

|                  |                  |                                                                                                 |
|------------------|------------------|-------------------------------------------------------------------------------------------------|
| Riferimento:     | 2023.59          |                                                                                                 |
| Redatto da:      |                  |                                                                                                 |
| Revisionato da:  |                  |                                                                                                 |
| Data:            | 24/07/2023       |                                                                                                 |
| Destinatari:     | Pubblico         |                                                                                                 |
| Classificazione: | Non Classificato | range: non classificato (verde), Confidenziale (giallo), Riservato (arancione), Segreto (rosso) |

|                 |                        |                                             |
|-----------------|------------------------|---------------------------------------------|
| Oggetto:        | Weekly Threats 29.2023 |                                             |
| Ente Impattato: |                        |                                             |
| Area impattata: |                        |                                             |
| Criticità:      | Media                  | range: nulla, bassa, media, alta, altissima |

## Sommario

|                                       |    |
|---------------------------------------|----|
| Sommario                              | 2  |
| 1. Executive Summary                  | 3  |
| 2. Weekly Threats                     | 3  |
| 2.1 Phishing                          | 3  |
| 2.2 Brand Monitor                     | 4  |
| 2.3 DataLeak, DataBreach e Ransomware | 5  |
| 2.4 IoC - Malware                     | 8  |
| 2.5 Generic Threat Intelligence       | 10 |
| 3. Vulnerabilità                      | 12 |

## 1. Executive Summary

Rassegna dei principali avvenimenti analizzati quotidianamente dal Cyber Threat Intelligence Team di D3Lab durante la scorsa settimana al fine di fornire un aggiornamento puntuale sulle minacce cyber identificate.

## 2. Weekly Threats

Di seguito si riepilogano suddivisi per punti i principali threats individuati.

### 2.1 Phishing

La settimana è stata caratterizzata dall'individuazione e analisi di 440 campagne di Phishing.

Durante la settimana l'ente maggiormente colpito dal phishing è stato Poste Italiane con 83 campagne di phishing, seguita dalle Credit Agricole Francese con 64 campagne e dalla Banca Postale Francese con 36 segnalazioni.

Nelle ultime due settimane si è rilevato un considerevole aumento delle campagne di phishing ai danni di PayPal Italia, l'intento dei criminali è come di consueto quello di carpire le credenziali di accesso al portale della nota piattaforma di pagamenti digitali. L'incremento registrato questo trimestre, dalle ignote motivazioni, ha registrato il doppio delle segnalazioni rispetto al trimestre precedente.

Si rileva inoltre un incremento delle campagne malevoli ai danni dei principali vettori nazionali e non, come GLS, DHL, UPS, ecc che notificano all'utente finale la necessità di pagare un piccolo importo per sbloccare una consegna. L'intento dei criminali è quello di carpire le credenziali e i dati delle carte di credito degli utenti.

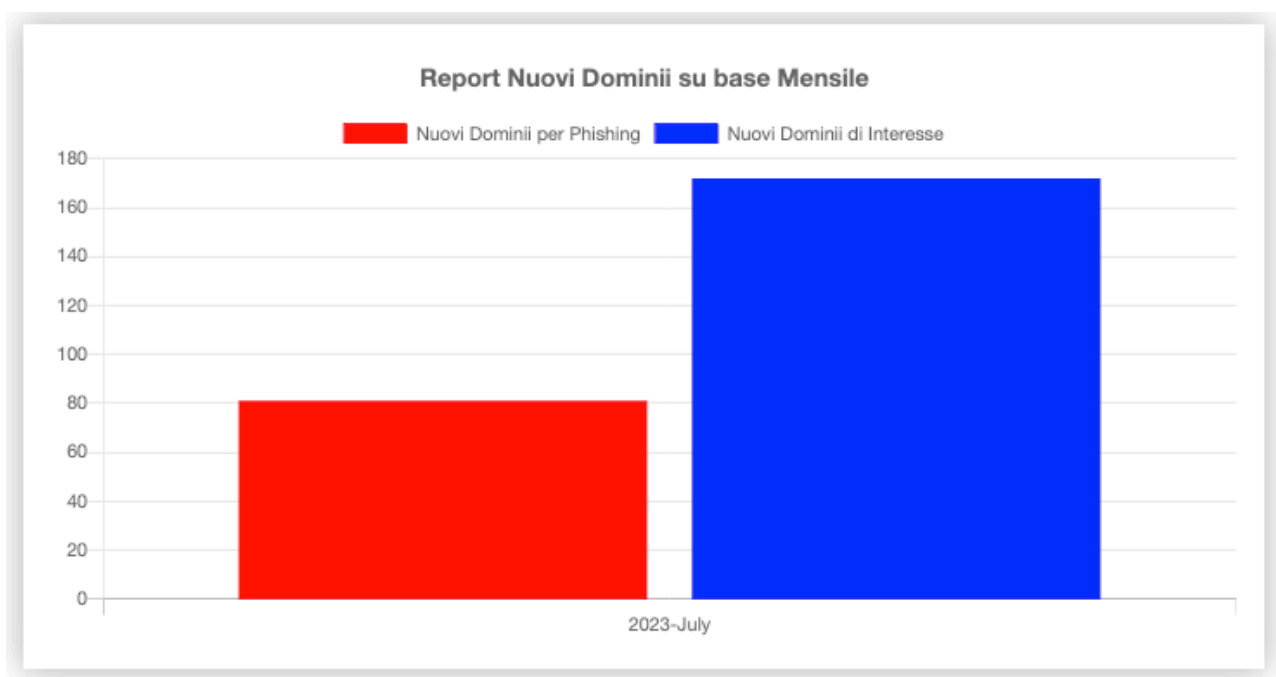
Sono ritornate le segnalazioni di phishing ai danni di Q8 con il probabile intento di generare buoni carburati dalle aree clienti per poi essere rivenduti a prezzi scontati nei diversi market illegali.

Si segnalano infine campagne di phishing anche ai danni di enti minori quali Cassa di Risparmio di Bolzano (SparKasse), Banca Popolare dell'Alto Adige VolksBank e Deutsche Bank Italia.

Gli enti più colpiti della settimana permangono quelli del settore Bancario e Finanziario con oltre il 75% della campagne veicolate a loro danno.

## 2.2 Brand Monitor

Nel corso della precedente settimana sono stati rilevati 172 nuovi domini che hanno similitudini con brand noti e che quindi sfruttando la tecnica del typosquatting, o che contengono parole comuni ipoteticamente utili per la divulgazione di una frode online (es. “verifica”, “login”, “password”, “accedi”, etc.).



Di questi 172 nuovi domini, sempre nella settimana, 81 sono stati utilizzati per divulgare campagne malevole per la diffusione di Phishing o Malware.

## 2.3 DataLeak, DataBreach e Ransomware

Durante la settimana sono stati diffusi gratuitamente i seguenti data leak:

| Data Rilevamento | Nome                                                           | Email Coinvolte | Domini Email Coinvolti |
|------------------|----------------------------------------------------------------|-----------------|------------------------|
| 2023-07-17 23:58 | <a href="http://Fastation.co.th">Fastation.co.th</a>           | 1157            | 53                     |
| 2023-07-17 23:58 | <a href="http://Tripodo.de">Tripodo.de</a>                     | 69966           | 4746                   |
| 2023-07-17 23:58 | <a href="http://Ngobox.org">Ngobox.org</a>                     | 39758           | 2775                   |
| 2023-07-17 23:58 | <a href="http://Machenike.com">Machenike.com</a>               | 19096           | 223                    |
| 2023-07-17 23:58 | <a href="http://Nafpo.in">Nafpo.in</a>                         | 1860            | 139                    |
| 2023-07-17 23:58 | <a href="http://Exportgenius.in">Exportgenius.in</a>           | 4306            | 3583                   |
| 2023-07-17 23:58 | <a href="http://Georgetown.edu">Georgetown.edu</a>             | 95463           | 7                      |
| 2023-07-17 23:58 | <a href="http://Mininghamster.com">Mininghamster.com</a>       | 5656            | 445                    |
| 2023-07-17 23:58 | <a href="http://Bilisremitonline.com">Bilisremitonline.com</a> | 79              | 31                     |
| 2023-07-17 09:19 | <a href="http://Locally.com">Locally.com</a>                   | 1517524         | 25745                  |

Sono stati pubblicati annunci di vendita di dataleak ai danni di diversi siti web italiani:

- \* famaspeed.it
- \* anticoattico.com
- \* astebook.it
- \* colasantiaste.com
- \* faraonecasadaste.it
- \* farsettiarte.it
- \* gonnelli.it
- \* maisonbibelot.com
- \* toseli.com
- \* astedams.it
- \* astexpo.it

In ambito internazionale ha fatto notizia la pubblicazione di un documento caricato accidentalmente sulla piattaforma VirusTotal di Google che ha portato alla potenziale esposizione di nomi e indirizzi email di dipendenti di agenzie di intelligence e di difesa di diverse nazioni.

Il file è stato rimosso da VirusTotal entro un'ora dal caricamento, tuttavia tale file caricato da un dipendente VirusTotal sembra abbia fatto trapelare un elenco di circa 5.600 clienti di VirusTotal, tra cui dipendenti dei servizi segreti statunitensi, Nsa e dei servizi segreti tedeschi.

Il set di dati include email di dipendenti di ministeri in Germania, Giappone, Emirati Arabi Uniti, Qatar, Lituania, Israele, Turchia, Francia, Estonia, Polonia, Arabia Saudita, Colombia, Repubblica Ceca, Egitto, Slovacchia e Ucraina.

## Ransomware

Dal monitoraggio dei blog afferenti i team ransomware, è stata rilevata la rivendicazione di attacchi ai danni dei seguenti enti privati e pubblici italiani:

- **VOG Consorzio delle Cooperative Ortofrutticole dell'Alto Adige** - vog.it - **ALPHV**
- **Confartigianato Federimpresa FC** - confartigianatofc.it - **Cactus**
- **Artemide S.p.A** - artemide.com - **Cactus**
- **Rotomail Italia SpA** - rotomail.it - **Cactus**
- **CWS Digital Transformation SRL** - cws.it - **Cactus**
- **Girardini Srl** - girardini.it - **NoEscape**
- **Azimut** - azimut.it - **BlackCat**

Il team denominato Cactus recentemente apparso nello scenario ransomware ha già pubblicato 18 vittime sul proprio blog nella TOR, tra le quali sono stati pubblicati i dettagli di attacco alle quattro società italiane sopra elencate.

Tra gli altri team ransomware citiamo gli ormai noti attacchi del gruppo **Clop** e lo sfruttamento di vulnerabilità note insite nel software di trasferimento file **MOVEit**, che ha portato ad un forte aumento delle vittime pubblicate sul blog di rivendicazione che attualmente ha superato quota 380.

Oltre a ciò, Clop recentemente è salito agli onori della cronaca in merito ad una nuova tecnica di estorsione, consistente nella creazione di un dominio ad hoc, nel web emerso, per il rilascio dei dati esfiltrati alle vittime.

L'uso di tale tecnica agevola il download dei file oltre ad arrecare maggiore danno alla vittima, data la possibilità di chiunque di accedere al sito creato per il ricatto.

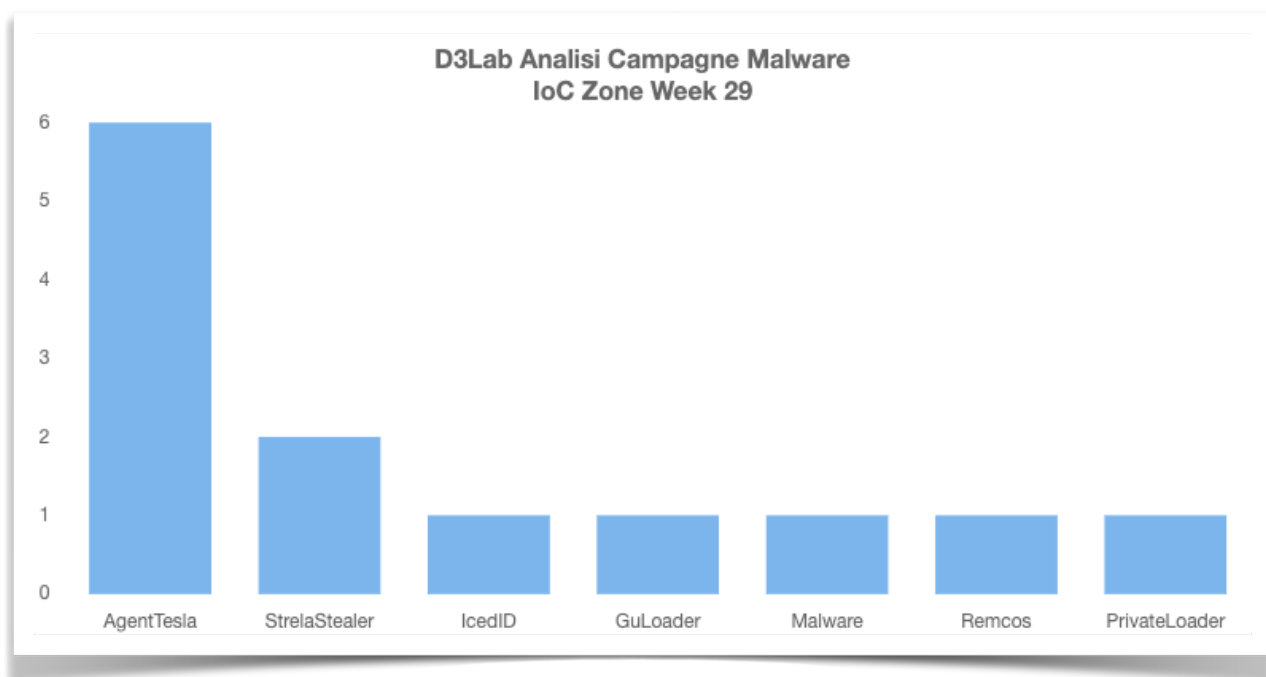
Questa metodica è stata applicata attualmente solo ai danni della società **PWC** - pwc.com, che ha visto pubblicare i suoi dati nel clear web.

PWC è una società con sede a Londra ma opera anche in Italia.

PWC fornisce servizi professionali di revisione, di consulenza e di consulenza legale/fiscale alle imprese.

Infine, Sophos ha avvisato gli utenti della nascita di un ransomware che sta abusando del proprio marchio denominato SophosEncrypt.

## 2.4 IoC - Malware



Anche questa settimana il malware AgentTesla è stato il più diffuso nel territorio italiano. Sono state rilevate email aventi ad oggetto falsi Ordine e Pagamenti con allegati file archivio ZIP o 7z contenente file EXE, ma anche allegato file DOC e PDF.

È stata osservata ed analizzata la ricomparsa di due campagne malware StrelaStealer a tema Documenti e Fattura, le email contengono allegati file 7z o PDF con link a JS. Strela Stealer è in infostealer che tende a carpire le credenziali di accesso dell'account email preso di mira si rivolge a client di posta elettronica come Microsoft Outlook e Mozilla Thunderbird.

Si segnala il rilevamento di un campagna malware PrivateLoader scritta in lingua inglese ma veicola in maniera massiva nel territorio italiano, la campagna riportava dettagli in merito ad una falsa Transazione effettuata a favore dell'account Facebook / Meta del destinatario. La campagna allega file archivio RaR contenente due eseguibili.

La campagna aveva il fine di scaricare ed eseguire uno o più payload che sono stati associati a noti Stealer.

È analizzata una campagna Malware IcedID, la malspam di risposta a precedenti conversazioni allega file PDF contenente un JS malevolo.

Infine, si segnala la persistenza di campagne malware RemcosRat a tema bancario che continuano a colpire il territorio italiano con efficaci riferimenti a Bonifici proveniente da noti Istituti di Credito nostrani.

## 2.5 Generic Threat Intelligence

### Quattro entità commerciali Europee bandite dagli Stati Uniti

Il governo degli Stati Uniti ha bandito i produttori europei di spyware commerciale **Intellexa** e **Cytrox**, citando i rischi per la sicurezza nazionale e gli interessi di politica estera degli Stati Uniti. Pertanto sono state aggiunte quattro realtà commerciali alla lista di entità bandite tra le quali:

- Intellexa SA dalla Grecia,
- Intellexa Limited dall'Irlanda,
- Cytrox Holdings Zrt dall'Ungheria
- Cytrox AD dalla Macedonia del Nord

La decisione è stata motivata dal coinvolgimento delle quattro società nel traffico di exploit sfruttati per fini illeciti ed ottenere l'accesso a dispositivi di individui ad alto rischio in tutto il mondo, minacciando la loro sicurezza e privacy.

La Regione Umbria ha subito un attacco DDoS rendendo irraggiungibile il portale dell'USL Umbria 2 e il sito ufficiale regionale, l'attacco durato almeno cinque ore non è stato attualmente rivendicato da nessun team criminale.

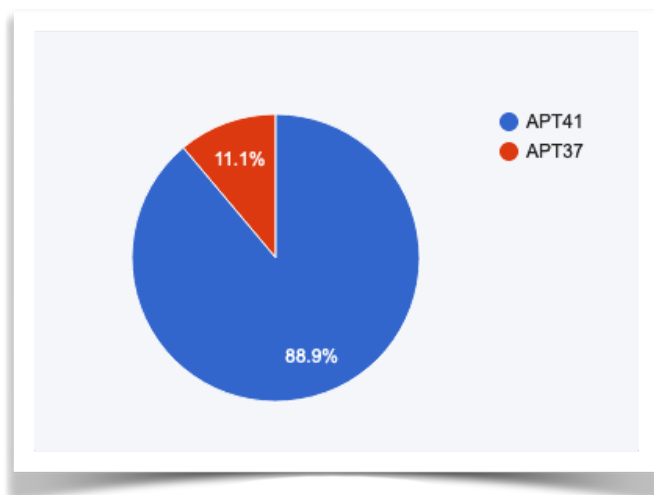
### Russia/Ucraina

Nell'ambito dei risvolti cyber che riguardano l'Italia relativamente al conflitto Russia/Ucraina, nel corso della settimana i gruppi **UserSec** - **Killnet** e **Anonymous Russia** hanno rilasciato dettagli di attacchi DDoS effettuati nei confronti degli **aeroporti di Rimini e Palermo**.

Separatamente la polizia ucraina ha dichiarato di aver smantellato un'enorme **bot farm** gestita da oltre 100 individui. I bot sono stati utilizzati per spingere la propaganda russa e per disinformazione sull'attacco della Russia in Ucraina.

## APT

A seguire l'analisi di campagne afferenti noti gruppi APT e campagne di cyber spionaggio osservate di recente.



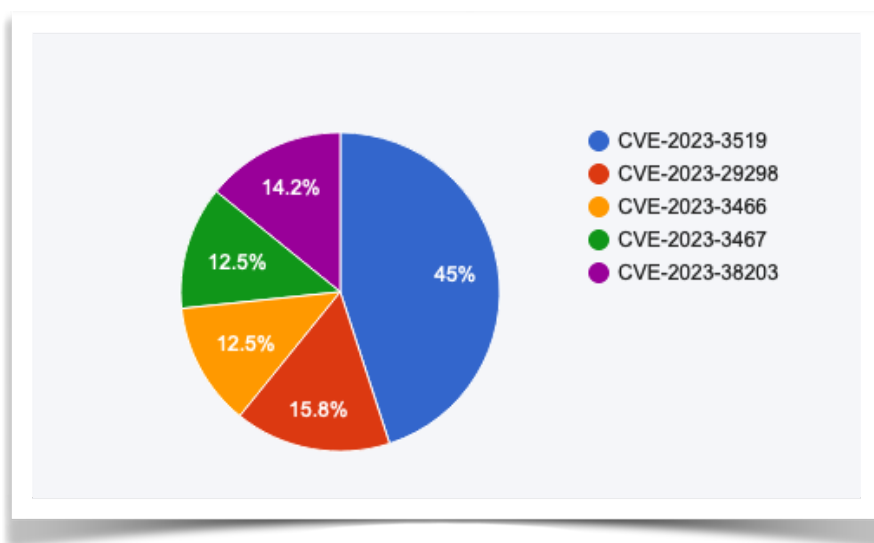
## APT41

Il gruppo **APT41** sostenuto dallo stato cinese sta prendendo di mira i dispositivi Android con due spyware scoperti di recente, soprannominati **WormSpy** e **DragonEgg**.

APT41 è un gruppo noto per condurre operazioni di spionaggio informatico contro entità in vari settori industriali, tra cui sviluppo di software, produzione di hardware, think tank, società di telecomunicazioni, università e governative.

I ricercatori di Lookout hanno scoperto il collegamento di APT41 con gli spyware citati dopo aver individuato un server C2 collegato all'infrastruttura di attacco di APT41 conclamata e già rilevata a settembre 2020 del Dipartimento di giustizia degli Stati Uniti.

### 3. Vulnerabilità



Un gruppo di attaccanti ha violato la rete di un'organizzazione statunitense nel settore delle infrastrutture critiche dopo aver sfruttato una vulnerabilità ZeroDay attualmente identificata con CVE-2023-3519, un problema di tipo RCE di gravità critica insito in **NetScaler ADC e Gateway**, appena corretto da **Citrix**.

**Adobe** ha rilasciato un aggiornamento out-of-band per affrontare vulnerabilità critiche e moderate in **ColdFusion**, incluso uno ZeroDay attivamente sfruttato in the wild.

Le vulnerabilità sono state identificate con i seguenti CVE:

- CVE-2023-38204: una vulnerabilità critica per l'esecuzione di codice remoto (RCE) (valutazione 9,8);
- CVE-2023-38205: una vulnerabilità critica insita nei meccanismi di accesso alla piattaforma (valutazione 7,8);
- CVE-2023-38206: una vulnerabilità moderata insita nei meccanismi di accesso alla piattaforma (valutazione 5,3).

Adobe ha confermato che la vulnerabilità CVE-2023-38205 è attivamente sfruttata ed è stato appurato che la correzione rilasciata in precedenza per il CVE-2023-29298 e ritenuta incompleta è inclusa nel bollettino APSB23-47 ed identificata nell'attuale CVE-2023-38205.

Sono stati rilasciati gli aggiornamenti trimestrali **Oracle**, con correzioni per 508 vulnerabilità.