

|                  |                  |                                                                                                 |
|------------------|------------------|-------------------------------------------------------------------------------------------------|
| Riferimento:     | 2023.57          |                                                                                                 |
| Redatto da:      |                  |                                                                                                 |
| Revisionato da:  |                  |                                                                                                 |
| Data:            | 10/07/2023       |                                                                                                 |
| Destinatari:     | Pubblico         |                                                                                                 |
| Classificazione: | Non Classificato | range: non classificato (verde), Confidenziale (giallo), Riservato (arancione), Segreto (rosso) |

|                 |                        |                                             |
|-----------------|------------------------|---------------------------------------------|
| Oggetto:        | Weekly Threats 27.2023 |                                             |
| 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                     | 7  |
| 2.5 Generic Threat Intelligence       | 9  |
| 3. Vulnerabilità                      | 15 |

## 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 406 campagne di Phishing.

Durante la settimana l'ente maggiormente colpito dal phishing è stato Poste Italiane con 85 campagne di phishing, seguita dalle Credit Agricole Francese con 56 campagne e da Nexi con 22 campagne.

È stata identificata una campagna di phishing ai danni della Banca del Piemonte, un ente che era estraneo al phishing dal 2016. La campagna probabilmente diffusa via SMS richiedeva agli utenti Username e Password di accesso al home banking ed inoltre un contatto telefonico.

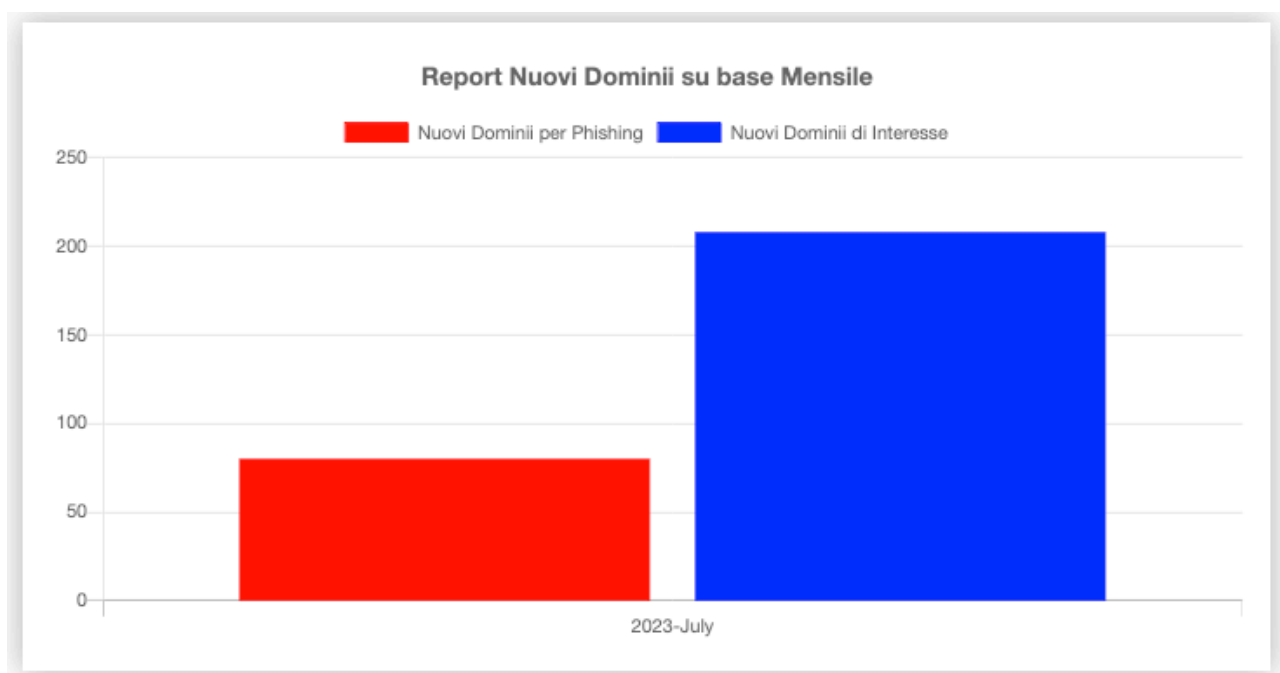
Una particolare campagna di phishing ai danni di Wind è stata diffusa mediante la creazione di due domini Ad Hoc, il target della campagna non erano gli utenti finali come usualmente capita ma i rivenditori (Dealer) del noto operatore telefonico. Il probabile intento è quello di ottenere l'accesso alla loro piattaforma di gestione della customer base per estrarre dati o effettuare SIM Swap.

La prima campagna di phishing dell'anno ai danni della Banca Popolare di Puglia e Basilicata è stata identificata questa settimana con il consueto intento di sottrarre username, password e numeri telefonici per proseguire la frode telefonicamente.

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 208 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 208 nuovi domini, sempre nella settimana, 80 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 presumibilmente ai danni di:

| Data Rilevamento | Nome                                                                      | Email Coinvolte | Domini Email Coinvolti |
|------------------|---------------------------------------------------------------------------|-----------------|------------------------|
| 2023-07-05 11:55 | <a href="https://Mercadazo.com.mx">Mercadazo.com.mx</a>                   | 14918           | 1278                   |
| 2023-07-05 11:55 | <a href="https://Zvendostore.com">Zvendostore.com</a>                     | 9387            | 459                    |
| 2023-07-05 11:55 | <a href="https://Rockpointlegalfunding.com">Rockpointlegalfunding.com</a> | 44160           | 9459                   |
| 2023-07-05 11:55 | <a href="https://Tigerairtw.com">Tigerairtw.com</a>                       | 719161          | 14762                  |
| 2023-07-05 11:55 | <a href="https://Justice.fr">Justice.fr</a>                               | 1159            | 46                     |
| 2023-07-05 11:55 | <a href="https://Appsindicato.org.br">Appsindicato.org.br</a>             | 119868          | 1970                   |
| 2023-07-05 08:33 | <a href="https://Lepipe.it">Lepipe.it</a>                                 | 8457            | 1096                   |
| 2023-07-05 08:31 | <a href="https://Electrical4all.co.uk">Electrical4all.co.uk</a>           | 38355           | 287                    |
| 2023-07-05 08:31 | <a href="https://Excellentcrafts.in">Excellentcrafts.in</a>               | 20079           | 257                    |
| 2023-07-05 08:31 | <a href="https://Barryandclark.com">Barryandclark.com</a>                 | 943             | 66                     |
| 2023-07-05 08:31 | <a href="https://Hayalabs.es">Hayalabs.es</a>                             | 1054            | 126                    |
| 2023-07-05 08:31 | <a href="https://Percufrance.com">Percufrance.com</a>                     | 1085            | 98                     |
| 2023-07-05 08:31 | <a href="https://Webmarketpoint.it">Webmarketpoint.it</a>                 | 17642           | 356                    |
| 2023-07-05 08:31 | <a href="https://Inffusions.com">Inffusions.com</a>                       | 456             | 50                     |
| 2023-07-05 08:31 | <a href="https://Emporiotambo.com.br">Emporiotambo.com.br</a>             | 2339            | 169                    |
| 2023-07-05 08:31 | <a href="https://Ducati.com.my">Ducati.com.my</a>                         | 8               | 3                      |
| 2023-07-05 08:31 | <a href="https://Oshoppingtv.com">Oshoppingtv.com</a>                     | 1437            | 67                     |
| 2023-07-05 08:31 | <a href="https://Melroseshopp.com">Melroseshopp.com</a>                   | 386             | 26                     |

Le informazioni sopra riportate sono state tratte dai forum e dagli ambienti underground di pubblicazione dei data leak.

## 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:

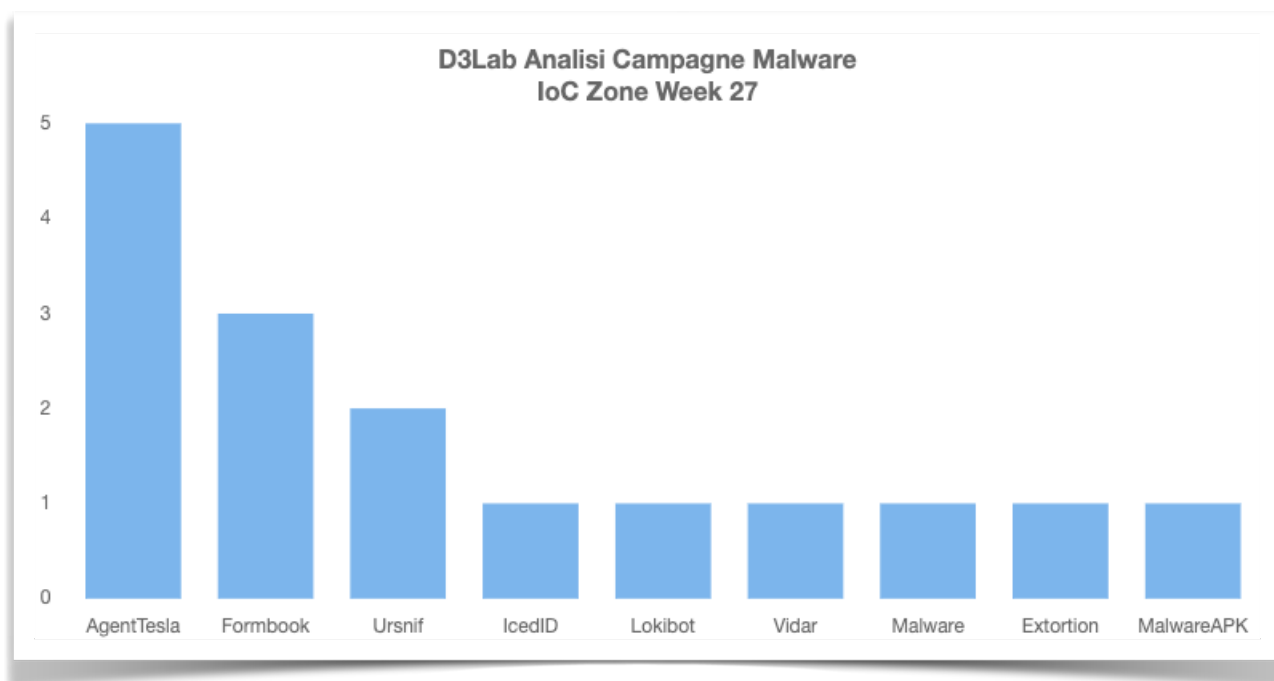
- **Peroni Pompe** - *peronipompe.com* - ransomware **D#NUT**
- **Credit Team Srl** - *creditteam.eu* - Ransomware **NoEscape**
- **Lawer SpA** - *lawer.com* - ransomware **Play**

Sempre in ambito italiano il 4 Luglio, l'**Azienda Ospedaliera Universitaria Luigi Vanvitelli** ha pubblicato un avviso, sul sito web *policliniconapoli.it*, in cui affermava di essere stata vittima, il 1° Luglio di un attacco ransomware, e che stava indagando sull'accaduto.

Il 5 luglio è stato dichiarato che gli attaccanti potrebbero far parte di un gruppo di origine cinese. Il suggerimento apparentemente si basa sul tipo di indirizzo e-mail fornito dall'aggressore all'ospedale per contattare i negoziati.

Un portavoce dell'ospedale ha anche affermato che l'attacco ha colpito principalmente il software utilizzato nei laboratori di analisi. Al momento non sono state fornite ulteriori dichiarazioni ufficiali sull'accaduto.

## 2.4 IoC - Malware



Come di consueto il malware più diffuso in Italia nelle ultime settimane è AgentTesla, veicolato attraverso email a tema commerciale come Ordini e Pagamenti.

Si segnala l'analisi di numerose campagne Formbook anch'esse veicolate tramite malspam a tema commerciale, come Fatture o Pagamenti allegano file archivio ZIP e RaR.

È stata osservata una campagna Ursnif, noto trojan banker che settimanalmente colpisce il territorio italiano. L'ultima campagna analizzata a tema delivery sfrutta il logo del corriere BRT, con allegato una falsa notifica file PDF contenente un link a JS malevolo che rimanda ad un ulteriore collegamento per il rilascio del malware.

Interessante notare il rilevamento di una campagna malware IcedID veicolata tramite la medesima tecnica usata negli attacchi Ursnif, ovvero tramite file PDF contenente JS.

La mail osservata è una risposta generica ad una precedente conversazione intrattenuta dalle vittime.

Infine, nel corso della settimana è stata osservata una nuova campagna malware avente come target account di Posta Elettronica Certificata (PEC), volta a veicolare il malware Vidar.

La malspam riporta un link a file ZIP contenente una falsa Fattura VBS che rimandava ad un collegamento per il rilascio del malware. In questa particolare campagna è stato osservato lo sfruttamento di comunicazioni con canali Telegram usati come C&C.

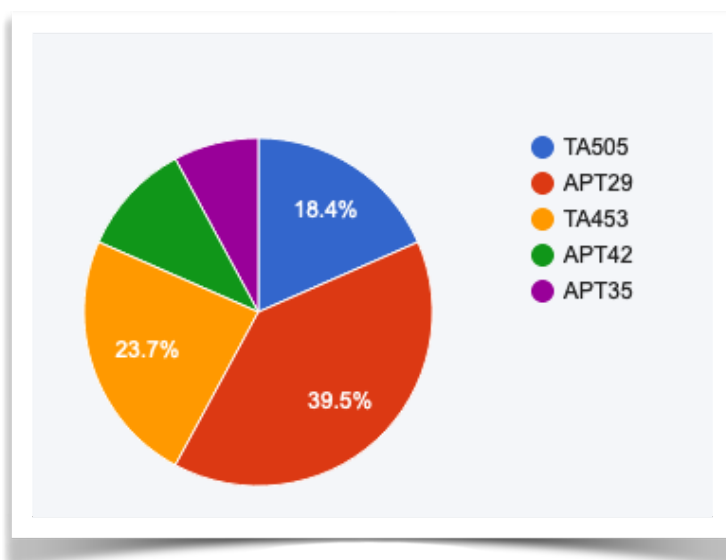
Vidar è un Malware-as-a-Service rilevato per la prima volta nel 2022 appartenente alla famiglia degli infostealer.

Si segnala la persistenza di campagne malware rivolte a dispositivi mobile Android, la campagna attraverso SMS veicola una falsa applicazione bancaria che rilascia il malware Brata un malware capace di prendere il controllo del dispositivi e carpire, SMS e credenziali.

## 2.5 Generic Threat Intelligence

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

### APT



### TA453 - APT49

I ricercatori di Proofpoint hanno osservato una nuova campagna che attribuiscono al gruppo Charming Kitten - TA453 - APT49 in cui gli attaccanti hanno utilizzato un nuovo malware denominato NokNok che prende di mira i sistemi macOS.

Sembra che gli attaccanti abbiano veicolato il malware tramite false email provenienti da esperti statunitensi in tema di nucleare ed hanno attirato le vittime con un'offerta su argomenti di politica estera. L'attacco avviene tramite l'uso di file LNK. Proofpoint afferma di aver collaborato con Dropbox per smantellare parte dell'infrastruttura del gruppo. Charming Kitten è anche noto come APT42 o Phosphorus e ha avviato almeno 30 operazioni in 14 paesi dal 2015.

Google ha collegato l'attaccante allo stato iraniano, in particolare al Corpo delle guardie rivoluzionarie islamiche (IRGC).

**TA505**

La CISA e l'FBI hanno pubblicato un avviso in merito a delle nuove varianti del malware Truebot distribuite su reti compromesse utilizzando una vulnerabilità critica di esecuzione di codice remoto (RCE) nel software Netwrix Auditor, veicolata in attacchi rivolti a organizzazioni negli Stati Uniti e in Canada.

La vulnerabilità identificata con CVE-2022-31199 ha un impatto sul server Netwrix Auditor e sui sistemi di rete monitorati e consente agli attaccanti non autorizzati di eseguire codice con i privilegi SYSTEM.

TrueBot è un downloader di malware collegato al gruppo criminale informatico Silence di lingua russa e utilizzato dagli attaccanti TA505, associati al gruppo FIN11, osservato nella distribuzione del ransomware Colp da Dicembre 2022.

## World Maps / Word Cloud relativa al settore energetico:



Recenti studi hanno osservato che centinaia di installazioni di sistemi di monitoraggio e diagnostica di fotovoltaici (FV) sono esposte online e risultano esposte ad attacchi a causa di una vulnerabilità sfruttata attivamente.

I software interessati in genere vengono utilizzati dalle società energetiche per il monitoraggio remoto delle prestazioni, la risoluzione dei problemi, l'ottimizzazione del sistema delle unità di produzione di energia rinnovabile.

Nello specifico una ricerca pubblicata da Cyble ha rilevato oltre 134.000 prodotti appartenenti a vari fornitori esposti tra cui: Solar-Log, Danfoss Solar Web Server, SolarView Contec, SMA Sunny Webbox, SMA Cluster Controller, SMA Power Reducer Box, Kaco New Energy & Web, Fronis Datamanager, Saj Solar Inverter e ABB Solar Inverter Web GUI.

Non tutti i prodotti esposti online risultano vulnerabili, tuttavia, la ricerca di Cyble evidenzia che potenziali malintenzionati non autenticati possono raccogliere informazioni che potrebbero essere utilizzate per organizzare un attacco.

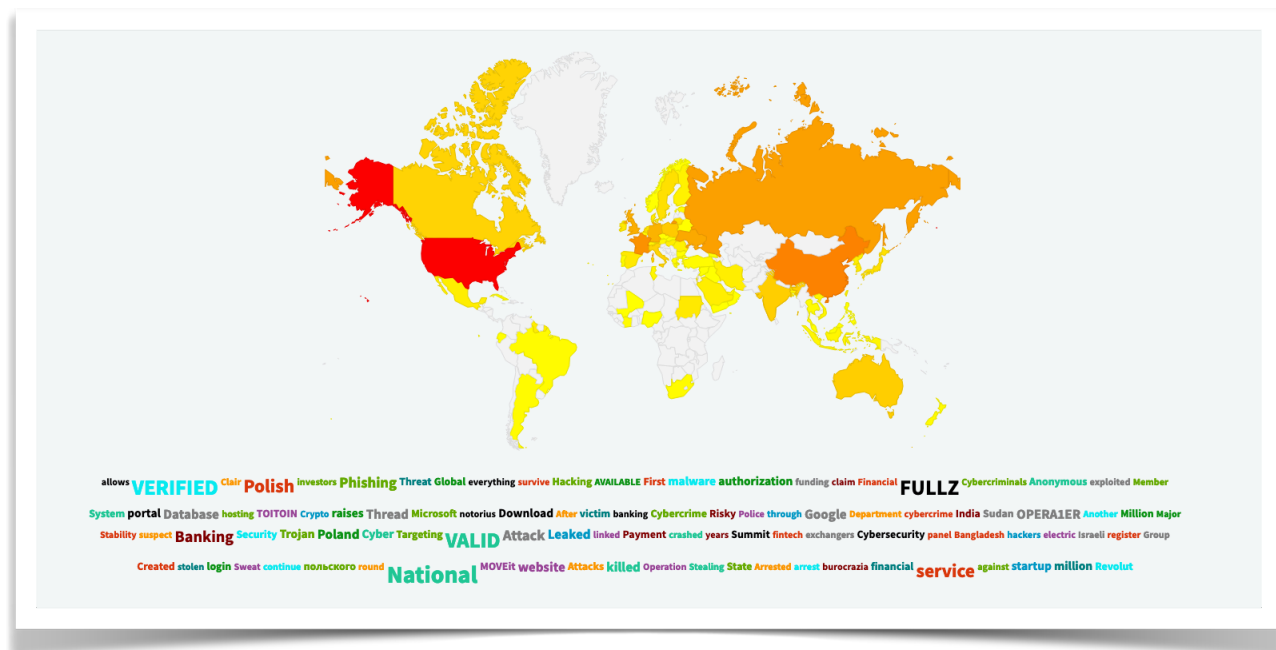
Inoltre, sono state rilevate e segnalate vulnerabilità per i prodotti di cui sopra e che per molti di essi è disponibile un codice exploit Proof of Concept (PoC) come nel caso dei pannelli Web SolarView che sono stati presi di mira dalla botnet Mirai per attacchi DDoS.

La vulnerabilità sfruttata è stata risolta ed identificata con CVE-2022-29303.

Le scansioni Shodan pubblicate di Cyble hanno rilevato 7.309 dispositivi SolarView esposti a livello globale, mentre un altro rapporto pubblicato da VulnCheck afferma che dei 600 sistemi SolarView attualmente esposti su Internet, circa 400 sono versioni vulnerabili agli attacchi.

Il rapporto di VulnCheck evidenzia che un'altra vulnerabilità di esecuzione di codice remoto non autenticato, scoperta di recente, identificata con CVE-2023-23333, ha impatto sullo stesso prodotto SolarView ed è potenzialmente sfruttabile a causa di più exploit rilasciati in the wild.

## World Maps / Word Cloud relativa al settore bancario:



La Reserve Bank of India ha multato l'AP Mahesh Cooperative Urban Bank per la somma di 80.000 dollari, in quanto ritenute responsabile di una violazione che ha causato la perdita di 1,5 milioni di dollari fondi dei clienti. La banca è stata vittima di un attacco di phishing nel gennaio 2022 che ha consentito agli attaccanti il pieno accesso alla rete della banca. La polizia di Hyderabad ha ritenuto la banca colpevole della violazione in quanto non ha implementato le misure di sicurezza informatica di base.

Recentemente la Deutsche Bank ha avvisato i clienti di aver subito una violazione che ha interessato i loro dati. Anche la controllata Postbank è interessata dal furto di dati.

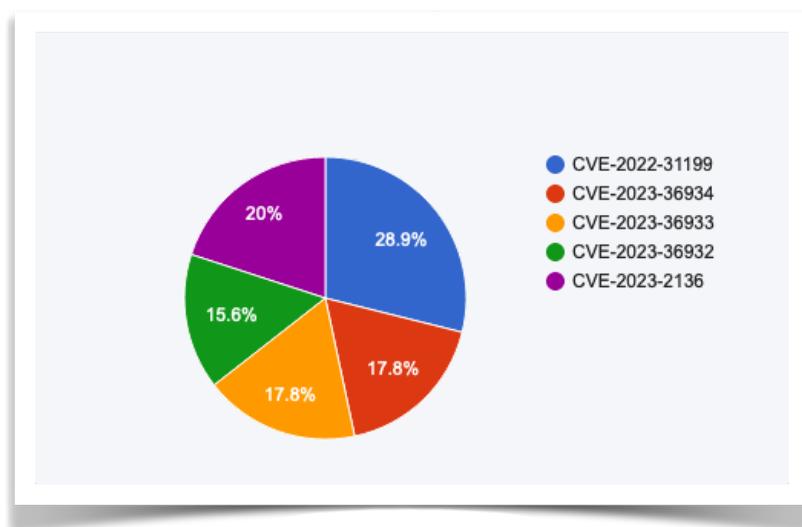
Deutsche Bank ha confermato il 7 luglio 2023 a Francoforte che si era verificato un incidente di sicurezza presso un fornitore esterno di servizi di cambio.

Un attacco di origine sconosciuta ha sfruttato una vulnerabilità nel servizio di elaborazione dei pagamenti Revolut e ha rubato più di 23 milioni di dollari dai conti dell'azienda. Gli attacchi hanno sfruttato una vulnerabilità in un sistema Revolut che analizzava le transazioni tra utenti europei e statunitensi.

Le autorità della Costa d'Avorio hanno arrestato un uomo sospettato di essere un membro di un grande cartello criminale informatico noto come OPERA1ER. L'uomo è il primo sospettato ad essere arrestato in relazione alla banda, uno dei pochi gruppi di criminalità informatica a colpire

ripetutamente i paesi africani. Conosciuto anche come DESKTOP Group e Common Raven, il gruppo è attivo dal 2019 e si ritiene che abbia rubato tra gli 11 e i 30 milioni di dollari in più di 30 attacchi. La maggior parte delle vittime sono banche e servizi finanziari africani.

### 3. Vulnerabilità



È stata scoperta una vulnerabilità di escalation di privilegi nel kernel Linux, denominata StackRot (CVE-2023-3269), la vulnerabilità ha origine nel sistema di gestione della memoria virtuale del kernel e consente agli aggressori di effettuare una privilege escalation ed eseguire il codice come root.

Sono stati rilasciati aggiornamenti di sicurezza di AndroidOS, Google afferma che tre delle vulnerabilità risolte questo mese (CVE-2021-29256, CVE-2023-2136 e CVE-2023-26083.) sono state attivamente sfruttate in the wild.

Cisco ha rilasciato quattro aggiornamenti di sicurezza. Uno di questi, CVE-2023-20185, è piuttosto critico in quanto consente a attaccanti remoti non autenticati di leggere o modificare il traffico crittografato tra i siti. Cisco non rilascerà aggiornamenti perché il problema riguarda la vecchia linea di switch per data center della serie Nexus 9000.

Progress Software ha rilasciato un aggiornamento di sicurezza per il suo software MOVEit MFA. Sono stati corretti tre nuove vulnerabilità, incluso un problema critico identificato con CVE-2023-36934 che consente un bypass dell'autenticazione.

VMware ha avvertito i clienti in merito al rilevamento di codice exploit di sfruttamento di una vulnerabilità critica in VMware Aria Operations for Logs. La vulnerabilità identificata con CVE-2023-20864 è stata risolta ad Aprile, con il rilascio di VMware Aria Operations for Logs 8.12,

e consente agli aggressori non autenticati di ottenere l'esecuzione remota su dispositivi non aggiornati.

Apple ha emesso nuovi aggiornamenti Rapid Security Response (RSR) per risolvere un nuovo ZeroDay (CVE-2023-37450) attivamente sfruttato in attacchi che hanno un impatto su iPhone, Mac e iPad.