



AGID

Agenzia per l'Italia Digitale

FormezPA

La sicurezza nella gestione documentale

Gianni Amato – AgID



CERT-AGID
Computer Emergency Response Team
AGID



UNIONE EUROPEA
Fondo europeo
Fondo europeo di sviluppo regionale



Agenzia per la
Cooperazione
Internazionale



Presidenza del Consiglio dei Ministri
Dipartimento della
Funzione Pubblica



GOVERNANCE
E CAPACITÀ
ISTITUZIONALE
2014-2020



AGID | Agenzia per
l'Italia Digitale

Identificazione e classificazione dei documenti

Assicurare che i documenti ricevano un adeguato livello di protezione in linea con la loro importanza.

Identificare e classificare in relazione al loro valore e alla criticità in caso di divulgazione o modifiche non autorizzate.

Controllo degli accessi alle informazioni

Una volta identificati i documenti, è importante gestire gli accessi per garantire che, in caso di documenti sensibili, solo le persone o gruppi autorizzati possano accedervi e siano autorizzati alla lettura e/o scrittura e/o modifica.

La domanda da porsi è: **chi ha accesso/permesso a fare cosa?**



Abuso di privilegi utente I/II

Il sistema o la piattaforma di gestione deve prevedere un processo, accessibile ai responsabili della piattaforma, per la gestione degli account utente: registrazione, privilegi, revoca.

- **User ID amministrative generiche:** Evitare se non indispensabili!
- **User ID individuali:** Ogni utente è responsabile delle proprie azioni.
 - **Need to know:** Assicurarsi che il livello di accesso alle informazioni sia in linea con tale principio e con il principio di separazione dei compiti. Privilegi minimi necessari per svolgere l'attività lavorativa.
 - **Revoca:** Immediata disabilitazione/rimozione delle utenze che hanno cessato il rapporto di lavoro o per le quali sono scaduti i diritti.
 - **Verifica periodica:** Accertarsi periodicamente (almeno trimestralmente) dell'assenza di account ridondanti o obsoleti. Procedere con la rimozione.

Abuso di privilegi utente II/II

- **Utenze tecniche:** Assicurarsi che, in caso di compromissione, non abbiamo accesso non autorizzato a risorse di sistema, configurazioni, etc.
 - **Utilizzo di ACL:** Per proteggere le risorse di sistema.
 - **Crittografia:** Rispettare gli algoritmi standard e di comprovata robustezza per memorizzare i dati sensibili nei file di configurazione di sistema.
- **Utenze di terze parti:** Considerare ed identificare tutti i requisiti di sicurezza prima di concedere a partners, fornitori/clienti, anche in fase di trattativa, l'accesso a informazioni o beni ospitati nel sistema/piattaforma. Effettuare una accurata analisi dei rischi per valutare l'impatto nel caso di violazione della sicurezza, divulgazione non autorizzata (es. a concorrenti), illecito trattamento delle informazioni.



Crittografia dei dati

Proteggere i documenti tramite la crittografia. Utilizzare algoritmi per rendere i dati illeggibili a chi non ha le autorizzazioni necessarie al fine di garantire riservatezza, l'autenticità e/o l'integrità delle informazioni.

- Utilizzare funzioni e algoritmi crittografici la cui robustezza sia comprovata da certificazioni e standard **riconosciuti a livello internazionale**. Soprattutto che risultino esenti da vulnerabilità note.
 - Hash quanto meno *SHA-256*. *MD5* e *SHA-1* sono deprecati!
- Quindi **evitare** di utilizzare o sviluppare algoritmi di crittografia personalizzati.
- Consultare **bollettini di sicurezza** emessi sia dai vendor sia da fonti nazionali ed internazionali autorevoli.

Sicurezza fisica e ambientale

Prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni dell'organizzazione e alle strutture di elaborazione delle informazioni.

- Perimetro di sicurezza fisica.
- Controlli di accesso fisico.
- Protezione contro minacce esterne ed ambientali.
- Isolamento delle aree di carico e scarico.

L'uso di infrastrutture **cloud** qualificate e certificate per la PA devono prevedere questi requisiti minimi di sicurezza fisica.

Attività operative

- Procedure operative **documentate**.
- Gestione dei **cambiamenti** (alle informazioni o ai sistemi che influenzano la sicurezza).
- **Separazione ambienti** di sviluppo, test e produzione.
- Controlli di individuazione, prevenzione e di ripristino in caso di **compromissione malware**.
- Devono essere effettuate **copie di backup** delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.
- **Log degli eventi**: attività utente, eccezioni, malfunzionamenti legati alla sicurezza. I log devono essere sincronizzati ad una singola sorgente temporale di riferimento e protetti da manomissioni e accessi non autorizzati.

Sicurezza applicativa

Prevenire lo sfruttamento di vulnerabilità tecniche. Valutare l'esposizione e prevedere misure per mitigare i rischi.

- Attività periodiche di **VA/PT** sull'applicativo.
- Le attività di audit devono essere **pianificate** e concordate per minimizzare interferenze con altri processi.
- Porre attenzione ai flussi di interoperabilità, definire politiche e procedure per la condivisione delle informazioni:
 - **Come**: protocolli utilizzati (https, sftp, smtps, ssh, etc)
 - **Dove**: verso interno o all'esterno?
 - **Quando**: tempistiche
 - **Perché**: motivare

Form di autenticazione e password policy

Assicurarsi che le specifiche di autenticazione siano idonee, quindi valutare che:

- Venga utilizzato il **MFA** o quanto meno che le password rispettino i **requisiti minimi di sicurezza**.
- Che le password **non** vengano **trasmesse in chiaro** all'utente.
- Che le form di autenticazione **sia sicura** e protetta da eventuali manomissioni.
- Che tutti gli step siano supportati da un **protocollo di comunicazione sicuro**.

In caso di incidenti di sicurezza

- **Responsabilità e procedure:** Stabilite per assicurare una risposta rapida, efficace ed ordinata agli incidenti di sicurezza.
- **Segnalazione:** Gli eventi devono essere segnalati il più velocemente possibile attraverso appropriati canali di gestione.
- **Valutazione e decisione:** A seguito di una valutazione deve essere stabilito se classificarli come incidenti.
- **Risposta:** Deve essere fornita in accordo con le procedure documentate.
- **Apprendimento dalla raccolta di evidenze:** La conoscenza deve essere utilizzata per ridurre la verosimiglianza o futuri incidenti.



Classificazione degli incidenti

La classificazione di un incidente di sicurezza consente di **determinare il livello di gravità** dell'incidente e di individuare le azioni di contenimento più appropriate tramite la definizione di:

- Livelli di Severity e Priorità;
- Modalità di escalation;
- Strategie di contrasto;
- Tempistiche per la risoluzione dell'incidente.

Gli incidenti saranno pertanto classificati in base al livello di severity, in modo da poter intraprendere correttamente le successive azioni e attivare i corretti livelli di escalation.

Incidenti: eventi di sicurezza logica

- **Accesso non autorizzato**: violazione di sistema/informazioni dovute ad una errata attribuzione di privilegi di accesso o ad un attacco informatico volontario;
- **Malware/Trojan**: questa categoria riguarda gli attacchi derivanti dalla diffusione in rete di software malevolo;
- **Denial of Services (DoS)**: attacchi finalizzati al degrado del funzionamento di un servizio/sistema fino al blocco dello stesso;
- **Utilizzo improprio delle risorse informatiche**: installazione di software illegali o non autorizzati dall'azienda, modifica non autorizzata della configurazione della postazione di lavoro, ecc.



Il Data Breach

Una situazione che può comportare, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione o l'accesso non autorizzato a informazioni qualificate dal GDPR come dati personali trasmesse, memorizzate o elaborate per mezzo di sistemi informatici.

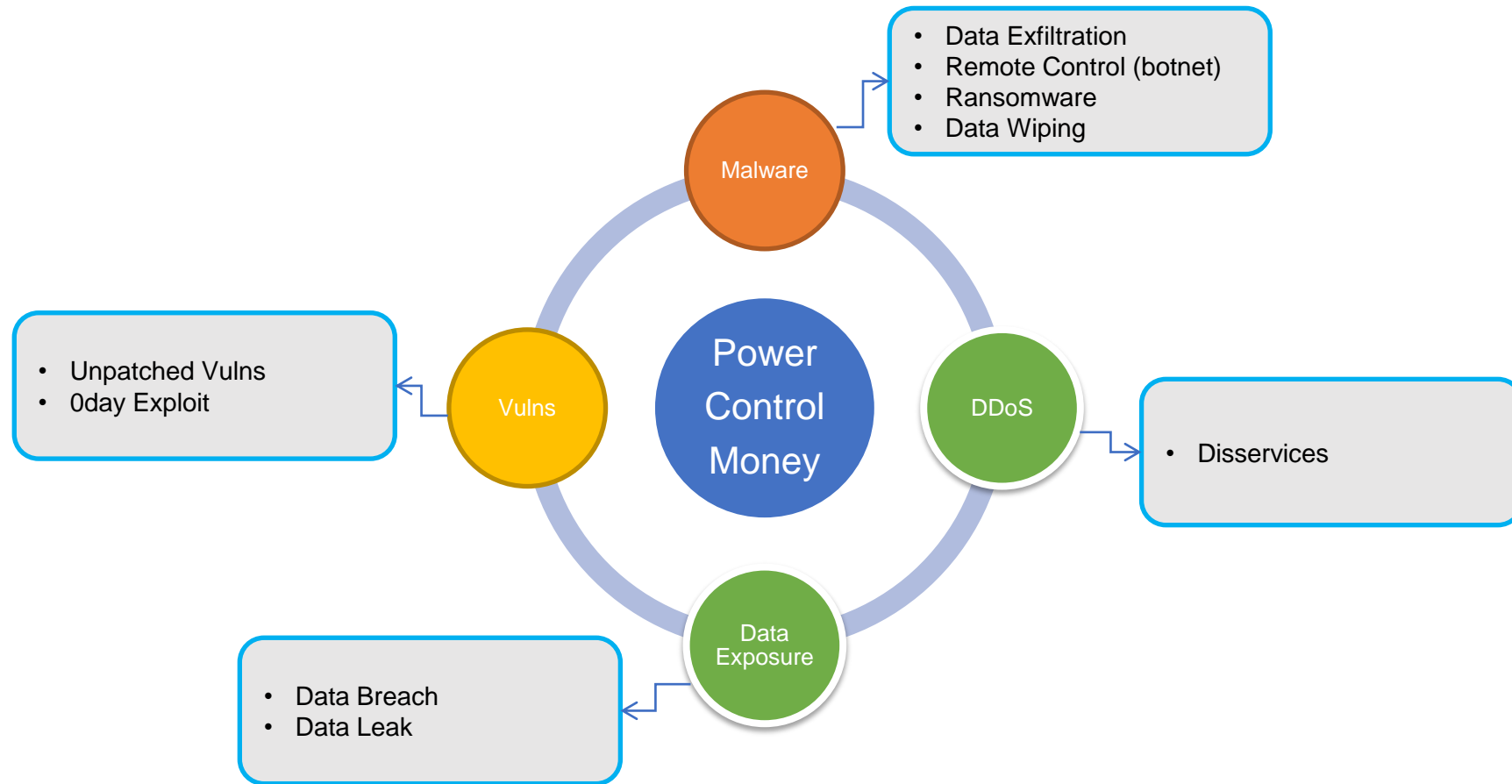
- **Violazione della riservatezza:** in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- **Violazione della disponibilità:** in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- **Violazione dell'integrità:** in caso di alterazione non autorizzata o accidentale dei dati personali.

Livelli di severity

La seguente classificazione costituisce l'applicazione delle più recenti **indicazioni di ENISA** (così come da Regolamento del 21/12/2021 emanato da AgID).

TLP	Livello	Classificazione	Tempistica remediation
Green	1	NESSUN IMPATTO (<i>"no impact"</i>)	≤ 15 gg lavorativi
Yellow	2	IMPATTO LIEVE (<i>"minor impact"</i>): le risorse sono state influenzate o in parte compromesse ma non vi è impatto sui servizi principali e nei confronti degli utenti.	≤ 7 gg lavorativi
Amber	3	IMPATTO MEDIO (<i>"high impact"</i>): influenzati parte dei servizi principali ed una parte più o meno ampia di utenti.	≤ 3 giorni lavorativi
Red	4	IMPATTO ALTO (<i>"very high impact"</i>): influenza la maggior parte o tutti i servizi coinvolgenti tutti o, comunque, un'ampia percentuale di utenti del servizio.	≤ 24 ore lavorative

Cyber Threat Landscape



Gli attori: Le vittime

Le vittime, chi sono?

- Possono essere scelte o casuali
- Sistemi informatici esposti e vulnerabili
- Personale non adeguatamente preparato

Target mirato, scelto per brand o categoria specifica

Nessun target specifico, attacchi massivi

Vulnerabilità note
Default password

Phishing
Smishing

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

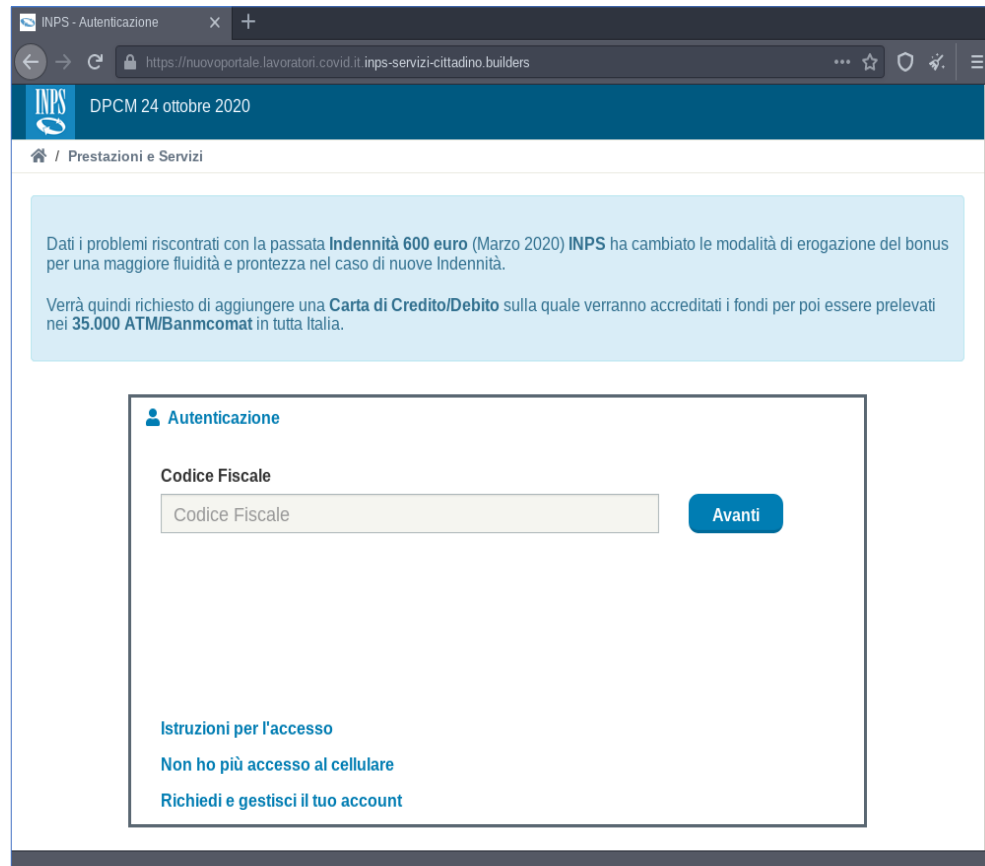
Sorvegliare

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.
- Lo scopo è sempre quello di **esfiltrare informazioni**: credenziali di accesso.
- 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



Esempio di minaccia malware italiana

Da ricevuta.pagaonline@agenziaiscossione.gov.it ☆

Oggetto **Ricevuta di pagamento - Transazione n. 202208988150460269** 11:36

A [redacted] ☆

Gentile contribuente,
in allegato la ricevuta di pagamento della transazione numero 202208988150460269 eseguita in data: 30/08/2022 alle ore 11:45 sul nostro portale.
La invitiamo a conservare la ricevuta a conferma del pagamento effettuato.
Grazie per aver utilizzato i nostri servizi on-line.

Nella speranza di averLe fornito un servizio utile, Le auguriamo una buona giornata.
.....
Si prega di non rispondere a questa e-mail, perchè il messaggio viene generato in modo automatico.

 **iscossione**
Agenzia Entrate

Agenzia delle entrate-Riscossione

Via Giuseppe Grezar, 14
00142 Roma
www.agenziaentrateriscossione.gov.it

Le informazioni contenute in questo messaggio sono riservate e confidenziali e ne e' vietata la diffusione in qualunque modo eseguita. Qualora Lei non fosse la persona a cui il presente messaggio e' destinato, La invitiamo gentilmente ad eliminarlo dopo averne dato tempestiva comunicazione al mittente e a non utilizzare in alcun caso il suo contenuto. Qualsivoglia utilizzo non autorizzato di questo messaggio e dei suoi eventuali allegati espone il responsabile alle relative conseguenze civili e penali.

> 1 allegato: 2_202208988150460269.xls 50,0 kB

Salva

File Home Inserisci Layout di pagina Formule Dati Revisione Visualizza

Calibri 11 A A



G C S

Carattere

Allineamento

D4

--Visualizza--

Ricevuta di pagamento

Identificativo	202208988150460269
Importo	100,00
Importo netto	100,00
Importo lordo	100,00
Importo netto	100,00
Importo lordo	100,00
Importo netto	100,00
Importo lordo	100,00

Dettaglio transazione

Importo	100,00
Importo netto	100,00
Importo lordo	100,00
Importo netto	100,00
Importo lordo	100,00

Transazione e copia

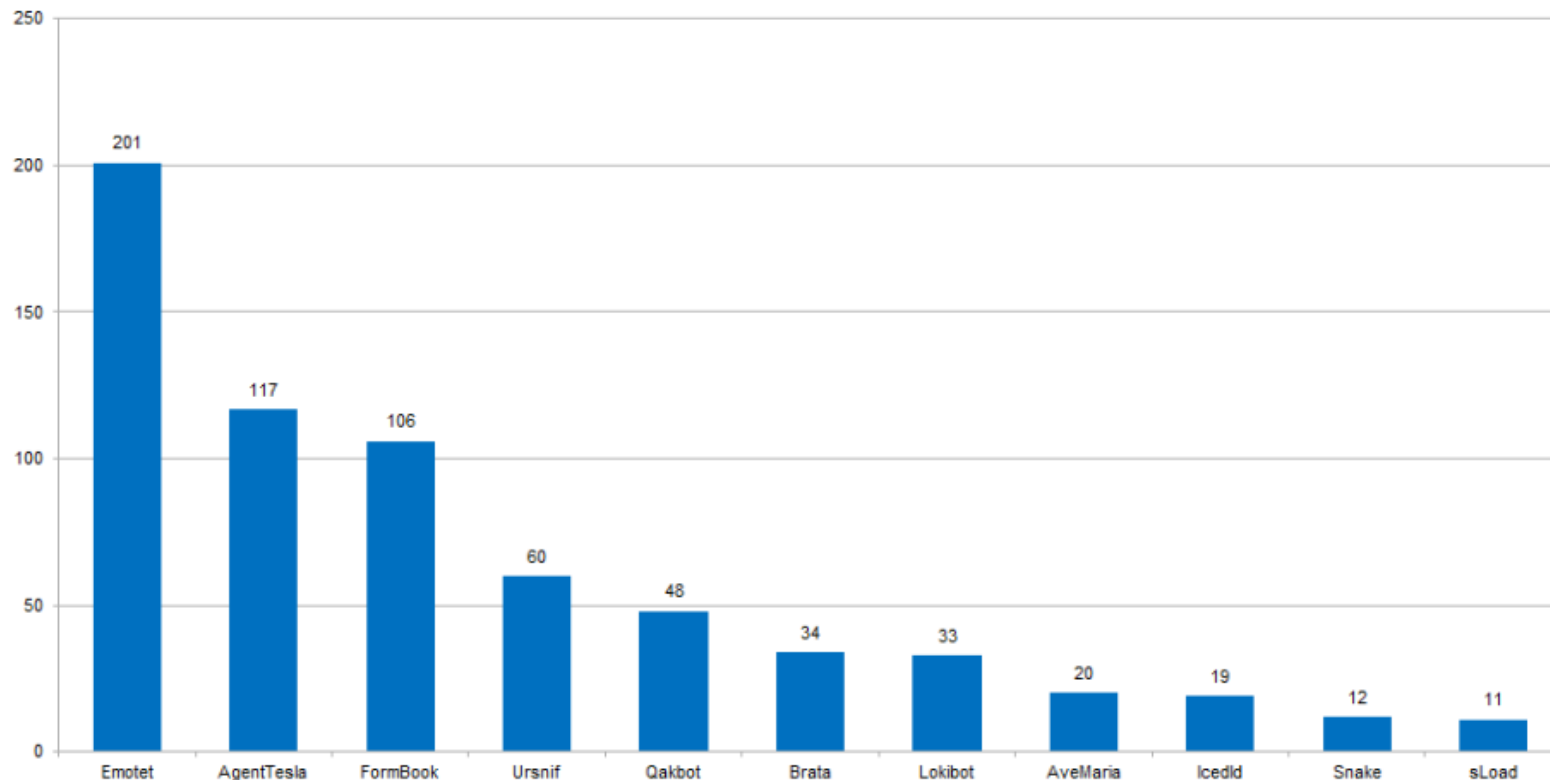
Il pagamento e' stato registrato correttamente.
Grazie per aver utilizzato il servizio.
Allegati: Ricevuta di pagamento.

2022_agosto

 **Agenzia per la
Coordinazione Interministeriale**

Report Malware Italia 2022 – CERT-AGID

I malware più rilevanti nel 2022
Numero di eventi > 10



Dati esfiltrati da malware (AgentTesla)

URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox
URL: https://www.governo.it Username: www.governo.it Password: www.governo.it Application: Firefox

Agent Tesla

3.2.9.0

English

MAIN

LOGGER

PASSWORD RECOVERY

SETTINGS

OTHERS

BUILD

EXPLOIT

SCANNER

INSTALLATION

FILE BINDER

ASSEMBLY ICON

INSTALLATION

☐ 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

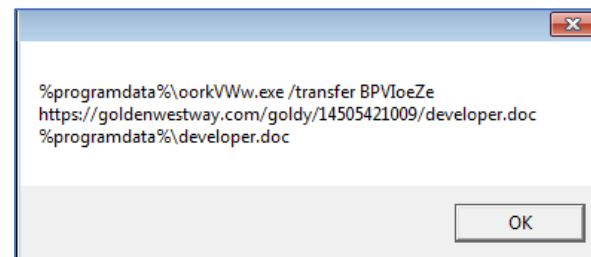
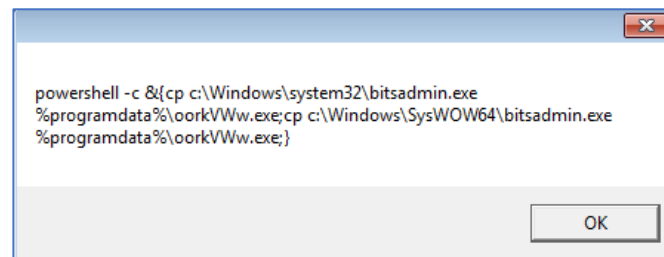
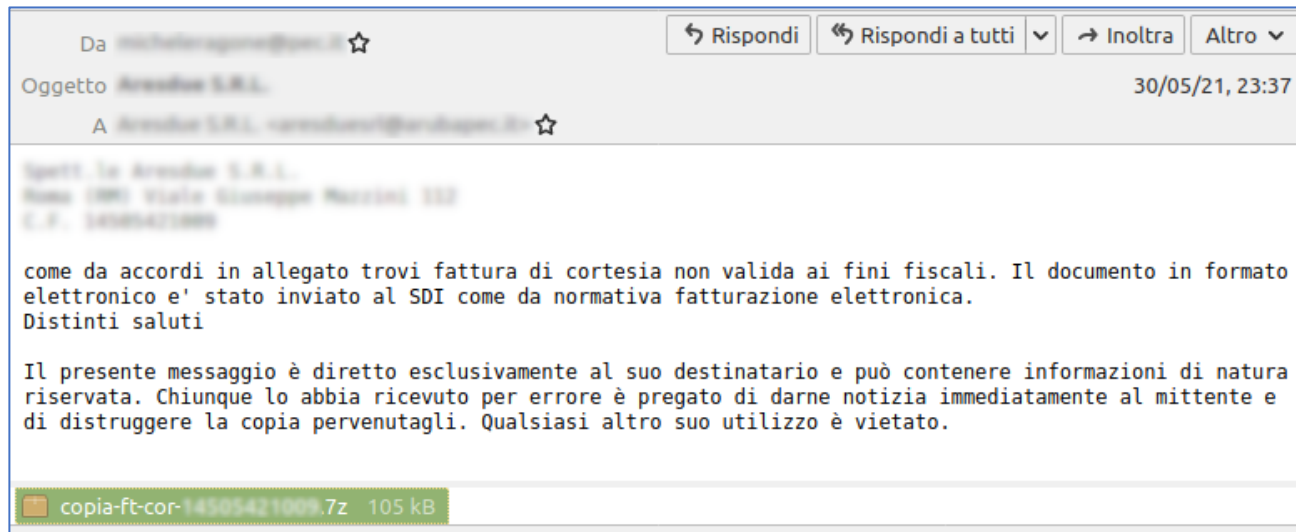
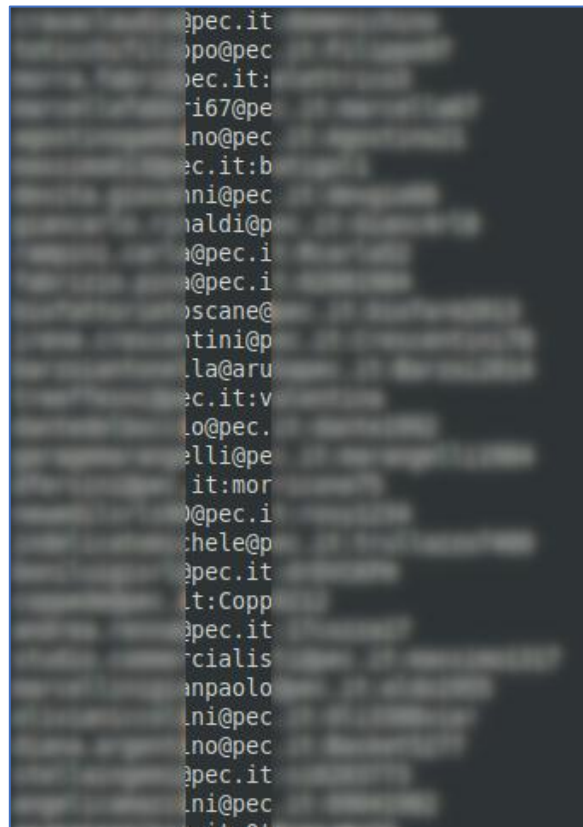
☐ MSConfig

☐ Run

☐ Folder Options

☐ Control Panel

Posta Elettronica Certificata (e compromessa)



Compromissione OTP via SMS

applicativo-...com/B8Wasu1hMmnc0xi4bxNzihYBY5sIZ/list.php

CONTROL PANEL Dati Dispositivi UTENTI DELETE LOGS Logout

Dati ricevuti

Show 10 entries Search:

N	Ricevente	Mittente	Messaggio	Data	Username
38	not_found	666	Il tuo codice OTP è 11111	2023-01-24 20:50:42	pablo
37	not_found	666	Il tuo codice OTP è 11111	2023-01-24 20:50:28	pablo
36	353-136	FCA Bank	102559 è il codice di sicurezza	2023-01-24 16:34:35	admin
35	353-136	FCA Bank	195755 è il codice di sicurezza	2023-01-24 16:32:39	admin
34	351-786	AllianzBank	SMS Allianz Bank (C/C 0634323) - Il 24/01/23 alle 16:49 abbiamo preso in carico il tuo bonifico di EUR -6.600,00. Per segnalazioni chiama il +39.02.55.50.6655 dal tuo numero di cellulare registrato in Home Banking	2023-01-24 15:49:16	admin
33	351-786	AllianzBank	Per completare la procedura di attivazione sulla App Allianz Bank chiama il +39.02.55.50.6655 dal tuo numero di cellulare registrato in Home Banking	2023-01-24 15:44:16	admin
32	351-786	AllianzBank	Il tuo PIN e' 67982481, utilizzalo ESCLUSIVAMENTE sull'App Allianz Bank. Non fornire il PIN a nessuno; se hai dubbi chiama subito il Servizio Clienti al	2023-01-24 15:43:55	admin
31	351-786	AllianzBank	Gentile cliente, le confermiamo che l'APP di Sicurezza SMS è stata abilitata con successo.	2023-01-24 15:40:58	admin
30	354-184	AllianzBank	SMS Allianz Bank (C/C 0670162) - Il 24/01/23 alle 16:39 abbiamo preso in carico il tuo bonifico di EUR -9.800,00. Per segnalazioni chiama il +39.02.55.50.6655 dal tuo numero di cellulare registrato in Home Banking	2023-01-24 15:39:20	pablo
29	354-184	AllianzBank	App Allianz Bank: nuovo accesso da dispositivo SM-A520F, SM-A520F; se non sei stato tu chiama il Servizio Clienti al nr. 02.55.50.6655	2023-01-24 15:33:35	pablo

Showing 1 to 10 of 38 entries

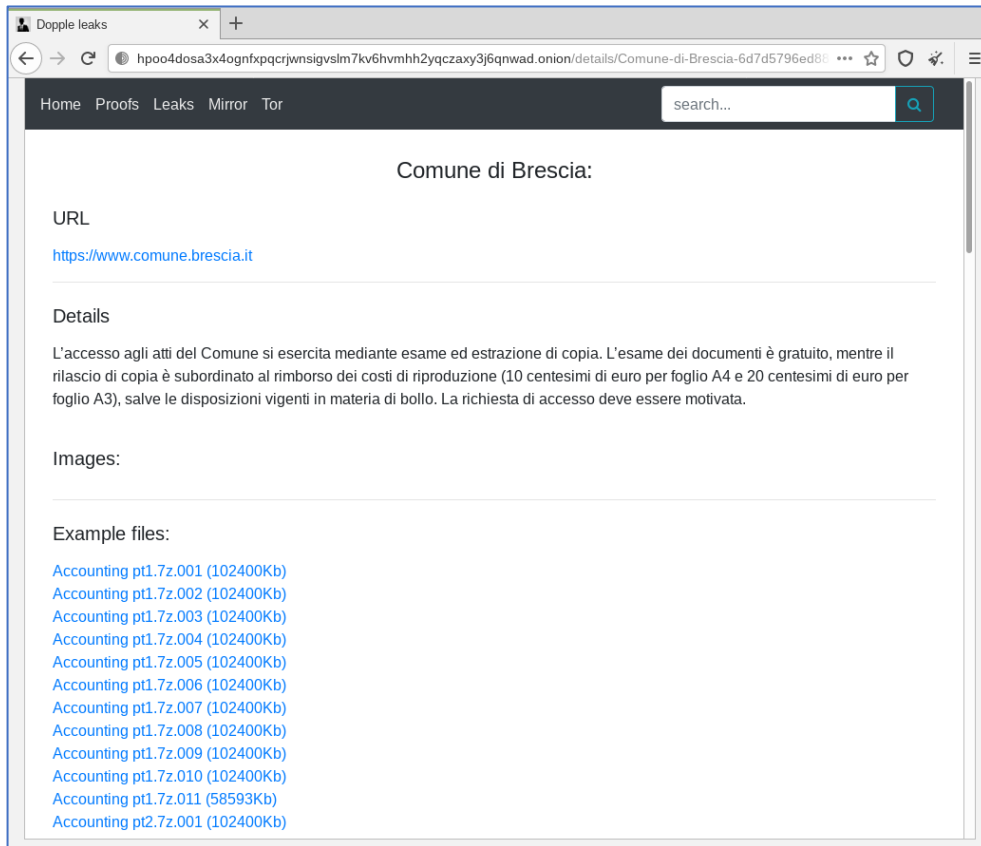
Previous 1 2 3 4 Next

È **aumentato** il numero di campagne veicolate tramite messaggi **SMS** al fine di diffondere **malware** volti a compromettere dispositivi mobili con lo scopo di **prenderne il controllo** e **carpire informazioni**.

L'obiettivo principale è quello di **acquisire gli SMS ricevuti** dalle vittime come secondo fattore di autenticazione (**2FA**).

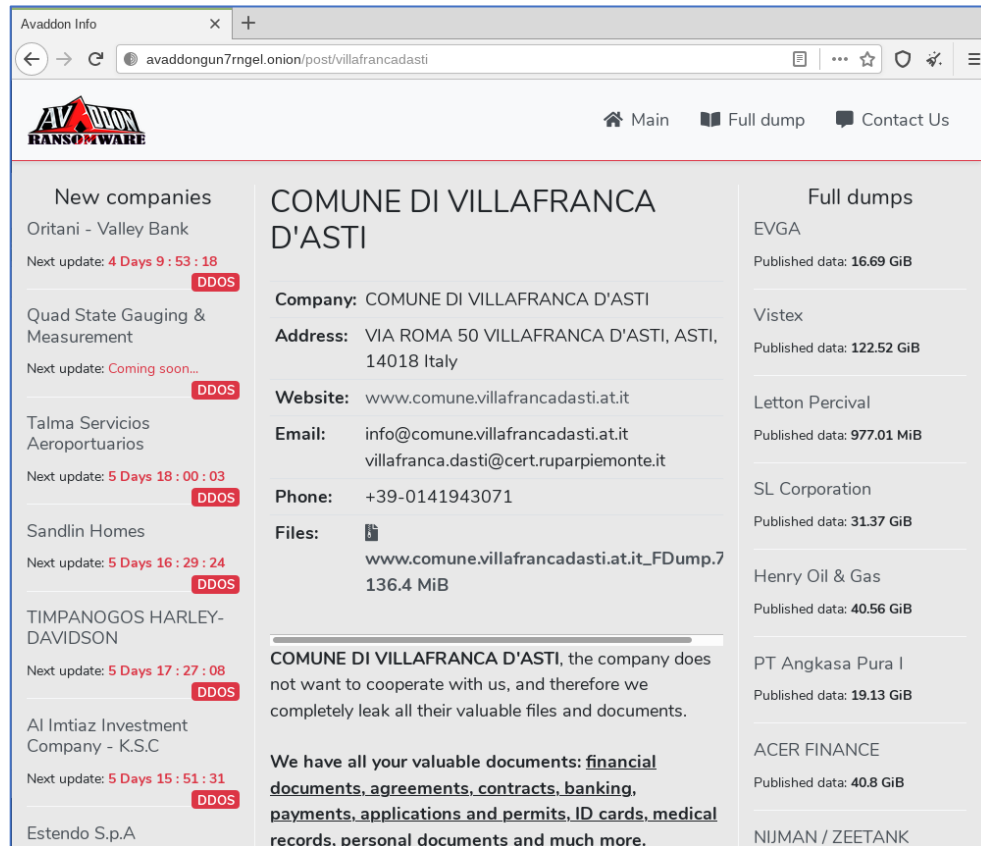


Double extortion



The screenshot shows the 'Dopple leaks' website. The URL bar displays a long alphanumeric string. The page has a navigation bar with 'Home', 'Proofs', 'Leaks', 'Mirror', and 'Tor'. A search bar is present. The main content area is titled 'Comune di Brescia:'. It includes sections for 'URL' (https://www.comune.brescia.it), 'Details' (describing the access to public acts and the cost of reproduction), 'Images:', and 'Example files:' (listing various accounting files).

Dopple Ransomware



The screenshot shows the 'Avaddon Info' website. The URL bar displays 'avaddongun7rngel.onion/post/villafrancadasti'. The page has a navigation bar with 'Main', 'Full dump', and 'Contact Us'. The main content area is titled 'COMUNE DI VILAFRANCA D'ASTI'. It includes sections for 'New companies' (listing Oritani - Valley Bank, Quad State Gauging & Measurement, Talma Servicios Aeroportuarios, Sandlin Homes, TIMPANOGOS HARLEY-DAVIDSON, Al Intiaz Investment Company - K.S.C, and Estendo S.p.A.), 'Full dumps' (listing EVGA, Vistex, Letton Percival, SL Corporation, Henry Oil & Gas, PT Angkasa Pura I, ACER FINANCE, and NIJMAN / ZEETANK), and a detailed description of the ransomware attack on the Comune di Villafranca d'Asti, including the company's refusal to cooperate and the types of documents leaked.

Avaddon Ransomware



Problemi per le vittime, risorse per gli attaccanti

[Home](#)
[News](#)
[Events](#)
[Archive](#)
[Archive](#)
[Onhold](#)
[Notify](#)
[Stats](#)
[Register](#)
[Login](#)

NOTIFIER

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date:

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 Bantler 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.i...	Linux	mirror
2021-01-02	Royal Bantler BD			R			simeno.gov.it/...	Linux	mirror
2020-12-11	PikunPeoPle	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	JavidI373						.it/images/H3...	Linux	mirror
2020-04-23	moncet			M			modo.gov.it/im...	FreeBSD	mirror
2020-04-03	ErrOr Squad						gov.it/BD.txt	Linux	mirror
2020-04-01	Mr.dexter.305			M	R		/doc/trasp...	Linux	mirror
2020-03-30	Paran 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	„Cyber00t						cbetta.gov.it/...	Win 2012	mirror
2020-02-24	SeRaVo BlackHaT			R			loridia.gov.i...	Linux	mirror
2020-02-22	Paran Cyber Mafia	H	M	R			ov.it	Linux	mirror
2020-02-22	Paran Cyber Mafia	H	M	R			.gov.it	Linux	mirror
2020-02-22	Paran Cyber Mafia	H	M	R			ttico.gov.it	FreeBSD	mirror
2020-02-22	Paran 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:

- verified the vulnerability and confirmed its existence;
- 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:	Oxrocky
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>
```





AGID

Agenzia per l'Italia Digitale

FormezPA

GRAZIE PER L'ATTENZIONE



CERT-AGID
Computer Emergency Response Team
AGID

