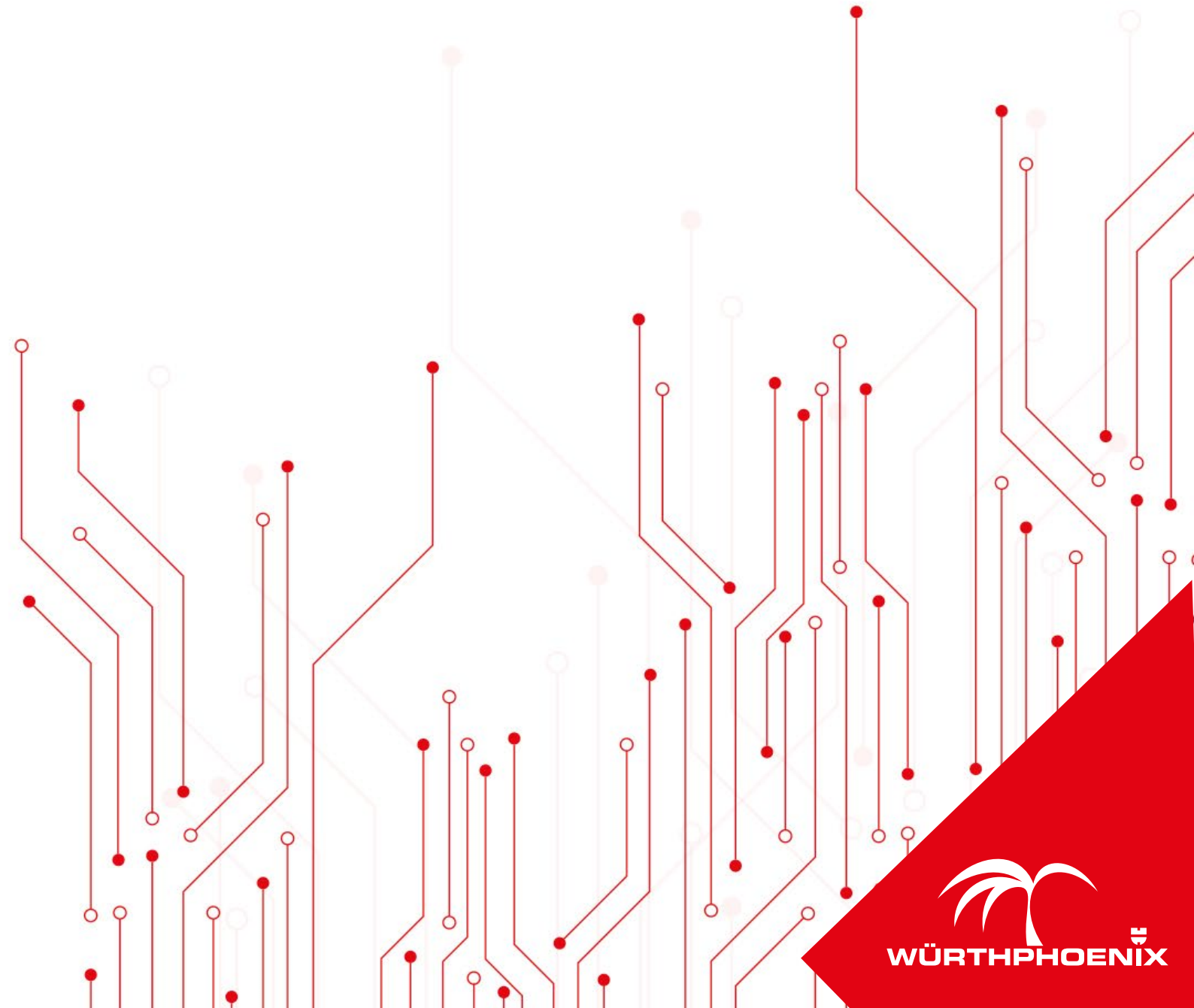
® Würth Phoenix Srl

maggio 2023

Italian Banks – WP CTI Report 2023

Valutazione dell'esposizione cyber delle principali banche italiane



Indice

Indice delle tabelle

Indice dei grafici

Indice delle immagini

Glossario

Capture The Flag (CTF): una competizione in cui i partecipanti cercano di risolvere sfide di sicurezza informatica al fine di trovare e catturare una "bandiera" (flag).

BEC: Business Email Compromise: un tipo di attacco informatico in cui i cyber criminali compromettono un account email aziendale per effettuare truffe o rubare informazioni.

Data Leak Site: un sito web in cui i dati rubati o compromessi vengono pubblicati o venduti.

DDoS - Distributed Denial of Service (DDoS): un attacco informatico in cui un grande numero di dispositivi collegati a Internet viene utilizzato per sovraccaricare un sito web o un server, rendendolo inaccessibile agli utenti legittimi.

Exploit: un metodo o un codice che sfrutta una vulnerabilità o una debolezza di un sistema o di un'applicazione.

FTP - File Transfer Protocol: un protocollo di rete utilizzato per trasferire file da un computer a un altro computer attraverso una connessione Internet/Intranet.

Indicators of Compromise (IoC): dati o informazioni che indicano un possibile attacco o compromissione di un sistema o di una rete.

Infostealer: un tipo di malware progettato per rubare informazioni sensibili, come password, numeri di carta di credito o informazioni bancarie.

Infostealer market place: un luogo online in cui vengono acquistati e venduti gli archivi esfiltrati attraverso l'utilizzo degli infostealer malware.

Jackpotting: un attacco informatico in cui gli hacker prendono il controllo di un ATM (Automated Teller Machine) e lo costringono ad erogare tutte le banconote contenute all'interno.

Malware: software malevolo progettato per danneggiare o compromettere un sistema o una rete.

Penetration Test: una valutazione della sicurezza informatica in cui un team di esperti cerca di identificare vulnerabilità e violare la sicurezza di un sistema o di un'organizzazione, documentando le vulnerabilità riscontrate.

Phishing: una tecnica di attacco informatico in cui gli utenti vengono ingannati per fornire informazioni personali o sensibili tramite email, siti web falsi o altre forme di comunicazione.

Ransomware: un tipo di malware che crittografa i dati di un sistema o di un'organizzazione e richiede il pagamento di un riscatto per ripristinare l'accesso.

Ransomware double extortion: una tattica utilizzata da alcuni threat actors in cui i dati dell'organizzazione vengono rubati e minacciati di essere pubblicati, a meno che non venga pagato un riscatto per impedire la pubblicazione.

Reconnaissance: l'attività di raccolta di informazioni riguardanti un target specifico, come un sistema o un'organizzazione, al fine di identificare eventuali vulnerabilità o debolezze.

Regola di detection: una serie di criteri o parametri utilizzati per identificare e rilevare minacce informatiche.

Remote Desktop Protocol (RDP): un protocollo di rete che consente a un utente di controllare un computer da un altro computer o dispositivo.

Secure Shell (SSH): un protocollo di rete che consente agli utenti di accedere in modo sicuro a un sistema remoto.

Social Engineering: l'uso della manipolazione psicologica per ottenere informazioni o accesso ad informazioni utilizzabili in un contesto di attacco.

Strong Customer Authentication (SCA): è una tipologia di autenticazione che richiede l'utilizzo di un sistema multifattoriale per la gestione di servizi di pagamento bancario e per servizi informativi che richiedono lo scambio di dati confidenziali. L'utilizzo della SCA è un requisito disciplinato dalla seconda Direttiva sui Sistemi di Pagamento PSD2 e dalla successiva RTS (Regulatory Technical Standards) dell'EBA.

TELNET: un protocollo di rete che consente agli utenti di accedere a un sistema remoto tramite una connessione Internet/Intranet.

Threat Actor: un individuo o un gruppo che ha come obiettivo compromettere la sicurezza informatica di un'organizzazione o di un individuo.

Trojan: un tipo di malware che si presenta come un'applicazione legittima, ma che in realtà esegue funzioni dannose.

VNC - Virtual Network Computing: un protocollo di rete che consente agli utenti di controllare un computer remoto tramite una connessione Internet/Intranet.

Whaling: un tipo di attacco di phishing rivolto ai dirigenti o ai dipendenti di alto livello di un'organizzazione.

Prefazione

A cura della Dott.ssa Petra Chistè, Responsabile Sicurezza Informatica di Volksbank.

Nell'era digitale di oggi, il settore finanziario è diventato uno dei principali obiettivi per gli attacchi informatici. L'avanzamento tecnologico ha rivoluzionato il modo in cui gestiamo le transazioni e conserviamo le informazioni finanziarie, ma ha anche creato nuove vulnerabilità e sfide per le istituzioni finanziarie. Le diverse tipologie di attacchi informatici e le modalità di attacco nel mondo finance sono in costante aumento e diviene sempre più importante comprenderne il funzionamento con l'obiettivo di sensibilizzare e promuovere la consapevolezza sulla crescente minaccia che questi attacchi rappresentano per il settore bancario.

Gli aggressori utilizzano tecniche sempre più avanzate per penetrare le difese delle istituzioni finanziarie, sfruttando vulnerabilità sia nelle infrastrutture tecnologiche che nelle risorse umane. Per affrontare le sfide future della cyber security nel settore bancario, le istituzioni finanziarie dovranno adottare un approccio proattivo e resiliente alla sicurezza informatica.

Ciò implica investire nella formazione e nella consapevolezza del personale, implementare politiche e procedure rigorose per la gestione delle vulnerabilità e delle violazioni dei dati, e collaborare con altre istituzioni, autorità di regolamentazione e organismi internazionali per condividere informazioni sulle minacce e sviluppare soluzioni comuni.

In questo contesto di crescente minaccia di attacchi informatici e di frodi, l'uomo è al centro degli attacchi, ma al tempo stesso è la migliore misura di sicurezza. L'importanza della consapevolezza e della formazione in ambito cyber security anche nei clienti delle banche, soprattutto i giovani, è un ambito dove bisogna maggiormente investire.

I nativi digitali interagiscono costantemente con le tecnologie e i servizi finanziari online, il che li rende un gruppo particolarmente vulnerabile alle frodi e agli attacchi informatici. Per queste generazioni appare naturale che una banca possa interagire con loro tramite uno smartphone o con una chiamata dal call center. Sicuramente la passata pandemia ha amplificato questa tendenza.

La formazione e la consapevolezza non solo aiuta i giovani a comprendere i rischi associati all'uso delle piattaforme finanziarie digitali, ma gli fornisce anche le competenze e le conoscenze necessarie per proteggersi e per prendere decisioni informate riguardo alle loro attività finanziarie. Tra gli argomenti chiave che dovrebbero essere affrontati in questi programmi di formazione, troviamo la protezione delle credenziali di accesso, l'identificazione di e-mail e siti web fraudolenti, la prevenzione del furto d'identità e l'adozione di misure di sicurezza informatica, come l'utilizzo di software antivirus e di reti VPN.

È altresì essenziale che le istituzioni finanziarie, le scuole e le università collaborino per sviluppare programmi di formazione efficaci e accessibili. Attraverso l'introduzione di corsi, seminari e workshop sul tema della cyber security e delle frodi, è possibile sensibilizzare i giovani sui rischi e le minacce a cui sono esposti, fornendo loro gli strumenti per agire in modo responsabile e sicuro nel mondo digitale. Un'altra strategia fondamentale per aumentare la consapevolezza e la formazione in materia di cyber security e frodi tra i giovani è quella di incoraggiare la partecipazione attiva delle famiglie e delle comunità locali, comprese le realtà ICT presenti sul territorio. Queste devono essere coinvolte nell'educazione dei giovani sulle questioni relative alla sicurezza informatica e alla prevenzione delle frodi, contribuendo a creare un ambiente di apprendimento solido e supportivo.

I nativi digitali si dimostrano poco reattivi ai canali classici di comunicazione utilizzati da una banca, siano essi email o sms. Il ruolo che possono giocare i social media nell'informare i giovani non deve essere sottovalutato. Diversamente attraverso l'utilizzo di messaggi accattivanti e la diffusione di informazioni accurate e pertinenti, è possibile raggiungere un pubblico più ampio e contribuire a creare una cultura di responsabilità e consapevolezza in materia di cyber security.

Anche l'utilizzo delle modalità di gaming appassionano i giovani: contest e le note Capture the Flag rappresentano degli ottimi momenti educativi che devono poter includere anche i non addetti ai lavori.

Non possiamo dimenticare il fondamentale ruolo che giocheranno le tecnologie emergenti come le intelligenze artificiali o l'elaborazione di grandi quantità di dati. Se da un lato queste potranno diventare degli ottimi meccanismi di difesa, capaci di migliorare la risposta ad un attacco o analizzare sempre più puntualmente le transazioni finanziarie, dall'altra diventeranno anche degli ottimi strumenti di attacco, con una maggiore capacità offensiva e adattativa.

Mentre gli attaccanti fin dagli inizi hanno una rete di interscambio efficiente e veloce di informazioni e di tecniche, i "difensori" ancora peccano su questo ambito.

Le diverse normative emergenti in questo ambito hanno cercato di spingere sempre maggiormente verso la cooperazione ed una svolta importante è data dal regolamento Dora dove vi è una esplicita richiesta di impegno alla cooperazione. Scopo della cooperazione è favorire lo scambio di informazioni tra stati membri e istituzioni finanziarie, quali i nuovi attacchi, le tecniche utilizzate e le misure di mitigazione adottate.

In questo contesto il CTI Report 2023 - Italian Banks non solo permette di avere un quadro statistico della postura di sicurezza del settore bancario italiano, ma anche di comprendere le minacce maggiormente presenti nel nostro settore e il funzionamento delle stesse.

1 Introduzione

Il report Italian Banks - CTI Report 2023 è stato sviluppato dal Security Operation Center Attacker Centric di Würth Phoenix con l'obiettivo di valutare l'esposizione cyber dei principali gruppi bancari del nostro Paese.

Le banche sono una parte fondamentale del tessuto economico di un paese e spesso la cartina al tornasole dello stato di salute del paese stesso.

Le funzioni principali di una banca sono: la funzione di intermediazione creditizia, la funzione monetaria, la funzione di prestazione di servizi e la funzione di trasmissione della politica economica e monetaria. Funzioni che necessitano di una solidità importante, continuativa e resiliente ai cambiamenti, sempre più repentini e presenti a livello globale.

Gli elementi che vengono utilizzati per valutare, al di fuori del contesto cyber, la solidità di una banca, sono differenti e la classifica che è stata utilizzata come input per il presente report prende in considerazione il valore del requisito P2R.

Il requisito di secondo pilastro (P2R) è un requisito patrimoniale specifico della banca che si applica in aggiunta al requisito patrimoniale minimo (noto come primo pilastro) quando questo sottostima o non copre determinati rischi. Il P2R di una banca viene determinato nell'ambito del processo di revisione e valutazione prudenziale (SREP). Questo requisito è legalmente vincolante e, se gli istituti non lo rispettano, possono essere soggetti a misure di vigilanza (comprese le sanzioni). Il P2R non comprende il rischio di leva finanziaria eccessiva, che è coperto dal requisito del coefficiente di leva finanziaria del secondo pilastro (P2R-LR).

Oltre a rispettare il P2R, gli istituti sono tenuti a seguire le linee guida del secondo pilastro (P2G) emanate dalla BCE. Il P2G di una banca indica il livello di capitale che dovrebbe mantenere per resistere agli stress finanziari. A differenza delle P2R, le P2G non sono giuridicamente vincolanti, in quanto riflettono solo le aspettative della vigilanza.

Ai sensi degli articoli 431(1), 433a(1) e 438(b) del Regolamento sui requisiti patrimoniali (CRR), i grandi istituti (come definiti all'articolo 4(1)(146) del CRR) sono tenuti a comunicare i propri P2R su base annuale.

Inoltre, la BCE continua la sua recente prassi di pubblicare i P2R consolidati di tutte le istituzioni significative su cui vigila, dopo aver ottenuto il loro consenso alla pubblicazione. Proprio da questa lista, raggiungibile al link https://tinyurl.com/mr289nnf, sono stati estratti gli istituti di credito italiani oggetto dell'analisi presente all'interno di questo report.

2 Banche e cyber security - riferimenti normativi

Da sempre l'ambito finanziario risulta essere uno di quelli più interessanti agli occhi dei Threat Actor, consapevoli del fatto di poter investire tempo e denaro nella preparazione delle attività di attacco, considerata la disponibilità economica delle potenziali vittime. Per gli attaccanti si tratta di una mera valutazione del ROI (Return Of Investment), dove quindi il costo delle diverse fasi dell'attacco deve essere inferiore al profitto derivante dagli attacchi andati a segno. Chiaramente questa è una voluta semplificazione che non prende in considerazione le molte sfaccettature nell'organizzazione dei gruppi di attaccanti, dove di norma vi è una struttura fortemente gerarchizzata, nella quale sono presenti figure apicali di gestione della singola gang di attaccanti e affiliati che operano utilizzando gli strumenti messi a disposizione dalla gang stessa.

Se andiamo a verificare le vittime di attacchi di tipo ransomware double extortion (questa tipologia di attacco si verifica quando i cyber attaccanti chiedono due riscatti: il pagamento per decriptare i dati e/o i backup e il pagamento per non far trapelare i dati esfiltrati, o rubati), prelevando i dati (all'8 aprile 2023) dall'ottimo progetto DoubleExtortion.com di Luca Mella, che raggruppa le evidenze dai Data Leak Site delle diverse ransomware gang, possiamo notare come su un totale di 8103 vittime, 379 appartengono al settore finance. Se a questi target, aggiungiamo anche quelli che fanno parte del settore insurance, arriviamo a 488 target. Sia chiaro che questi dati si riferiscono per la maggior parte ad attacchi che non hanno indotto la vittima al pagamento del riscatto, motivo per cui le ransomware gang hanno quindi pubblicato la notizia dell'avvenuto attacco, pubblicando parte di o tutti i dati esfiltrati.

Proprio in virtù del particolare interesse da parte dei cyber attaccanti per questo ambito, sono state nel tempo introdotte normative e regolamenti, delle quali di seguito riassumiamo le più importanti a livello nazionale ed europeo, in grado di aumentare sensibilmente la resilienza agli attacchi ed in generale la capacità di difesa, sia reattiva che predittiva, da parte delle organizzazioni finanziarie.

2.1 Circolare n. 285/2013

La nota circolare n. 285/2013 della Banca d'Italia e relativi aggiornamenti (fino al 42 del 30 marzo 2023), nella PARTE IV - Sistemi informativi e sicurezza informatica, chiede di descrivere le caratteristiche del sistema informativo in relazione alle proprie esigenze operative e al fabbisogno informativo degli organi aziendali per assumere decisioni consapevoli e coerenti con gli obiettivi aziendali e definire il sistema di gestione della sicurezza informatica, indicando cinque diversi elementi:

1. i ruoli e le responsabilità attribuiti agli organi e alle funzioni aziendali in materia di sviluppo e gestione dei sistemi informativi, con particolare riferimento all'organizzazione della funzione ICT;

2. il processo di analisi del rischio informatico e la sua interazione con il rischio operativo;

3. il sistema di gestione della sicurezza informatica, con particolare riferimento: alla policy di sicurezza informatica; alle misure adottate per assicurare la sicurezza dei dati e il controllo degli accessi, incluse quelle dedicate alla sicurezza dei servizi telematici per la clientela; alla gestione dei cambiamenti e degli incidenti di sicurezza; alla disponibilità delle informazioni e dei servizi ICT;

4. il sistema di gestione dei dati;

5. le politiche di esternalizzazione di sistemi e servizi ICT, con particolare riferimento all'esternalizzazione di sistemi informativi critici.

2.2 Normativa europea PSD2

Nell'ambito dei servizi di pagamento, la normativa che a livello europeo ha formalizzato tutte le strutture necessarie a garantire il corretto funzionamento delle transazioni che avvengono digitalmente è la Direttiva europea 2015/2366 sui Servizi di Pagamento, meglio nota come Payment Services Directive, arrivata alla sua seconda versione. La PSD2 è una disposizione, voluta dall'UE, che pone le fondamenta giuridiche per un mercato unico dei pagamenti in tutta Europa, volto a stabilire servizi di pagamento innovativi e sicuri per gli Stati Membri. Pubblicata ufficialmente in Gazzetta europea nel 2015, essa è stata poi recepita in maniera effettiva il 14 settembre 2019.

Uno degli obiettivi principali della normativa PSD2 è quella di garantire la sicurezza delle informazioni e dei dati dei consumatori finali attraverso l'utilizzo della Strong Customer Authentication.

È in questa ottica che viene sviluppato un nuovo modo di autenticare l'utente che effettua un pagamento. A partire dal 31 dicembre 2020, i prestatori di servizi di pagamento hanno dovuto implementare obbligatoriamente la Strong Customer Authentication (SCA), ovvero l'autenticazione forte che i consumatori devono effettuare quando realizzano un pagamento con uno strumento elettronico.

I fattori che l'utente deve verificare affinché il pagamento possa essere eseguito sono due fra i seguenti tre:

- "Something you know", ovvero qualcosa che solo il cliente conosce (password, PIN, etc.)

- "Something you have", quindi qualcosa che solo il cliente possiede (smartphone, token bancario, etc.)
- "Something you are", ovvero qualcosa che solo il cliente è (riconoscimento facciale, impronta digitale, etc.)

Il meccanismo introdotto, inoltre, aumenta la sicurezza generando un codice univoco per ogni transazione che viene effettuata, non basato su una logica esclusivamente temporale come nel caso dei codici OTP delle chiavette bancarie.

2.3 Orientamenti EBA n. 2021/03

Attraverso il documento EBA/GL/2021/03 del 10 giugno 2021, la EBA (European Banking Authority) ha voluto mettere a disposizione degli orientamenti che specificano i criteri per la classificazione dei gravi incidenti operativi o di sicurezza riscontrati dai prestatori di servizi di pagamento, nonché il formato e le procedure da seguire per comunicare tali incidenti all'autorità competente dello Stato membro di origine, ai sensi dell'articolo 96, paragrafo 1, della PSD2.

Gli orientamenti EBA diventano particolarmente interessanti in quanto indicano dei valori oggettivi che i prestatori di servizi di pagamento devono tenere in considerazione per valutare un incidente:

Criteri	Livello di impatto minore	Livello di impatto maggiore
Transazioni interessate	> 10 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) **e** durata dell'incidente > 1 ora* **o** > 500 000 EUR **e** durata dell'incidente > 1 ora*	> 25 % del livello normale delle transazioni del prestatore di servizi di pagamento (in termini di numero di transazioni) **o** > 15 000 000 EUR
Utenti di servizi di pagamento interessati	> 5 000 **e** durata dell'incidente > 1 ora* **o** > 10 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento **e** durata dell'incidente > 1 ora*	> 50 000 **o** > 25 % degli utenti di servizi di pagamento del prestatore di servizi di pagamento
Periodo di indisponibilità del servizio	> 2 ore	Non applicabile
Violazione della sicurezza della rete o dei sistemi informativi	Sì	Non applicabile
Impatto economico	Non applicabile	> Max (0,1 % del capitale di classe 1**, 200 000 EUR)

Tabella 1 - criteri per la classificazione dei gravi incidenti operativi o di sicurezza

Gli orientamenti EBA indicano inoltre le informazioni che devono essere trasmesse dal prestatore di servizi di pagamento alle autorità nazionali rilevanti, in caso di incidente grave:

- data e ora della classificazione dell'incidente come grave;
- data e ora di rilevazione dell'incidente;
- data e ora di inizio dell'incidente;
- data e ora in cui l'incidente è stato risolto o in cui si prevede di risolverlo;
- breve descrizione dell'incidente (comprese le parti non sensibili della descrizione dettagliata);
- breve descrizione delle misure adottate o previste per il ripristino dopo l'incidente;
- descrizione di come l'incidente potrebbe interessare altri prestatori di servizi di
- pagamento e/o infrastrutture;
- descrizione (se del caso) della copertura mediatica;
- causa dell'incidente.

2.4 Direttiva NIS1

La Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi), è stata recepita nel nostro ordinamento attraverso il decreto legislativo 18 maggio 2018, n. 65 (anche detto "decreto legislativo NIS"), in vigore dal 24 giugno 2018.

La direttiva Nis, adottata dall'Unione Europea nel 2016 e recepita in Italia dal Decreto Legislativo del 18 maggio 2018, stabilisce i requisiti minimi per la sicurezza delle reti e dei sistemi informativi nell'UE.

Si applica agli operatori di servizi essenziali (OSE) e ai fornitori di servizi digitali (DSP). I primi sono soggetti pubblici o privati che prestano servizi la cui interruzione avrebbe un impatto significativo sulla società o sull'ambiente (settori energia, trasporti ferroviari, trasporti aerei, acqua potabile e gestione delle acque reflue, sanità.). I secondi sono aziende che offrono servizi basati su tecnologie digitali (internet, cloud computing) e forniscono servizi digitali ai consumatori, come lo shopping online o il banking online. Ciascuno Stato membro ha la possibilità di identificare i propri operatori di servizi essenziali e fornitori di servizi digitali e di applicare i requisiti della direttiva NIS in modo da garantire un livello adeguato di sicurezza delle informazioni.

La direttiva si basa essenzialmente su tre pilastri:

- prevenzione: gli operatori di servizi essenziali e i fornitori di servizi digitali devono mettere in atto misure per prevenire gli attacchi informatici;
- rilevamento: gli stessi devono essere in grado di individuare tempestivamente gli attacchi informatici;
- mitigazione: essi devono essere in grado di ripristinare rapidamente i propri servizi in caso di attacco informatico.

Agli operatori ed ai relativi fornitori sono richiesti alcuni obblighi, tra i quali:

- progettare misure tecniche capaci di gestire i rischi informatici e designare un responsabile della sicurezza delle informazioni;
- puntare sulla prevenzione di incidenti che violino la sicurezza delle proprie reti informatiche;
- contenere i danni di eventuali attacchi e garantire la continuità dei servizi;
- notificare alle autorità competenti, entro 24 ore, gli incidenti che minano la continuità e la fornitura dei servizi o comportino la divulgazione di dati sensibili. Successivamente, inviare entro le 72 ore un report dettagliato di quanto avvenuto.

2.5 Direttiva NIS2

Per quanto valida, negli anni la direttiva NIS ha mostrato dei limiti, come la mancanza di condivisione delle informazioni per affrontare crisi in modo congiunto. Il 14 dicembre 2022 è stata definitivamente approvata la Direttiva n. 2555/2022, entrata in vigore il 17 gennaio 2023. La direttiva, anche detta Direttiva NIS2, è relativa all'adozione di misure volte a garantire un livello comune elevato di cyber security nell'Unione Europea.

LA NIS2 rafforza la cyber security a livello comunitario, prevedendo la creazione di una rete europea, la EU-CyCLONe, che riunisca le varie organizzazioni nazionali che si occupano della gestione delle crisi informatiche, in modo da garantire una risposta coordinata in caso di cyber attacchi su larga scala in Europa. Inoltre, prevede che l'ENISA, l'Agenzia Europea per la cyber security, dia vita a un database condiviso che collezioni tutte le vulnerabilità informatiche note, simile al National Vulnerability Database (NVD) americano.

La Direttiva NIS2 disciplina le misure di gestione del rischio di sicurezza informatica e gli obblighi di segnalazione nei settori destinatari della direttiva, come il settore energetico, i trasporti, le telecomunicazioni, le infrastrutture digitali e l'**ambito bancario e finanziario**.

La Direttiva NIS2 integra e potenzia le misure già adottate dalla precedente Direttiva NIS1, stabilendo, in particolare:

a) obblighi in capo agli Stati membri di adottare strategie nazionali in materia di cyber security e di designare o creare autorità nazionali competenti, anche per la gestione delle crisi informatiche;

b) l'adozione di misure in materia di gestione dei rischi di cyber security e obblighi di segnalazione per i destinatari della Direttiva stessa;

c) norme e obblighi in materia di condivisione delle informazioni sulla cyber security;

d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.

2.6 Regolamento Dora

Il Digital Operational Resilience Act ha l'obiettivo di consolidare e armonizzare a livello europeo i principali requisiti di cyber security con riferimento alla resilienza operativa digitale nel settore finanziario, rivolgendosi quindi a banche, compagnie di assicurazione, società di servizi di criptovalute, istituzioni finanziarie ed i loro fornitori critici. Il Regolamento DORA, entrato in vigore il 16 gennaio 2023, troverà applicazione e sarà vincolante a partire dal 17 Gennaio 2025 (decorsi 24 mesi dalla sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea).

Il Regolamento propone sei diversi "pillar" che le organizzazioni dovranno implementare:

ICT Governance: obiettivo un potenziamento delle responsabilità per le funzioni interne ICT ed un migliore allineamento delle strategie di gestione dei rischi ICT da parte delle entità finanziarie. L'Organo di Gestione avrà un ruolo fondamentale nell'attribuire responsabilità e ruoli per tutte le funzioni ICT, controllare e monitorare la gestione dei rischi ICT ed allocare adeguatamente investimenti e formazione in ambito ICT.

Gestione dei rischi ICT e cyber: obiettivo di migliorare e armonizzare le regole per la gestione del rischio ICT. Le entità finanziarie dovranno istituire e mantenere strumenti e sistemi ICT resilienti attraverso l'identificazione dei rischi ICT, la predisposizione di misure di protezione e prevenzione, il rilevamento di minacce, la gestione degli incidenti, l'implementazione di strategie di continuità operativa e piani di ripristino in caso di disastro.

Reporting degli incidenti ICT e cyber: prevede specifici obblighi in materia di gestione degli incidenti ICT. Le organizzazioni di settore dovranno implementare un sistema di mappatura, in cui si classificheranno i vari incidenti sulla base di criteri descritti nel Regolamento e ulteriormente definiti dalle AEV (Autorità Europee di Vigilanza) per specificare le soglie di rilevanza.

Digital Resilience testing: obiettivo è far sì che le entità finanziarie siano sottoposte periodicamente a test per accertarne il grado di maturità, identificarne punti deboli e definire eventuali misure correttive. Tale disposizione evidenzia l'obiettivo del regolatore di adottare un approccio proattivo che non si limiti alle sole misure correttive "di reazione". In questa fase, le attività di Penetration Test e di Adversary Simulation (Red Teaming), dovranno essere svolte solo da soggetti autorizzati e opportunamente certificati. Al riguardo, per lo svolgimento di questi test, può essere utilizzato il Framework previsto dalla Comunità Europea, ossia il TIBER EU, recepito in Italia come TIBER IT, adottato anche da Banca d'Italia, la Consob e l'IVASS.

Outsourcing - Rischi Terze Parti: per questo ambito il regolatore specifica che le varie entità dovranno garantire il rispetto di norme che si applicano al monitoraggio dei rischi ICT derivanti da Terze Parti, includendo anche una descrizione completa dei servizi in ambito, l'indicazione dei centri di elaborazione dei dati, descrizioni complete degli SLA garantiti. Ulteriore obiettivo l'armonizzazione degli elementi essenziali del servizio in tutte le fasi del contratto: stipula, esecuzione, estinzione e fase post-contrattuale.

Condivisione delle informazioni: In questo pillar l'obiettivo è quello di sopperire alla mancanza di comunicazioni tra le varie entità all'interno della Comunità Europea. Si esortano le entità finanziarie alla creazione di un sistema strutturato di comunicazione e condivisione delle informazioni in tempo reale sui dati relativi agli attacchi. Obiettivo è favorire la creazione di un sistema di infosharing nazionale, sia a livello di settore finance sia nell'ambito di una più stretta collaborazione tra settore pubblico e privato.

3 Come si attacca un istituto di credito?

Di fatto non esiste una ricetta specifica utilizzata dai cyber attaccanti per svolgere azioni malevole ai danni di organizzazioni operanti all'interno dell'ambito finanziario. Come vedremo nel capitolo "Le fasi di un attacco" ciò che fa davvero la differenza tra un attacco avente ampie probabilità di successo ed un attacco destinato al fallimento, è **la capacità da parte dell'attaccante di recuperare informazioni di contesto relative al proprio target**. Più informazioni l'attaccante sarà in grado di collezionare e più sarà in grado di costruire scenari di attacco plausibili e realizzabili.

Oltre alle caratteristiche in comune con tipologie di attacchi sviluppati verso organizzazioni di altri ambiti, ve ne sono però certamente anche di esclusive dell'ambito oggetto di questo report, in virtù degli elementi distintivi degli strumenti utilizzati, soprattutto dalla clientela delle organizzazioni dell'ambito stesso.

Come indicato nello "SPECIALE FINANCE" all'interno del Rapporto Clusit 2023[1] (da pag. 135 a pag. 150), nel 2022 finanza e assicurazioni sono stati i settori più attaccati, con il 25% degli attacchi totali gestiti da IBM X-Force. Nel rapporto, viene inoltre indicato come

"*il financial fraud, frode bancaria o finanziaria, passa quasi sempre attraverso il furto delle credenziali d'accesso ai sistemi bancari o di pagamento e riutilizzate per transazioni fraudolente all'insaputa del titolare. Invece di attaccare direttamente l'istituzione finanziaria, si preferisce attaccarne i clienti in quanto obiettivo indubbiamente più permeabile.*"

Ed ancora, facendo un focus sui vettori di attacco:

"*L'analisi delle principali campagne del 2022 mostra che la frode avviene prevalentemente attraverso i seguenti vettori di attacco:*

- *phishing per la fase di furto di credenziali di accesso (credential theft), spesso combinata con una successiva interazione con un finto operatore per il furto dei fattori di autenticazione forte;*
- *malware per il furto di credenziali o fattori addizionali di autenticazione o manipolazione di una transazione;*
- *hacking del dispositivo mobile tramite SIM Swap o emulazione software dello smartphone;*
- *e infine ma in misura inferiore, con l'attacco diretto all'infrastruttura dell'istituzione finanziaria, sfruttando vulnerabilità[2] quasi sempre note ma ancora non fissate.*

[1] Il Rapporto Clusit 2023 è scaricabile al link https://clusit.it/rapporto-clusit/

[2] All'interno del progetto deepdarkCTI (https://github.com/fastfire/deepdarkCTI/blob/main/cve_most_exploited.md), fondato da membri del team del SOC Attacker Centric di Würth Phoenix, è possibile trovare la lista aggiornata delle vulnerabilità maggiormente sfruttate

La tecnica, o la combinazione di tecniche, varia in base alla tipologia di vittima, con sostanziali differenze tra il cliente finale (retail) oppure aziendale (corporate)."

Ecco quindi qual è la risposta alla domanda che dà il titolo a questo capitolo: un mix di phishing, social engineering, utilizzo di malware, utilizzo di exploit. Nulla di nuovo, verrebbe da dire.

Dal nostro punto di vista, ulteriori importanti possibilità di attacco, soprattutto da parte di chi non vuole sporcarsi direttamente le mani come diretto utilizzatore di exploit e malware, sono riconducibili alle evidenze riscontrabili all'interno degli *infostealer market place*. Si tratta di quei mercati online, presenti sia nel deep che nel dark web, che mettono in vendita credenziali frutto dell'attività di esfiltrazione compiuta attraverso l'utilizzo di specifici malware, gli infostealer appunto. Tra i più noti Redline, Raccoon, Vidar, i quali raccolgono credenziali da strumenti quali i browser internet e che permettono agli attaccanti di acquistare a cifre modiche (spesso pochi dollari) utenze potenzialmente valide che diventano così gli Initial Access verso le organizzazioni target. In questo contesto le forze dell'ordine, a livello globale, stanno facendo uno sforzo notevole per limitare la potenza di fuoco di cyber criminali e a volte questi sforzi portano a risultati tangibili, come è stato con il sequestro di uno dei più noti market place, Genesis Market. Purtroppo successivamente ad eventi di questo tipo, si può quasi sempre notare la significativa capacità da parte dei cyber criminali di riorganizzare le proprie risorse, mettendo a disposizione differenti mercati dove ricominciare la propria attività.

Ulteriori mercati che possono causare danni economici nell'ambito finanziario sono i *credit card market place*, mercati specializzati nella messa in vendita di carte di credito. Come è possibile notare dalle statistiche messe a disposizione all'interno del report "STATE OF THE CYBERCRIME UNDERGROUND" prodotto da CyberSixgill, il numero di carte di credito messe in vendita all'interno dei market place presenti nel deep e nel dark web è diminuito in modo sostanziale negli ultimi anni, ma indubbiamente si tratta di un fenomeno che deve ancora essere preso in considerazione in modo attento e contrastato con tutti gli strumenti che i vari attori in gioco possono utilizzare.

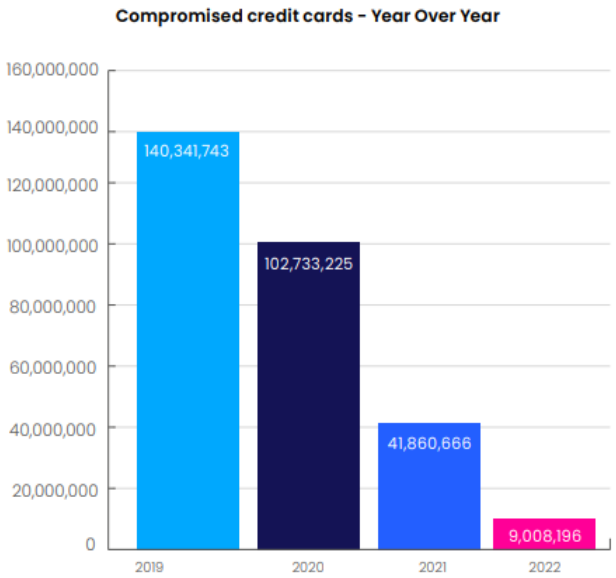


Grafico 1 – Carte di credito messe in vendita all'interno dei market place

All'interno di questo report, considerata l'importanza che rivestono nel panorama attuale degli attacchi, abbiamo dedicato due paragrafi a queste due tipologie di mercati.

Da non dimenticare infine gli attacchi fisici ai danni degli ATM (Automated Teller Machine), i quali hanno una lunga storia alle spalle (il primo exploit ATM pubblicamente noto è stato presentato al mondo alla Black Hat Conference del 2010[3]) ma che continuano ad essere sviluppati da alcuni gruppi cyber criminali, tra i quali happyATM che non più tardi di qualche mese fa ha reso noto di aver sviluppato un malware utilizzabile per gestire attacchi di tipo jackpotting su dispositivi di recente produzione e di noti vendor quali Diebold, NCR e Wincor Nixdorf.

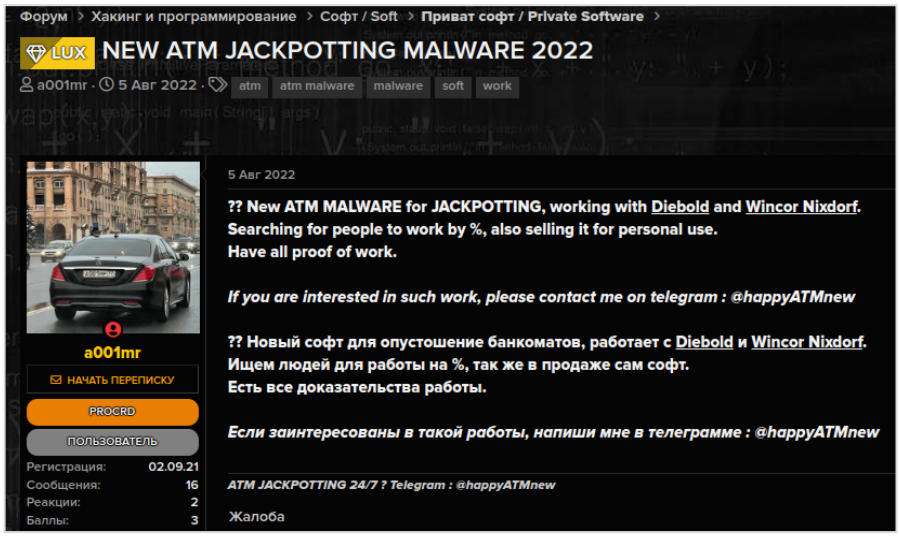


Immagine 1 – attacco di tipo jackpotting su ATM

A marzo 2023 inoltre è stato identificato un nuovo malware sviluppato per ATM battezzato FiXS e che è stato utilizzato per attaccare dispositivi di banche messicane. Il malware dispone di alcune interessanti caratteristiche:

- indica al bancomat di erogare denaro 30 minuti dopo l'ultimo riavvio del bancomat.
- è nascosto all'interno di un altro programma dall'aspetto non dannoso
- è vendor-agnostic e si rivolge a qualsiasi ATM che supporti CEN XFS
- interagisce con i malviventi tramite una tastiera esterna
- attende che le cassette siano caricate per iniziare l'erogazione
- contiene metadati russi

[3]https://media.blackhat.com/bh-us-10/video/Jack/BlackHat-USA-2010-Jack-JackpottingATM-video.m4v

4 I malware "bancari" - storia passata e recente

All'interno di questo capitolo viene riportata la lista ed una breve descrizione dei principali malware bancari e delle loro variazioni nel tempo, come ad esempio i targets presi in considerazione e le tecniche di attacco utilizzate. Vengono riportate informazioni di contesto relative ad alcuni tra i più noti malware bancari che hanno operato a partire dagli anni 2000. Le informazioni sono state recuperate partendo principalmente dal portale https://malpedia.caad.fkie.fraunhofer.de.

Per ogni malware, laddove possibile, abbiamo riportato delle regole da importare sui propri sistemi di detection, utili per individuare la presenza di questi elementi malevoli.

Cos'hanno in comune tutti questi malware? La costante necessaria affinché il malware infetti un dispositivo è lo sfruttamento delle vulnerabilità intrinseche del fattore umano. Quindi la tendenza delle persone a fidarsi, di agire ponendo scarsa attenzione alle attività svolte, spinti da sentimenti quali la fretta o la curiosità. Tutto ciò può essere ricondotto ad azioni mirate utilizzanti tecniche di social engineering, la cui puntuale descrizione esula però dallo scopo di questo report. Oggi come in passato, la maggior parte degli attacchi informatici verso istituti di credito si basa su campagne di phishing mirato (spear phishing, whaling, BEC) che puntano a recuperare credenziali valide o ad infettare il dispositivo bersaglio con pericolosi malware dei quali ora verranno presentati alcuni esempi.

4.1 Emotet

Questo malware è stato identificato per la prima volta nel 2014 come un semplice trojan bancario. Le versioni successive si sono evolute e hanno incluso l'aggiunta di servizi di distribuzione del malware, tra cui la capacità di installare altri trojan bancari. A settembre 2018, Emotet utilizzava la vulnerabilità EternalBlue di Windows (vista per la prima volta con il ransomware WannaCry) per propagarsi. Dopo essere stato indicato come il più pericoloso malware in circolazione, all'inizio del 2021 un'ampia operazione delle forze dell'ordine compiuta a livello globale ha portato al quasi totale smantellamento dell'infrastruttura utilizzata dai cyber criminali per propagare il malware. Emotet è tornato alla ribalta a fine 2022, con nuove modalità di evasione.

Regole di detection:

Potential Emotet Activity
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_malware_emotet.yml

Potential Emotet Rundll32 Execution
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_malware_emotet_rundll32_execution.yml

4.2 Gozi

Conosciuto anche come Ursnif, è uno dei più vecchi trojan bancari. È in circolazione dal 2007 e nel 2010 è trapelato il codice sorgente del malware, che ha portato alla creazione di diverse varianti. Nel 2016, il cyber criminale lettone Deniss Calovskis è stato condannato a scontare una pena di 21 mesi per aver sviluppato il codice originale di Gozi. L'arresto di uno sviluppatore chiave spesso blocca lo sviluppo del relativo malware, ma sembra aver avuto poco effetto su Gozi. Dopo oltre dieci anni, questo malware continua ad essere uno dei più sofisticati ed in costante evoluzione. Recentemente ha aggiunto tecniche di evasione sia lato client che lato server e ha continuato ad evolversi, venendo così considerato ancora oggi uno dei più pericolosi malware trojan bancari.

Regole di detection:

Detects Ursnif C2 traffic
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_add/registry_add_malware_ursnif.yml

Detects registry keys related to Ursnif malware
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_add/registry_add_malware_ursnif.yml

4.3 IceID

IcedID, noto anche come BokBot, ha fatto la sua comparsa nel settembre del 2017 e negli anni successivi la sua fama superò quella di noti malware che operavano nel settore già da tempo, come ad esempio Gozi. I primi attacchi, attribuiti a shathak TA551 (un gruppo di criminali di origine russa), si concentrarono principalmente su suolo tedesco, tramite una campagna di phishing su vasta scala che mirava a recuperare credenziali di accesso a servizi bancari. IcedID è attualmente una delle famiglie di malware maggiormente diffuse sul territorio italiano e ha modificato il proprio modello di business scegliendo il sistema noto come Malware as a Service (MaaS), una tipologia di distribuzione malware che facilita altri Threat Actor nel condurre attacchi complessi senza la necessità di conoscere tecniche avanzate, attraverso la messa a disposizione di infrastruttura e tools gestiti direttamente dal proprietario del MaaS.

Regole di detection:

Detects a registry key used by IceID in a campaign that distributes malicious OneNote files
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_event/registry_event_malware_qakbot_registry.yml

Detects a possible IcedID Downloader
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_event/registry_event_malware_qakbot_registry.yml

4.4 Alienbot

Introdotto nel 2020 come MaaS, Alienbot (o più semplicemente Alien) è un malware progettato per targetizzare dispositivi Android, che punta ad ottenere informazioni sensibili associate ad applicazioni finanziarie e account bancari. Viene distribuito usando un dropper, ossia una normalissima applicazione scaricabile da Play Store (l'app store ufficiale di Google) che al suo interno però contiene del codice malevolo, il quale installa e gestisce il malware a insaputa dell'utente. Attualmente Alienbot è il mobile malware più diffuso al mondo e la lista di dropper che utilizza conta ormai più di 200 applicazioni.

4.5 Anubis

Anubis è un Android malware creato da un Threat Actor russo noto come "Maza-in", che nel 2017 finì sotto i riflettori per la sua propaganda di malware bancari e nello specifico per la creazione di Anubis. Fu in seguito arrestato in Russia nel 2019 e condannato a 5 anni. Una volta approdato sul dispositivo bersaglio, anch'esso tramite l'ausilio di centinaia di dropper disponibili su Play Store, Anubis prende il totale controllo del dispositivo e oltre ad intercettare le comunicazioni in entrata e uscita, implementa altre funzionalità come la registrazione dello schermo o l'invio di messaggi in massa con lo scopo di diffondersi facilmente all'interno della rete di contatti della vittima.

4.6 Cerberus

È uno dei più recenti malware bancari che, come Anubis e Alien, infetta dispositivi Android ottenendone il pieno controllo attraverso l'ausilio di molteplici dropper sparsi per il web. È stato presentato per la prima volta nel giugno del 2019, sulla pagina "ufficiale" Twitter di Cerberus. Anch'esso introdotto sul mercato come MaaS, Cerberus è particolarmente noto per la propaganda pubblicitaria effettuata direttamente su Twitter, la quale avveniva tramite la condivisione di immagini e video dove venivano mostrati Indicators of Compromise (IoC) degli attacchi che venivano effettuati.

Il profilo Twitter è stato dismesso nel gennaio del 2020 e ora le comunicazioni avvengono sul noto forum cyber criminale russo XSS.

4.7 Ramnit

Questo trojan bancario è nato nel 2010 come worm e, qualche tempo dopo la fuga di notizie sul codice sorgente di Zeus, ha acquisito parti di questo malware trasformandosi in trojan bancario. Nel tempo Ramnit ha continuato a evolversi in termini di sofisticazione, tecnica e portata. Rimane attivo nonostante il blocco di 300 server Command & Control nel febbraio 2015. Dopo questa battuta d'arresto, Ramnit è riapparso alla fine del 2015 e di nuovo a metà 2016. Come molti altri trojan bancari, Ramnit ha ampliato la sua portata negli ultimi anni. Secondo alcune statistiche, nel 2017 l'elenco dei target di Ramnit era composto per il 64% da rivenditori di eCommerce oltre che da istituzioni di servizi finanziari. Nel 2019 è tornato a colpire in modo

massiccio le istituzioni finanziarie, soprattutto quelle italiane ed è stato utilizzato in combinazione con il web-inject toolkit drIBAN, avente l'obiettivo di iniettare script custom a livello client e di veicolare in questo modo attacchi di tipo man-in-the-browser (MitB). Un'altra importante campagna di attacco avente questo malware come protagonista è stata effettuata nel 2022.

5 Attacchi 2023

In questo capitolo vengono presi in rassegna gli attacchi più importanti subiti da organizzazioni finanziarie in questo primo scorcio di 2023.

5.1 NoName057 group

Questo gruppo, noto negli ultimi mesi per gli innumerevoli attacchi di tipo DDOS (Distributed Denial of Service) compiuti, ha inserito tra i propri target diverse organizzazioni finanziarie, tra le quali:

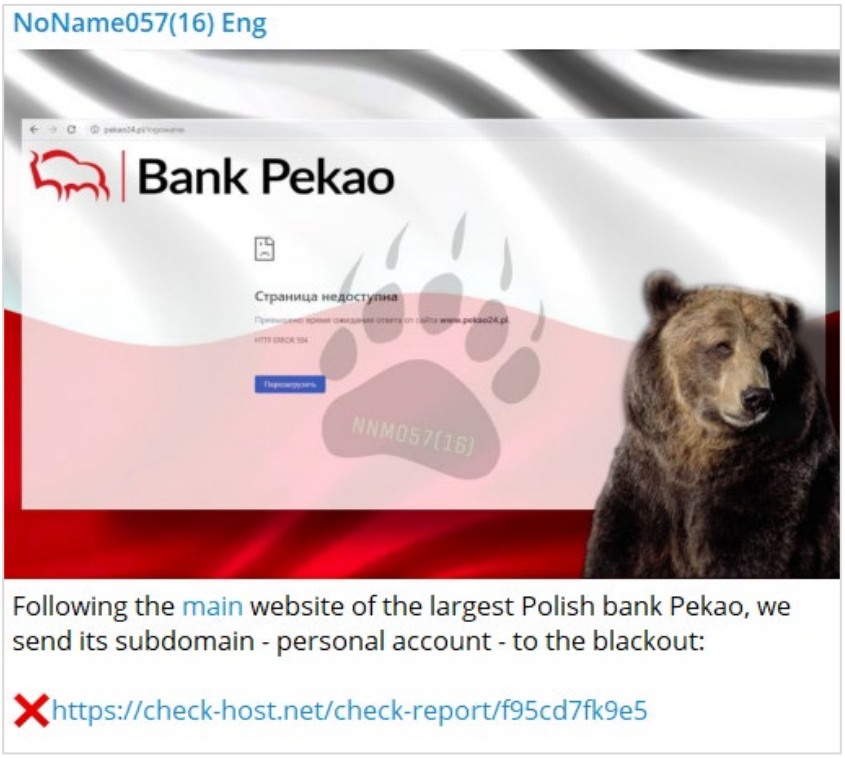


Immagine 2 – attacco verso la banca polacca Pekao

- 25 aprile 2023 - organizzazioni italiane: Federazione Italiana Banche di Credito Cooperativo, Fingenia, SACE (Gruppo CDP), Unipol Gruppo SpA, Generali Group, Banca Popolare di Sondrio, Mediobanca, BPER
- 19 aprile 2023 - banche polacche Raiffeisen Bank Polska e BOŚ Bank, banca italiana BPER
- 17 aprile 2023 - banca polacca Pekao
- 13 aprile 2023 - banche canadesi Canada Laurentian Bank e Toronto Dominion Bank
- 9 aprile 2023 - banca tedesca KfW

5.2 Various Israel Banks

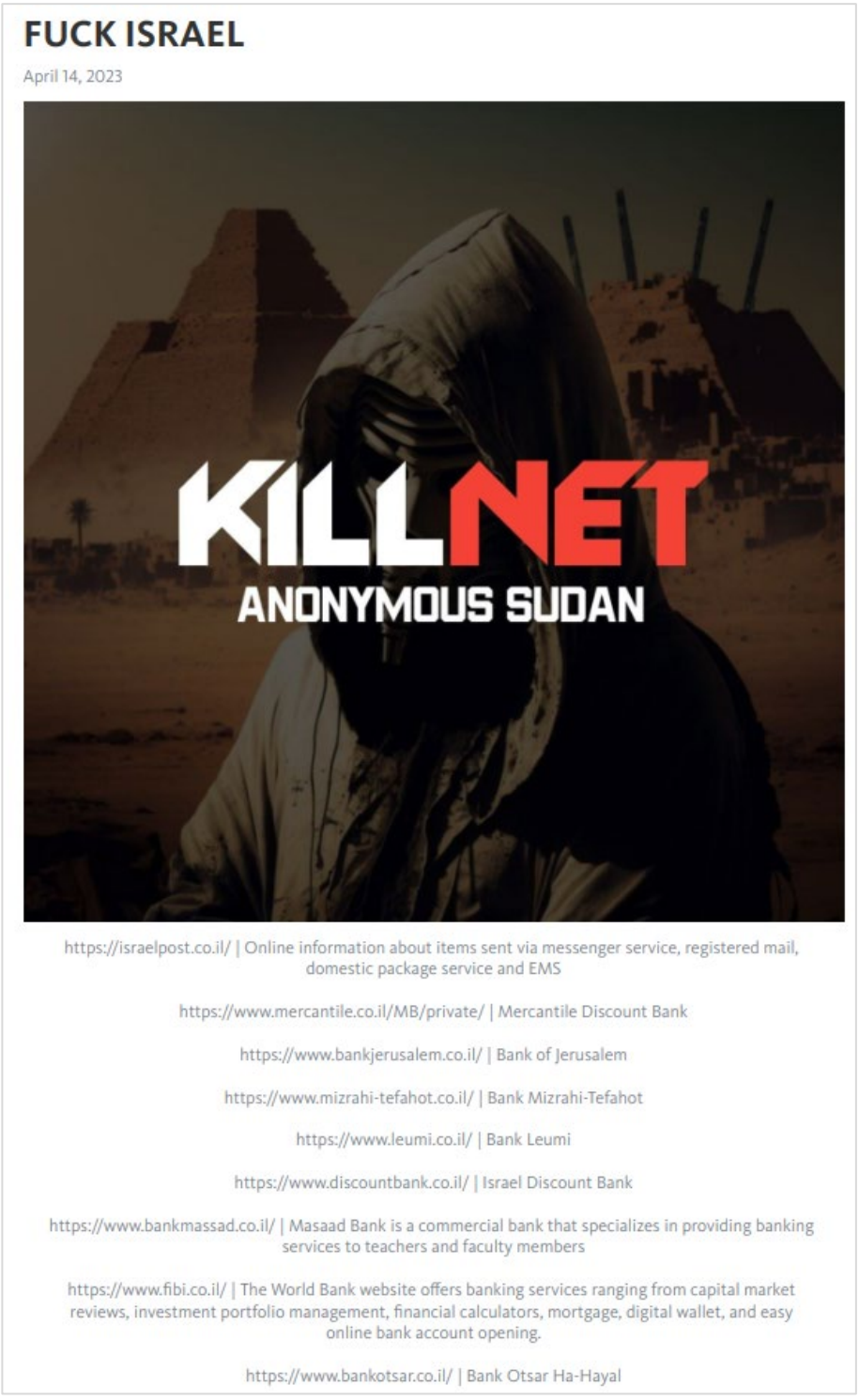


Immagine 3 – attacco verso varie banche israeliane

Il 14 aprile 2023 i siti web di alcune banche israeliane, dell'ufficio postale e dell'azienda elettrica, sono stati colpiti da un attacco informatico, andando offline.

Il gruppo di cyber attaccanti noto come "Anonymous Sudan" si è assunto la responsabilità, affermando che gli obiettivi sono Israel Post, oltre a Bank Leumi, Discount Bank, Mizrahi-Tefahot, Bank Mercantile, Bank Benleumi (First International Bank of Israel) e le sue filiali Bank Otzar Ha-hayal e Bank Massad.

5.3 Tradex Bank

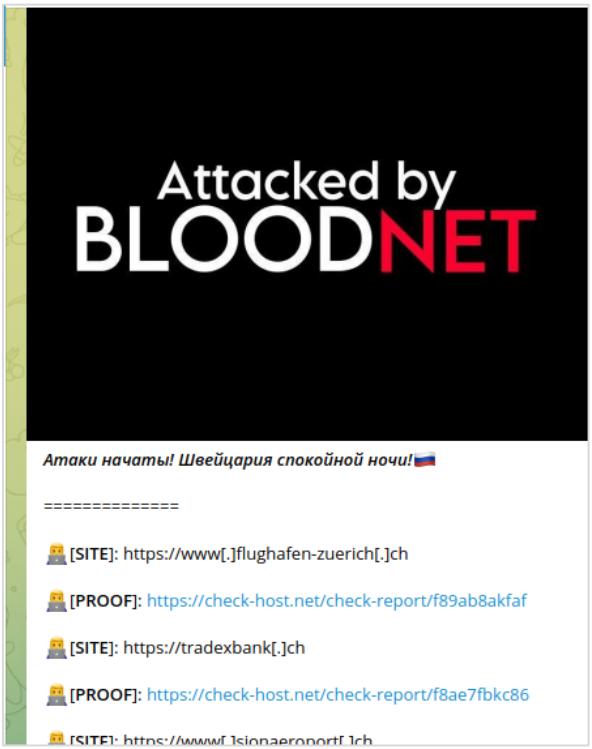


Immagine 4 – attacco verso la banca svizzera Tradex Bank

Il 13 aprile 2023 il gruppo russo Bloodnet attacca diversi target svizzeri, tra i quali Tradex Bank.

5.4 Bank Hapoalim

Il 31 marzo 2023 il gruppo AnonGhost dichiara di aver compiuto un attacco ai danni della banca israeliana Bank Hapoalim e di essere in possesso di informazioni personali di migliaia di account.

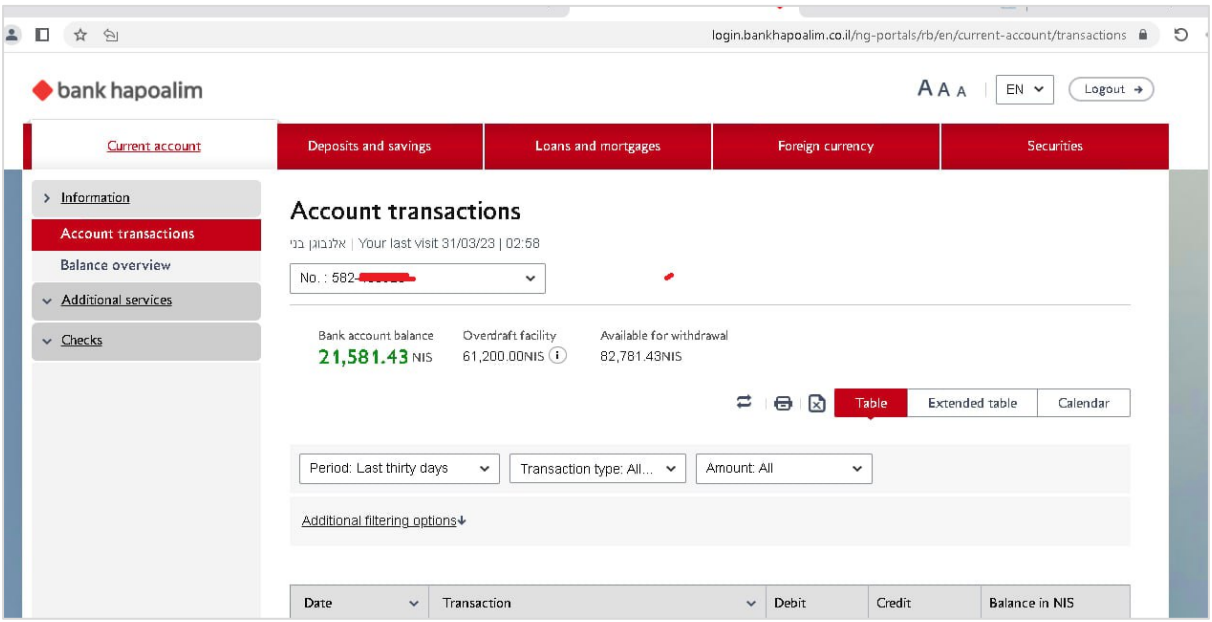


Immagine 5 – attacco verso la banca israeliana Bank Hapoalim

5.5 Tri Counties Bank

A febbraio 2023 la ransomware gang BlackBasta attacca la banca statunitense Tri Counties Bank.

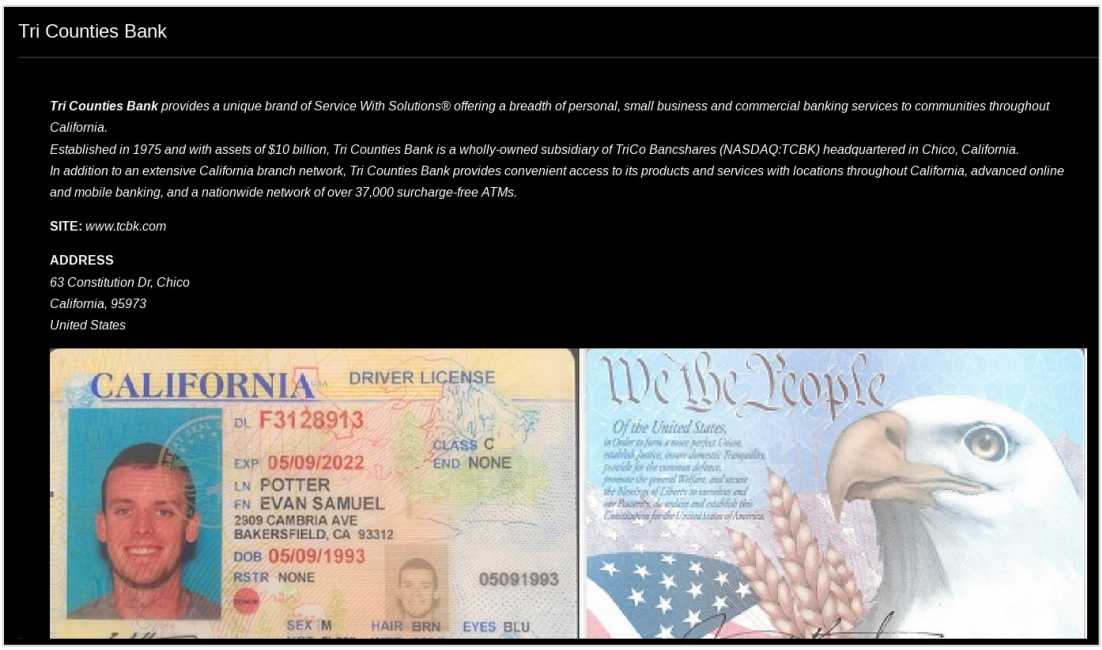
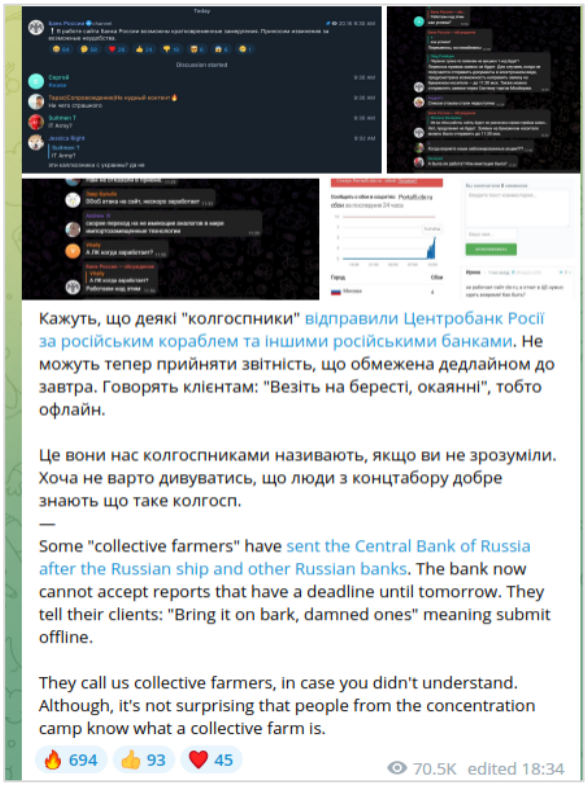


Immagine 6 – attacco verso la banca statunitense Tri Counties Bank

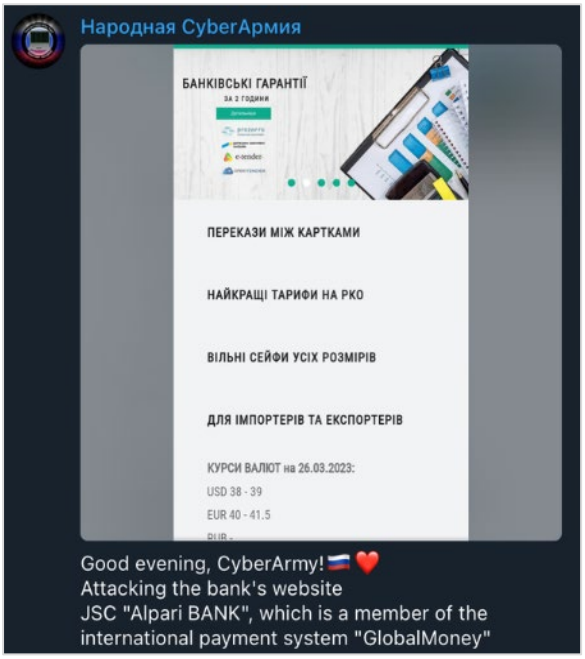
5.6 Central Bank of Russia



Il 28 marzo il gruppo ucraino IT Army of Ukraine esegue un attacco DDoS contro la Central Bank of Russia.

Immagine 7 – attacco verso la Central Bank of Russia

5.7 Alpari Bank



Il 26 marzo il gruppo di cyber criminali russi Cyber Army of Russia esegue un attacco DDoS contro la banca ucraina Alpari Bank.

Immagine 8 – attacco verso la banca ucraina Alpari Bank

5.8 Hatch Bank

A marzo la ransomware gang Clop, sfruttando la vulnerabilità presente sul software di file sharing Fortra GoAnywhere MFT, attacca decine di organizzazioni: tra cui la banca statunitense Hatch Bank.

Headquarters:
1001 W San Marcos Blvd, San Marcos, California, 92078, United States
Phone:
(760) 736-2000
Website:
www.hatchbank.com
Revenue:
<$5Million
Industry:
Banking, Finance

Warning:

> The bank doesn't care about its customers, it ignored their security!!!

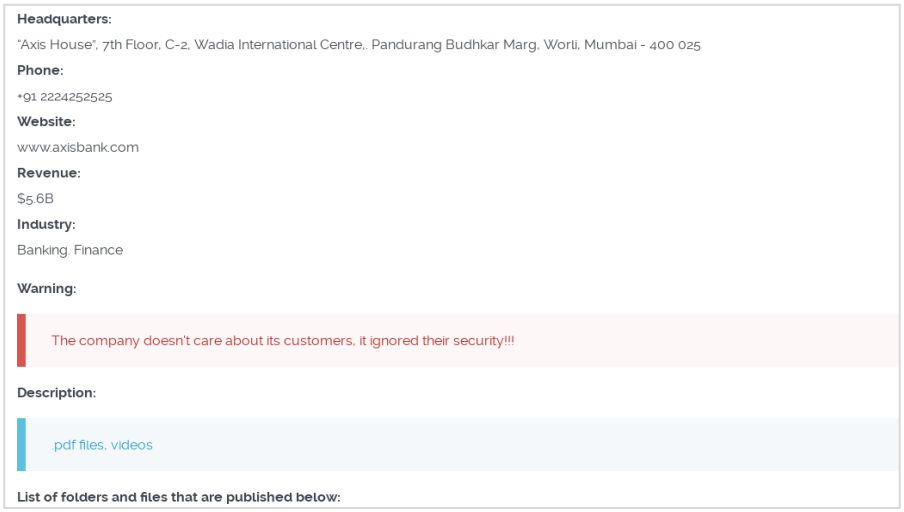
Description:

> Client data files: name, email, phone number, address, in some cases SSN. Transaction lists with id numbers instead of customer names. Loan agreements. Invoices. Encrypted files

List of folders and files that are published below:

Immagine 9 – attacco verso la banca statunitense Hatch Bank

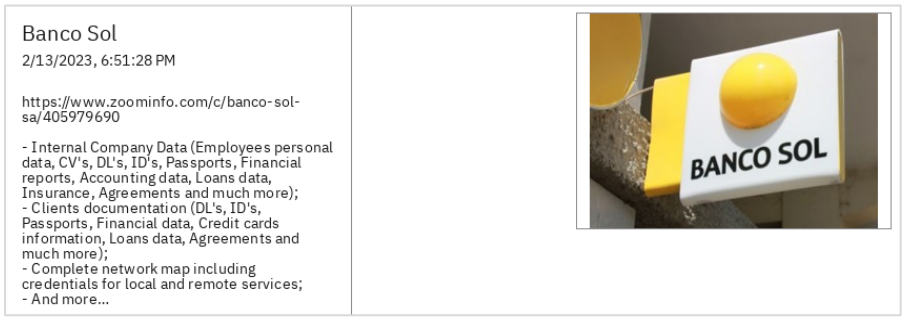
5.9 Axis Bank



A febbraio 2023 la ransomware gang Clop attacca Axis Bank, istituto finanziario del Regno Unito.

Immagine 10 – attacco verso la banca inglese Axis

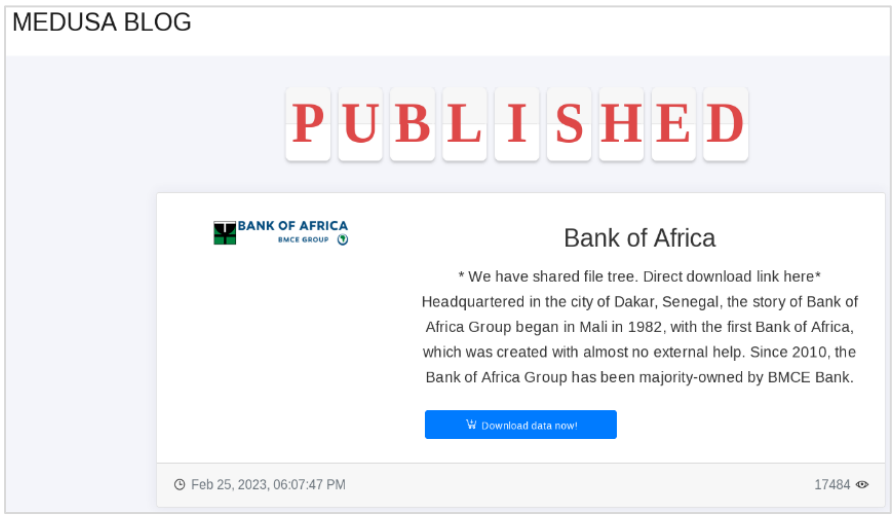
5.10 Banco Sol



A febbraio 2023 la ransomware gang Alphv attacca la banca boliviana Banco Sol.

Immagine 11 – attacco verso la banca boliviana Banco Sol

5.11 Bank of Africa



A febbraio 2023 la ransomware gang Medusa attacca la banca senegalese Bank of Africa.

Immagine 12 – attacco verso la banca senegalese Bank of Africa

5.12 Commonwealth Bank

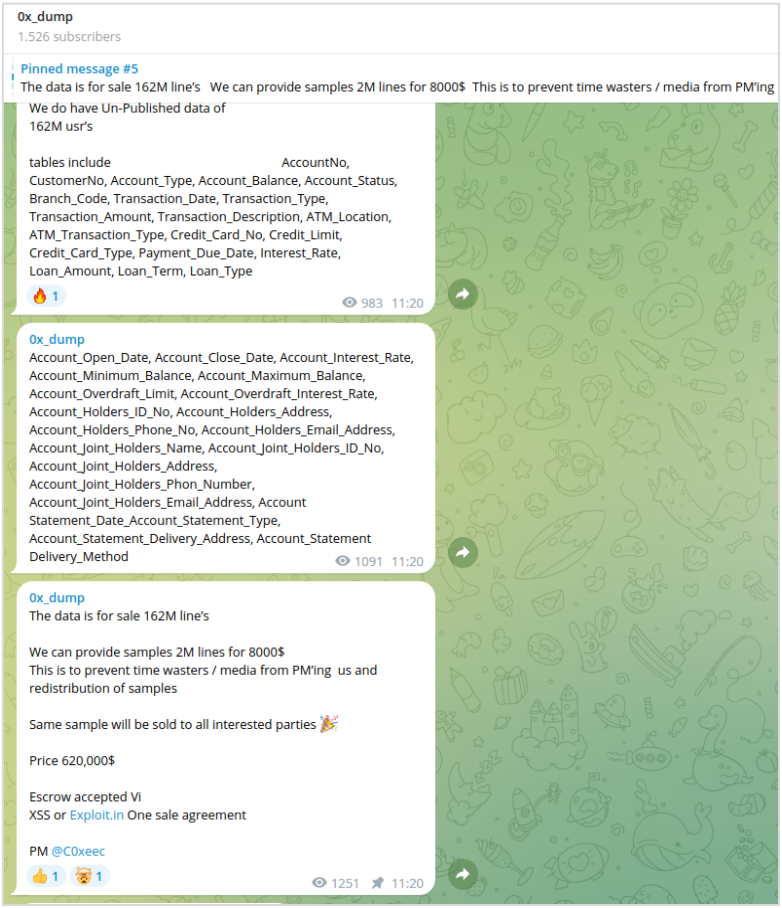


Immagine 13 – attacco verso la banca australiana Commonwealth bank

Il 5 marzo 2023 il gruppo 0x_dump, all'interno del proprio canale Telegram, ha affermato di essere in possesso di 162 milioni di anagrafiche riguardanti clienti della banca australiana ed ha fissato il prezzo di vendita a $620000.

5.13 Banco de Venezuela

Il 19 aprile 2023 la ransomware gang Lockbit attacca il Banco de Venezuela, istituto finanziario venezuelano.

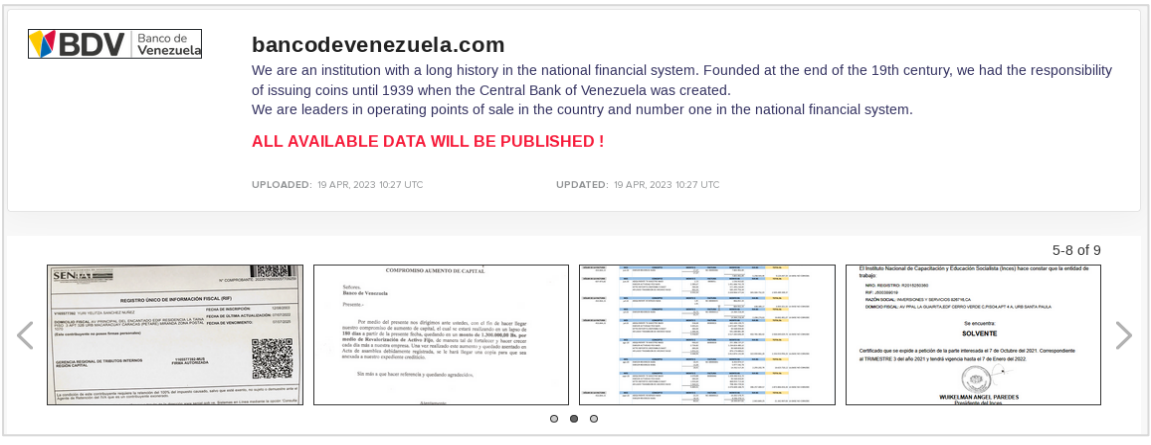


Immagine 14 – attacco verso la banca venezuelana Banco de Venezuela

6 Le fasi di un attacco

Un attacco attraversa diverse fasi e ogni fase ha caratteristiche fortemente differenzianti. I principali framework di riferimento utilizzati per descrivere le diverse fasi sono due:

- The Cyber Kill Chain® di Lockheed Martin
- MITRE ATT&CK® di Mitre Corporation

6.1 The Cyber Kill Chain®

La Cyber Kill Chain® fa parte del modello Intelligence Driven Defense® per l'identificazione e la prevenzione delle minacce informatiche. Il modello identifica ciò che gli avversari devono completare per raggiungere il loro obiettivo.

Il modello sottolinea anche come il fermare gli avversari in qualsiasi fase interrompe la catena di attacco, in quanto gli avversari devono attraversare completamente tutte le fasi per avere successo.

Il concetto di Cyber Kill Chain è stato pubblicato per la prima volta dalla Lockheed Martin, principale industria americana del settore Difesa, nel white paper: "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. All'interno del white paper vengono descritte le 7 fasi di attacco che il framework contempla.

La prima fase si chiama **Reconnaissance** (perlustrazione) e consiste nell'effettuazione di ricerche per identificare e selezionare l'obiettivo.

La seconda fase si chiama **Weaponization** (armamento) e consiste nel creare o nell'identificare un malware utilizzabile per l'attacco.

La terza fase si chiama **Delivery** (consegna) e consiste nella trasmissione dell'arma cyber (weapon) all'obiettivo.

La quarta fase è nota come **Exploitation** (sfruttamento) e consiste nello sfruttamento di una o più vulnerabilità da parte dei software malevoli introdotti nel sistema sotto attacco.

La quinta fase si chiama **Installation** (installazione) e consiste nell'installare elementi aggiuntivi all'interno del sistema obiettivo allo scopo di consentire all'attaccante di creare persistenza all'interno del sistema.

La sesta fase è chiamata **Command and Control** (C2 o C&C, Comando e Controllo) e consiste nello stabilire una catena di comando e controllo che consenta all'attaccante di dare ordini e ricevere feedback.

La settima fase si chiama **Actions on Objectives** (azioni sugli obiettivi) e consiste nel vero e proprio attacco al sistema target, eseguendo azioni quali esfiltrazione di dati e/o cifratura degli stessi.

6.2 MITRE ATT&CK®

MITRE ATT&CK® è una base di conoscenza accessibile a livello globale di tattiche e tecniche avversarie basate su osservazioni reali. La base di conoscenze ATT&CK è utilizzata come fondamento per lo sviluppo di modelli e metodologie di minaccia specifici nel settore privato, nel governo e nella comunità dei prodotti e dei servizi di cyber security.

All'interno della matrice di attacco Enterprise (https://attack.mitre.org/tactics/enterprise/) vengono identificate 14 tattiche di attacco, vale a dire gli step che gli attaccanti possono svolgere all'interno di un'azione malevola. Le 14 tattiche sono:

- **Reconnaissance** (l'avversario sta cercando di raccogliere informazioni da utilizzare per pianificare operazioni future)
- **Resource Development** (l'avversario sta cercando di stabilire le risorse da utilizzare per supportare le operazioni)
- **Initial Access** (l'avversario sta tentando di entrare nella vostra rete)
- **Execution** (l'avversario sta cercando di eseguire codice dannoso)
- **Persistence** (l'avversario sta cercando di mantenere il proprio punto d'appoggio)
- **Privilege Escalation** (l'avversario sta cercando di ottenere autorizzazioni di livello superiore)
- **Defense Evasion** (l'avversario sta cercando di evitare di essere individuato)
- **Credential Access** (l'avversario sta cercando di rubare nomi di account e password)
- **Discovery** (l'avversario sta cercando di capire il vostro ambiente)
- **Lateral Movement** (l'avversario sta cercando di muoversi nel vostro ambiente)
- **Collection** (l'avversario sta cercando di raccogliere dati interessanti per il suo obiettivo)
- **Command and Control** (l'avversario cerca di comunicare con i sistemi compromessi per controllarli)
- **Exfiltration** (l'avversario sta cercando di rubare i dati)
- **Impact** (l'avversario sta cercando di manipolare, interrompere o distruggere i vostri sistemi e dati).

7 Focus sulla fase di Reconnaissance

Come possiamo quindi notare, in entrambi i framework (The Cyber Kill Chain® e MITRE ATT&CK®) vi è la presenza della fase di **Reconnaissance**.

All'interno della Cyber Kill Chain® questa fase viene descritta come quella che identifica i targets e viene fatta distinzione degli obiettivi dei 2 attori principali (Adversary e Defender):

Adversary: gli avversari sono nella fase di pianificazione delle operazioni. Essi conducono ricerche per capire quali target gli permetteranno di raggiungere i loro obiettivi. I principali elementi ricercati sono: indirizzi email; collaboratori dell'organizzazione target e loro presenza sui social network; comunicati stampa, contrattualistica, partecipazione ad eventi; identificazione dei servizi esposti in internet.

Defender: individuare la ricognizione nel momento stesso in cui avviene può essere molto difficile, ma quando i difensori la scoprono, anche molto tempo dopo il verificarsi del fatto, possono individuare l'intento degli avversari. Obiettivi principali dei defender sono: raccogliere i registri degli eventi relativi ai visitatori dei servizi web esposti; creare elementi di rilevamento di pattern comportamentali indicatori di attività di ricognizione; privilegiare le difese in base a particolari tecnologie o persone in base all'attività di ricognizione rilevate.

MITRE ATT&CK® invece identifica una serie di 10 Tecniche all'interno della Tattica di Reconnaissance: Active Scanning, Gather Victim Host Information, Gather Victim Identity Information, Gather Victim Network Information, Gather Victim Org Information, Phishing for Information, Search Closed Sources, Search Open Technical Databases, Search Open Websites/Domains, Search Victim-Owned Websites. Il framework, per ognuna di queste 10 Tecniche, mette a disposizione della SubTecniche. Andando in profondità nella conoscenza delle diverse SubTecniche, è facile rendersi conto del fatto che la maggior parte di esse (ad esclusione della Tecnica "Active Scanning") sono attività che l'attaccante può eseguire in modo totalmente passivo, senza generare il minimo rumore nell'infrastruttura dei target.

8 OSINT nel contesto cyber criminale

Di seguito indichiamo una lista di ambiti e di fonti dai quali i cyber attaccanti possono trarre beneficio per andare a fondo nell'attività di Reconnaissance e guadagnando quindi del vantaggio competitivo nei confronti dei difensori.

8.1 Credit card market place

Come già accennato in precedenza, una parte della nostra analisi ha riguardato la ricerca di evidenze all'interno dei credit card market place più noti, in particolare la nostra analisi è stata svolta su Biden Cash.

8.1.1 Biden Cash

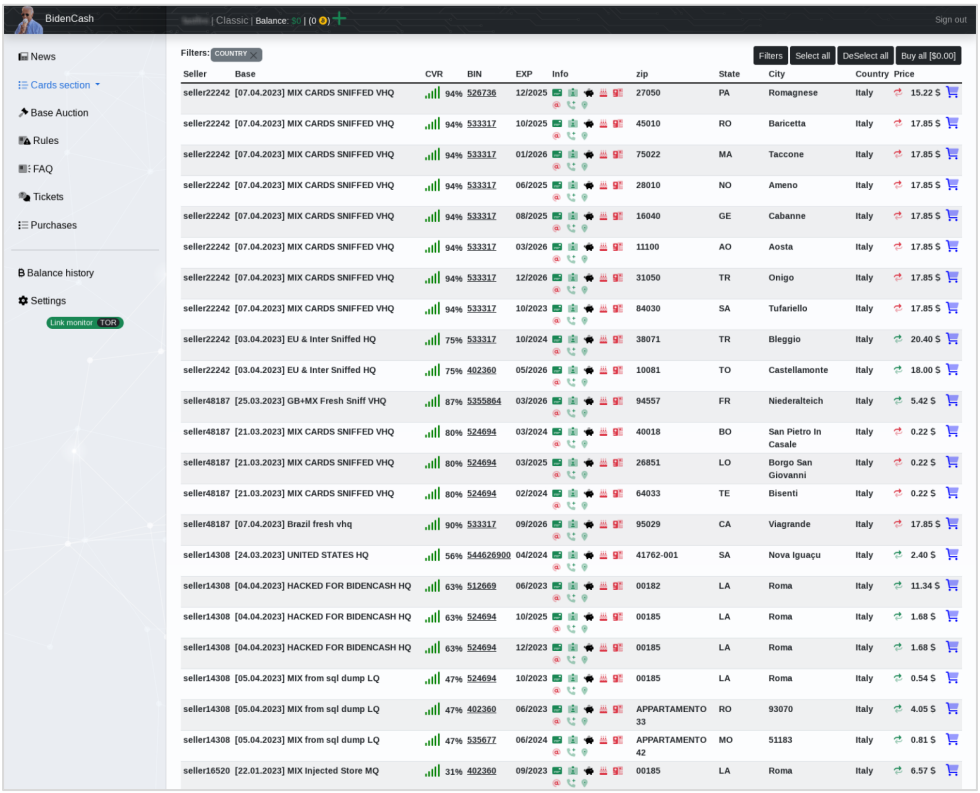


Immagine 15 – credit market place Biden Cash

Si tratta del più noto credit card market place al momento attivo, presente da febbraio 2022. All'interno del market risultano indicizzate e messe in vendita milioni di carte di credito, carte di debito e carte ricaricabili. Biden Cash mette a disposizione un motore di ricerca interno che consente di individuare facilmente evidenze relative ad una specifica country o istituto di credito, permettendo anche di utilizzare il BIN come elemento di ricerca.

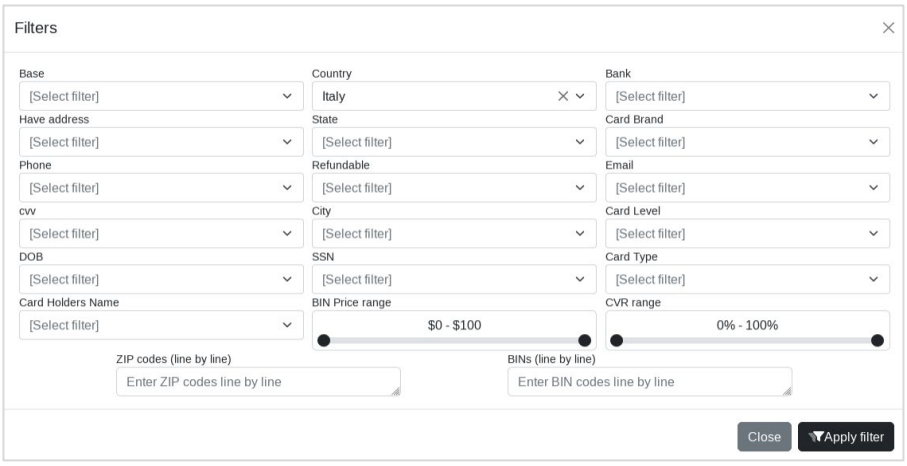


Immagine 16 – Filtri di ricerca market place Biden Cash

Il market è diventato noto alla massa all'inizio del mese di marzo 2023, quando ha diffuso gratuitamente oltre 2 milioni di record di carte di pagamento per celebrare il suo primo anniversario.

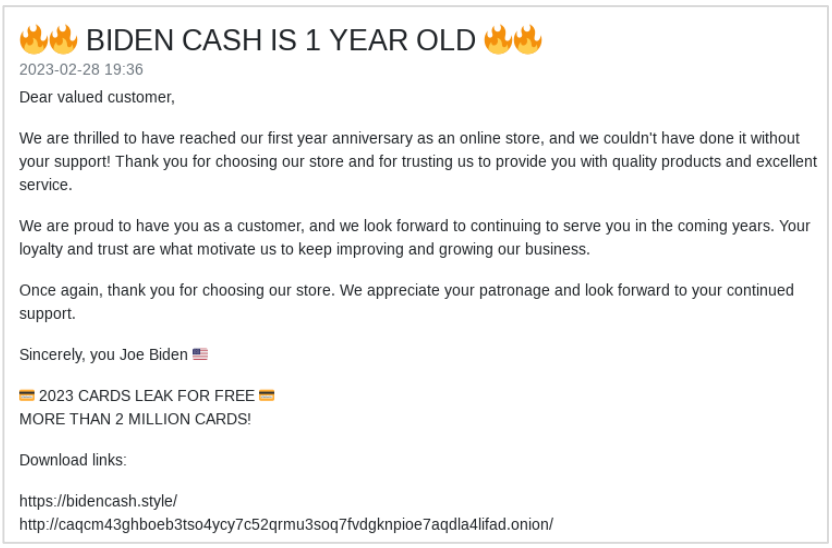


Immagine 17 – annuncio rilascio gratuito di record di carte di pagamento da Biden Cash

Ad onor del vero Biden Cash non è nuovo a questi rilasci, in quanto già ad ottobre 2022 aveva diffuso un primo stock di 1.2 milioni di carte.

8.2 Infostealer market place

Un'altra parte della nostra analisi ha riguardato la ricerca di evidenze all'interno degli infostealer market place più noti, in particolare la nostra analisi è stata svolta su Russian Market.

È comunque bene sottolineare che solo una minima parte delle evidenze collezionate attraverso gli infostealer malware viene convogliata all'interno degli infostealer market place, mentre la maggior parte viene condivisa all'interno di centinaia di canali Telegram.

8.2.1 Russian Market

Questo market è diventato nel tempo il punto di riferimento per la messa in vendita di record collezionati dagli infostealer malware. A maggior ragione successivamente al sequestro, avvenuto all'inizio di aprile 2023 e portato avanti dalla Federal Bureau of Investigation (FBI) con il supporto di altre Forze dell'Ordine presenti a livello globale, di Genesis Market.

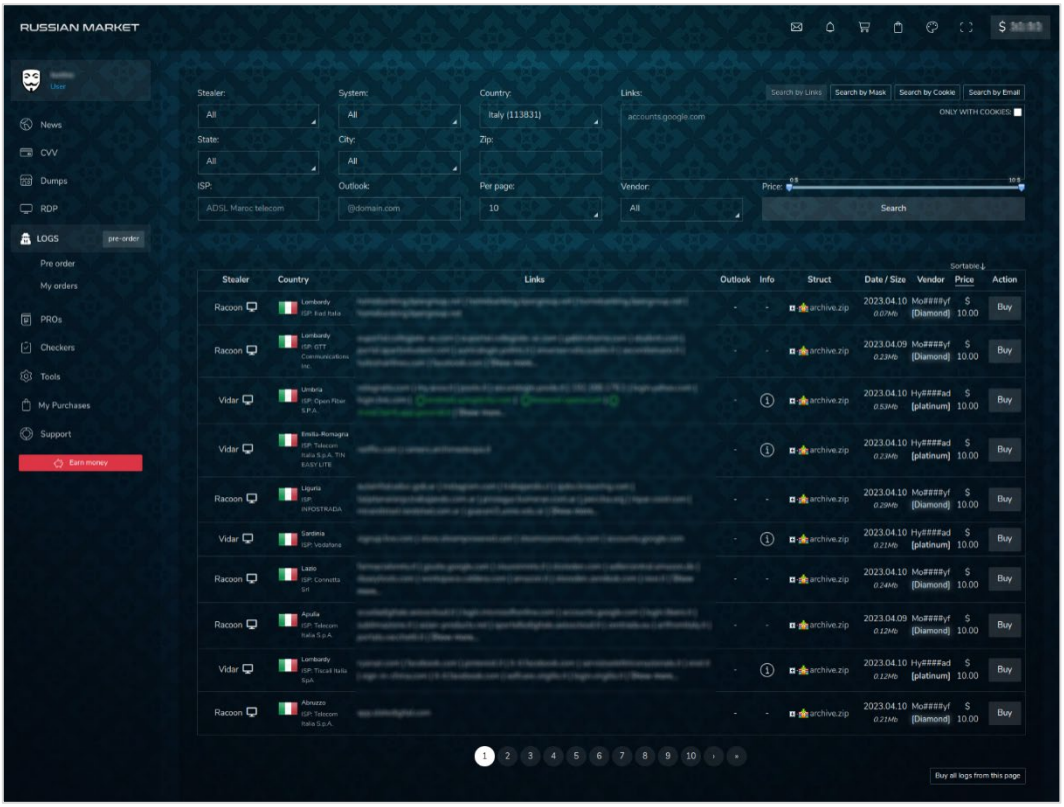


Immagine 18 – pagina di ricerca Russian Market

Il market mette a disposizione una pagina di ricerca che permette anche di selezionare i record in base alla tipologia di infostealer, la country della workstation compromessa, i subdomain ai quali fanno riferimento le credenziali esfiltrate.

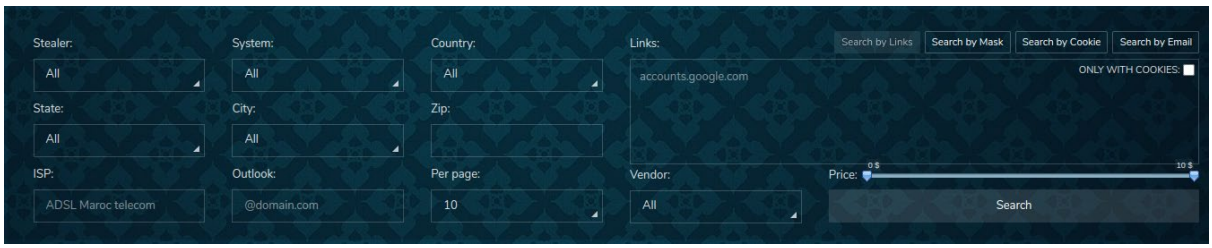


Immagine 19 – filtri di ricerca Russian Market

Russian Market contiene una sezione specifica anche per quanto riguarda le carte di credito, anche se non risulta essere il principale elemento di business del market e per il nostro Paese risultano messe in vendita poco più di 2000 carte di credito.

8.2.2 Genesis Market

Riguardo a Genesis Market, come già indicato, il market è stato messo sotto sequestro, anche se è più corretto specificare che non si tratta di una messa offline del servizio, in quanto accedendo ai link in surface web appare effettivamente il messaggio di sequestro:

Immagine 20 – messa offline Genesis Market

mentre il link in dark web risulta, al momento della scrittura del presente report, attivo, evidenziando così il fatto che l'infrastruttura del servizio è ancora attiva e non è stata quindi posta sotto sequestro.

8.2.3 2Easy

Il terzo infostealer market place per notorietà è 2Easy, con gli amministratori del market che a fine 2022 avevano investito molto nella riscrittura del frontend, ma che nelle ultime settimane hanno fatto perdere le loro tracce, con il market che risulta al momento irraggiungibile.

8.2.4 Solomon

Successivamente al sequestro dell'infostealer market place Genesis si è assistito alla nascita di diversi aggregatori di record recuperati dagli infostealer malware. Uno di questi è Solomon. Questo market place, ancora in fase beta, al momento è presente esclusivamente all'interno della rete Tor e gli update del servizio vengono attualmente pubblicati all'interno del canale Telegram del progetto. Il market place al momento della stesura del report conta circa 800000 record.

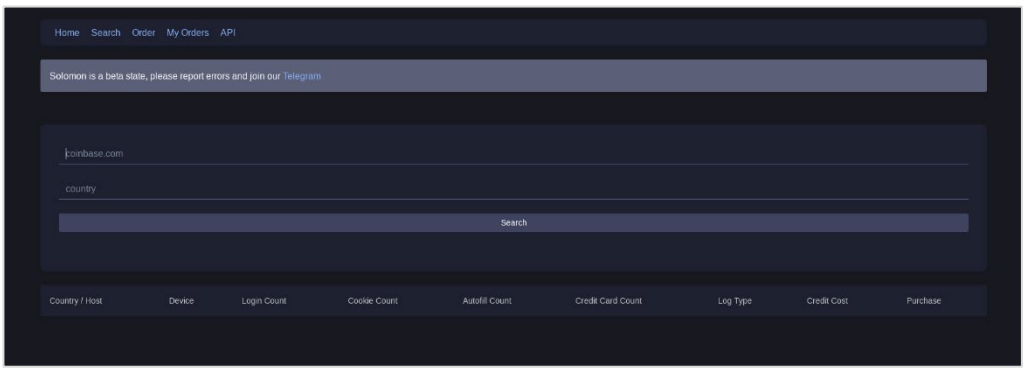


Immagine 21 – market place Solomon

8.3 Forum

Nel deep e nel dark web esiste una gran quantità di forum, i più noti dei quali sono utilizzati quotidianamente sia da cyber criminali che da Threat Intelligence analysts. Vi sono alcuni di questi forum che sono noti per mettere a disposizione in vendita, all'interno di specifiche sezioni, Initial Access quali accessi RDP, SSH o reverse shell o pannelli amministrativi web.

8.3.1 XSS

All'interno di questo forum è presente una sezione *Auctions*, all'interno della quale vengono messi in vendita accessi di varia tipologia. All'interno del threat solitamente il Threat Actor mette a disposizione informazioni relative al target quali la country di provenienza, la tipologia di accesso (protocollo/servizio), il settore di attività, il fatturato.

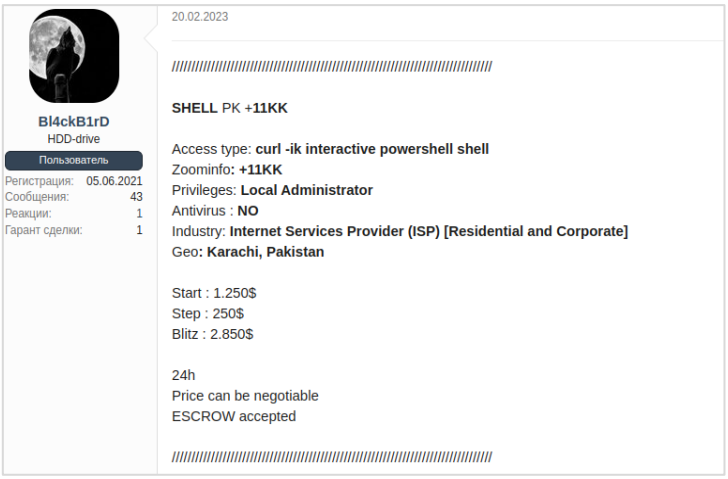


Immagine 22 – informazioni sul target nel forum XSS

Una menzione particolare rispetto a questo forum, considerato il target del presente report, è doveroso farla per quanto riguarda un post pubblicato il giorno 11 aprile 2023 dall'utente *resetmyname*, il quale affermava di essere in possesso di numeri di telefono mobile della maggior parte degli istituti di credito italiani. Il Threat Actor stava mettendo in vendita i record ad un prezzo variabile tra i 100$ e i 200$ per singola banca, a seconda del numero di record. Lo stesso Threat Actor era già noto per aver pubblicato, nel recente passato, post dello stesso tipo afferenti istituti di credito di altri paesi.

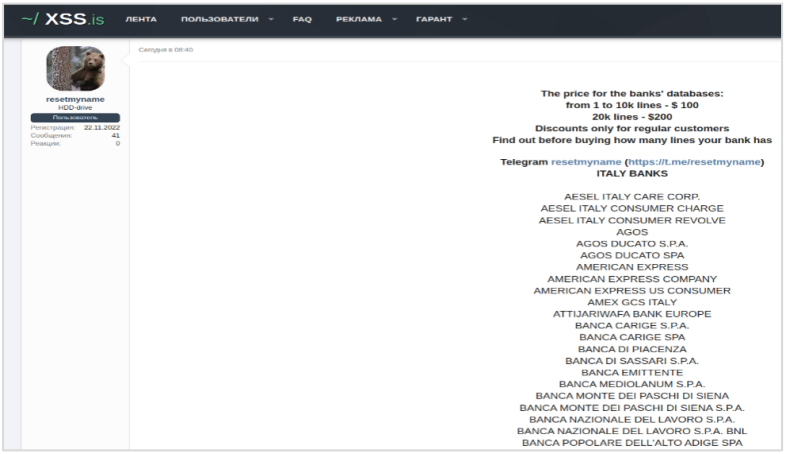


Immagine 23 – post resetmyname su numeri di telefono mobile degli istituti bancari

8.3.2 Exploit.IN

All'interno di questo forum è presente una sezione *Auctions*, all'interno della quale vengono messi in vendita accessi di varia tipologia. All'interno del threat solitamente il Threat Actor mette a disposizione informazioni relative al target quali la country di provenienza, la tipologia di accesso (protocollo/servizio), il settore di attività, il fatturato.

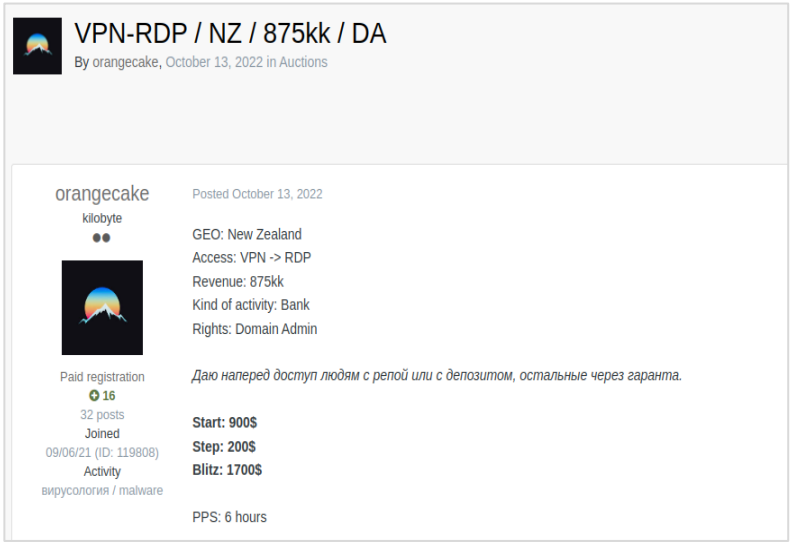


Immagine 24 – informazioni sul target nel forum Exploit.IN

8.3.3 RAMP

All'interno di questo forum è presente una sezione *Access (SSH/RDP/VNC/Shell)* \ *访问*, all'interno della quale vengono messi in vendita accessi di varia tipologia. All'interno del thread solitamente il Threat Actor mette a disposizione informazioni relative al target quali la country di provenienza, la tipologia di accesso (protocollo/servizio), il settore di attività, il fatturato.

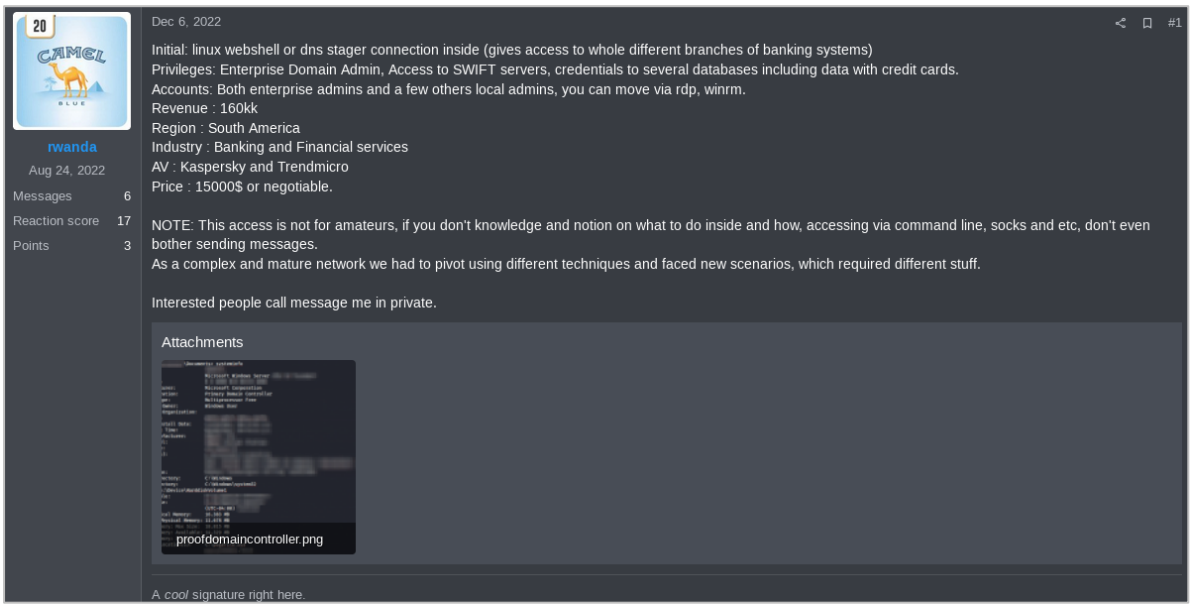


Immagine 25 - informazioni sul target nel forum RAMP

9 Modalità di analisi

L'attività di analisi compiuta dal SOC di Würth Phoenix si è concentrata esclusivamente proprio sulla copertura delle tecniche presenti all'interno della Tattica della Reconnaissance.

Nessuna attività di tipo attivo è stata compiuta verso i target dell'analisi e anche le attività della Tecnica "Active Scanning" sono state coperte attraverso l'utilizzo di fonti terze quali Shodan[4], Censys[5] e ZoomEye[6], motori di ricerca che svolgono periodicamente attività di scansione attiva verso l'intera rete internet. Per farsi un'idea dei protocolli e delle porte che questi servizi prendono in considerazione per le proprie scansioni è possibile osservare quanto uno di questi servizi, Censys, mette a disposizione pubblicamente[7].

Per ognuno degli istituti di credito elencati nel capitolo "Lista degli istituti di credito analizzati" è stato individuato il dominio internet principale e lo stesso è stato utilizzato come elemento di input per l'analisi. Sono stati identificati i diversi elementi di Reconnaissance correlati ai domini internet e questi sono stati utilizzati per avvalorare le metriche indicate nel capitolo successivo.

Per l'analisi non sono stati volutamente presi in considerazione domini internet afferenti ai centri servizi che gestiscono in outsourcing attività per conto degli istituti di credito analizzati, in quanto senza una precedente intervista (la cui fattibilità non è stata presa in considerazione, considerato che l'analisi aveva l'obiettivo di simulare il punto di vista di un attaccante) ad almeno un referente tecnico risulta impossibile valutare il corretto confine di asset rappresentativi del singolo istituto di credito all'interno del perimetro dell'outsourcer.

Un altro elemento utilizzato come input è stato il codice BIN (Bank Identification Number). Per "numero di identificazione bancaria" o codice BIN si intende la sequenza iniziale di quattro o sei numeri che compare su una carta di credito. Il numero viene utilizzato per identificare la banca emittente della carta o un altro istituto finanziario. Il numero BIN collega l'emittente a tutte le carte emesse e a tutte le transazioni effettuate su tali carte. Il BIN è stato utilizzato durante la nostra analisi per ricercare evidenze all'interno dei credit card market place.

Per svolgere la ricerca è stata utilizzata la piattaforma di Cyber Threat Intelligence SATAYO®, direttamente sviluppata da Würth Phoenix. La piattaforma, per ogni dominio analizzato, calcola un indice di esposizione (EAIV - Exposure Assessment Index Value), che è stato riportato nel capitolo "Risultati".

[4] https://www.shodan.io/
[5] https://search.censys.io/
[6] https://www.zoomeye.org/
[7] https://support.censys.io/hc/en-us/articles/360059603231-Censys-Internet-Scanning-Intro

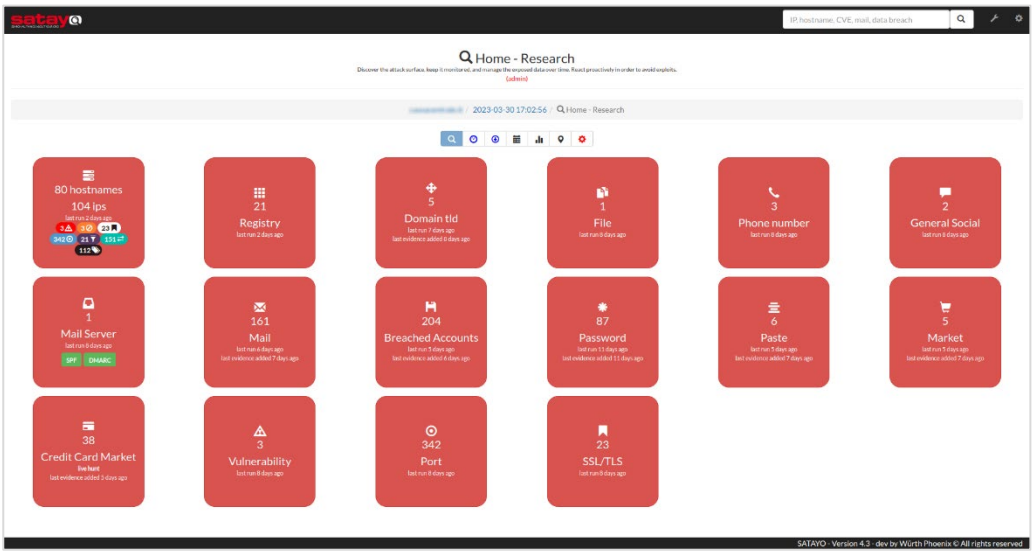


Immagine 26 – servizi disponibili nella piattaforma di Cyber Threat Intelligence SATAYO

L'attività ha simulato esattamente il punto di osservazione di un cyber attaccante e le specifiche attività che egli svolge nella prima fase dell'attacco.

Partendo dai domini internet, è stata identificata la lista di subdomains di ciascun dominio e per ogni subdomain sono stati identificati i servizi esposti, verificando la presenza di banner mostranti la versione dello specifico servizio e dando così la possibilità di associare eventuali vulnerabilità note. È stata verificata l'esposizione di porte di management quali RDP, SSH, VNC e di protocolli obsoleti quali TELNET e FTP.

Per ciascun dominio è stata ricercata la presenza di domini look-alike, potenzialmente utilizzati per organizzare attacchi di typosquatting. Questa pratica, di frequente utilizzata dai cyber attaccanti, ha l'obiettivo di registrare domini che a prima vista somigliano al dominio target. Gli utenti sono pertanto portati a credere che si tratti del dominio legittimo o comunque legittimamente collegato al dominio originale.

Una verifica è stata svolta anche per quanto riguarda la presenza di domini di primo livello (TLD) registrati e per domini, non per forza di cose look-alike, per i quali nel momento dell'analisi erano in corso attività di phishing correlabili agli istituti di credito analizzati.

Valutazioni sono state fatte anche per la presenza di file potenzialmente interessanti indicizzati all'interno dei motori di ricerca, misconfiguration sui servizi web esposti, corretta configurazione dei mail server dell'organizzazione, esposizione di numeri telefonici, presenza all'interno di siti di tipo pastes (Pastebin, Ghostbin,...).

Sono inoltre stati identificati gli account email pubblicamente disponibili e per gli stessi è stata valutata la presenza all'interno di data breach ed il loro utilizzo all'interno di servizi web.

10 Metriche di valutazione

Per determinare l'esposizione di ogni singolo istituto di credito analizzato sono state create delle metriche che prendono in considerazione le numeriche di alcuni elementi come gli indirizzi IP esposti in internet e gli account email pubblicamente riscontrabili, calcolando infine dei rapporti in modo tale da raggiungere dei valori finali non dipendenti esclusivamente dalla dimensione del singolo istituto di credito.

Vengono di seguito forniti i dettagli sulle diverse metriche per i quali sono stati calcolati dei rapporti:

- indice di presenza nei data breach (*numero di account nei data breach / numero account email)*
- indice di disponibilità di credenziali *(numero di password / numero account email)*
- indice di vulnerabilità *(numero di ip / numero di vulnerabilità)*

Viene di seguito riportato il ranking, anonimizzato, relativo ai suddetti rapporti:

Banca	Breached Account (per email)	Password disponibili (per email)	Vulnerabilità (per ip)
Bank01	34,19	4,66	0,01
Bank02	7,06	3,03	0,97
Bank03	8,68	5,59	1,99
Bank04	12,66	4,89	0,23
Bank05	20,41	0,82	0,23
Bank06	3,44	0,30	0,30
Bank07	2,84	0,77	0,34
Bank08	42,88	2,44	0
Bank09	14,71	6,86	0,03
Bank10	19,47	8,07	0,50
Bank11	22,41	4,17	0,21
Bank12	13,90	6,33	1,12

Tabella 2 – ranking anonimizzato relativo a dati di compromissione recuperati da fonti OSINT

Vengono inoltre forniti i dettagli relativi alle metriche indipendenti, per le quali non sono stati calcolati dei rapporti con altri elementi:

- numero domini simili
- numero domini sospetti
- numero domini di phishing

11 Istituti di credito analizzati - Ranking P2R

Viene qui riportata la lista di istituti di credito analizzati, con l'indicazione per ognuno di essi del valore di P2R e del valore correlato al CET1:

ISTITUTO DI CREDITO	P2R TOTALE	DI CUI MINIMO CET1
Credito Emiliano Holding S.p.A.	1.00%	0.56%
Banca Mediolanum S.p.A.	1.50%	0.84%
Mediobanca - Banca di Credito Finanziario S.p.A.	1.68%	0.94%
Intesa Sanpaolo S.p.A.	1.72%	0.97%
Finecobank S.p.A.	1.75%	0.98%
UniCredit S.p.A.	2.00%	1.13%
Cassa Centrale Banca – Credito Cooperativo Italiano S.p.A.	2.50%	1.41%
Banco BPM S.p.A.	2.57%	1.45%
BPER Banca S.p.A.	2.61%	1.47%
Banca Popolare di Sondrio S.p.A.	2.66%	1.50%
BANCA MONTE DEI PASCHI DI SIENA S.p.A.	2.75%	1.55%
Iccrea Banca S.p.A. - Istituto Centrale del Credito Cooperativo	2.80%	1.58%

Tabella 3 - lista di istituti di credito analizzati, con l'indicazione del valore di P2R e del valore correlato al CET1

12 Risultati

Vengono di seguito riportati, in forma aggregata, i risultati dell'analisi.

12.1 IP

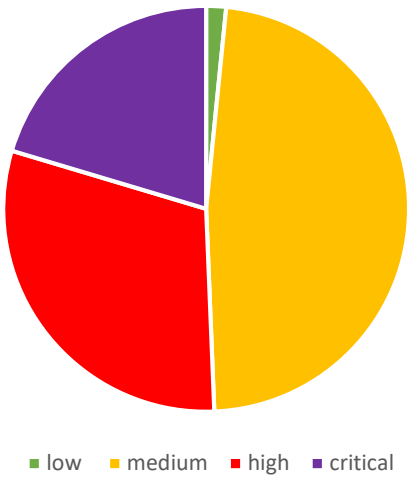
Mostriamo di seguito il numero di ip pubblicamente esposti e sui quali sono attivi servizi di vario genere.

4.517

12.2 Vulnerabilità

Viene di seguito mostrata l'evidenza delle vulnerabilità totali rilevate e suddivise per valore di gravità. Le informazioni sulle vulnerabilità forniscono all'attaccante path di attacco potenzialmente sfruttabili ma in generale anche informazioni relative alle tecnologie presenti all'interno dell'organizzazione.

1.325



Low = 21

Medium = 633

High = 401

Critical = 270

Grafico 2 - vulnerabilità totali rilevate e suddivise per valore di gravità

12.3 Dettaglio esposizione porte

Di seguito viene riportata la top 15 di porte esposte.

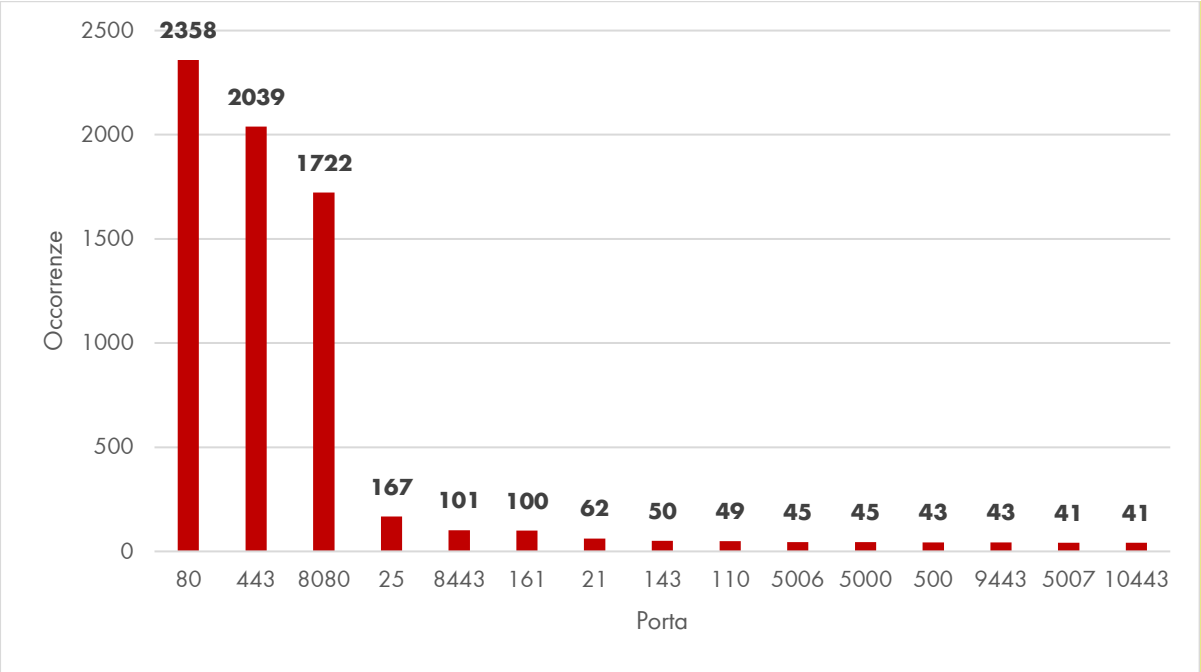


Grafico 3 – Lista delle prime 15 porte esposte

12.4 Esposizione porte di management

Viene indicato il numero di porte esposte e relative a servizi (RDP, SSH, telnet,...) utilizzati normalmente per svolgere attività di management. Un servizio di management direttamente esposto, senza alcuna altra misura di sicurezza al di là della coppia username / password, fornisce all'attaccante la possibilità di svolgere tentativi di attacco a dizionario o di brute force.

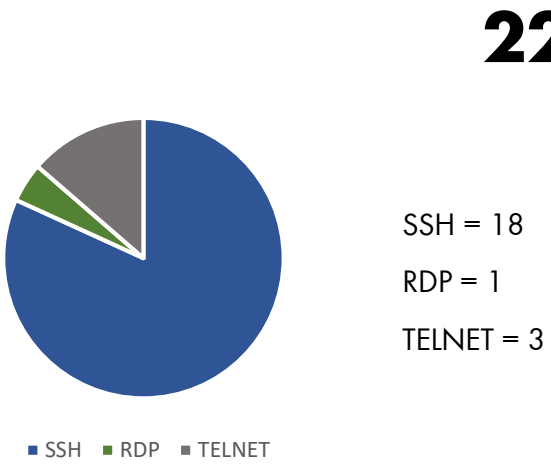


Grafico 4 – porte esposte e relativi a servizi di management

12.5 Record SPF e DMARC

Abbiamo verificato, per ciascuno dei 12 domini coinvolti nell'analisi, la presenza dei record **SPF** e **DMARC**.

SPF (Sender Policy Framework) consente di proteggere il dominio dallo spoofing e impedire che i messaggi in uscita vengano contrassegnati come spam. Grazie a SPF è possibile specificare i server di posta autorizzati a inviare email per conto del dominio. I server di destinazione utilizzano SPF per verificare che i messaggi in arrivo che sembrano provenire dalla tua organizzazione siano stati inviati da server che hai autorizzato.

DMARC (Domain-based Message Authentication, Reporting & Conformance) è un sistema per la validazione delle email ed è stato sviluppato principalmente per evitare l'email spoofing (cioè email inviate con mittente contraffatto).

Il risultato è il seguente:

SPF = 12/12

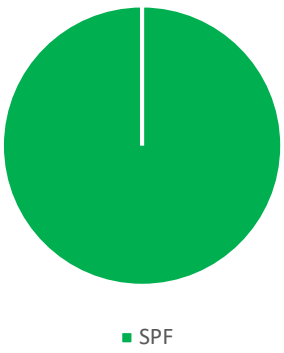


Grafico 5 – numero di record SPF rilevati nell'analisi

DMARC = 7/12

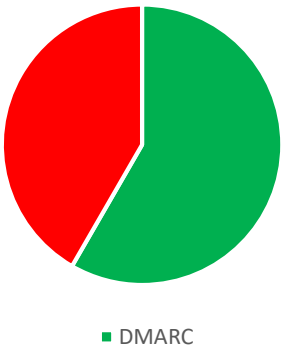


Grafico 6 - numero di record DMARC rilevati nell'analisi

12.6 Domini look-alike

Per dominio look-alike si intende un dominio creato con l'intento di essere simile al dominio originale. Viene mostrato il totale di domini look-alike individuati.

305

12.7 Domini sospetti

Durante l'analisi abbiamo ritenuto sospetti i domini, non per forza di cose di tipo look-alike, ma contenenti il base name del dominio analizzato.

34

12.8 Domini di phishing

Viene di seguito riportato il numero di domini che al momento della stesura del presente report vengono utilizzati per svolgere attivamente attacchi di phishing.

1

12.9 Data breach

Viene di seguito elencato il numero di email aziendali presenti all'interno di data breach, relative quindi a servizi che nel tempo sono stati violati e per i quali sono stati esfiltrati i database degli utenti registrati a quei servizi. La presenza nei data breach fornisce all'attaccante informazioni di contesto riguardo alla superficie di attacco dei diversi collaboratori delle organizzazioni.

120.775

12.10 Password

Viene di seguito riportato il numero di password rilevate e presenti nei data breach da noi analizzati. Le credenziali possono potenzialmente essere utilizzate per svolgere attività di Password Guessing, Credential Stuffing, Account Takeover.

Password in chiaro	Password hashate
37.324	**1.664**

12.11 Email in account out of business

Viene di seguito riportato il numero di account email aziendali utilizzati per iscriversi a servizi presumibilmente non collegati al business aziendale ed i servizi maggiormente rilevati. Queste informazioni sono utili all'attaccante per identificare la superficie di attacco di ogni singolo collaboratore.

9.293

4306	78	232	62	2051	66	530	370

12.12 Infostealer market place

Di seguito viene mostrato il numero di hosts compromessi a bordo dei quali sono presenti credenziali afferenti i servizi delle organizzazioni analizzate.

3.340

12.13 Credit card market place

Viene mostrato il numero di carte di credito che risultano essere in vendita all'interno dei credit card market place.

1.094

13 Exposure Assessment Index Value

La piattaforma SATAYO®, per ogni dominio analizzato, calcola un indice di esposizione (**EAIV** - Exposure Assessment Index Value) per 3 differenti macro aree di analisi, chiamate:

- Infrastructure
- Data, Files & People
- Deep & Dark Web

EAIV può assumere valori in un range che va da 0 a 100. A valore più elevato corrisponde un livello di esposizione maggiore.

Per ogni macro area viene preso in considerazione un set di differenti tipologie di evidenze:

Immagine 27 – Indice di esposizione EAIV rappresentato graficamente su 3 macro aree di analisi

14 Istituti di credito analizzati - Ranking EAIV

Viene di seguito riportato il ranking, anonimizzato, dei valori EAIV calcolati dalla piattaforma SATAYO® per i diversi domini oggetto di analisi.

Banca	Infrastructure	Data, Files & People	Deep & Dark Web	Totale
Bank01	13	13	31	57
Bank02	23	13	29	65
Bank03	17	26	24	67
Bank04	20	24	31	75
Bank05	24	30	30	84
Bank06	20	34	47	101
Bank07	24	53	33	110
Bank08	20	60	50	130
Bank09	29	67	37	133
Bank10	35	67	34	136
Bank11	49	53	40	142
Bank12	45	67	40	152

Tabella 4 - ranking, anonimizzato, dei valori EAIV calcolati dalla piattaforma SATAYO

15 Conclusioni

L'analisi svolta dal Security Operation Center di Würth Phoenix mostra certamente una situazione di esposizione interessante dal punto di vista di un attaccante, che può in generale acquisire facilmente informazioni, sia sul contesto generale dell'organizzazione che sulla specificità delle persone operanti all'interno della stessa.

Obiettivo del presente report è quello di fornire maggior consapevolezza riguardo alle tecniche utilizzate dai Threat Actors per collezionare informazioni utili nel contesto dell'attacco. Come descritto all'interno del capitolo "Focus sulla fase di Reconnaissance", vi sono sono una serie di tecniche che se applicate alle corrette fonti consentono agli attaccanti di recuperare un numero elevatissimo di informazioni. Il resto lo fa la capacità di automazione delle tecniche, che se applicata garantisce un notevole risparmio di tempo che l'attaccante potrà dedicare alle fasi successive.

La maggior consapevolezza riguardo a queste tecniche a nostro modo di vedere è l'elemento che deve essere utilizzato come input per rendere più difficoltosa l'azione degli attaccanti. Come indicato nel capitolo "Banche e cyber security - riferimenti normativi", spesso per l'attaccante la decisione del target dell'attacco dipende dall'idea che si fa riguardo alla complessità di collezionare informazioni utili nel contesto dell'attacco stesso. La risposta alla domanda "Quanto tempo devo investire per collezionare informazioni utili su questo target?" sarà l'elemento cardine nella scelta del target.

Da questo possiamo quindi intendere che più sarà complesso per l'attaccante recuperare informazioni sulla nostra organizzazione e meno sarà la probabilità di essere scelti come target dell'attacco.

Deve quindi nascere la **cultura della riduzione della superficie di attacco** e questo dovrebbe diventare un elemento di valutazione per ogni attività che contempla il possibile rilascio di informazioni che fin da subito o in seguito possono diventare di pubblico dominio. Le domande da porsi sono le seguenti:

- questa attività causa l'esposizione pubblica di informazioni utili in un contesto di attacco?
- questa attività fornisce informazioni a stakeholder che in un futuro potrebbero decidere di rendere pubbliche le stesse?
- dispongo delle capacità di identificare le informazioni che già in questo momento risultano pubblicamente disponibili?
- per quali tipologie di attacco possono essere utilizzate le informazioni che sono attualmente pubblicamente disponibili?
- la postura difensiva della mia organizzazione è sufficiente per difendermi da queste tipologie di attacco?

- per le informazioni che sono in questo momento disponibili esistono delle attività che mi consentono di eseguire il takedown delle stesse?
- sono in grado di identificare i primi step di attacco di tipo attivo nei quali vengono utilizzate le informazioni pubblicamente disponibili?

Risulta fondamentale diminuire il gap competitivo che in questo momento le organizzazioni scontano nei confronti degli attaccanti, acquisendo conoscenze in ambito Cyber Threat Intelligence, in grado talvolta di anticipare le mosse dell'avversario e di guadagnare del tempo che può diventare fondamentale per implementare misure difensive in grado di arginare le minacce. Nella scelta delle fonti di Cyber Threat Intelligence è opportuno valutare l'affidabilità delle fonti stesse e la qualità delle informazioni messe a disposizione.

Dal punto di vista della possibilità del singolo istituto di credito di essere contattato nel caso in cui un attore esterno, che agisca in modo etico, venga a conoscenza dell'esistenza di una o più vulnerabilità, si suggerisce di implementare il file security.txt (https://securitytxt.org), in modo tale da consentire un corretto processo di disclosure. È necessario uscire da quel paradigma che porta tante organizzazioni a vedere come nemico chi segnala una vulnerabilità ed anzi è necessario premiare chi comunica in modo corretto, utilizzando un processo di Vulnerability Disclosure condiviso, quelle vulnerabilità che se sanate possono portare ad aumentare velocemente la postura difensiva delle organizzazioni.

Il fattore umano, come già citato in precedenza, rimane l'anello più debole all'interno del sistema difensivo. Le istituzioni finanziarie dal punto di vista della comunicazione hanno certamente la possibilità di raggiungere un'ampia platea di utenti, grazie alla diffusione di sistemi di remote banking che possono essere utilizzati per condividere news e allarmi relativi alle campagne malevole in atto. Ecco che quindi diventa fondamentale sfruttare questo vantaggio nella comunicazione, fornendo consigli utili, tempestivi e semplici da applicare.

Infine, le attività di Adversary Simulation, se gestite da team in grado di governare l'ambito della Cyber Threat Intelligence ed utilizzare la stessa all'interno delle simulazioni di attacco, possono certamente rappresentare un importante banco di prova dello stato dell'arte delle capacità di detection & response delle singole organizzazioni.

16 Chi siamo

Würth Phoenix è un'azienda appartenente al Gruppo Würth, che é oggi presente in 89 Paesi con oltre 400 Società e una rete di vendita con più di 70.000 collaboratori. SEC4U è l'area di Würth Phoenix dedicata alla cyber security. All'interno dell'area è presente il team del Security Operation Center Attacker Centric, che ha curato l'analisi presentata in questo report.

Il team SEC4U ha ideato e sviluppato la piattaforma di Cyber Threat Intelligence SATAYO, che è stata la principale fonte delle informazioni utilizzate durante l'analisi. SATAYO è stata la prima piattaforma di Cyber Threat Intelligence ad ideare un indice di esposizione (EAIV - Exposure Assessment Index Value) in grado di valutare la superficie di attacco di un'organizzazione utilizzando le stesse metriche utilizzate dai Threat Actors. Questa peculiarità consente di rendere il nostro SOC "Attacker Centric", in grado quindi di sfruttare con scopi difensivi le informazioni collezionate durante la fase più importante di un attacco, la Reconnaissance.

16.1 Analisi

Massimo Giaimo

Federico Corona

16.2 Contributi Tecnici

Würth Phoenix SOC Attacker Centric Team

16.3 Contributi Grafici

Arianna Zuzolo

16.4 Contatti

Würth Phoenix S.r.l.

Via Johann Kravogl 4, 39100 Bolzano BZ, Italy

+39 0471 564 111 (HQ)

info@wuerth-phoenix.com

16.5 Il SOC di Würth Phoenix nella community internazionale

Il nostro impegno verso la community è in continuo miglioramento ed in continua espansione.

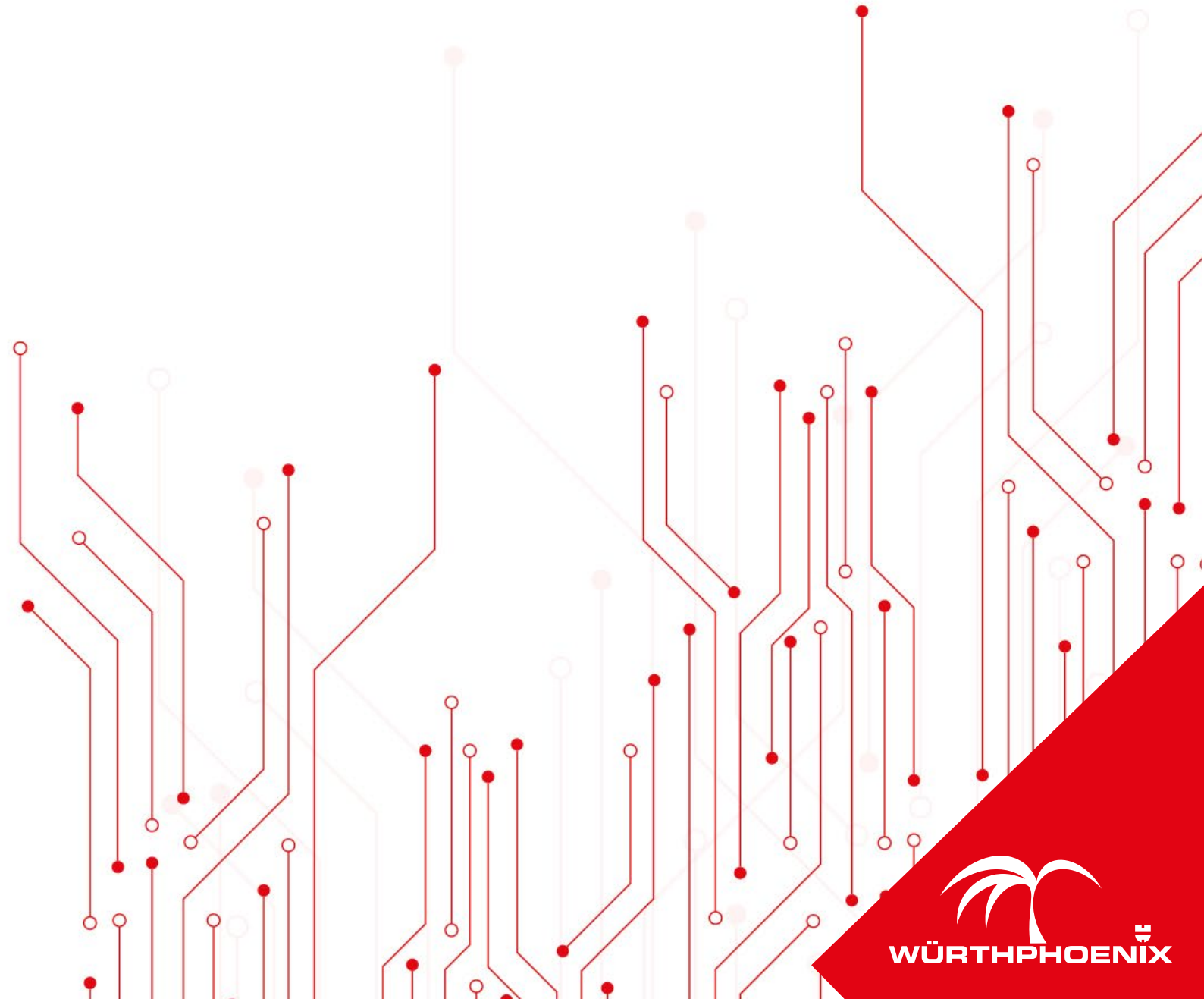
Siamo fondatori del progetto **deepdarkCTI** (https://github.com/fastfire/deepdarkCTI). Il progetto è nato nel 2021 con l'obiettivo di raggruppare fonti utili alle attività di Cyber Threat Intellligence ed in breve tempo è diventato un punto di riferimento importante, con più di 2000 persone che seguono il progetto su GitHub e decine di contributori che quotidianamente partecipano all'obiettivo di rendere deepdarkCTI la più completa collezione di fonti per chi si occupa di CTI.

Siamo membri della community **Curated Intelligence** (https://www.curatedintel.org/). Questa community, all'interno della quale vi sono mediamente 200 professionisti selezionati attraverso un rigoroso processo e facenti parte delle più importanti organizzazioni operanti nell'ambito della cyber security a livello globale, è attiva una continua condivisione di informazioni, talvolta in modalità classificata come riservata (TLP:RED).

Il nostro Security Operation Center Attacker Centric è ufficialmente parte della community **TF-CSIRT Trusted Introducer** come membro di tipo **ACCREDITED**. Solo chi di**mostra di aver implementato dei rigorosi processi di gestione dei propri servizi ha la** possibilità di entrare in questa importante community. Il Trusted Introducer Service, noto anche come TI, è stato istituito dalla comunità europea CERT nel 2000 per rispondere a esigenze comuni e costruire un'infrastruttura di servizi che fornisca un supporto vitale a tutti i team di sicurezza e di risposta agli incidenti. Essere parte di questa community significa avere la possibilità di confrontarsi periodicamente tra alcuni dei team più preparati nel panorama internazionale e di essere parte di un team di persone che fanno della condivisione delle informazioni un elemento fondamentale per aumentare la qualità dei propri processi. Puoi verificare lo stato della nostra membership al link https://www.trusted-introducer.org/directory/teams/cert-wuerthphoenix-it.html

info@wuerth-phoenix.com
www.wuerth-phoenix.com

© Würth Phoenix



WÜRTHPHOENIX