CYBER INTELLIGENCE REPORT

MERIDIAN GROUP

WEEKLY UPDATE

TLP: GREEN

DATA: 02.04.2024

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.

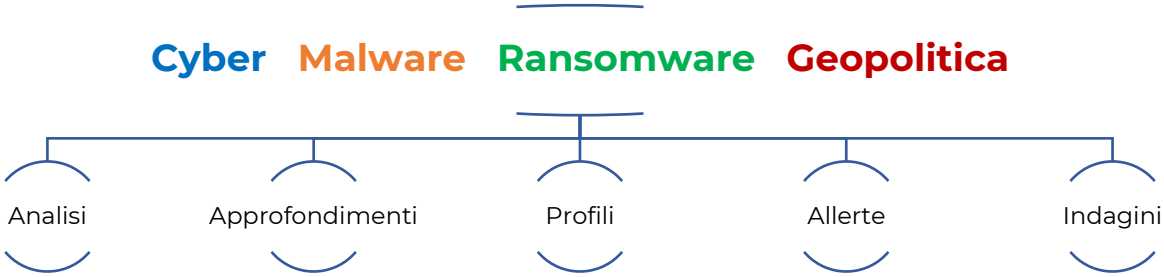
Kitsune è una piattaforma di Cyber Intelligence che si pone l'obiettivo di essere uno strumento indispensabile per gli analisti di intelligence.

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.

Attacco all'AGCOM

Esposizione del codice sorgente di "piracy shield" italiano

Il 26 marzo 2024 informazioni basate su ricerca OSINT hanno segnalato la fuga del codice sorgente e della documentazione interna del sistema italiano "Piracy Shield", scatenando significative polemiche e sollevando preoccupazioni sulla censura, sulla trasparenza e sulla privacy dei dati.

La pubblicazione dei nove repository è stata accompagnata da un annuncio in italiano e inglese pubblicato su GitHub, da un utente chiamato Fuckpiracyshield, che ha criticato l'AGCOM, l'autorità italiana di regolamentazione delle telecomunicazioni, e SP Tech Legal, lo sviluppatore collegato allo studio legale dietro Piracy Shield, identificando Piracy Shield come "uno strumento di censura camuffato da soluzione alla pirateria".

Fuck Piracy Shield, AGCOM and SP Tech Legal

IT - Italiano

Piracy Shield, una piattaforma sviluppata da SP Tech Legal per AGCOM, non è solo un tentativo all'italiana di combattere la pirateria online, ma è anche una pericolosa porta verso la censura. Il suo blocco indiscriminato di siti web e indirizzi IP legittimi costituisce un pericolo immenso, aprendo la strada a una censura incontrollata sotto il pretesto dell'applicazione delle leggi sul copyright.

Concedere alle autorità il potere incontrollato di bloccare contenuti online, Piracy Shield rappresenta una minaccia significativa alla libertà di espressione e all'accesso alle informazioni. Questo approccio draconiano non solo fallisce nel combattere efficacemente la pirateria, ma mina anche i principi democratici fondamentali.

È necessario riconoscere Piracy Shield per ciò che realmente è: uno strumento di censura mascherato come una soluzione alla pirateria. Piracy Shield è semplicemente il risultato di incompetenza tecnica ed eccessiva burocrazia, una costante nel governo italiano.

GB - English

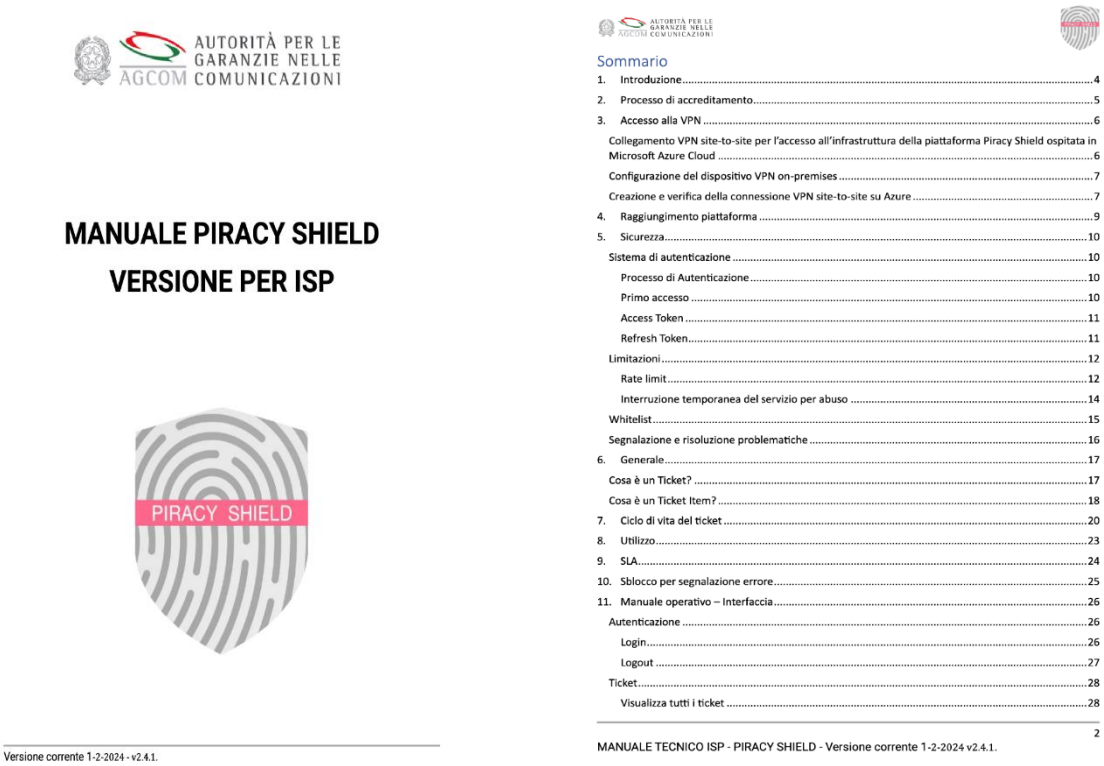
Piracy Shield, a platform developed by SP Tech Legal for AGCOM, is not just a failed attempt to combat online piracy, but it's also a dangerous gateway to censorship. Its indiscriminate blocking of legitimate websites and IP addresses poses an immense danger, paving the way for unchecked censorship under the guise of copyright enforcement.

Granting authorities unchecked power to block online content, Piracy Shield represents a significant threat to freedom of expression and access to information. This draconian approach not only fails to effectively combat piracy but also undermines fundamental democratic principles.

It is necessary to recognize Piracy Shield for what it truly is: a tool of censorship disguised as a solution to piracy. Piracy Shield is simply the result of technical incompetence and excessive bureaucracy, a constant in the Italian government.

Figura 1 - Annuncio di Fuckpiracyshield su GitHub

Il materiale trapelato include la versione 2.4.1, aggiornata al 2 febbraio, del “MANUALE TECNICO ISP – PIRACY SHIELD”.



AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

MANUALE PIRACY SHIELD
VERSIONE PER ISP

PIRACY SHIELD

Versione corrente 1-2-2024 - v2.4.1.

Sommario

2

MANUALE TECNICO ISP - PIRACY SHIELD - Versione corrente 1-2-2024 v2.4.1.

Figura 2 - Versione 2.4.1 del MANUALE TECNICO ISP – PIRACY SHIELD

Phishing contro la PA

Tentativo di furto delle credenziali degli account Outlook

È in corso una campagna di phishing mirato alla Pubblica Amministrazione (PA), con l'obiettivo di rubare le credenziali degli account di posta elettronica MS Outlook".

Il phishing è una delle minacce più insidiose nel panorama della sicurezza informatica. Gli hacker, utilizzando tecniche di ingegneria sociale, inviano mail con allegati malevoli che assomigliano a un servizio legittimo, come il login di una banca o il modulo di reset della password. Quando gli utenti inseriscono le loro credenziali su questi moduli, le informazioni vengono inviate direttamente agli attaccanti.

Figura 3 - Modulo dannoso presente nelle mail di phishing

Nel caso specifico riportato gli attaccanti inviano e-mail fraudolente che promettono aggiustamenti salariali o accessi a buste paga elettroniche, inducendo le vittime a scaricare allegati con doppia estensione (.pdf.html) che conducono a pagine di phishing.

Figura 4 - Mail di phishing inviata ai dipendenti della PA

L'Espansione di AgentTesla in Italia

La nuova ondata di AgentTesla, il Malware-As-A-Service dei forum underground aumenta gli attacchi in Italia

Di recente il malware AgentTesla sta aumentando le campagne di phishing in Italia, sfruttando un sempre maggior utilizzo di allegati PDF apparentemente innocui.

Gli allegati presenti all'interno delle mail di phishing contengono un link malevolo che avvia il download di un file a doppia estensione ".pdf.js", che racchiude codici Javascript. Tale codice ha l'obiettivo di scaricare ed eseguire uno script PowerShell che avvierà l'eseguibile di AgentTesla.

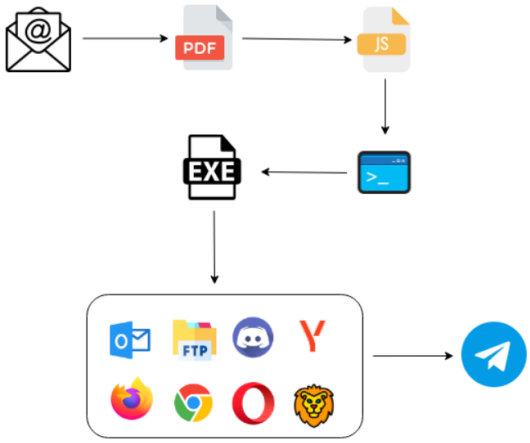


Figura 5 - Catena di Infezione AgentTesla

L'eseguibile in questione non è salvato sul disco, ma caricato ed eseguito direttamente in memoria. Tutte le informazioni riguardanti la macchina infettata come "hostname", specifiche hardware/software e credenziali vengono inviate a un bot Telegram portando a termine l'esfiltrazione dei dati.

Il modus operandi alquanto astuto di AgentTesla ha portato il gruppo ad affermarsi nel panorama cybercriminale tra i più noti Initial Access Brokers (IAB), offrendo ai gruppi cybercriminali l'accesso "chiavi in mano" a sistemi aziendali.

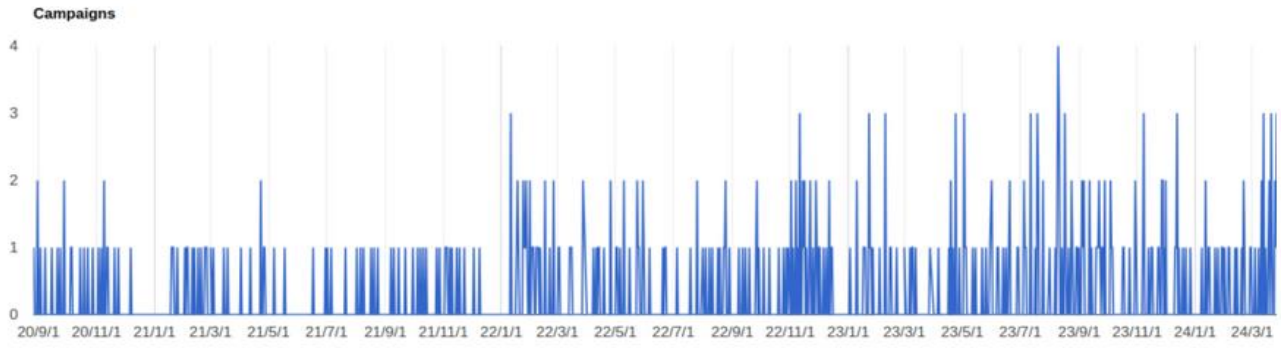


Figura 6 - Trend quadriennale delle campagne AgentTesla in Italia

MERIDIAN GROUP

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

p.Iva: 13693001003

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