organizzazione da parte di una entità non autorizzata.
Un data breach è solitamente dovuto ad una compromissione di un database o di credenziali di accesso ai dati della vittima.

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 *Senstive Data Exposure* o ad errati processi aziendali di *conservazione dei dati*.

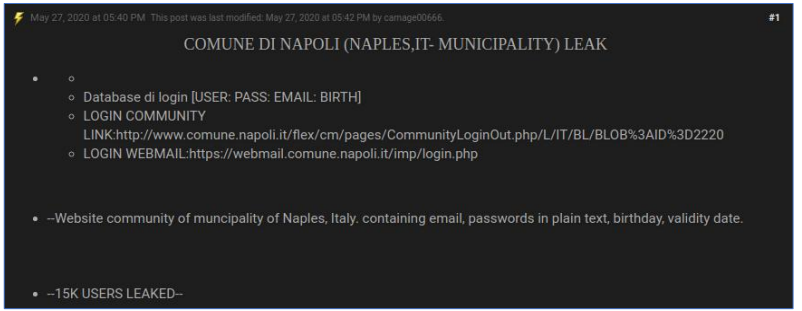
Data leak

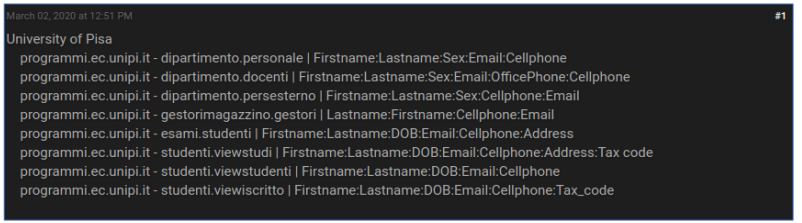
- Sono sempre esistiti ma oggi sembra essere diventata una moda
- È nato un mercato di nicchia in forte crescita
- I black market sono migrati dal dark al deep web e a Telegram
- Prezzi sempre più accessibili



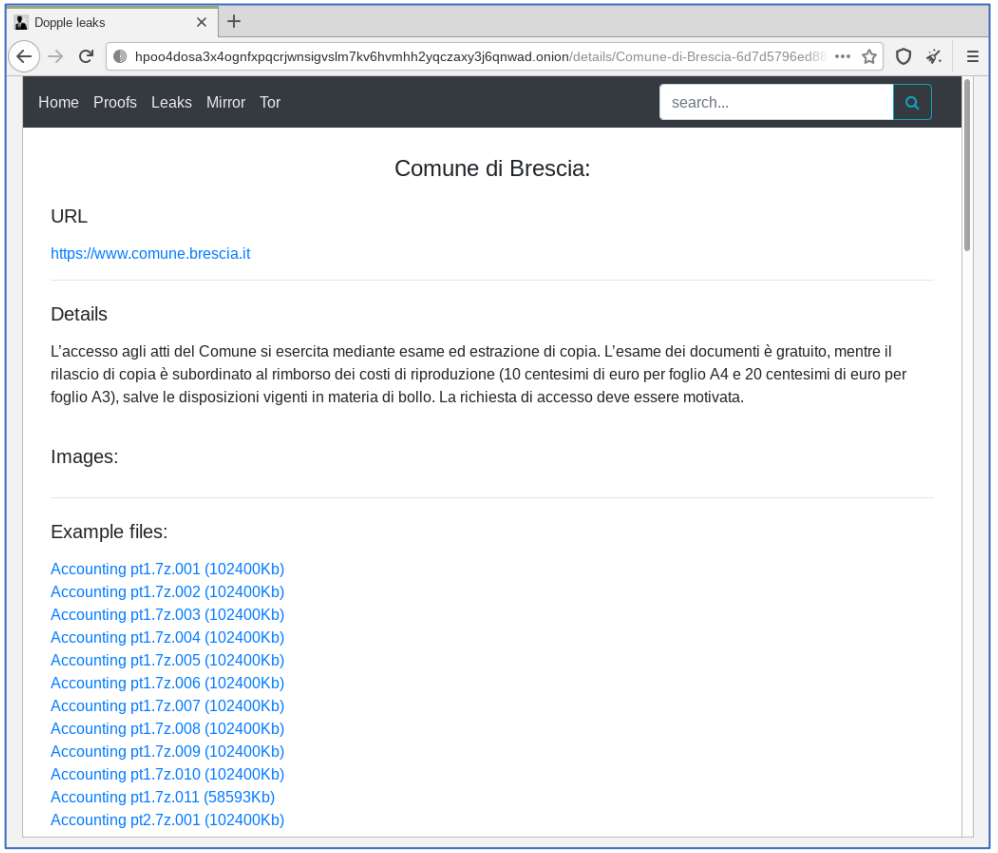
Quali dati in vendita? Ma soprattutto, sono sempre in vendita?

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

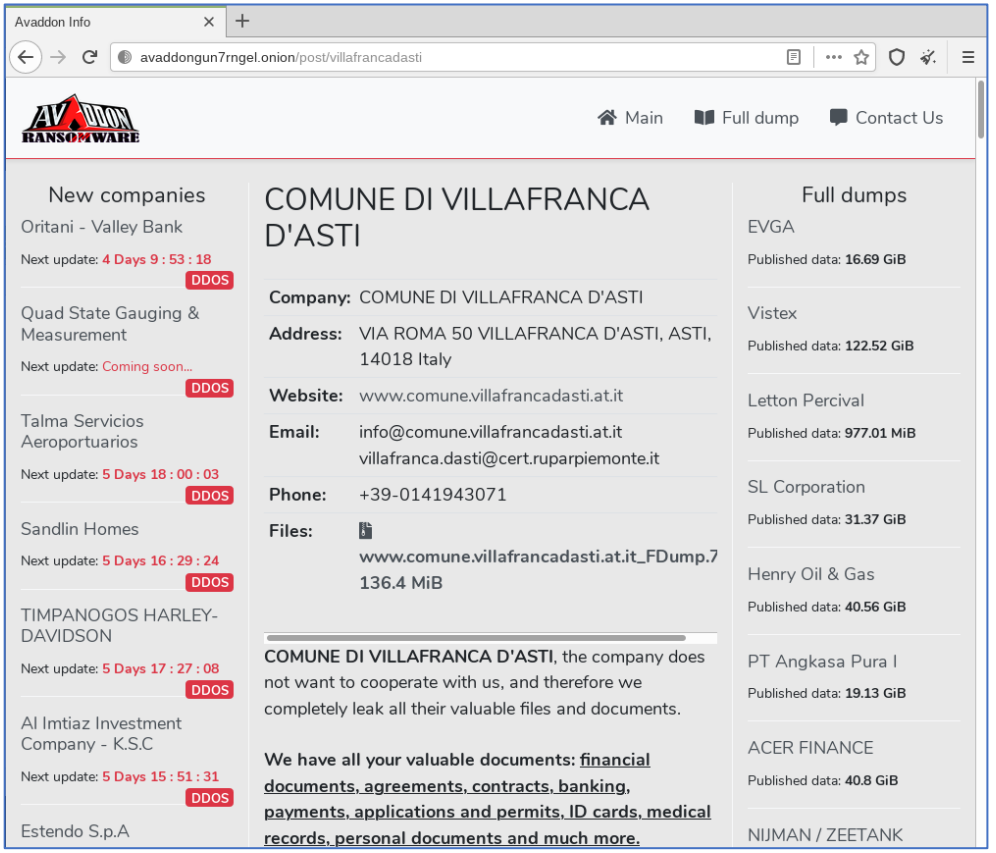




Double extortion

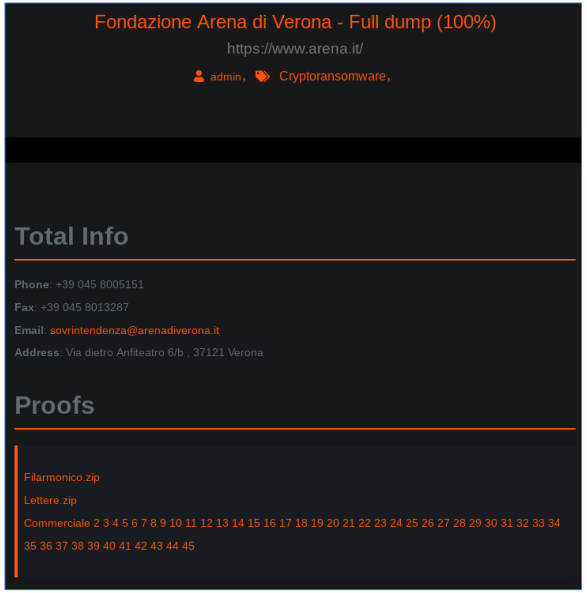


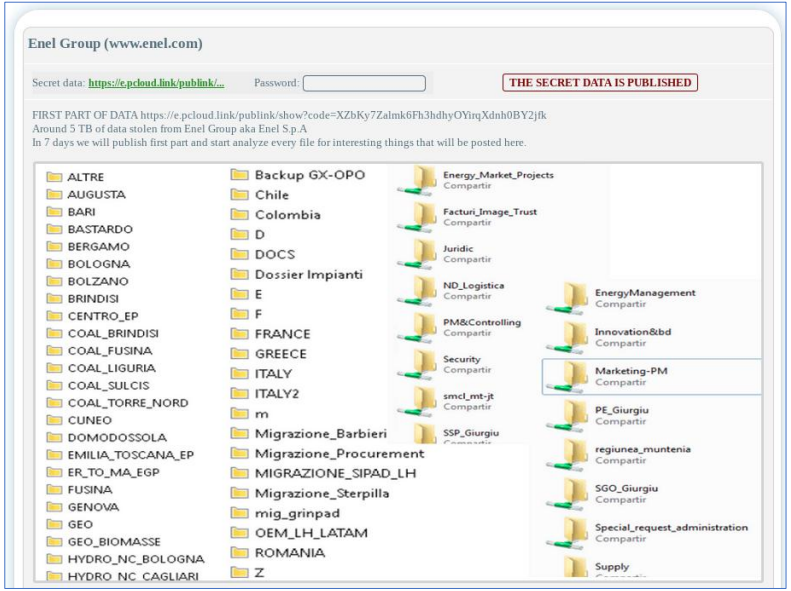
Dopple Ransomware

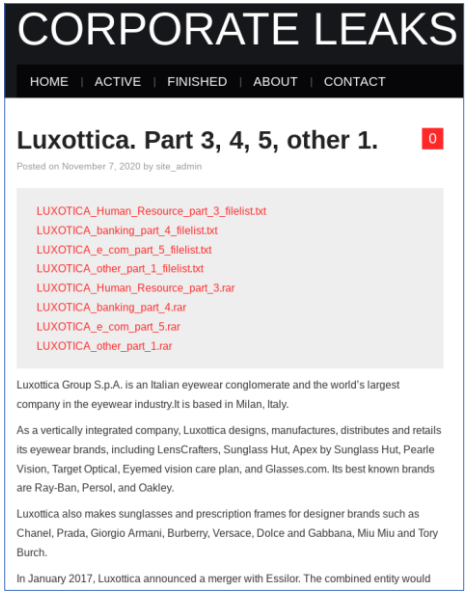


Avaddon Ransomware

Recenti leak con pubblica minaccia di estorsione



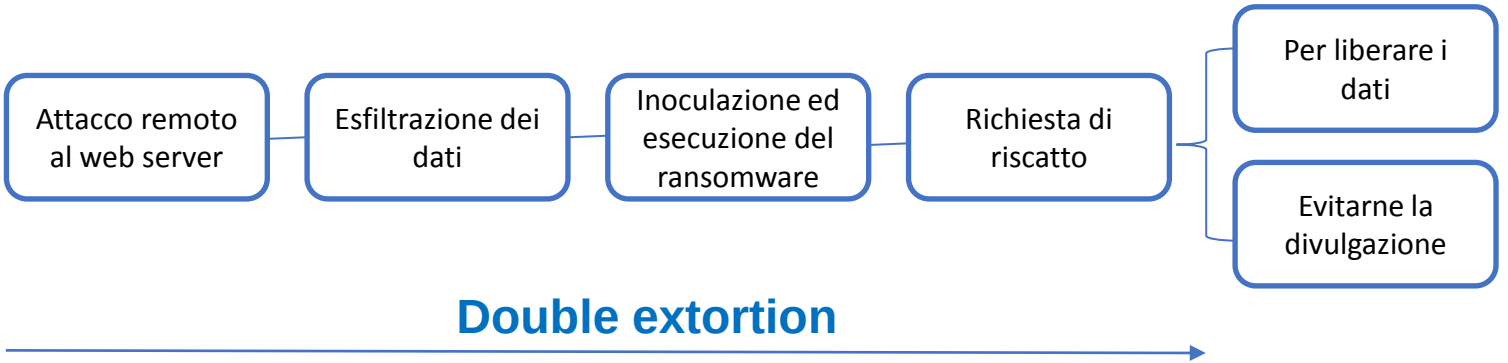




Ransomware + data leak

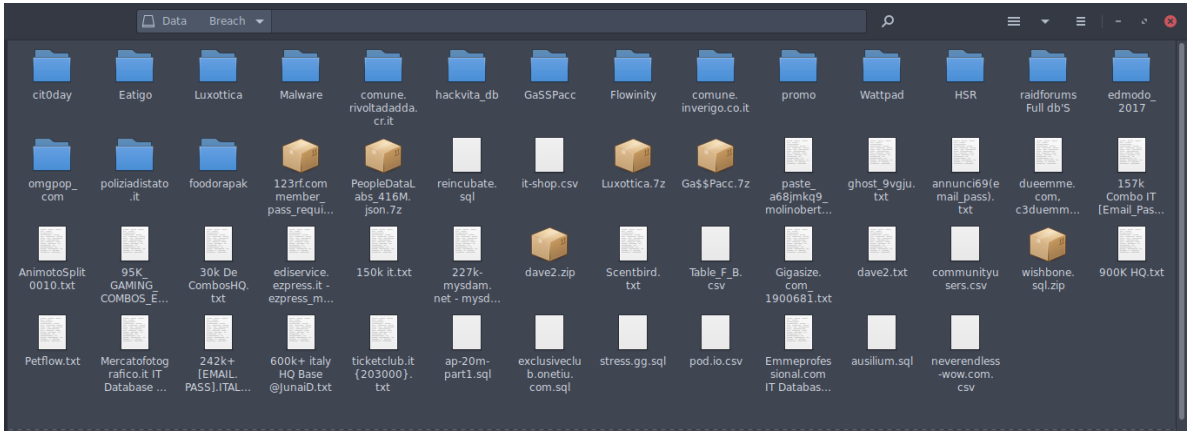
I ransomware sono noti per la cifratura dei dati e la conseguente richiesta di riscatto per liberarli. Di recente si è parlato di data leak causato dai ransomware Maze, NetWalker e Nefilim, ma la realtà è diversa, il Cert-AgID ha analizzato i sample nel dettaglio e dimostrato che questi ransomware non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

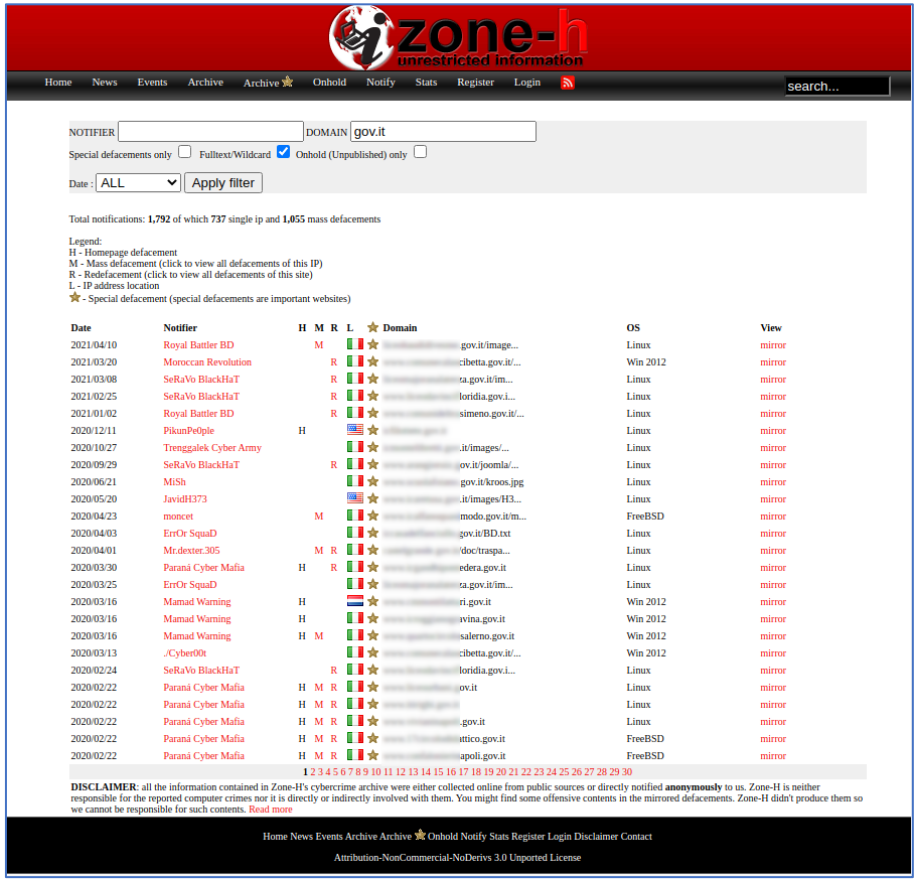


Fake breach e leak

Pubblicazione 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



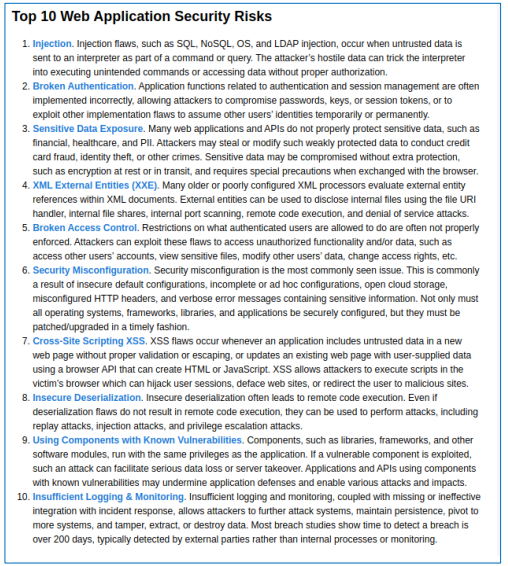
Web Application Attack

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/upgraded 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'
```

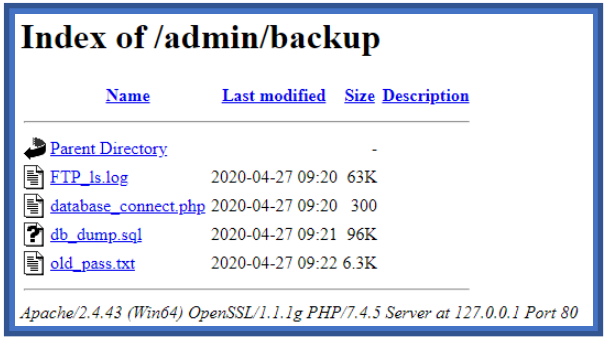
restituirà in output tutti i progetti, compresi quelli con flag visibile = 0

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 sui 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
Parent Directory		-	
FTP_ls.log	2020-04-27 09:20	63K	
database_connect.php	2020-04-27 09:20	300	
db_dump.sql	2020-04-27 09:21	96K	
old_pass.txt	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

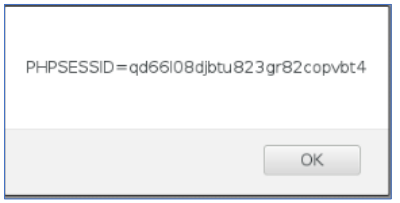
Cross-Site Scripting (XSS) Reflected o Persistent

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.

AGID | Agenzia per l'Italia Digitale

FormezPA

GRAZIE PER L'ATTENZIONE