FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

Progetto Informazione e formazione per la transizione digitale della PA nell'ambito del progetto «Italia Login – la casa del cittadino»

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

Tipologie di attacchi informatici verso la PA

dalle minacce più comuni al mercato delle informazioni

11/11/2021

Gianni Amato
CERT-AGID

Gli attacchi informatici

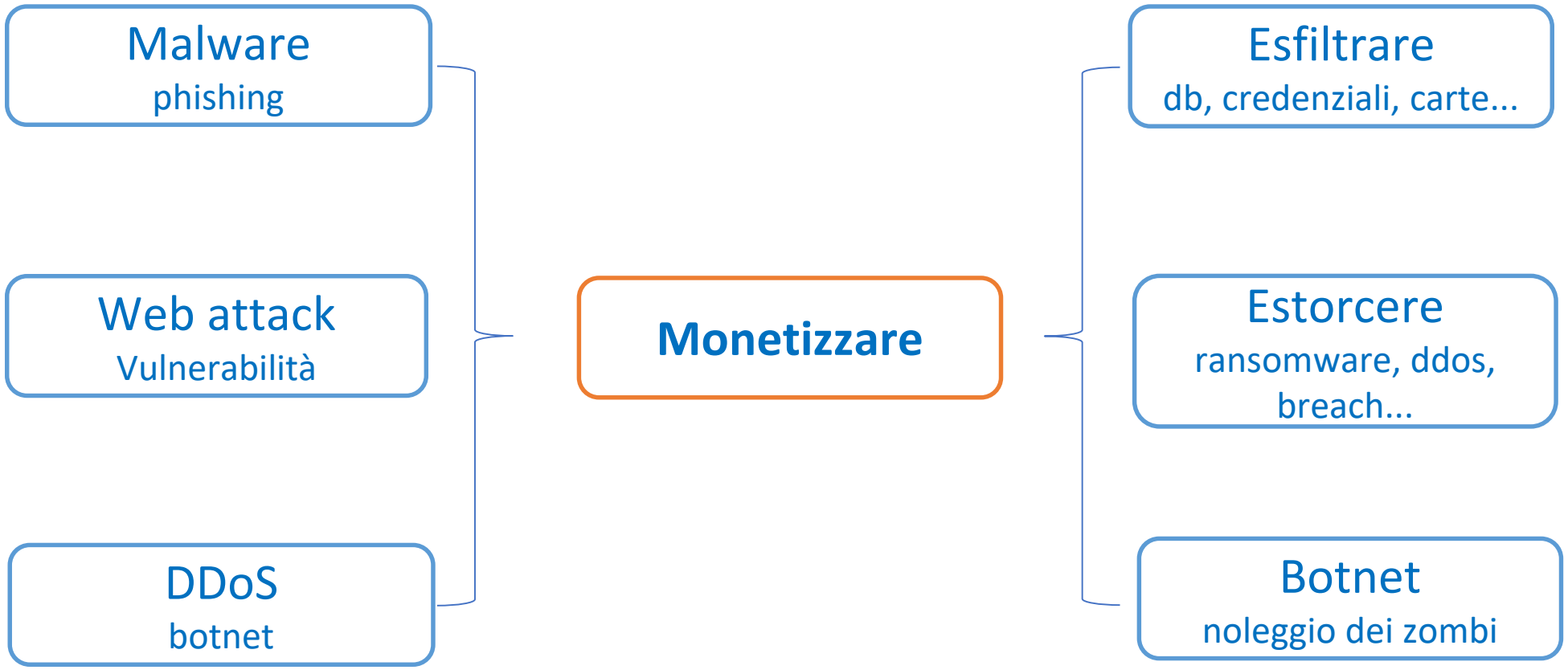
Attività ostili nei confronti di una componente informatica, spesso compiute sfruttando le debolezze della componente umana.

Perché la PA?

Per la tipologia di informazioni trattate e per la «complessa e dispersiva» infrastruttura informatica e organizzativa. Qualche esempio:

- Inconsapevolezza degli **asset esposti**: *quanti sono esattamente? cosa espongono?*
- Ambienti di **test dimenticati**: *esposti senza alcuna protezione.*
- Servizi in **esercizio non aggiornati**: *framework e/o cms obsoleti.*
- Problemi con le **commesse** e il **passaggio di consegna**.
- **Numerosi uffici**, non tutti adeguatamente informati sulle minacce e su come evitarle.

Panorama delle minacce principali



Chi sono gli attori?

Le vittime

Possono essere **scelte** o **casuali**:

- *Target mirato, scelto per brand o categoria specifica.*
- *Nessun target specifico, attacchi massivi.*

Sistemi informatici **esposti** e **vulnerabili**:

- *Vulnerabilità note, password di default.*

Personale **non adeguatamente preparato**:

- *Vittime di phishing/smishing/malware.*

Eventi di **interesse nazionale**:

- Es. click day

Chi sono gli attori?

Gli attaccanti

Criminali:

- *Assoldati o in autonomia.*
- *Singoli o in gruppo.*

Hacktivisti, Terroristi, Paesi ostili:

- *Sabotare, spiare, sorvegliare.*

Proteste da Anarchici e Ambientalisti:

- *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*.
- Per coinvolgere «volontariamente» più persone possibili l'attività viene pubblicizzata sui social e su Telegram.

Tipologie di mailbombing osservate:

- si fornisce il testo e viene chiesto di inviare una email dal proprio account di posta.
- si mettono a disposizione uno o più server da cui inoltrare le email.

Es. 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

FormezPA

Es. 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 essenziali
Covid, saranno sostanzialmente esclusi dalla maggior parte de

L'unico modo per fermare questa usurpazione è quello di **esercitare**
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 così che possa essere approv

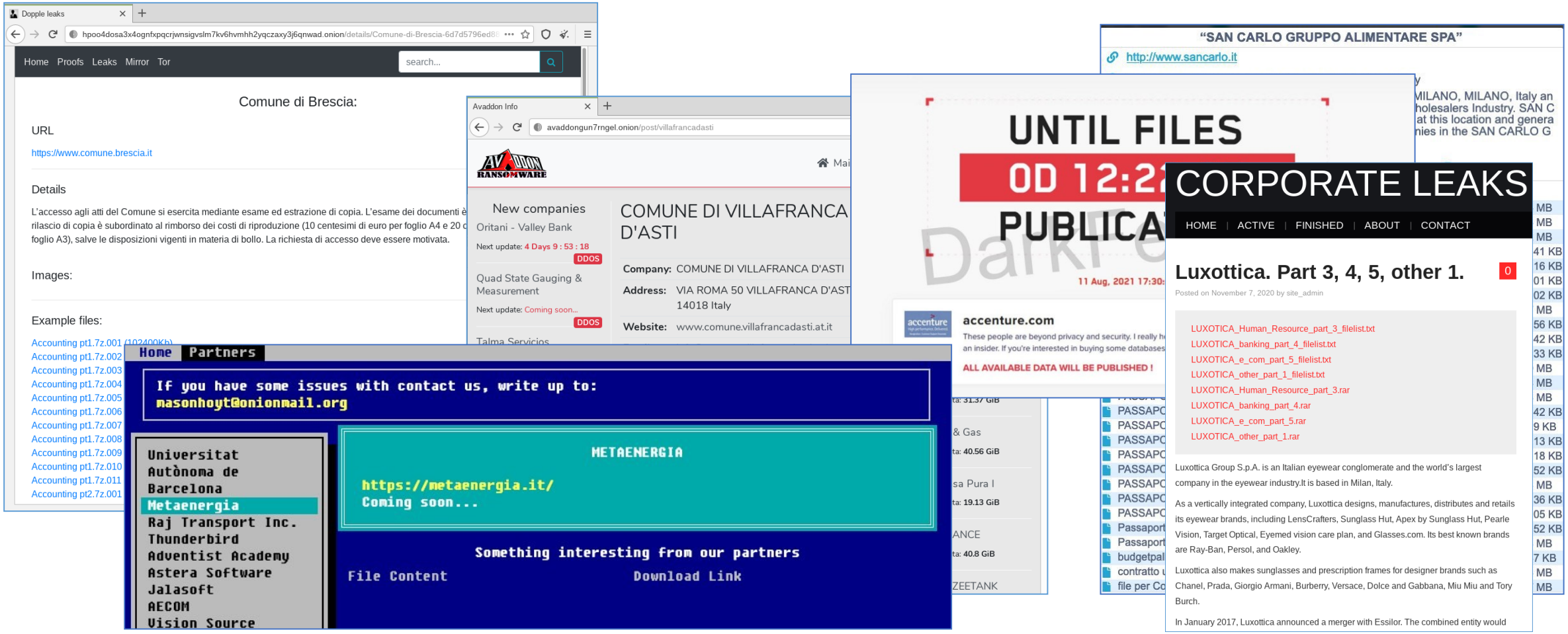
Siamo tanti e, unendoci attraverso un'azione sistematica e coor
ed accolte. Dobbiamo chiedere con massima risoluzione la rim

Campagne malevole

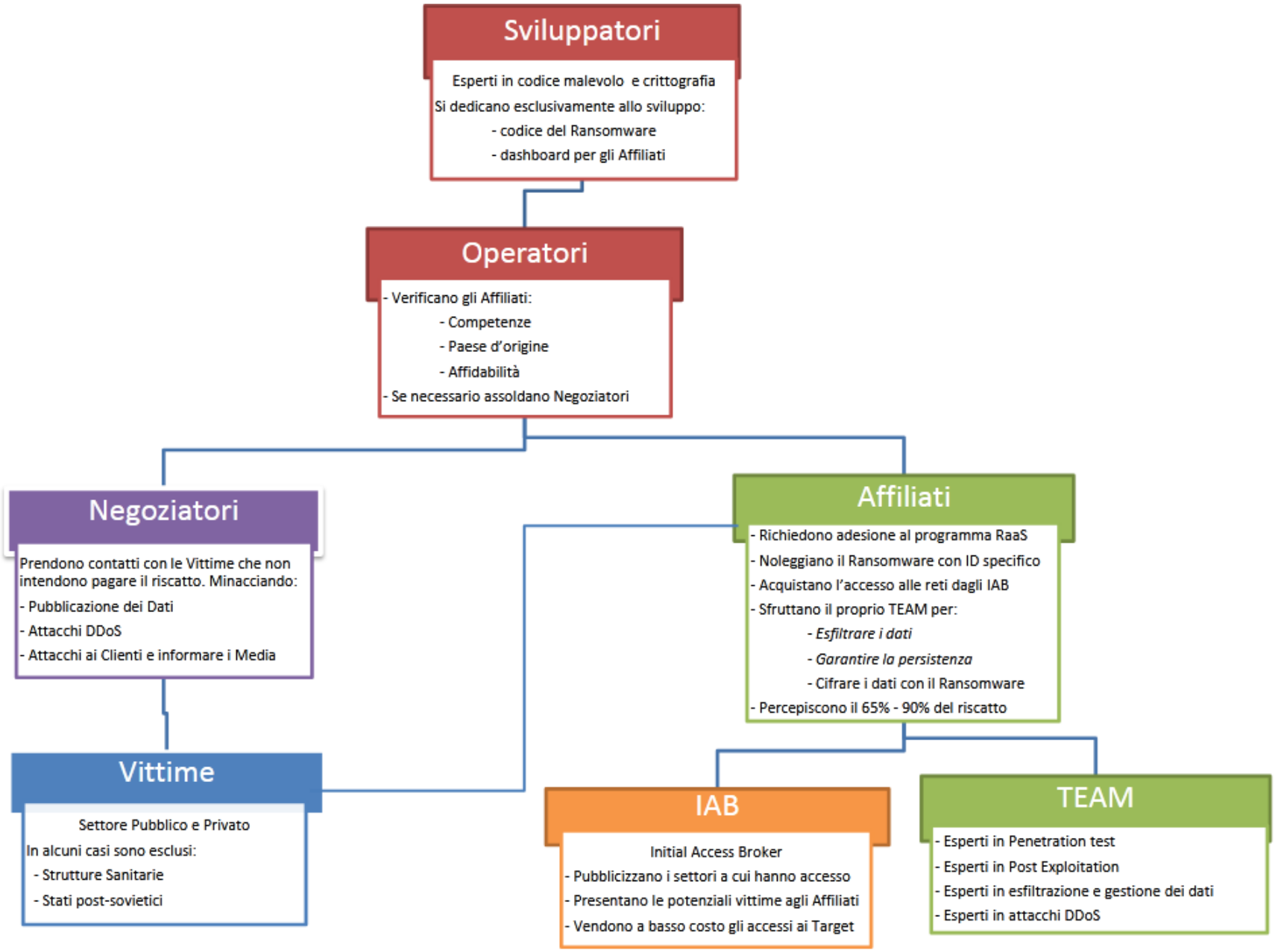
- La PA **non è immune** agli attacchi di malware tramite campagne malspam.
- Le **comunicazioni della PA** sono spesso sfruttati per confezionare **campagne ad hoc** verso aziende o privati cittadini.
- Molte delle campagne riscontrate ~~sono~~ sembrano progettate da **cyber criminali italiani**.
- 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 ottenuto l'accesso e/o esfiltrato i dati.*

Attacchi Ransomware

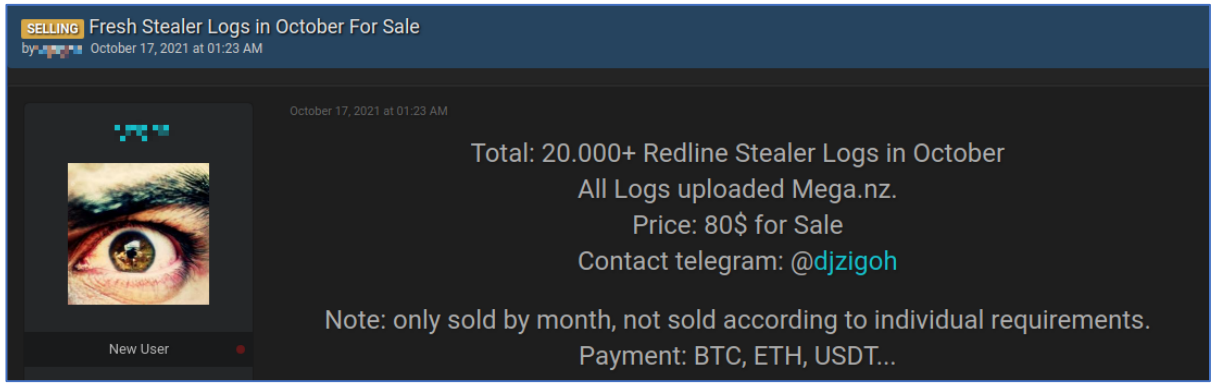
Si stimano **in Italia 100+ attacchi** ransomware nel 2021, solo tra settore Pubblico e Privato (SpA).

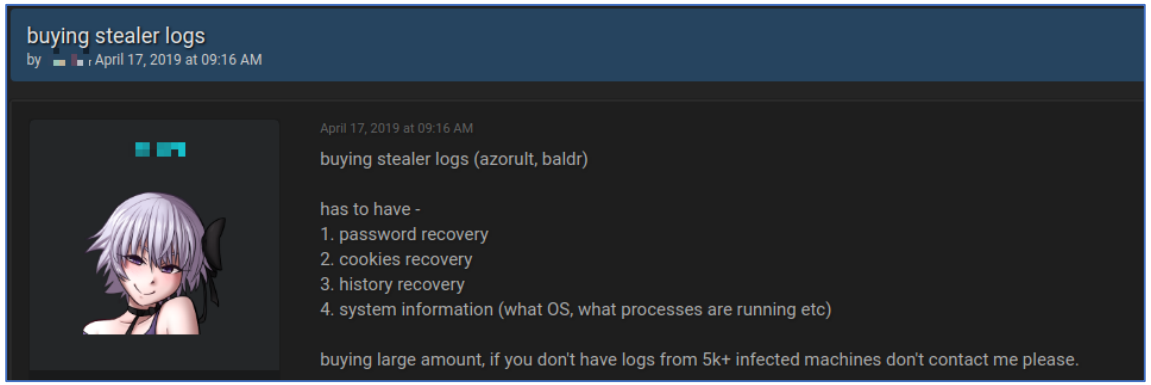


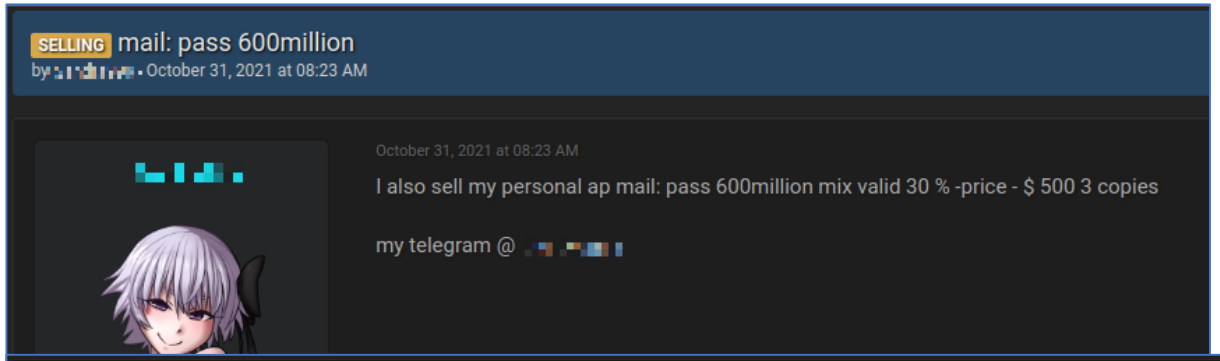
RaaS

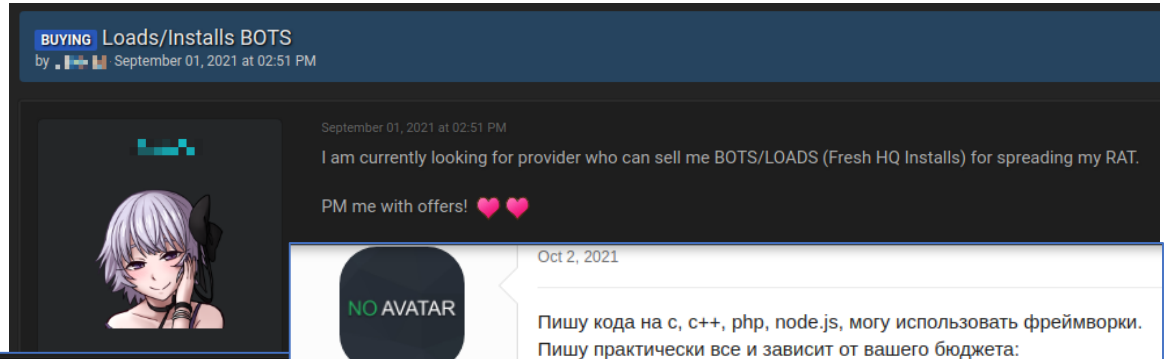

Sviluppatori
Esperti in codice malevolo e crittografia
Si dedicano esclusivamente allo sviluppo:
- codice del Ransomware
- dashboard per gli Affiliati
Operatori
- Verificano gli Affiliati:
- Competenze
- Paese d'origine
- Affidabilità
- Se necessario assoldano Negoziatori
Negoziatori
Prendono contatti con le Vittime che non intendono pagare il riscatto. Minacciando:
- Pubblicazione dei Dati
- Attacchi DDoS
- Attacchi ai Clienti e informare i Media
Affiliati
- Richiedono adesione al programma RaaS
- Noleggiano il Ransomware con ID specifico
- Acquistano l'accesso alle reti dagli IAB
- Sfruttano il proprio TEAM per:
- Esfiltrare i dati
- Garantire la persistenza
- Cifrare i dati con il Ransomware
- Percepiscono il 65% - 90% del riscatto
Vittime
Settore Pubblico e Privato
In alcuni casi sono esclusi:
- Strutture Sanitarie
- Stati post-sovietici
IAB
Initial Access Broker
- Pubblicizzano i settori a cui hanno accesso
- Presentano le potenziali vittime agli Affiliati
- Vendono a basso costo gli accessi ai Target
TEAM
- Esperti in Penetration test
- Esperti in Post Exploitation
- Esperti in esfiltrazione e gestione dei dati
- Esperti in attacchi DDoS

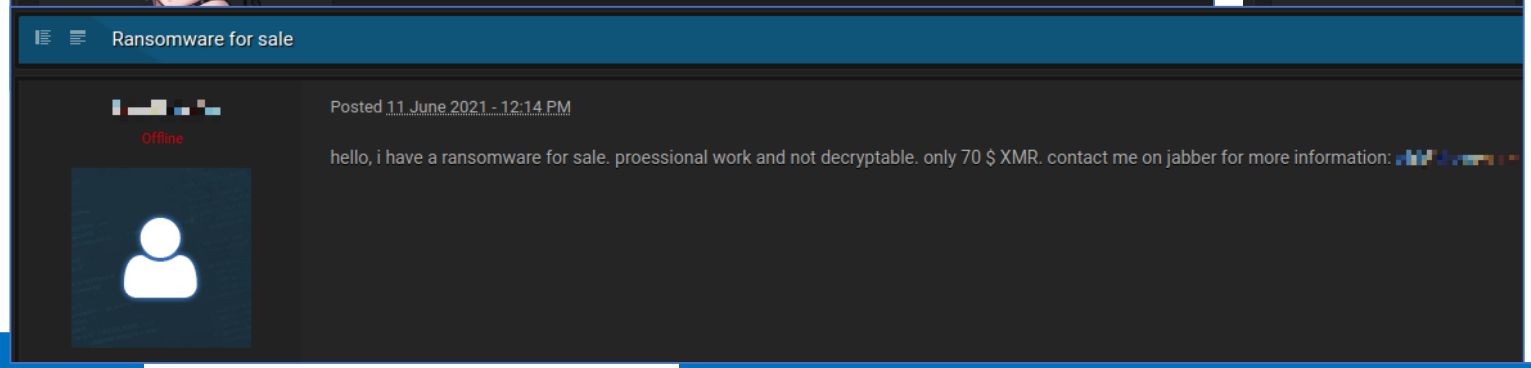
Compravendita di Malware e Informazioni

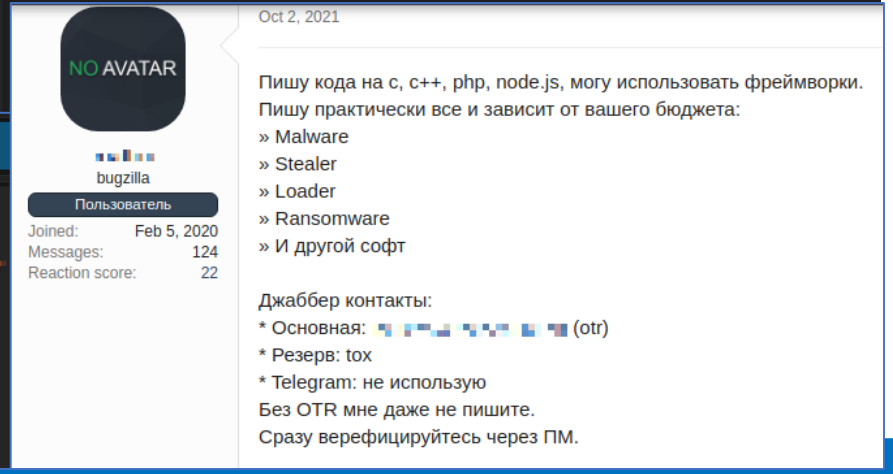












Quali dati in vendita? Ma soprattutto, sono sempre in vendita?

- Dati anagrafici
- Email e Password di account di Posta Elettronica
- Credenziali di accesso a servizi
- Carte di credito
- Metadati

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

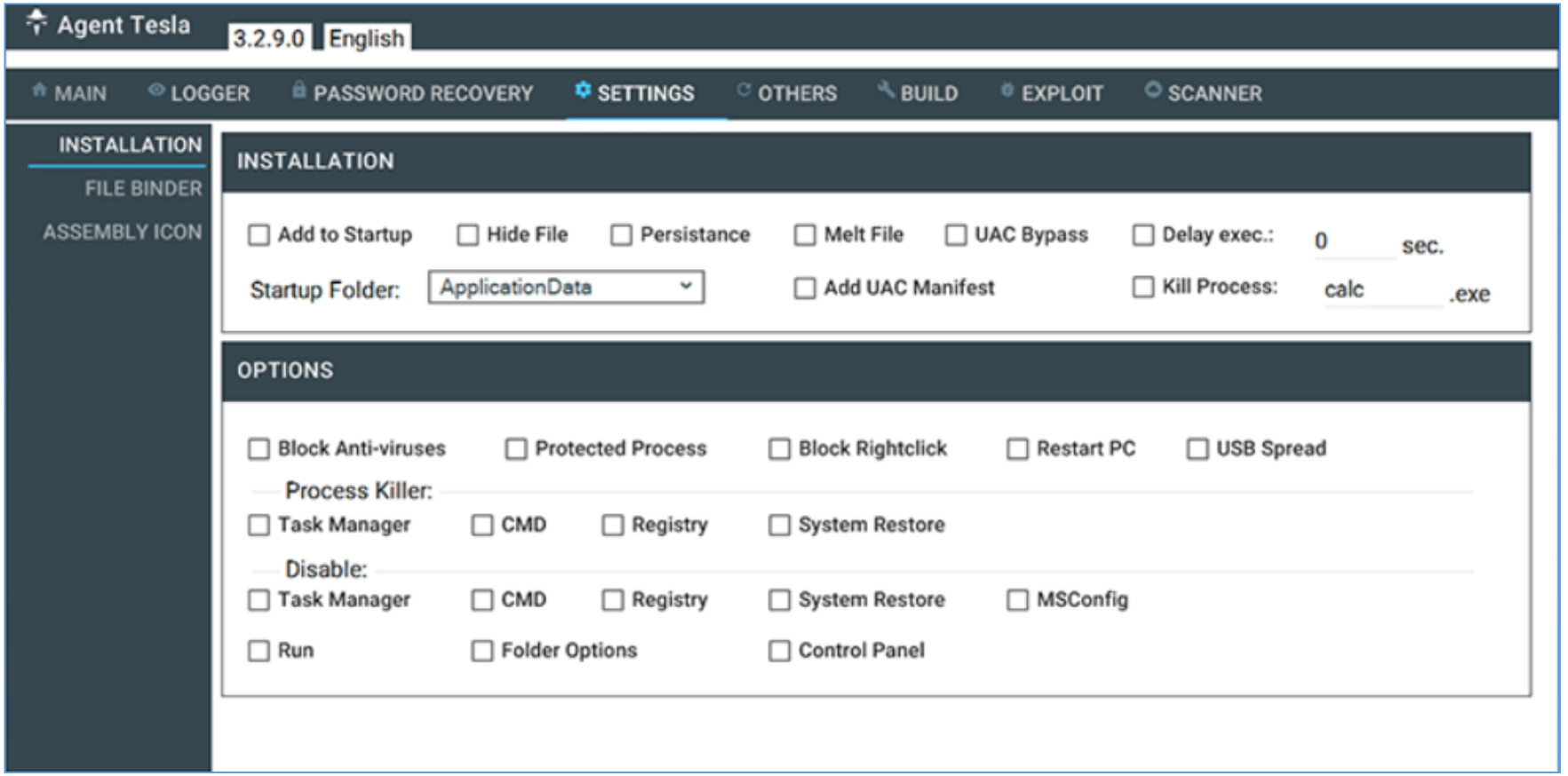
URL:[redacted].it
Username:[redacted]
Password:[redacted]
Application:Firefox

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

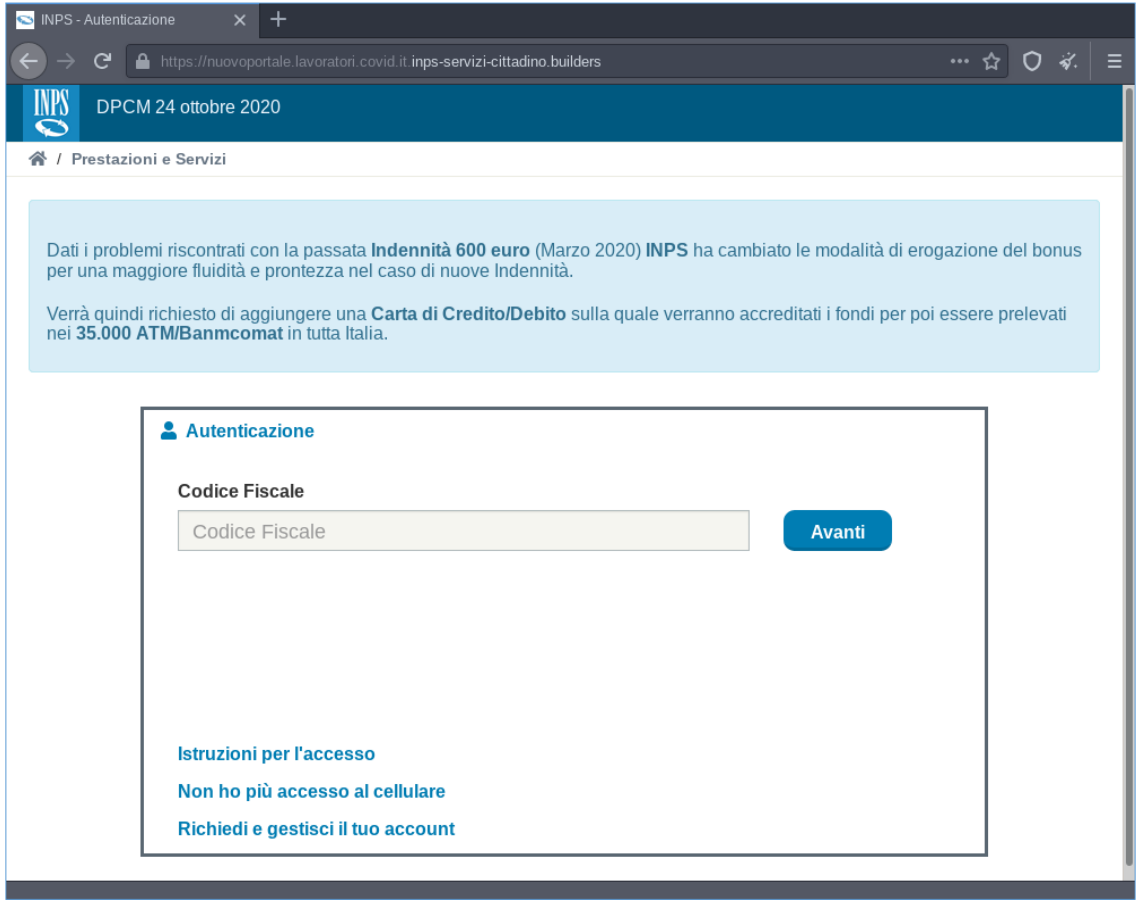
URL:[redacted].istruzione.it
Username:[redacted]
Password:[redacted]
Application:Firefox

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

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



Esempi di campagne malevole



FormezPA

Esempi di campagne malevole

Da Infocert S.p.A <comunicazioni@infocert.it>
Oggetto **Aggiornamento critico Dike**
A comunicazioni@infocert.it

Rispondi

Gentile Cliente,

Ti informiamo che è necessario effettuare un aggiornamento critico sulla sicurezza del programma Dike.

Segui le indicazioni riportate nel documento pdf allegato.

Grazie per la collaborazione

Lo staff Infocert

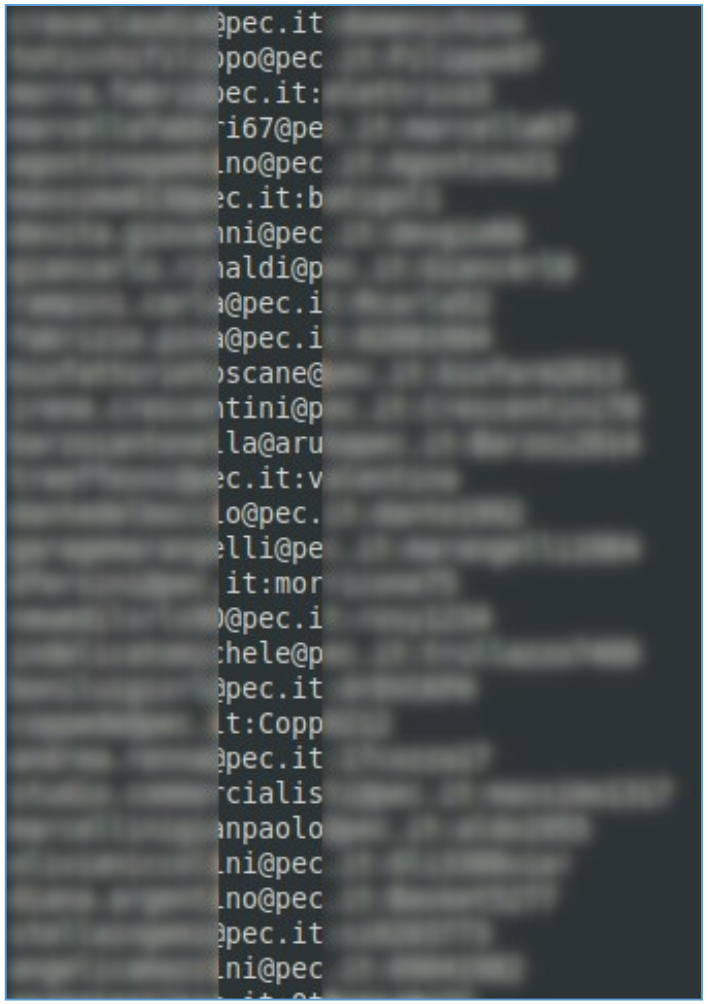
Questa e-mail e i relativi allegati possono contenere informazioni riservate esclusivamente al DESTINATARIO specificato in indirizzo. Le informazioni trasmesse attraverso la presente e-mail ed i suoi allegati sono diretti esclusivamente al destinatario e devono ritenersi riservati con divieto di diffusione e di uso salva espressa autorizzazione. Se la presente e-mail e i suoi allegati fossero stati ricevuti per errore da persona diversa dal destinatario siete pregati di distruggere tutto quanto ricevuto e di informare il mittente con lo stesso mezzo. Qualunque utilizzazione, divulgazione o copia non autorizzata di questa comunicazione è rigorosamente vietata e comporta violazione delle disposizioni di Legge sulla tutela dei dati personali REGOLAMENTO EUROPEO 2016/679.Grazie per la collaborazione
InfoCert S.p.A

1 allegato: Dike-Infocert-Upgrade.pdf 167 kB

Salva

https://cert-agid.gov.it/news/nuova-campagna-malspam-ateraagent-a-tema-dike/

Posta Elettronica Certificata (e compromessa)



Da [redacted] ☆

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

A [redacted] ☆

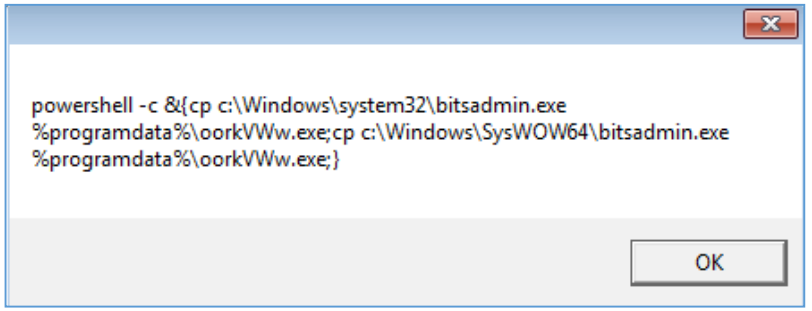
Rispondi | Rispondi a tutti | Inoltra | Altro

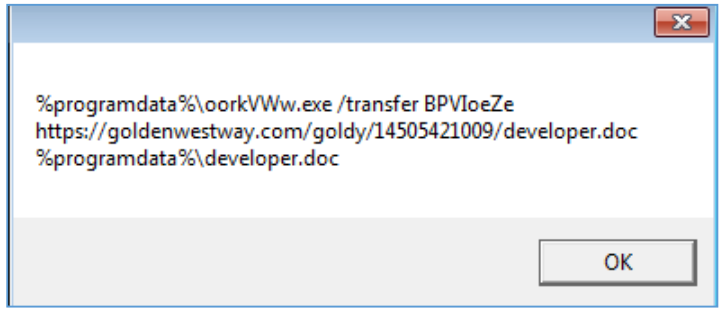
[redacted]

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-[redacted].7z 105 kB



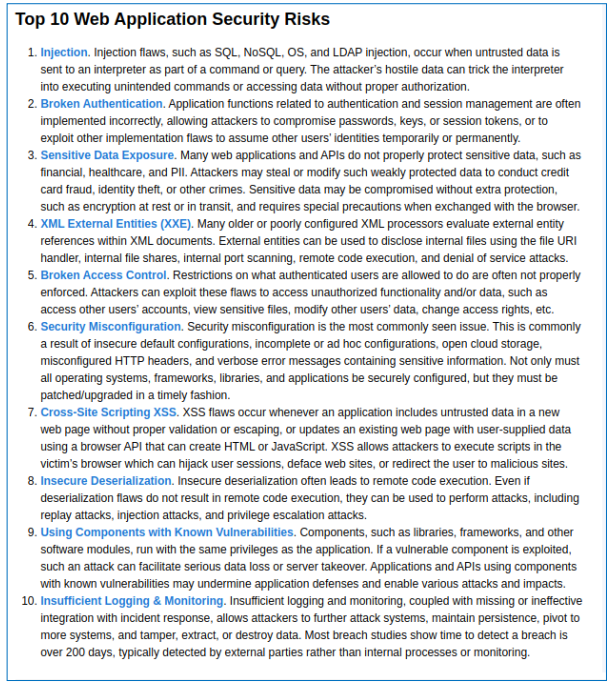


Web Application Attack

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.

Secondo monitoraggio dello stato di aggiornamento del protocollo HTTPS e dei CMS sui sistemi della PA

- https://cert-agid.gov.it/news/secondo-monitoraggio-dello-stato-di-aggiornamento-del-protocollo-https-e-dei-cms-sui-sistemi-della-pa/

Uno sguardo ai server della Pubblica Amministrazione attraverso i dati di Shodan

- https://cert-agid.gov.it/news/mappatura-delle-vulnerabilita-della-pubblica-amministrazione-mediante-fonti-osint/

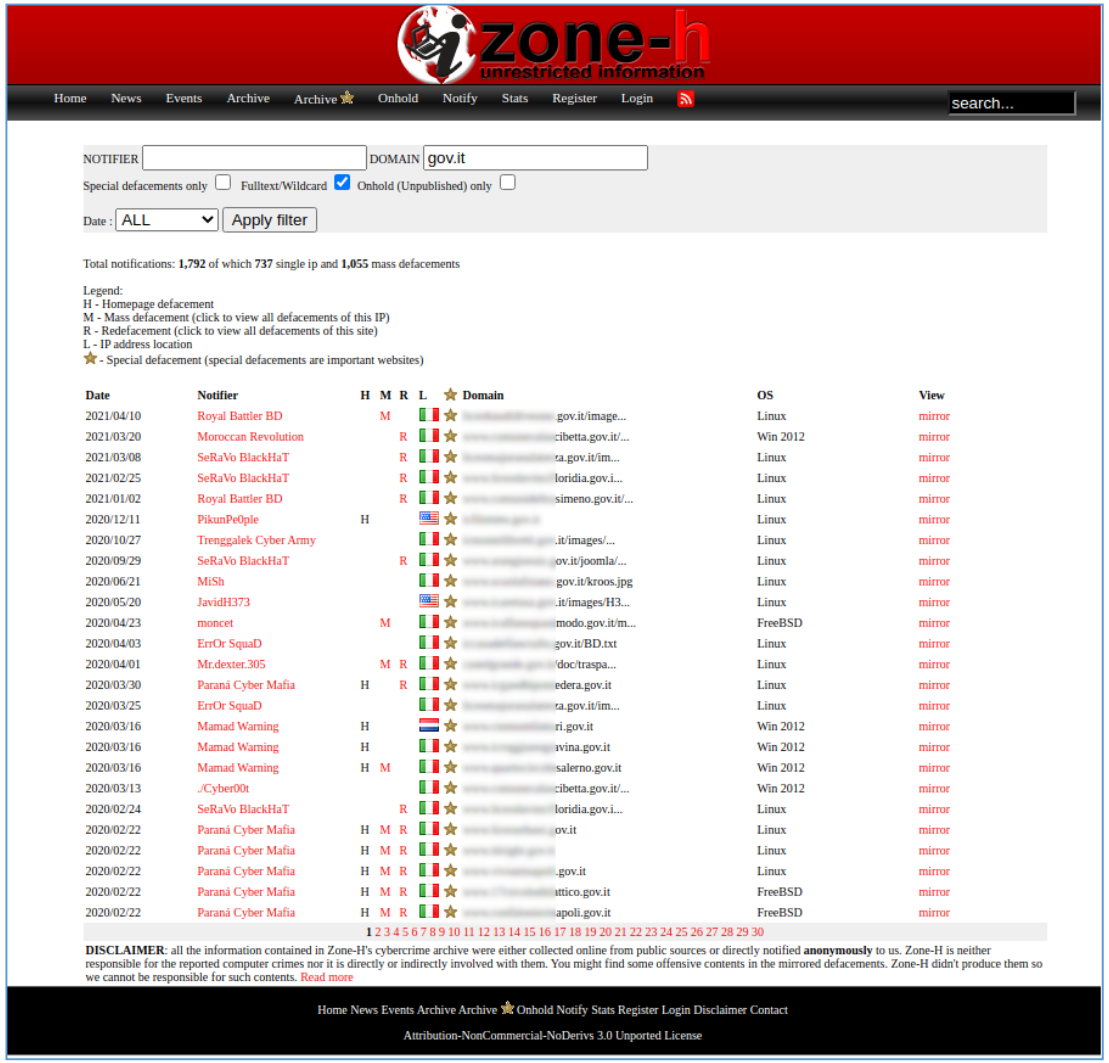
Proteggersi da questi attacchi?

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.

Problemi per le vittime, risorse per gli attaccanti



zone-h
unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

NOTIFIER DOMAIN gov.it

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date : ALL Apply filter

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 Battler BD		M				.gov.it/image...	Linux	mirror
2021/03/20	Moroccan Revolution			R			:ibetta.gov.it/...	Win 2012	mirror
2021/03/08	SeRaVo BlackHaT			R			ta.gov.it/im...	Linux	mirror
2021/02/25	SeRaVo BlackHaT			R			loridia.gov.i...	Linux	mirror
2021/01/02	Royal Battler BD			R			simeno.gov.it/...	Linux	mirror
2020/12/11	PikunPe0ple	H						Linux	mirror
2020/10/27	Trenggalek 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						ta.gov.it/im...	Linux	mirror
2020/03/16	Mamad Warning	H					ri.gov.it	Win 2012	mirror
2020/03/16	Mamad Warning	H					avina.gov.it	Win 2012	mirror
2020/03/16	Mamad Warning	H	M				salerno.gov.it	Win 2012	mirror
2020/03/13	./Cyber00t						:ibetta.gov.it/...	Win 2012	mirror
2020/02/24	SeRaVo BlackHaT			R			loridia.gov.i...	Linux	mirror
2020/02/22	Paraná Cyber Mafia	H	M	R			ov.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 **0xrocky**, 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:	**rica.crea.gov.it**
Open Bug Bounty Program:	**Create your bounty program now**. It's open and free.
Vulnerable Application:	Custom Code
Vulnerability Type:	**XSS (Cross Site Scripting)** / 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 **ISO 29147** guidelines
Discovered and Reported by:	**0xrocky**
Remediation Guide:	**OWASP XSS Prevention Cheat Sheet**
Export Vulnerability Data:	Bugzilla Vulnerability Data JIRA Vulnerability Data [Configuration] Mantis Vulnerability Data Splunk Vulnerability Data XML Vulnerability Data [XSD]

Vulnerable URL:

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

FormezPA

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.

Condivisione di indicatori di compromissione per la protezione della Pubblica Amministrazione

Le Pubbliche Amministrazioni interessate possono esprimere la volontà di aderire al flusso di Indicatori di compromissione (**Feed IoC**) del **CERT-AGID** per la protezione della propria Amministrazione da minacce Malware e Phishing compilando l'apposito modulo.

Come aderire

1. Scarica e compila il modulo di accreditamento in formato Libre Office o in formato Microsoft Office.
2. Compila il modulo con i riferimenti della persona tecnica e l'elenco (max 20) di indirizzi IPv4 da abilitare.
3. Invia il modulo compilato per e-mail a **info@cert-agid.gov.it**

https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/

CERT-AGID

CERT-AGID

- **e-mail** : info@cert-agid.gov.it
- **web** : https://cert-agid.gov.it
- **twitter** : @agidcert
- **telegram** : @certagid

Per segnalarci nuove campagne malware / phishing / scam da analizzare basta allegare l'email originale sospetta e inviarla all'indirizzo:

malware@cert-agid.gov.it