CYBER INTELLIGENCE REPORT

MERIDIAN GROUP

WEEKLY UPDATE

TLP: GREEN

DATA: 08.04.2024

Sommario

Indice Figure

Company Overview

Meridian Group si posiziona come un leader nel campo della sicurezza informatica, offrendo consulenza aziendale di alto livello. Grazie alla nostra vasta esperienza e alla collaborazione con rinomate aziende nazionali e internazionali, abbiamo sviluppato una profonda comprensione delle specifiche esigenze nel settore della sicurezza informatica. La nostra capacità di stabilire relazioni significative con governi e istituzioni a livello globale ci contraddistingue, fornendo un prezioso supporto alle aziende nella ricerca di partnership industriali e commerciali.

Con una rete di oltre 50 partner professionisti in paesi chiave come Belgio, Italia, Francia, Regno Unito, Germania, Romania, Tunisia, Qatar, Brasile, Cina ed Emirati Arabi Uniti, Meridian Group si impegna a offrire soluzioni innovative ed etiche. Queste fondamenta sono alla base della nostra filosofia aziendale e guidano ogni nostra azione. La nostra costante attenzione all'innovazione ci spinge ad esplorare nuovi orizzonti nel campo della sicurezza informatica, mentre il nostro impegno verso la responsabilità assicura che ogni soluzione sia etica e sostenibile.

Offriamo ai nostri clienti servizi personalizzati e competitivi progettando soluzioni in grado non solo di soddisfare le aspettative ma anche di superarle. Il nostro approccio si basa su competenze avanzate, idee innovative e una pianificazione accurata al fine di creare un valore tangibile aggiuntivo.

La nostra missione consiste nel trasformare le sfide in opportunità, creando strategie efficaci che consentano ai nostri clienti di ottenere risultati tangibili e di successo.

Kitsune Platform

Kitsune è la piattaforma di cyber intelligence completamente italiana sulla quale il team di cyber intelligence eroga servizi as a service ai clienti di Meridian Group.

Kitsune monitora l'underground con oltre 1.300 fonti dirette ed oltre 50.000 canali pubblici e privati garantendo ai clienti una larga visibilità sul mondo del crimine informatico.

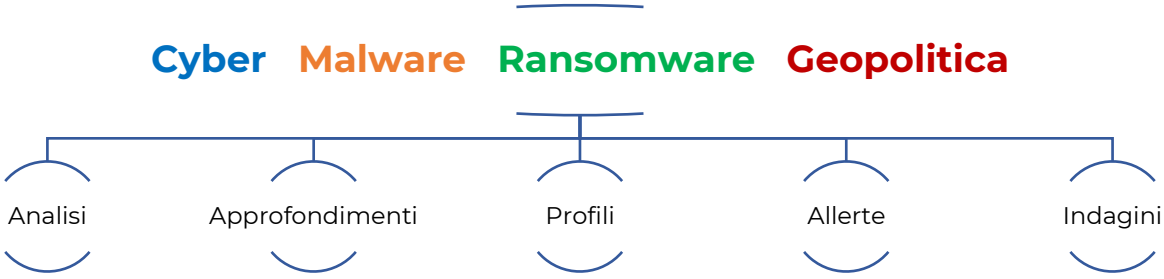
Kitsune è una piattaforma di Cyber Intelligence che si pone l'obiettivo di essere uno strumento indispensabile per gli analisti di intelligence.

La sua funzione principale è quella di raccogliere dati provenienti da diverse fonti e correlarli al fine di garantire un approccio proattivo nei confronti delle minacce che possono colpire aziende, istituzioni e persone. Kitsune offre agli analisti un ampio spettro di informazioni e strumenti avanzati per analizzare e comprendere le tendenze nel campo della sicurezza informatica. Attraverso l'utilizzo di tecniche avanzate di intelligenza artificiale e analisi dei dati, la piattaforma identifica potenziali minacce in tempo reale, consentendo agli analisti di adottare misure preventive tempestive.

Kitsune rappresenta quindi un valido alleato per gli analisti di intelligence, fornendo loro una panoramica completa delle minacce digitali e permettendo di agire in modo proattivo per mitigarle.

Metodologie e Risorse

Il team di Cyber Intelligence (CI) utilizza i seguenti metodi e risorse per l'analisi delle notizie e per l'acquisizione di informazioni utili al contenimento degli attacchi informatici.



Il Team di CI, attraverso questo report settimanale, mira a fornire analisi tempestive e accurate riguardo alle aree, di cui sopra, consentendo ai lettori di essere a conoscenza delle ultime notizie riguardanti nuove vulnerabilità, potenziali minacce e cambiamenti nello scenario geopolitico.

L'analisi giornaliera delle notizie sulla piattaforma Kitsune è essenziale per gli analisti di CI al fine di monitorare e comprendere i rischi emergenti nelle diverse categorie, sopra esposte, consentendo così di prevenire o mitigare le potenziali minacce alla sicurezza dei clienti.

Target sbagliato: colpita un'associazione di volontariato

In vendita presunte credenziali per l'accesso al portale della Protezione Civile Italiana

Recentemente, sul forum underground Breach Forums è stato messo in vendita un presunto accesso privilegiato al portale della Protezione Civile Italiana. Il post aveva come titolo "*selling 1 Admin login for access to the Italian civil protection*" ed elencava i dettagli per l'accesso amministrativo che consente la visualizzazione di informazioni e dati riservati di molti funzionari della Protezione Civile.

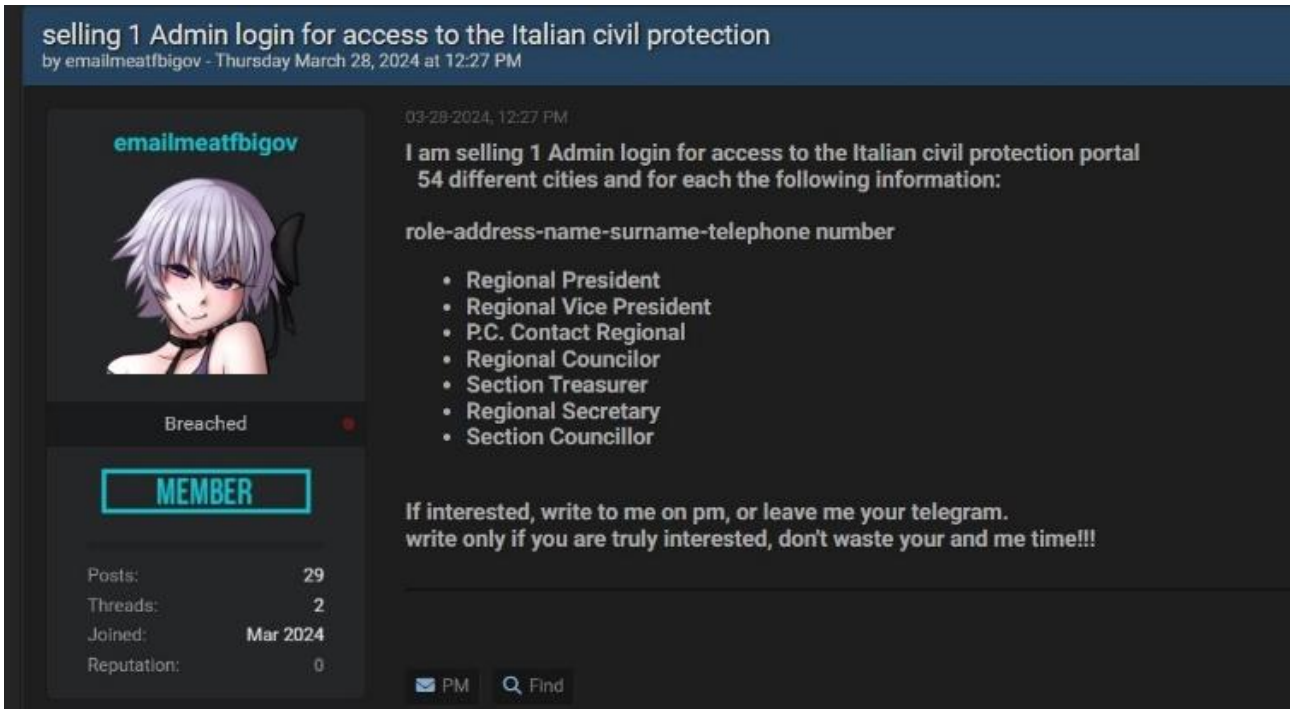


Figura 1 - Credenziali in vendita su Breach Forums

In seguito ai controlli effettuati dal team della Protezione Civile che si occupa delle attività di sicurezza cibernetica è emerso che ad essere stato violato non è stato il Portale del Dipartimento della Protezione Civile Italiana bensì il sistema informatico di un'associazione di volontariato.

Phishing: falsi avvisi della Polizia Giudiziaria

È in corso una nuova campagna di phishing riguardante false convocazioni giudiziarie a firma del Capo della Polizia

Martedì 2 aprile la Polizia Postale ha reso noto una nuova campagna di phishing contro gli utenti italiani, quest'ultimi si sono visti recapitare una presunta e-mail della Polizia Giudiziaria con filigrana dell'Agenzia Nazionale per la Cybersicurezza (ACN), che li convocava in merito ad un'inesistente indagine penale per i reati di pornografia infantile, pedofilia, esibizionismo e pornografia informatica.

REPUBBLICA ITALIANA
DIPARTIMENTO DELLA PUBBLICA SICUREZZA
DIREZIONE CENTRALE DELLA POLIZIA DI PREVENZIONE
BRIGATA DEI GIOVANI

CONVOCAZIONE GIUDIZIARIA

Alla vostra attenzione,

Sono **Dott. Vittorio Pisani**, Capo della Polizia in attuazione della decisione quadro del Consiglio dell'Unione europea **n. 2004/68/GAI del 22 dicembre 2003**

Secondo le disposizioni dell'articolo 372 del Codice Penale, "qualsiasi aggressione indecente commessa senza violenza o minaccia sulla persona o con l'aiuto di un minore di 16 anni, maschio o femmina, è punita con la reclusione". **L'articolo 227-23** del codice penale recita: "Il fatto di fissare, registrare o trasmettere un'immagine o una rappresentazione di natura pornografica al fine di diffonderla è punito con la reclusione da **3** a **6** anni e con una multa da **25.000 €** a **75.000 €**.

Avvieremo un procedimento legale contro di voi dopo il sequestro del computer effettuato da Cyber Infiltration per :

- **Pornografia infantile**
- **Pedofilia**
- **Esibizionismo**
- **Pornografia informatica**

Per vostra informazione, **la legge nr.38 del codice di procedura penale del 6 febbraio 2006** aumenta le pene quando proposte sessuali, aggressioni o stupri possono essere stati commessi usando internet. Lei ha commesso il reato dopo essere stato preso di mira su internet(sito di annunci), la visione di video di natura pedopornografica e le foto/video di nudo di minori sono state registrate dalla nostra cybersicurezza informatica e costituiscono la prova dei suoi reati.

Nell'interesse della riservatezza, le inviamo questa e-mail. Le chiediamo di far conoscere il suo caso via e-mail, scrivendo le sue giustificazioni in modo che possano essere esaminate e verificate per valutare le sanzioni; questo deve essere fatto entro un termine rigoroso di 72 ore.

Trascorso questo periodo, saremo obbligati ad inviare il nostro rapporto al procuratrice generale di Milan e Specialista in Cybercrime, al fine di emettere un mandato di arresto e si procederà al tuo arresto immediato da parte della polizia postale o municipale più vicina al tuo luogo di residenza e sarai iscritto nel registro nazionale dei sex offenders.

In questo caso, il suo file sarà anche trasmesso alle associazioni che lottano contro la pedofilia e ai media per la pubblicazione comepersona iscritta al **RNDS**.

Ora siete stati avvertiti.

Cordiali saluti,
Dott. Vittorio Pisani
Capo della Polizia e Direttore Generale della Pubblica Sicurezza

Dipartimento della Pubblica Sicurezza
Direzione Centrale della Polizia di Prevenzione
Via Quattro Novembre, 119/A, 00187 Roma RM

Figura 2 - Presunta convocazione giudiziaria

Lo scopo della mail è quello di indurre il destinatario a contattare il truffatore entro 72 ore e procedere al pagamento di una somma di denaro per evitare le condanna.

La Polizia Postale raccomanda di diffidare da simili messaggi poiché le Forze dell'Ordine non contattano direttamente i cittadini, attraverso email o messaggi, e non chiedono, a quest'ultimi, pagamenti in cambio del depennamento del procedimento penale.

“Balada Injector” colpisce l’Italia

È in corso una campagna di phishing denominata “Balada Injector” che colpisce utenti e aziende italiane: possibile coinvolgimento dell'APT iraniano MuddyWater

Nel complesso panorama delle minacce informatiche, gli attacchi di phishing continuano a rappresentare uno dei pericoli più insidiosi per la sicurezza online di aziende e privati. Recentemente è stata scoperta in Italia la sofisticata campagna di phishing denominata “Balada Injector”.

Questo tipo di attacco non è nuovo, infatti “Balada Injector” è una campagna malevola in corso dal 2017 che ha già compromesso oltre un milione di siti WordPress sfruttando vulnerabilità note in temi e plugin. Gli attacchi avvengono in ondate periodiche, utilizzando domini appena registrati per ospitare script malevoli. L'obiettivo principale è quello di rubare credenziali di database, creare falsi utenti admin, raccogliere dati dagli host compromessi e lasciare backdoor per un accesso persistente. Le vittime vengono reindirizzate verso falsi siti di supporto tecnico, truffe di vincite alla lotteria e pagine CAPTCHA fasulle che inducono ad abilitare le notifiche push per inviare pubblicità spam.

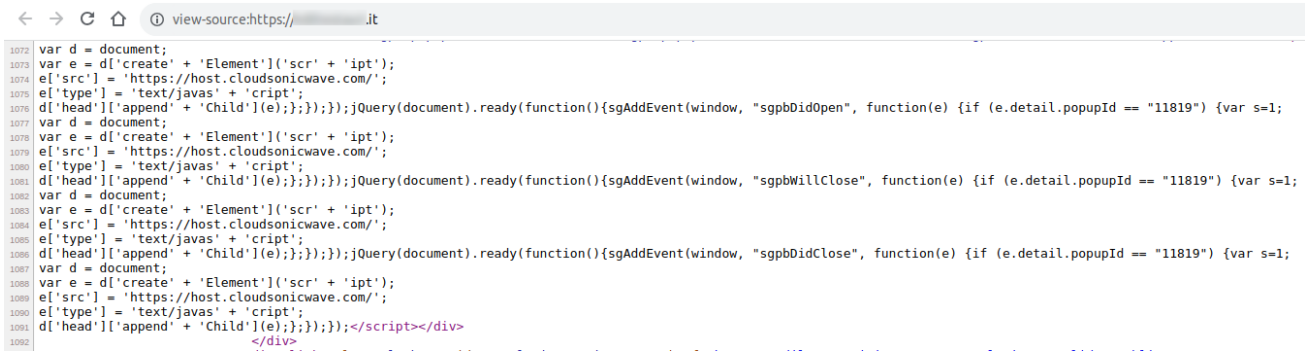


Figura 3 - Codice javascript malevolo per indirizzare le vittime verso falsi siti web

Nel nostro caso, l'attacco inizia con un'email apparentemente legittima, contenente un link che reindirizza a un sito web contenente un sofisticato PDF interattivo per ingannare le vittime. Il PDF contiene codice JavaScript che ruba i dati inseriti dall'utente e li invia tramite API a un sito WordPress iraniano.

Analisi più approfondite sulle tecniche utilizzate e sull’infrastruttura suggeriscono il coinvolgimento di MuddyWater, un noto gruppo di minacce persistenti avanzate (APT) di origine iraniana. Attivo dal 2017, MuddyWater è specializzato in operazioni di cyberspionaggio, utilizzando sia strumenti liberamente disponibili che malware unici sviluppati internamente. Sebbene il gruppo prenda di mira principalmente paesi del Medio Oriente, in particolare Israele e Arabia Saudita, non è estraneo ad attacchi verso altre nazioni.

Gruppo Benetton nel mirino degli hacker

Il gruppo ransomware “Hunters International” colpisce il colosso della moda

Hunters International ha rivendicato in settimana un attacco ransomware al noto marchio di abbigliamento italiano Benetton Group. Tuttavia, da successive analisi e informazioni trapelate, è emerso come in realtà i dati siano parte del furto telematico avvenuto un anno fa, nel gennaio del 2023. In quell’occasione i cybercriminali avevano portato avanti una campagna di attacco durata diversi giorni per poi essere definitivamente bloccati dal Security Operation Center dell’azienda trevigiana riuscendo però ad esfiltrare centinaia di gigabyte di dati.

Hunters, la cui localizzazione non è nota con certezza, è emerso nel terzo trimestre del 2023, poco dopo lo smantellamento del gruppo Hive da parte delle forze dell'ordine, ed è noto soprattutto per l'utilizzo di tattiche opportunistiche, prendendo di mira organizzazioni di diversi settori e aree geografiche, senza un focus specifico.

La loro tecnica, come nel caso di questo attacco, prevede la doppia estorsione, cifrando i dati delle vittime e minacciando di pubblicarli su il loro “Data Leak Site” (DLS) nel dark web in caso di mancato pagamento del riscatto.

Figura 4 - DLS di Hunters International

Un’altra particolarità del gruppo prevede l’attivazione di due timer una volta pubblicata la notizia dell’attacco sul loro DLS: uno per i samples, necessari per dare credito all’attacco e dimostrare che è avvenuto, e l’altro per la pubblicazione di tutti i dati esfiltrati.

Nella notte tra il cinque e il sei aprile è scaduto il termine per il primo timer e sono stati pubblicati i samples. I file in questione sono dieci in totale di tipo XLSX per una dimensione complessiva di 33.8MB e sono oggettivamente datati in quanto riferiti al periodo 2014-2019.

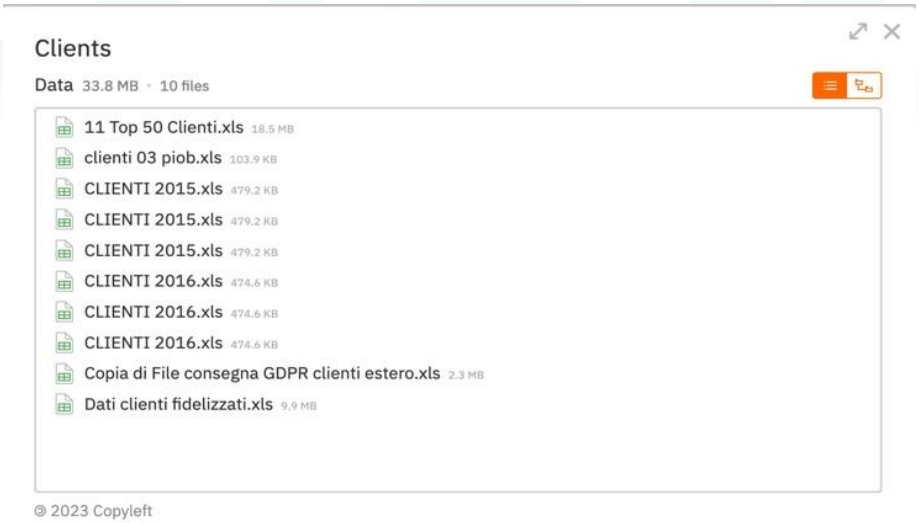


Figura 5 - Samples dei documenti

Successivamente, il pomeriggio del sette aprile è scaduto il secondo timer e così sono stati pubblicati tutti i 433.7GB che confermano come l'attacco abbia riguardato una sezione specifica dei file server della sede centrale di Benetton. Infatti i dati trafugati riguardano perlopiù documenti amministrativi afferenti al personale (2018-2022), documenti della fabbrica tessile del Gruppo Benetton a Osijek, in Croazia e altri documenti dell'azienda serba "Olimpias Knitting", parte di Olimpias Group Srl (Benetton Group) uno dei più importanti gruppi italiani per la fornitura di servizi dedicati al settore tessile.

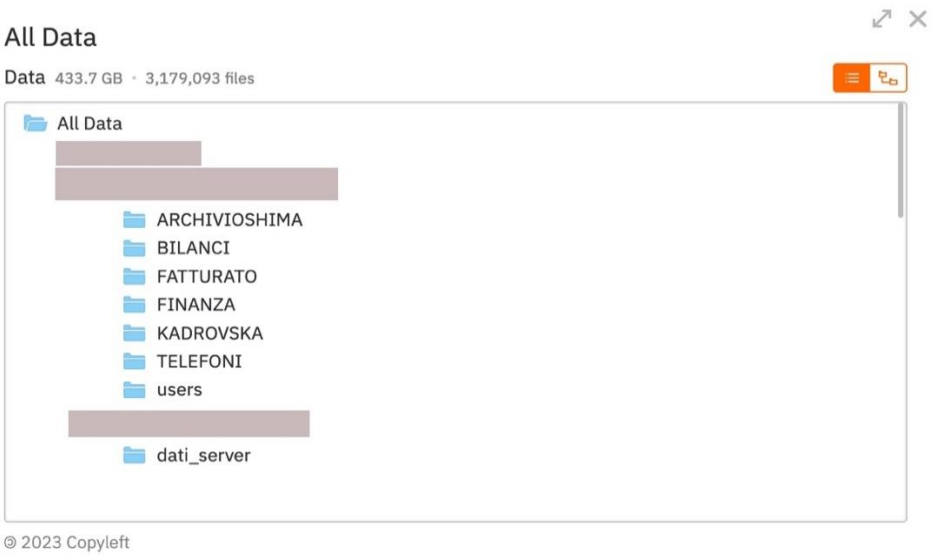


Figura 6 - Pubblicazione di tutti i dati

Nonostante Benetton non abbia ancora ufficializzato un comunicato per l'accaduto, fonti interne hanno riferito che stanno collaborando attivamente con le forze dell'ordine.

Il trojan Mispadu colpisce l'Italia

Dall'America Latina all'Europa: la strategia di infezione multi-stadio del malware

Il trojan bancario Mispadu, un malware che ruba le credenziali dei conti bancari, si è diffuso dall'America Latina all'Europa, prendendo di mira gli utenti in Italia, Polonia e Svezia.

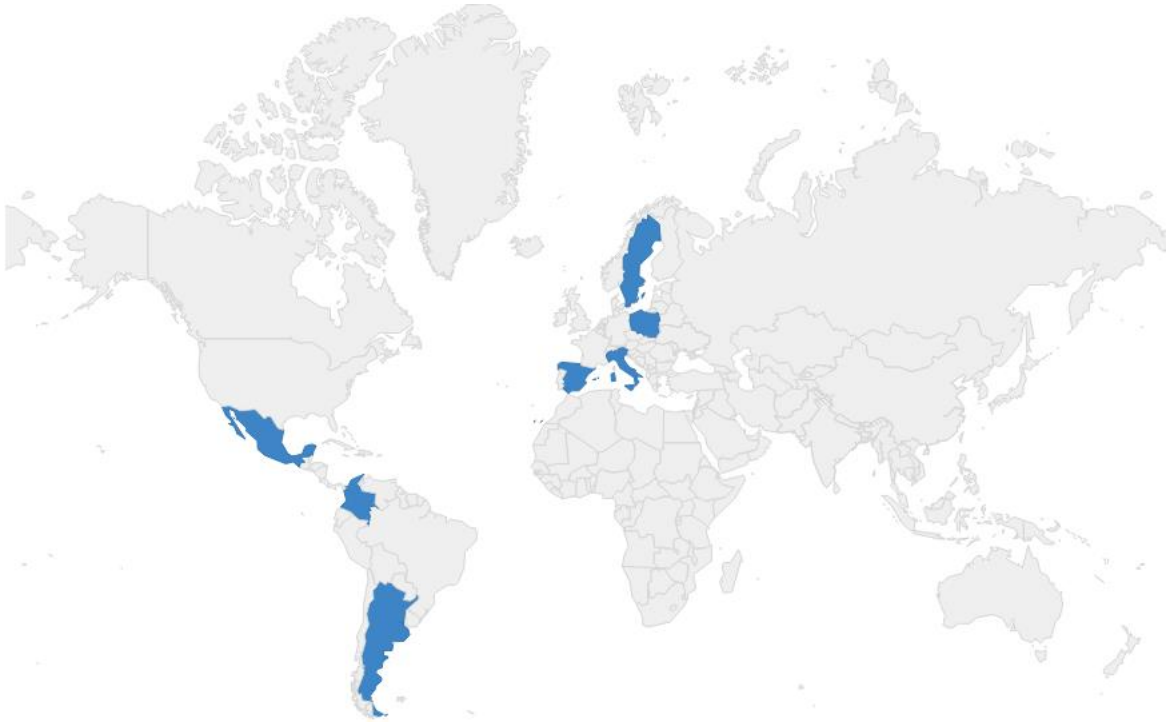


Figura 7 - Paesi colpiti dal trojan Mispadu

Originariamente scoperto nel 2019, Mispadu si è concentrato principalmente sulle istituzioni finanziarie del Brasile e del Messico, utilizzando falsi pop-up per rubare le credenziali degli utenti. Il trojan è ora evoluto utilizzando due server di comando e controllo (C2) separati per il recupero dei payload e l'esfiltrazione delle credenziali, colpendo oltre 200 istituti bancari.

Mispadu è noto per la sua strategia di infezione multi-stadio, che lo rende più difficile da rilevare. Il gruppo dietro al malware, molto attivo in America Latina, utilizza tecniche di spam e malvertising per distribuire il trojan, compromettendo siti web legittimi per diffondere ulteriormente il malware. Il gruppo ha anche aggiunto nuove tecniche, come l'utilizzo di certificati falsi e una nuova backdoor in linguaggio .NET; per mascherare i loro attacchi.

Negli ultimi mesi, Mispadu ha sfruttato una falla di sicurezza di Windows SmartScreen per compromettere gli utenti in Messico. Questa falla, corretta da

Microsoft a novembre 2023, è stata utilizzata da diversi gruppi di cybercriminali per vari malware, tra cui DarkGate e Phemedrone Stealer.

In conclusione, la minaccia rappresentata dal trojan bancario Mispadu è una grave minaccia per le banche e i conti bancari, consentendo ai cybercriminali di rubare informazioni sensibili e di eseguire transazioni fraudolente. Per questo motivo si richiede alle aziende un approccio proattivo alla sicurezza per mitigare i rischi e garantire la protezione degli asset mentre si ottimizzano gli investimenti nella sicurezza informatica.

MERIDIAN GROUP

MERIDIAN SRL
Viale dell'Oceano Atlantico,
182 – Roma – Italy

p.Iva: 13693001003

www.meridian-group.eu
info@meridian-group.eu