CYBER INTELLIGENCE REPORT

MERIDIAN GROUP

WEEKLY UPDATE

TLP: GREEN

DATA: 15.04.2024

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.

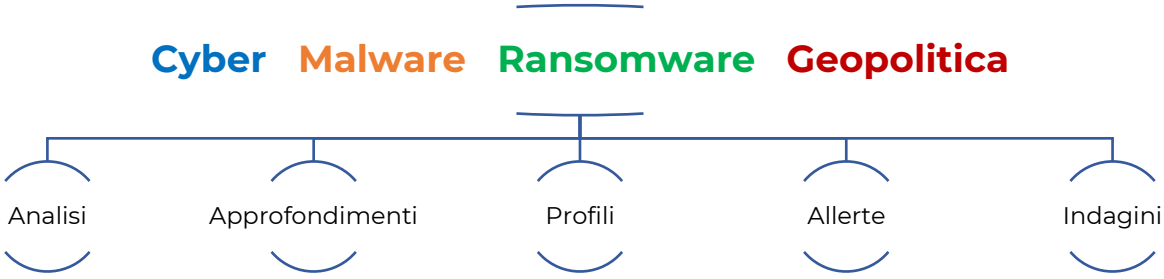
Kitsune è una piattaforma di Cyber Intelligence che si pone l'obiettivo di essere uno strumento indispensabile per gli analisti di intelligence.

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.

L’Iran attacca Israele con centinaia di droni

L’Iran ha dimostrato di non avere la forza né i mezzi per condurre una guerra contro Israele, anche se un attacco diretto contro il territorio dello Stato ebraico è comunque un inedito.

L’Iran ha lanciato nella serata di sabato 13 aprile un massiccio attacco contro Israele con più di 150 droni e missili sia di crociera sia balistici. Nelle prime ore dall’inizio dell’attacco è stato affermato che sono stati intercettati e distrutti la stragrande maggioranza degli attacchi fuori dallo spazio aereo israeliano, sopra Iraq e Siria in primis, con il sostegno di Giordania, Usa e Regno Unito. Israele, infatti, dispone di sistemi estremamente avanzati di difesa aerea per intercettare in volo droni e missili, e gli alleati, a partire dagli Usa hanno dispiegato negli scorsi giorni ulteriori sistemi di protezione analoga. Qualcuno però è arrivato a terra, colpendo obiettivi militari e causando decine di feriti sia militari sia civili.

Figura 1 - Lancio missilistico di Teheran

Nella tarda serata si è diffusa la notizia che altri droni sono stati lanciati dai ribelli Houthi dello Yemen, mentre dal Libano è partita una selva di razzi da parte di Hezbollah. Gli obiettivi designati sarebbero in particolare le Alture del Golan, al confine con la Siria, e una base aerea nel deserto del Negev, nel sud di Israele.

In una dichiarazione di fuoco l'Iran, presso le Nazioni Unite, ha rivendicato la rappresaglia di queste ore come «un'azione militare in risposta all'aggressione di Israele contro il complesso diplomatico iraniano a Damasco», ammonendo gli Usa a «restare fuori dal conflitto». Teheran però ha anche indicato che dal suo punto di vista, con l'azione notturna, «la questione può considerarsi conclusa» se Israele non contrattaccherà. Ma poco dopo l'una di notte in Italia dopo avere riunito il suo gabinetto di guerra il premier israeliano Benjamin Netanyahu ha annunciato la temuta risposta di Israele all'attacco iraniano, anche se non ne he svelato nè tempi nè modi.

Figura 2 - Intercettazione di un drone

La premier Meloni, in una nota di governo, dopo aver incontrato il ministro degli Esteri Antonio Tajani, quello della Difesa Guido Crosetto e il sottosegretario Alfredo Mantovano, Autorità delegata per la sicurezza della Repubblica, ha ribadito la condanna agli attacchi:

> "Esprimiamo forte preoccupazione per una destabilizzazione ulteriore della regione e continuiamo a lavorare per evitarla".

Il ministro degli Esteri Tajani aveva dichiarato la necessità di trovare una soluzione diplomatica per evitare una escalation:

> "Come prima cosa mobiliteremo i Paesi del G7 di cui abbiamo la presidenza di turno. Non possiamo rinunciare all'azione politica che deve viaggiare in parallelo con la valutazione della intensità dell'azione militare iraniana e dei danni prodotti. Il primo obiettivo è gettare acqua sul fuoco".

Anche oltreoceano si segue la situazione in Medio Oriente minuto per minuto con la massima apprensione. Il presidente americano Joe Biden, rientrato d'urgenza a Washington dal Delaware, incontrerà in serata i vertici politico-militari del Paese nella Situation Room della Casa Bianca: saranno presenti anche il segretario di Stato Antony Blinken, il segretario alla Difesa Lloyd Austin e il capo di Stato maggiore generale Charles Q. Brown. La Casa Bianca ha ribadito che il sostegno alla sicurezza di Israele, come detto nei giorni scorsi da Biden, è incrollabile, e che gli Usa:

> "sono al fianco del popolo di Israele e sostengo la sua difesa contro queste minacce dall'Iran"

In risposta all'attacco, la presidente del Consiglio Giorgia Meloni ha convocato i leader del G7 in videoconferenza nel primo pomeriggio di domenica 14 aprile per affrontare le conseguenze dell'attacco dell'Iran a Israele avvenuto la scorsa notte. L'Italia ha la presidenza di turno del Gruppo dei sette, e ha risposto alla richiesta del presidente degli Stati Uniti Joe Biden, che nel comunicato diffuso dopo il lancio di missili e droni da parte di Teheran aveva annunciato la necessità di una riunione straordinaria con gli altri leader per coordinare una risposta diplomatica unitaria. «Con le sue azioni, l'Iran ha compiuto ulteriori passi verso la destabilizzazione della regione e rischia di provocare un'escalation regionale incontrollabile. Questo deve essere evitato», affermano i leader del G7 nella nota congiunta.

DICHIARAZIONE DEI LEADER DEL G7 SULL'ATTACCO DELL'IRAN CONTRO ISRAELE

Noi, i Leader del G7, condanniamo inequivocabilmente e nei termini più forti l'attacco diretto e senza precedenti dell'Iran contro Israele. L'Iran ha lanciato centinaia di droni e missili verso Israele che, con l'aiuto dei suoi partner, ha sconfitto l'attacco.

Esprimiamo la nostra piena solidarietà e sostegno a Israele e al suo popolo e riaffermiamo il nostro impegno per la sua sicurezza.

Con le sue azioni, l'Iran ha compiuto ulteriori passi verso la destabilizzazione della regione e rischia di provocare un'escalation regionale incontrollabile. Questo deve essere evitato. Continueremo a lavorare per stabilizzare la situazione ed evitare un'ulteriore escalation. In questo spirito, chiediamo che l'Iran e i suoi proxies cessino i loro attacchi, e siamo pronti ad adottare ulteriori misure ora e in risposta a ulteriori iniziative destabilizzanti.

Rafforzeremo inoltre la nostra cooperazione per porre fine alla crisi a Gaza, anche continuando a lavorare per un cessate il fuoco immediato e sostenibile e per il rilascio degli ostaggi da parte di Hamas, e forniremo maggiore assistenza umanitaria ai palestinesi che ne hanno bisogno.

Figura 3 - Dichiarazione congiunta dei leader del G7

L’Italia nel mirino di Qilin

Il Ransomware Qilin attacca l’italiana Maccarinelli

In data 6 aprile 2024 è stato effettuato un nuovo attacco da parte del gruppo “Qilin” alla società bresciana Maccarinelli Srl, leader nel settore dei veicoli adibiti al servizio di piazza.

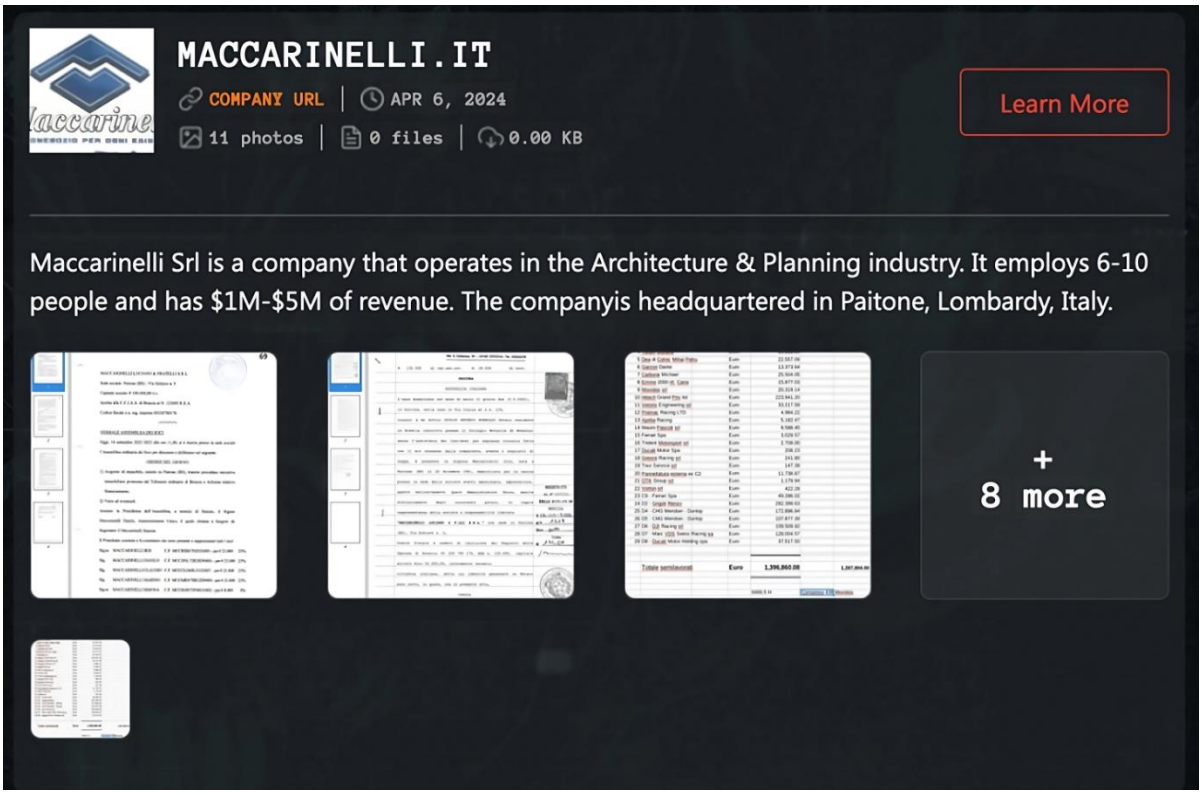


Figura 4 - Dati pubblicati di Maccarinelli sul DLS di Qilin

Agenda, anche noti con il nome di Qilin, è un gruppo ransomware scoperto nel giugno 2022, che, come modus operandi, adotta la tecnica della doppia estorsione. Gli hacker penetrano nelle reti aziendali, scaricano dati confidenziali e crittografano i dispositivi, obbligando la vittima a pagare il riscatto o a vedersi pubblicati tutti i dati sensibili rubati. Il periodo che trascorre dall’infiltrazione all’interno della rete dell'azienda vittima all’esecuzione del ransomware è tipicamente inferiore a due giorni.

In base alle analisi svolte, si ritiene che il gruppo conceda ai suoi affiliati la possibilità di personalizzare il ransomware, includendo l'ID dell'azienda, l'elenco di processi e servizi da interrompere e la chiave necessaria a crittografare i file.

Figura 5 - Paesi coinvolti negli attacchi di Qilin

Basandosi sulle vittime pubblicate sul loro DLS risulta chiaro che il gruppo non si concentra solamente su un determinato settore o Stato, bensì colpisce indistintamente le aziende di tutto il mondo a scopo di lucro. In questi primi mesi del 2024 Qilin aveva già colpito in altre aziende italiane, tra le quali Neafidi Scpa e Loran S.r.l.

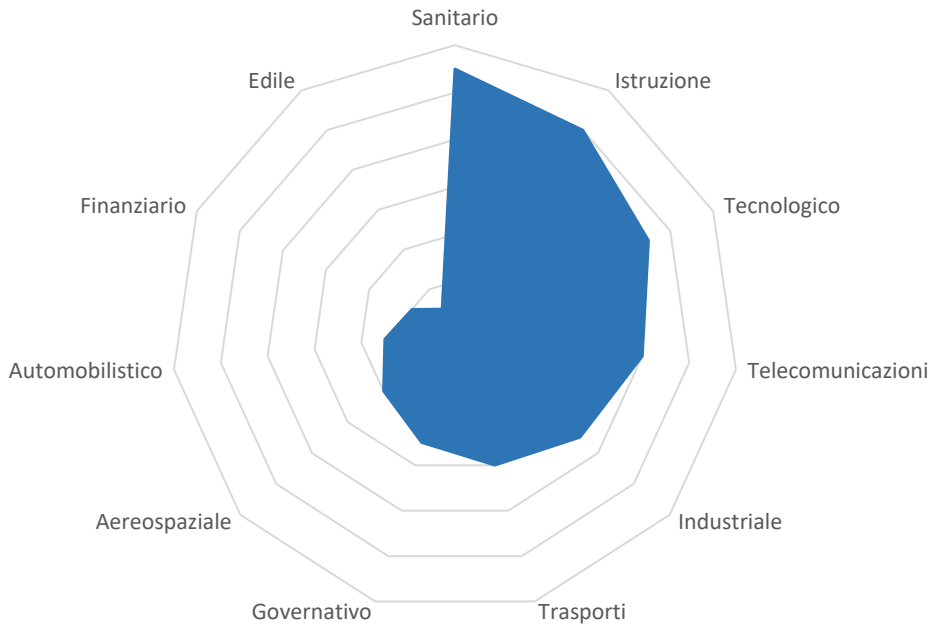


Figura 6 - Settori colpiti da Qilin

Garante privacy: sanzioni a Regione Lazio, LazioCrea e Asl Roma 3

Maxi multe per la gestione dell'attacco ransomware del 2021

L'attacco informatico alla Regione Lazio avvenuto tra il 31 luglio e il 1° agosto 2021 ha avuto ripercussioni importanti per tutti gli assistiti, compromettendo la sicurezza dei loro dati personali e causando un notevole danno di immagine per la Regione Lazio. Questo grave data breach ha avuto inoltre conseguenze devastanti, con blocchi d'accesso a servizi sanitari cruciali, tra cui gestione delle prenotazioni, pagamenti, ritiro dei referti e registrazione delle vaccinazioni nel periodo della pandemia da COVID-19.

GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGIONE
LAZIO

L'attacco è stato perpetrato attraverso l'introduzione di un ransomware tramite un portatile di un dipendente della Regione Lazio. Le indagini condotte dall'autorità Garante della Privacy hanno rivelato una serie di gravi violazioni da parte di LAZIOcrea, la società pubblica responsabile dei sistemi informativi della Regione Lazio stessa.

In particolare:

- LAZIOcrea è stata accusata di non aver agito prontamente per la gestione dell'attacco informatico e le sue conseguenze. La società ha deciso di spegnere tutti i sistemi senza essere in grado di determinare quelli effettivamente compromessi o di prevenire ulteriori propagazioni del malware;
- Regione Lazio è stata giudicata responsabile per non aver mantenuto un adeguato controllo su LAZIOcrea, non garantendo quindi un adeguato livello di sicurezza in proporzione ai rischi e non trattando i dati fin dall'inizio della progettazione dei sistemi informatici, in conformità con le attuali leggi sulla privacy;
- l'ALS Roma 3 è stata ritenuta responsabile di non aver notificato immediatamente il data breach.

Pertanto, per i motivi di cui sopra, il Garante della privacy ha multato LazioCrea, Regione Lazio e l'Asl Roma 3 rispettivamente per 271mila, 120mila e 10mila euro.

Dragonforce attacca in Italia

Colpita l'azienda del settore industriale "New Production Concept" dal gruppo ransomware Dragonforce di possibili origini malesi.

Il 9 aprile 2024 DragonForce ha fatto la sua comparsa in Italia attaccando l'azienda "New Production Concept" che si occupa di servizi relativi a macchinari industriali e hanno pubblicato dopo pochi giorni tutti i dati esfiltrati.

Figura 7 - Dati pubblicati sul DLS di Dragonforce

DragonForce è emerso sulla scena internazionale degli attacchi ransomware a metà dicembre 2023, in particolare il 24 dicembre quando è stata colpita l'azienda americana "Ohio Lottery". In questo attacco, il gruppo ha affermato di essere riuscito ad esfiltrare 600 GB di dati, tra cui tre milioni di record contenenti nomi, indirizzi email, numeri di previdenza sociale e altre informazioni sensibili.

Successivamente sono state colpite Yakult Australia, Coca-Cola a Singapore e per ultimo, nel marzo 2024, il governo di Palau. L'attacco ha fatto sì che fossero bloccati tutti i computer e venissero rilasciate contemporaneamente due note di riscatto: una da LockBit e l'altra da DragonForce. Quest'ultime fornivano istruzioni diverse su come comunicare con gli attaccanti, ma i link Tor forniti non erano raggiungibili. DragonForce ha minacciato, in seguito, di rilasciare informazioni rubate dal governo dell'isola, affermando che le trattative erano fallite.

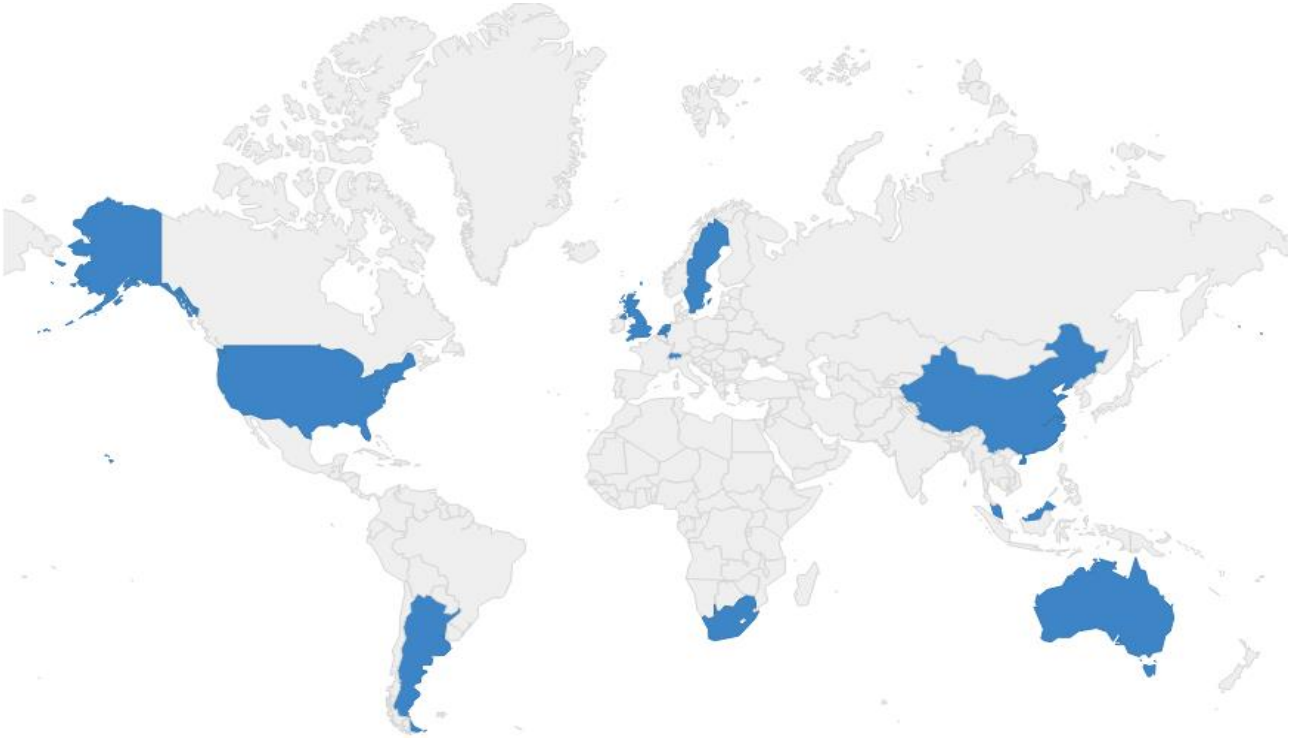


Figura 8 - Paesi coinvolti negli attacchi di DragonForce

Tuttavia, Dragonforce non è noto solo per utilizzare la tecnica della doppia estorsione che prevede la pubblicazione dei dati rubati alla vittima sul Data Leak Site (DLS) sul darkweb qualora decida di non pagare il riscatto richiesto ma anche per aver tentato un'estorsione diretta attraverso una telefonata. In quest'ultimo caso, infatti, gli hacker hanno deciso di telefonare al centralino dell'azienda attaccata per discutere i termini dell'accordo senza però raggiungere il risultato desiderato.

Attacchi di Dragonforce in Europa

Dragonforce allarga la sua sfera d'azione a tutta l'Europa, numerose le aziende colpite

Lo stesso giorno della rivendicazione dell'attacco all'azienda italiana NPC, il gruppo Dragonforce ha rivendicato e successivamente pubblicato i dati delle aziende:

- **Swansea** (Regno Unito): una società di investimenti in diversi settori tra cui alberghiero e immobiliare, con sede a Swansea, nel Galles meridionale.
- **TeamLocum** (Regno Unito): azienda leader per il reclutamento di personale nel settore sanitario.

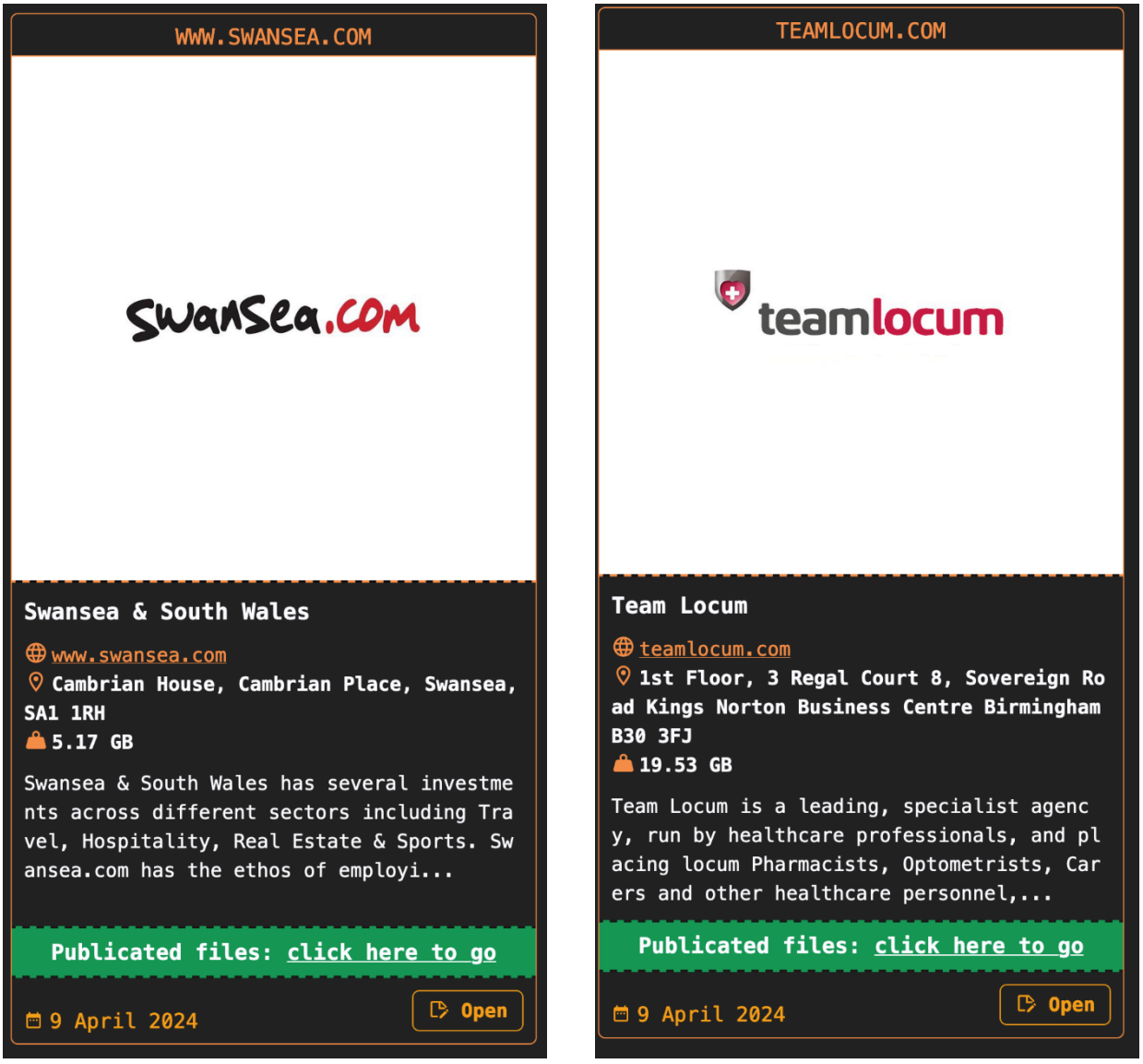


Figura 9 - DLS di Dragonforce

- **Kadushisoft** (Paesi Bassi): un'azienda che si occupa di fornire soluzioni tecnologiche e software per il settore agricolo.
- **Vmab** (Svezia): l'azienda Västblekinge Miljö AB (VMAB) si occupa principalmente di raccolta e riciclaggio dei rifiuti e servizi ambientali.

Cloak colpisce la Germania

Sotto attacco la società di logistica Speditionweise

Il gruppo Cloak, noto per l'acquisto di credenziali compromesse tramite attori malevoli IAB (Initial Access Broker), ha rivendicato ad inizio mese l'attacco all'azienda Speditionweise. La società, con sede a Limbach-Oberfrohna, in Germania, opera come partner logistico internazionale per la Svizzera e altri paesi europei.

I dati sono stati pubblicati l'8 aprile sul DLS del gruppo e contengono informazioni sui clienti, fornitori e altre informazioni sensibili come documenti di identità e documenti sulla situazione finanziaria della società.

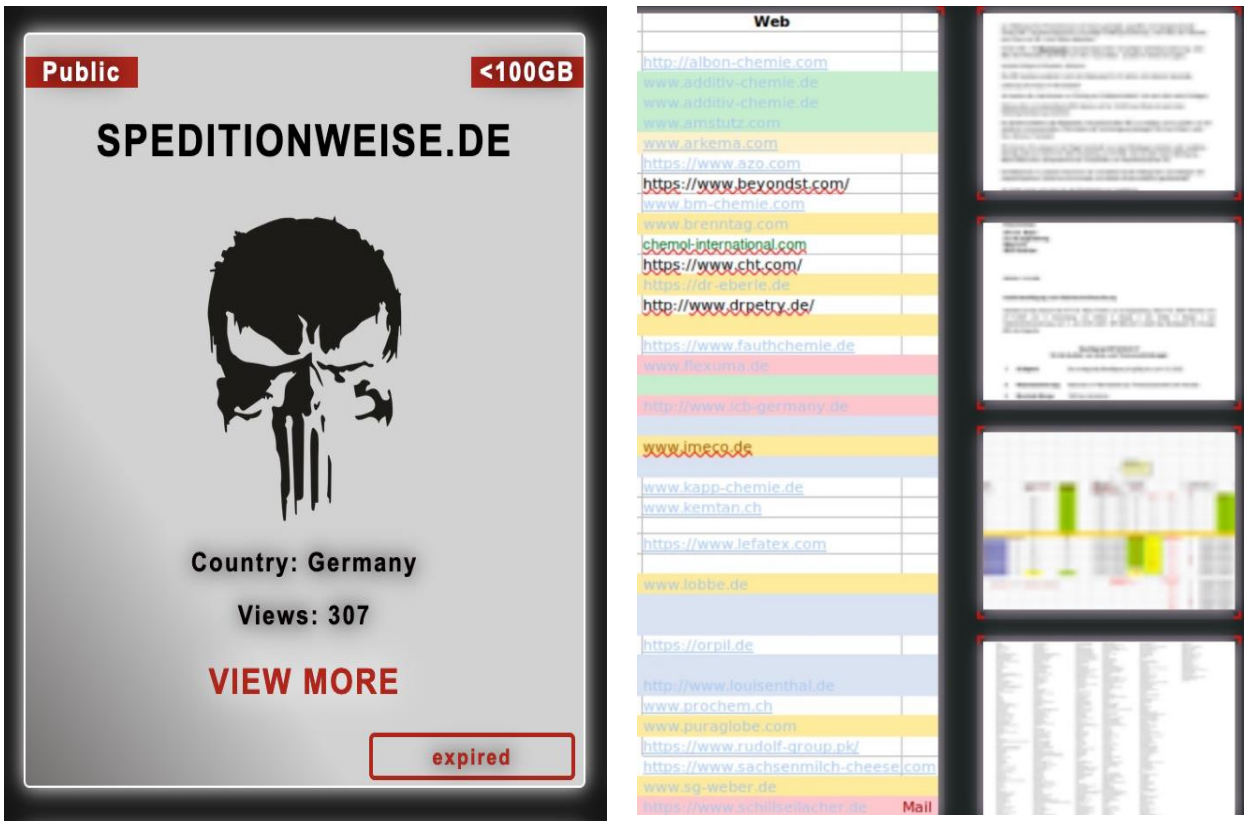


Figura 10 - Dati pubblicati di Speditionweise sul DLS di Cloak

RA World colpisce in Spagna

Gimex hackerata dai cybercriminali di RA World

In data 12 aprile, RA World ha preso di mira Gimex, azienda spagnola che opera nel settore della logistica. I documenti trapelati sono di varia natura: a partire dai contratti dei dipendenti ai documenti contabili, passando per i contratti di assicurazioni.

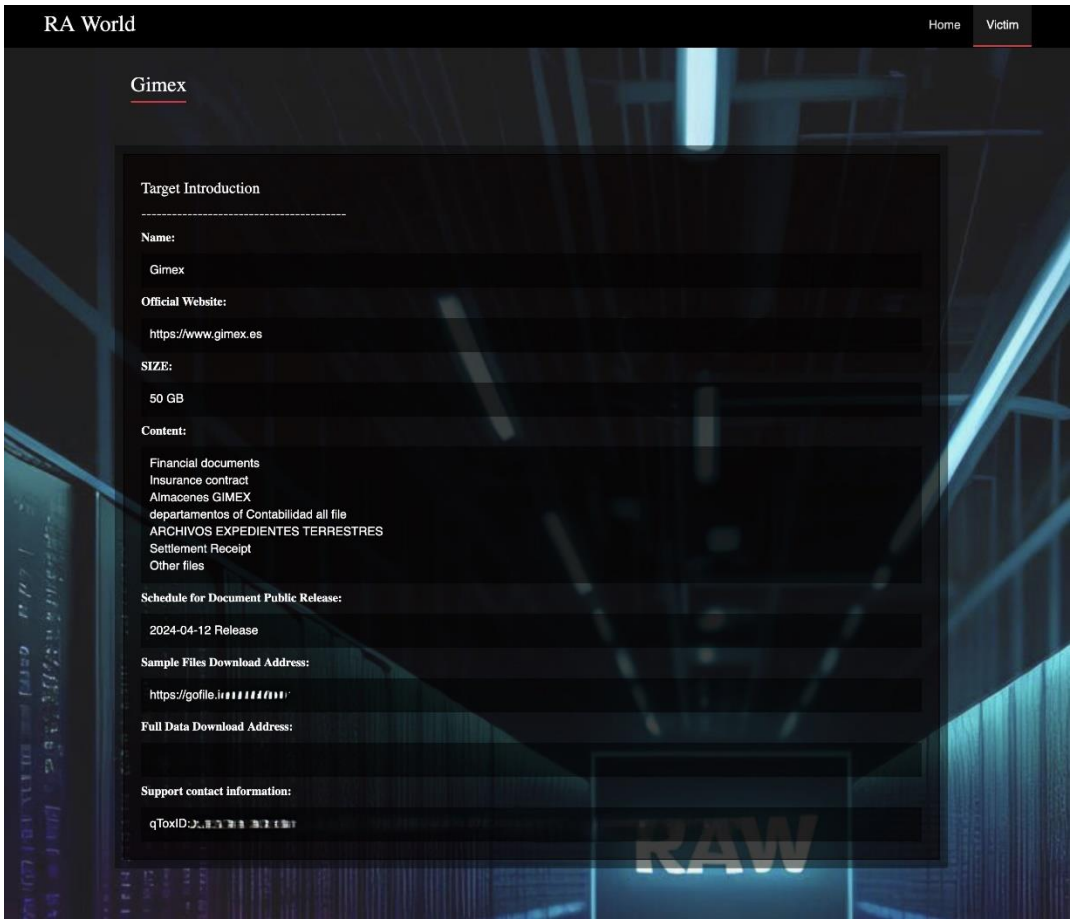


Figura 11 - DLS di RA World

Il gruppo RA World, noto dal dicembre 2023, ha iniziato a farsi spazio nel panorama cybercriminale grazie ad un modus operandi semplice ma efficace. Il gruppo prende possesso dei dati della vittima prima di rilasciare ed eseguire il loro ransomware per avviare la cifratura dei file. Inoltre, il gruppo sfrutta sia siti su rete Tor sia siti presenti sui tradizionali motori di ricerca per diffondere demo dei dati rubati alle vittime.

Dunghill Leak prende di mira Nexperia

Duro colpo per la società leader globale nel mercato e nella produzione dei semiconduttori

Nexperia, società con filiali in Asia, Europa e America, conta fino a 15.000 dipendenti ed è una delle società di punta nel settore produttivo dei semiconduttori. Questa è stata l'ultima vittima di Dunghill Leak che è riuscito a ottenere circa 1000 GB di dati tra cui: dati di controllo qualità, progetti strettamente riservati, dati dei dipendenti e dei ricercatori, dati riguardanti analisi di mercato, analisi interne di ricerca e tanto altro.

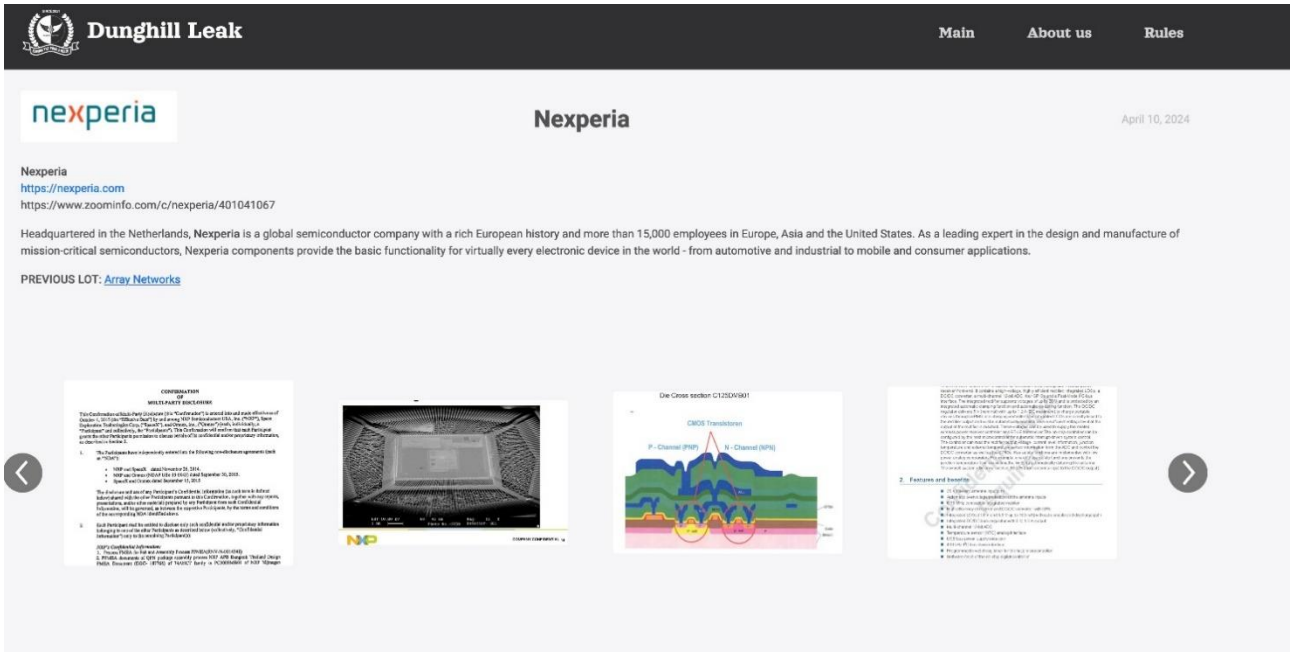


Figura 12 - Pubblicazione dei dati di Nexperia

Il gruppo informatico Dunghill Leak si fa conoscere nel mese di aprile 2023. Iniziano a farsi un nome tramite la loro pagina Telegram e iniziano le prime operazioni nel gennaio dello stesso anno. Tutte le loro opere di doppia estorsione vengono pubblicate prima sul canale Telegram e poi sul loro DLS su dark web. Il gruppo è noto anche con un altro nome: Dark Angels Team.

A partire dal momento in cui il gruppo ha cambiato nome, Dunghill Leak ha preso di mira organizzazioni di grandi dimensioni, non a caso le loro richieste sono per la maggior parte riscatti milionari.

“One Way Attack”: la controffensiva di Kiev alla guerra con i droni russa

Aumentano gli attacchi ucraini sul suolo russo con gli Unmanned combat aerial vehicle occidentali

La guerra tra Ucraina e Russia sta entrando in una fase nuova e tecnologicamente avanzata con l'introduzione di droni dotati di intelligenza artificiale (IA). L'Ucraina ha avviato un programma di sviluppo di droni guidati dall'IA, con un finanziamento di oltre 200 milioni di sterline, principalmente provenienti dal Regno Unito, al fine di lanciare la controffensiva. Dopo aver respinto l'invasione dell'esercito russo per mesi, le truppe ucraine hanno cambiato strategia, iniziando ad attaccare obiettivi al di là dei propri confini attraverso un massiccio uso di droni contro obiettivi strategici.

Strutture militari, industrie e raffinerie sono, infatti, gli obiettivi del programma One Way Attack, ovvero una costante “pioggia” di droni con cui Kiev mira ad indebolire ancora di più l’economia russa, militare e non. Finora, gli attacchi con i droni si sono dimostrati efficaci soprattutto contro industrie e raffinerie, meno protette, mentre hanno incontrato maggiore resistenza contro obiettivi più difesi come gli aeroporti.

Strutture militari, industrie e raffinerie sono, infatti, gli obiettivi del programma One Way Attack, ovvero una costante “pioggia” di droni con cui Kiev mira ad azzoppare ancora di più l’economia russa, militare e non.

Figura 13 - Droni Predator utilizzati dalle forze armate ucraine

Finora, gli attacchi con i droni si sono dimostrati efficaci soprattutto contro industrie e raffinerie, meno protette, mentre hanno incontrato maggiore resistenza contro obiettivi più difesi come gli aeroporti.

Tuttavia, questa strategia pone all'Ucraina diverse sfide, principalmente legate al sostegno internazionale. I Paesi della NATO sono preoccupati per un'escalation che potrebbe scaturire da un attacco ucraino sul suolo russo. Secondo il Pentagono, un tale attacco potrebbe essere interpretato come un'azione diretta dell'Alleanza, legittimando il Cremlino a rispondere colpendo l'Occidente. Per questo motivo, Washington ha finora esitato nel fornire a Zelensky missili a lunga gittata.

In risposta al programma One Way Attack Ucraino le forze russe hanno lanciato un massiccio attacco aereo, con 17 droni Shahed kamikaze, di cui 16 sono stati abbattuti dalla contraerea, in tutta l'Ucraina nella notte tra mercoledì 10 aprile e giovedì 11 aprile, prendendo di mira le infrastrutture energetiche di Odessa, Mykolayiv, Kherson e Dnipropetrovsk, causando morti e feriti e lasciando 200mila famiglie senza elettricità.

Figura 14 - Droni Shahed russi

Aziende tedesche prese di mira dall'infostealer Rhadamanthys

Il gruppo informatico TA547 sfrutta anche i modelli linguistici per le proprie campagne di phishing

Il gruppo di criminali informatici noto come TA547, in attività dal mese di novembre 2017, ha preso di mira dozzine di aziende tedesche, sfruttando l'infostealer di Rhadamanthys. Il loro marchio di fabbrica è l'utilizzo di campagne di phishing contenenti numerosi malware per android e windows come ZLoader, Gootkit, DanaBot, Ursnif e Adhubllka.

Negli anni più recenti, il gruppo si è evoluto diventando un Initial Access Broker (IAB) per gli attacchi ransomware di altri gruppi. I messaggi di mail di quest'ultima campagna vedono TA547 prendere le veci dell'azienda tedesca Metro AG e contengono una cartella compressa protetta da password la quale, una volta estratto il contenuto, inizializza l'esecuzione di uno script PowerShell remoto il quale avvia l'infostealer di Rhadamanthys.

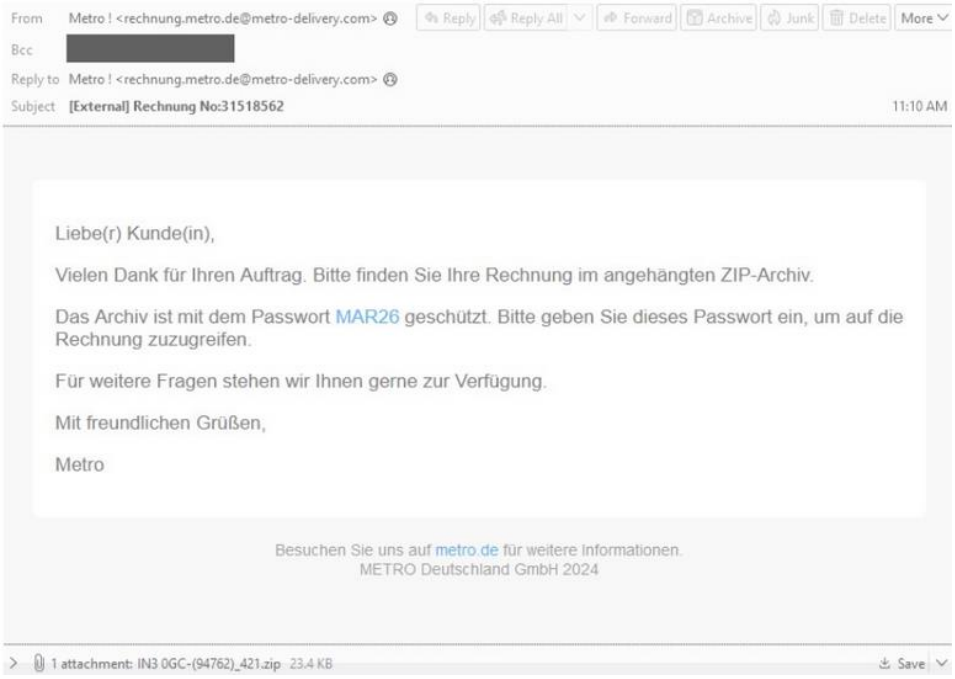


Figura 15 – Messaggio della campagna Phishing di TA547

Lo script PowerShell usato per caricare Rhadamanthys include messaggi e commenti fin troppo specifici e grammaticalmente corretti per ogni istruzione all'interno del programma, suggerendo l'utilizzo da parte del gruppo di modelli linguistici di grandi dimensioni (meglio noti come LLM) per la loro generazione.

Questa campagna fornisce un grande esempio di come TA547 abbia adottato tecniche diverse rispetto agli attacchi passati. Infine, il loro attacco fornisce informazioni e insights interessanti per quanto riguarda il sempre più crescente utilizzo di strumenti e contenuti generati con i modelli linguistici nelle campagne malware dei gruppi cybercriminali.

MERIDIAN GROUP

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

p.Iva: 13693001003

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