2 novembre 2023 | Centro nazionale per la cibersicurezza (NCSC)

Rapporto semestrale 2023/I (gennaio – giugno)

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

1 Panoramica / Contenuto

Management Summary

Tema principale: hacktivismo

Eventi politicamente rilevanti possono portare ad attività illegali nel ciberspazio, vale a dire al cosiddetto hacktivismo. In questo modo gli hacktivisti mirano a ottenere l'attenzione dei media e quindi dell'opinione pubblica. A giugno 2023 l'Amministrazione federale è stata per due volte vittima dell'hacktivismo. Prima si è verificato un attacco DDoS in seguito a una decisione del Consiglio degli Stati nell'ambito della legge federale sul materiale bellico. L'obiettivo era sovraccaricare il sito Internet dei Servizi del Parlamento e renderlo così inaccessibile agli utenti. Nel secondo attacco, il fattore scatenante è stato l'annuncio di un discorso online del presidente ucraino Wolodymyr Selenskyj all'Assemblea federale. Oltre a diverse pagine web di Uffici federali e del Parlamento sono stati colpiti da questo attacco DDoS anche i siti di grandi aziende svizzere, di diversi aeroporti, di numerose città e Cantoni e dell'Associazione svizzera dei banchieri. Il tema centrale del rapporto semestrale è quindi dedicato alle procedure e alle motivazioni degli hacktivisti. Due contributi ospite mostrano inoltre come le grandi aziende colpite hanno reagito all'attacco DDoS. Contemporaneamente a questo rapporto semestrale, l'NCSC pubblica un rapporto di analisi dettagliata su questi attacchi DDoS.

Aumento delle segnalazioni nel primo semestre del 2023

Nel primo semestre del 2023 l'NCSC ha ricevuto 19 048 segnalazioni di ciberincidenti. Ciò corrisponde a un aumento di circa 2000 segnalazioni rispetto al primo semestre del 2022 (16 951 segnalazioni). Nel primo semestre del 2023 le segnalazioni più frequenti all'NCSC hanno riguardato ancora una volta vari tipi di truffa. La maggior parte, circa il 30 per cento, sono e-mail minatorie, cosiddette «fake extortions». Nella maggior parte dei casi la vittima di tali e-mail è accusata di aver commesso un presunto reato. Queste minacce vengono apparentemente inviate a nome di autorità nazionali ed estere; nell'ultimo semestre è stato utilizzato sempre più frequentemente anche il nome dell'NCSC svizzero.

Aumento consistente delle segnalazioni di phishing

Il secondo incidente più segnalato è il phishing, il cui numero di segnalazioni è aumentato di oltre il 40 per cento e ha rappresentato un quinto delle segnalazioni ricevute lo scorso semestre. Il motivo principale di questo aumento è una vasta campagna di phishing contro i clienti SwissPass nel corso di quasi tutto il primo semestre del 2023. In generale, i tentativi fraudolenti stanno diventando più elaborati e gli aggressori stanno sperimentando nuovi metodi per camuffare il link di phishing.

Incidenti di ransomware: sviluppi differenti per aziende e privati

Nel primo semestre del 2023 sono stati segnalati 64 casi di ransomware, un numero pressoché invariato rispetto al semestre precedente (76 segnalazioni). Mentre le segnalazioni provenienti da privati sono diminuite drasticamente (da 27 a 8 casi), il numero di incidenti ransomware segnalati da aziende è aumentato (da 49 a 56 casi). Oltre alle restrizioni operative a breve termine dovute alla crittografia dei dati, la pubblicazione di dati aziendali trafugati provoca danni difficilmente calcolabili.

Editoriale

Lo scorso giugno i diversi attacchi volti a sovraccaricare siti web svizzeri («distributed denial of service», in breve DDoS), come quelli sferrati contro i Servizi del Parlamento e vari Uffici federali e organizzazioni, hanno conquistato i titoli di cronaca. In generale gli attacchi DDoS non sono nulla di straordinario, in quanto si verificano quotidianamente. Come mai, quindi, questi attacchi hanno suscitato tanto clamore?

A essere determinante è stato il contesto politico. Gli aggressori erano hacktivisti filorussi che, con le loro azioni, intendono esprimere le proprie opinioni politiche e dare l'impressione che nel ciberspazio potrebbe verificarsi in qualsiasi momento un attacco russo su ampia scala. Quando i media e i ciberesperti riportano questa narrazione contribuiscono a far sì che gli hacktivisti – i quali, in base alle conoscenze attuali, agiscono di propria iniziativa – raggiungano i loro obiettivi.

Anche in Svizzera gli hacktivisti sono riusciti a diffondere incertezza, perlomeno a breve termine, soprattutto tra organizzazioni, politici e cittadini non specializzati in questo campo. Risulta quindi essenziale analizzare gli attacchi in maniera oggettiva. Si pongono le seguenti domande: quanto ingenti sono stati effettivamente i danni? Una maggiore protezione da attacchi DDoS risulta economicamente sostenibile? Com'è possibile riferire sugli attacchi senza tuttavia offrire agli aggressori una piattaforma di propaganda? E come possiamo contestualizzare meglio simili attacchi nei confronti di persone non esperte?

L'NCSC ha elaborato un rapporto di analisi dettagliato sugli attacchi DDoS, che sarà disponibile per le persone interessate come supplemento al presente rapporto semestrale.

Le ripercussioni degli attacchi ransomware contro aziende e autorità rimangono in ogni caso nettamente più gravi rispetto agli attacchi DDoS. L'attacco più noto è probabilmente quello sferrato alla ditta Xplain, che fornisce prestazioni non solo ad aziende private ma anche a Confederazione e Cantoni. Poiché, tuttavia, è attualmente in corso un'inchiesta amministrativa, nel presente rapporto non entreremo nei dettagli dell'incidente. Il caso verrà trattato in un futuro rapporto, non appena saranno concluse tutte le inchieste. Tengo comunque a sottolineare già ora il seguente aspetto: fin dall'inizio abbiamo deciso di comunicare nel modo più trasparente possibile, senza pregiudicare le organizzazioni o le persone che hanno perso i propri dati. E chi comunica in maniera trasparente si espone automaticamente alle critiche. Vengono anche poste domande legittime cui intendiamo rispondere una volta concluse tutte le inchieste. Questo genere di analisi richiede tempo, e non sarebbe opportuno trarre conclusioni affrettate.

Il presente rapporto comprende anche un'analisi della situazione di minaccia nonché una panoramica dei ciberincidenti. Ancora una volta i casi più segnalati all'NCSC sono stati varie forme di truffa. Si riconferma quindi importante prestare grande cautela, in particolare quando vengono richieste informazioni personali come i dati delle carte di credito o dei login. Il rapporto fornisce infine un aggiornamento sulle ciberminacce in relazione alla guerra in Ucraina.

Cogliete l'occasione per darci il vostro feedback sul presente rapporto.

Vi auguriamo una piacevole lettura.

Florian Schütz, delegato federale alla cibersicurezza

2 Tema principale: hacktivismo

Sono numerosi gli attori che tentano di attaccare vari sistemi, adottando metodi diversificati. Il panorama degli artefici di tali minacce è molto vario per capacità (ossia complessità del procedimento) e per motivazioni. Dallo scoppio della guerra in Ucraina, si osserva un numero crescente di attacchi da parte di gruppi di cosiddetti hacktivisti, caratterizzati da due aspetti fondamentali: da un lato, non sono professionisti, dall'altro, sono spinti ad agire da motivazioni ideologiche (ad es. sociali, politiche o religiose), al contrario dei comuni criminali, i quali operano essenzialmente per interessi finanziari. Di conseguenza, gli hacktivisti possono accontentarsi anche di attacchi superficiali (p. es. il blocco temporaneo di un sito web) se sono sufficienti a farne parlare i media e attirare così l'attenzione della collettività sulle loro istanze. Il più famoso gruppo di hacktivisti è probabilmente Anonymous. Da oltre quindici anni, hacker di tutto il mondo operano sotto questo nome in difesa di tematiche come la libertà di espressione e l'indipendenza del web nonché contro autorità e multinazionali.

Da febbraio 2022, nel contesto del conflitto in Ucraina, si sono formati oppure evoluti numerosi gruppi di hacktivisti schierati dall'una o dall'altra parte, che muovono attacchi sistematici a istituzioni ritenute dannose per i loro interessi. I gruppi di hacktivisti filorussi, per esempio, colpiscono soprattutto enti di Stati che forniscono sostegno all'Ucraina o impongono sanzioni alla Russia.[1] Per contro, i gruppi di hacktivisti filoucraini mettono in atto meno iniziative e azioni di rappresaglia, anche perché sono meno numerosi rispetto a quelli filorussi.[2] Sebbene nella maggior parte dei casi non vi siano legami formali tra gli hacktivisti e gli organi di governo, essi possono operare come sostituti dello Stato nelle azioni pubblicamente deplorevoli, soprattutto favorendo la diffusione di messaggi propagandistici. Numerosi rapporti redatti da società di sicurezza informatica occidentali hanno messo in luce relazioni di questo genere.[3] Un caso particolare è invece quello dell'IT Army of Ukraine, che al contrario dei gruppi di hacktivisti filorussi è stato apertamente costituito su iniziativa del governo ucraino, il quale sta lavorando a una legge per legittimare lo status dell'IT Army of Ukraine e farla confluire ufficialmente nelle forze armate, quale unità di riservisti.[4]

2.1 DDoS: attacchi alla disponibilità di siti e servizi web

Gli attacchi alla disponibilità di un servizio online («distributed denial of service», in breve DDoS) sono tentativi, operati da un gran numero di computer e da molti punti di partenza diversi, di sovraccaricare un servizio con una quantità talmente elevata di richieste da renderlo indisponibile per gli utenti regolari. Tali attacchi non comportano tuttavia alcuna appropriazione indebita di dati né la distruzione di dati o sistemi. Nel mondo analogico, un attacco DDoS potrebbe essere paragonato a una folla di persone che partecipa, per esempio, a una conferenza stampa pubblica, e lì si mette a urlare sguaiatamente rendendo impossibile udire le domande legittime dei giornalisti, e impedendo di conseguenza ogni risposta.

---

1 Si veda il n. 2.1 e il n. 4.7.

2 Russia-Ukraine War - Cybertracker May 03 (cyberknow.medium.com)

3 A year of Russian hybrid warfare in Ukraine (microsoft.com);
GRU: Rise of the (Telegram) MinIOns (mandiant.com)

4 Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army (newsweek.com)

In genere, dunque, il risultato di un attacco DDoS è semplicemente quello di rendere temporaneamente inaccessibile un sito web, che costituisce in un certo senso lo sportello informativo dell'organizzazione in questione. Se però il sito web serve a eseguire fasi cruciali dell'attività commerciale, come nel caso dei negozi online, anche una breve interruzione del funzionamento può provocare ingenti danni economici. Allo stesso modo, quando vi è una particolare urgenza di far circolare comunicazioni o informazioni, i rispettivi processi possono subire interruzioni.

Lo scopo degli hacktivisti è quello di attirare l'attenzione e a volte anche di trasmettere incertezza, o più precisamente minare la fiducia nei confronti delle organizzazioni che gestiscono il sito. Le organizzazioni sono per lo più preparate ad affrontare attacchi DDoS e sono dunque in grado di ripristinare in brevissimo tempo la disponibilità delle loro risorse online. Nondimeno, l'attuazione di misure difensive come filtrare il traffico di attacco o incrementare le capacità richiede un certo tempo e comporta dei costi. Gli hacker sfruttano questo tempo per dimostrare che un sito web non era disponibile. Creano istantanee che diffondono sui social media dove, anche in caso di interruzioni di durata molto breve, vogliono far credere di essere riusciti ad hackerare un'azienda, disattivarne il sito web o addirittura cancellare la sua presenza online.

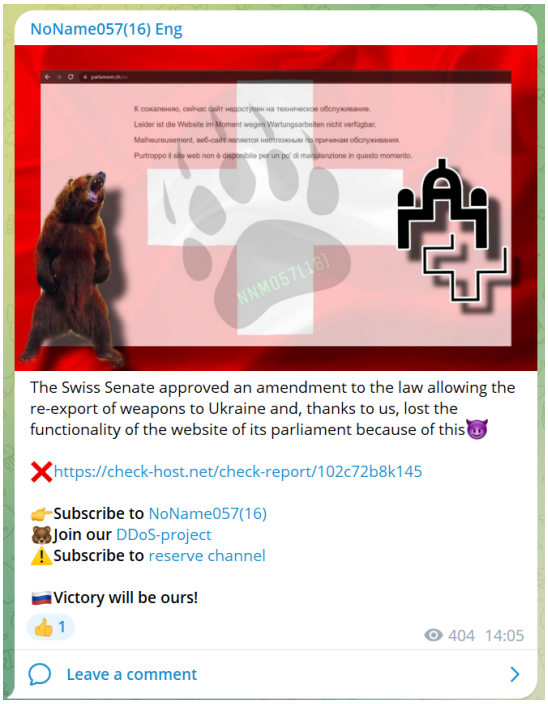


Fig. 1: Messaggio di rivendicazione di hacktivisti

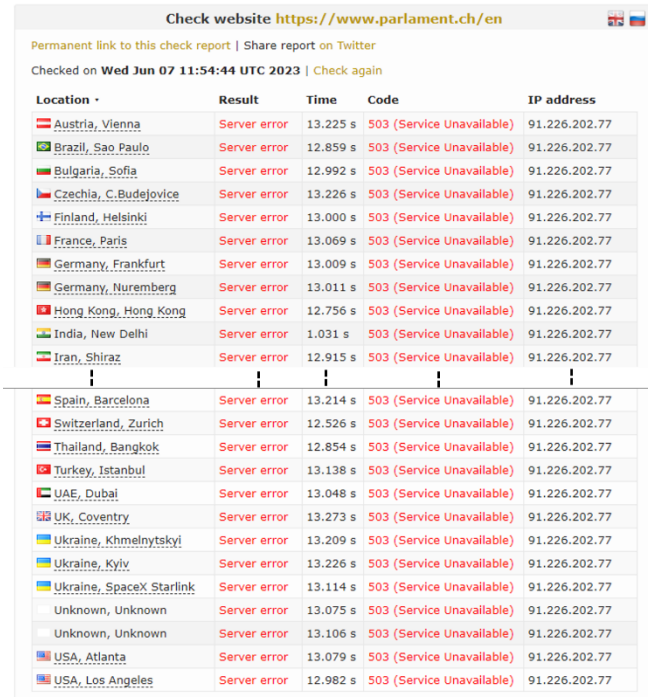


Fig. 2: Screenshot delle verifiche di accessibilità

Il 7 giugno 2023 il gruppo filorusso NoName057(16) ha messo in atto un attacco DDoS di questo tipo sul sito web del Parlamento svizzero. Nel messaggio di rivendicazione divulgato attraverso il servizio di messaggistica istantanea Telegram, gli hacker hanno indicato come motivazione la decisione (intermedia) del Consiglio degli Stati circa la revisione della legge federale sul materiale bellico (LMB). Immediatamente dopo l'avvio dell'attacco, prima che venissero adottate contromisure, il sito web si è trovato effettivamente in una situazione di sovraccarico causata da un numero eccezionale di richieste, risultando perciò inaccessibile o estremamente lento per gli utenti regolari. Nel momento stesso, gli hacker hanno fatto allestire un rapporto da un servizio che verifica la disponibilità globale dei siti web per sfruttarlo come dimostrazione del successo del loro attacco. Si tratta però di una semplice istantanea che non asserisce nulla sulla durata dell'interruzione. Nonostante l'attacco si sia protratto a lungo, le contromisure

adottate hanno permesso di rendere il sito web di nuovo fruibile entro breve tempo. Per riprendere la metafora citata in precedenza: è come se fosse stato girato un breve video della conferenza stampa, in cui si vedono gli ospiti indesiderati urlare tra loro ma che termina prima che la folla di disturbatori sia portata fuori dalla sala dalle forze di sicurezza e impossibilitata a rientrare.

Nel mirino del gruppo filorusso, oltre al Parlamento svizzero, nella settimana successiva sono finiti anche aeroporti, le Ferrovie Federali Svizzere (FFS) e La Posta Svizzera SA, l'Associazione svizzera dei banchieri (ASB), varie Città e Cantoni, nonché diversi siti web di uffici federali (si vedano a tal proposito anche i contributi ospite riportati di seguito).[5] Anche l'intervento del presidente ucraino davanti all'Assemblea federale ha contribuito a rendere la Svizzera un bersaglio degli hacktivisti. La trasmissione del video ha però funzionato senza interferenze. Come accaduto anche ad altri Paesi finiti nel mirino di NoName057(16), dopo una settimana gli attacchi si sono interrotti e gli hacker si sono dedicati ad altri obiettivi.[6] L'NCSC ha elaborato un rapporto di analisi dettagliato sugli attacchi DDoS.

Nel periodo in esame, oltre a NoName057(16), anche altri gruppi di hacktivisti filorussi, come KillNet[7] e il collettivo apparentemente associato ad esso Anonymous Sudan[8], sono saliti alla ribalta della cronaca per attacchi DDoS contro obiettivi soprattutto europei e nordamericani.[9] Si sono verificati inoltre attacchi DDoS di matrice religiosa con cui gli hacker volevano manifestare la loro indignazione nei confronti di attività a loro parere blasfeme, colpendo siti web di Paesi o organizzazioni ritenuti nemici della loro religione.[10]

Già nel dicembre del 2010 la Svizzera aveva subito un attacco DDoS di matrice politica, quando per ore presunti sostenitori di Wikileaks avevano pregiudicato il funzionamento del sito web di PostFinance.[11]

Raccomandazioni

Sul sito Internet dell'NCSC sono elencate diverse misure da attuare per prevenire e difendersi dagli attacchi DDoS: Attacchi alla disponibilità (DDoS) (ncsc.admin.ch)

Per i sistemi critici, è consigliabile sottoscrivere un abbonamento a un servizio di protezione contro gli attacchi DDoS («DDoS mitigation service» o «DDoS protection service»). Molti fornitori di servizi Internet offrono questo tipo di servizi.

---

5 Das Gespenst DDoS-Attacke geht um (inside-it.ch)

6 Following NoName057(16) DDoSia Project's Targets (sekoia.io);
DDoSia Project: How NoName057(16) is trying to improve the efficiency of DDoS attacks (avast.io)

7 KillNet Showcases New Capabilities While Repeating Older Tactics (mandiant.com)

8 Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks (microsoft.com)

9 Sulla piattaforma del CyberPeace Institute è disponibile un elenco completo dei ciberattacchi messi in atto nell'ambito del conflitto in Ucraina. I ciberattacchi possono essere filtrati in base a vari criteri (ad es. per «Event Type», «DDoS»): Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

10 Hacktivists Target Denmark in Ddos Attacks (truesec.com);
Radware Report Ranks Top 15 Most Active Political and Religious Hacktivists (radware.com);
Notable DDoS Attack Tools and Services Supporting Hacktivist Operations in 2023 (cyble.com)

11 Si veda il rapporto semestrale 2010/2 (ncsc.admin.ch), n. 3.2.

2.1.1 DDoS può essere sventato (Swisscom)

Contributo di Stefan Kuch, Product Owner CSIRT, Swisscom

Il 7 giugno 2023 il Parlamento svizzero ha subito un attacco DDoS. Il Cyber Defense Team di Swisscom ha avviato immediatamente una stretta collaborazione sia con i team operativi di rete addetti alla protezione contro gli attacchi DDoS, che con l'NCSC. Nell'immediato, sono stati attuati provvedimenti preventivi di protezione.

La settimana successiva sono seguiti ulteriori attacchi, mossi dal gruppo di hacktivisti filorusso NoName057(16) nei confronti di diversi obiettivi svizzeri. Tra questi, il 15 giugno sono finiti nel mirino anche clienti di Swisscom e l'azienda stessa. Nel presente rapporto, a titolo di esempio, entriamo nel merito di un attacco rivolto a uno dei nostri clienti. Si è trattato di un attacco DDoS layer 7, per la precisione di un HTTPS flood. Questo tipo di attacco DDoS prevede di bombardare un server web di richieste HTTP GET o HTTP POST apparentemente legittime e sempre diverse, finché le risorse non si esauriscono e il server web non è più in grado di rispondere alle richieste. A quel punto il server nega il servizio («denial of service»), che risulta dunque interrotto. Nel caso di NoName057(16), le richieste provenivano soprattutto da attivisti che hanno messo volontariamente a disposizione la loro infrastruttura per attacchi DDoS. Un attacco DDoS layer 7 di questo tipo è generalmente molto dinamico, per cui è praticamente impossibile prevenirlo del tutto. È però fondamentale disporre di un'infrastruttura tecnica in grado di reagire rapidamente ad attacchi del genere.

Nel caso specifico, l'attacco ha raggiunto un volume fino a 150 000 pacchetti al secondo (pps): una mole davvero eccessiva per il server. In giornate normali, il traffico di dati sul sito web oscilla tra i 400 e 500 pps, con brevi picchi che possono raggiungere i 1200 pps. Vi sono attacchi intensi che colpiscono al tempo stesso anche altri componenti di rete a monte dei server web aggrediti.

Come contromisura, Swisscom ha introdotto un servizio «DDoS mitigation» e, insieme al cliente, ha affinato e poi adeguato costantemente le relative regole:

- blocco del traffico dai Paesi da cui proviene la maggior parte delle richieste DDoS. Si tratta della misura immediata più semplice per proteggere un sito web la cui gran parte degli accessi proviene di norma dalla Svizzera;
- il sito web viene in seguito progressivamente riaperto e adeguato. Se il cliente desidera concedere l'accesso da determinati Paesi o da determinati intervalli di indirizzi IP, è possibile riattivarli;
- implementazione di una limitazione delle richieste («rate limiting») sul servizio di bilanciamento del carico («load balancer») a monte per le connessioni al dominio oggetto dell'attacco. In questo modo è possibile equilibrare il carico di lavoro del server web in modo duraturo;
- blocco permanente di determinate richieste layer 7 sul reverse proxy a monte, misura attuata grazie a una blocklist creata dall'NCSC.

Il servizio di «DDoS mitigation» ha permesso di riportare il volume di traffico a circa 500 pps, bloccando le richieste da circa 2000 indirizzi IP. L'indirizzo IP più attivo, da solo, ha inviato, per tutta la durata dell'attacco, circa 50 milioni di pacchetti di dati.

All'attacco sopracitato del 15 giugno ne è seguito un altro, nella notte del 19 giugno, con un volume tuttavia notevolmente inferiore, pari a 60 000 pps. Ma dato che il servizio di «DDoS

mitigation» era stato preventivamente attivato per una durata di cinque giorni, questo secondo attacco non ha avuto alcun impatto negativo.

Chi però, dopo un giugno così intenso sotto il profilo degli attacchi DDoS, continua a gestire il proprio servizio web senza adottare misure di protezione DDoS efficaci nella speranza di non cadere nel mirino degli hacker, farebbe meglio a rivedere la propria posizione. Adottare misure preventive professionali è infatti senza dubbio utile per evitare o quanto meno ridurre al minimo eventuali danni in caso di attacco. La maggior parte dei fornitori di servizi Internet offre soluzioni di protezione contro gli attacchi DDoS ed è in grado di aiutare i clienti sia a prepararsi a un attacco, che a difendersi nella fase acuta di una ciberaggressione.

L'ottima collaborazione tra i vari settori operativi di Swisscom, come quello addetto alla rete e quello responsabile del «major incident management», nonché l'assistenza professionale e le informazioni fornite dall'NCSC hanno permesso di reagire rapidamente agli attacchi e di proteggere così i servizi dei nostri clienti.

2.1.2 L'importanza di prepararsi ed esercitarsi (La Posta Svizzera)

Contributo del Swiss Post Computer Emergency Response Team (CERT-Post)

Nella gestione di crisi della tecnologia dell'informazione della Posta, affrontare attacchi DDoS rientra già da molti anni tra gli scenari predefiniti. A fronte di attacchi DDoS tendenzialmente sempre più intensi, anche noi miglioriamo la nostra capacità di difesa, ciò avviene grazie alla gestione degli attacchi stessi e all'esecuzione di controlli regolari delle funzioni. Oltre a verificare la capacità tecnica e la configurazione, ci esercitiamo soprattutto per ottimizzare la cooperazione tra i team coinvolti.

Risultati ottenuti in occasione dell'attacco di NoName057(16)

Dopo che, nella settimana precedente, si erano verificati i primi attacchi al sito web del Parlamento svizzero, il 12 giugno 2023 è seguito un attacco DDoS rivolto ad altre organizzazioni e aziende svizzere, tra cui anche due applicazioni web della Posta (portale e Login clienti).

La soluzione «Always-on DDoS Protection» acquistata dal nostro fornitore di servizi Internet ha inizialmente filtrato poco l'attacco, ma si è dimostrato affidabile, inviando un allarme alle ore 08.09, ancor prima che i clienti iniziassero a notificare cali di performance.

Le conseguenze dell'attacco erano misurabili, perciò alle ore 08.11 il Security Operations Center (SOC) de La Posta ha attivato i primi filtri geografici per le suddette applicazioni web, dato che era evidente che gli aggressori stessero usando una botnet distribuita a livello internazionale. La nostra priorità era innanzitutto quella di garantire il più possibile gli accessi dei clienti dalla Svizzera. Per le sue caratteristiche (HTTPS flood con larghezza di banda e flusso di pacchetti relativamente modesti), l'attacco non ha avuto ulteriori ricadute sulla connessione di rete e altri servizi de La Posta Svizzera.

Alle ore 08.15, il Computer Emergency Response Team della Posta (CERT-Post) ha assunto il coordinamento del caso, in accordo con il SOC e il nucleo di crisi IT. Nelle ore e nei giorni successivi il team ha inviato diversi bollettini per aggiornare tutte le parti interessate sugli sviluppi più recenti. Alle 08.31, il SOC ha attivato un livello di difesa per poter filtrare più efficacemente il traffico dell'attacco nel «mitigation center» DDoS appositamente previsto. In seguito il team, insieme ai suoi partner interni ed esterni, ha svolto anche valutazioni dei log e analisi di «threat intelligence» per scoprire il più possibile sulle capacità degli hacker e gli strumenti da essi utilizzati. Le informazioni emerse sono confluite a loro volta nelle soluzioni di difesa.

Cosa abbiamo imparato dalla prima ondata di attacchi

Nei giorni successivi sono stati sferrati ulteriori attacchi: il 15 giugno è stato colpito il portale di AutoPostale SA, mentre il 17 giugno c'è stata una seconda ondata di attacchi nei confronti del portale de La Posta. In questa fase abbiamo messo a frutto quanto appreso dalla prima ondata di ciberaggressioni nonché dal confronto all'interno delle community CERT svizzere, tanto che non si sono rese necessarie misure di emergenza come all'inizio della prima ondata. Tutte le conoscenze acquisite di volta in volta sono confluite costantemente nelle nostre soluzioni di difesa, permettendoci di contrastare in modo efficace le successive ondate di attacco.

Mentre nella prima fase di aggressione del 12 giugno il tempo di risposta medio del nostro server sotto attacco è aumentato in modo misurabile e notevole, nei giorni successivi non si è più riscontrato lo stesso rallentamento.

Le regolari e sistematiche esercitazioni svolte da anni in preparazione a eventuali attacchi DDoS si sono dimostrate utili, sebbene ogni ondata di attacco insegni qualcosa di nuovo. Nella riunione post-operativa («after action review»), abbiamo messo a fuoco diversi aspetti tecnici e organizzativi da apprendere per ottimizzare la nostra difesa.

2.2 Defacement

Si definisce «defacement» (termine inglese che significa «defacciare», una forma di deturpamento) la modifica di una pagina web attraverso un ciberattacco. L'azione equivale a tracciare, nel mondo reale, scritte o disegni con vernice spray sulla facciata di una casa o su un muro. Il più delle volte viene modificato solo l'aspetto della pagina iniziale con l'obiettivo di diffondere un messaggio politico o ideologico. Può capitare per esempio che un hacker defacci il sito web di un governo o di un determinato movimento perché non ne condivide le attività o gli obiettivi[12], sostituendo il contenuto reale con testo, immagini o un logo. Gli attacchi di defacement compromettono temporaneamente la disponibilità di un sito web e possono ledere la reputazione di chi lo gestisce.

Nel contesto della guerra in Ucraina, invece, alla fine di giugno del 2023, a pochi giorni dall'insurrezione della compagnia militare privata Wagner in Russia, su diversi siti web russi è apparso il logo della Wagner con un messaggio a sostegno del gruppo.[13] Nel ciberspazio, le tensioni politiche ricadono anche sui Paesi che assicurano il loro sostegno all'Ucraina, in particolare sugli Stati membri della NATO. Nel maggio del 2023, per esempio, un collettivo denominato UserSec ha annunciato di volere intraprendere un'ampia offensiva di defacement rivolta ai siti web degli Stati membri della NATO, in collaborazione con altri gruppi di hacktivisti. Alle minacce non sono però seguiti attacchi concreti tali da destare l'attenzione dei media.

---

[12] Nel 2017, per esempio, in Svizzera hanno subito azioni di defacement diversi siti di piccole aziende, dopo la manifestazione svoltasi a Berna contro il governo turco. Alla manifestazione era apparso infatti uno striscione che riportava la scritta «Kill Erdogan with his own weapons!» («Uccidete Erdogan con le sue stesse armi!»), provocando un incidente diplomatico.

[13] Nell'anno precedente, anche il sito web del gruppo Wagner era stato a sua volta oggetto di defacement, quando alcuni hacker filoucraini vi avevano pubblicato foto di vittime di guerra e un messaggio politico a sostegno dell'Ucraina.

Raccomandazioni

Fate in modo che il vostro sito sia monitorato automaticamente, in modo da ricevere un avviso nel caso subisca modifiche. Questo vi consentirà di reagire rapidamente e cancellare eventuali manipolazioni non autorizzate. Rivolgetevi al vostro fornitore di servizi di hosting per conoscere le possibili soluzioni a disposizione.

2.3 Hack and leak

Attraverso le operazioni di «hack and leak» gli hacktivisti penetrano in sistemi IT per acquisire i dati che vi sono archiviati e quindi pubblicarli. Tali soggetti cercano in particolare materiale atto a screditare o a ledere le vittime, per diffonderlo in forma originale o falsificata su piattaforme come Wikileaks o DDoSecrets, su social media o su pagine del dark web e suscitare una reazione nella collettività. A seconda dell'ideologia e dei dati acquisiti, gli hacktivisti possono anche scegliere di fornire le informazioni rubate a giornalisti d'inchiesta perché approfondiscano la questione, anziché pubblicarle in prima persona.

All'inizio del 2023 ha attirato l'attenzione dei media il caso di una hacker svizzera che era riuscita ad appropriarsi di una lista di divieto di volo negli Stati Uniti risalente al 2019, contenente circa 1,5 milioni di voci, accedendo al server di una compagnia aerea non sufficientemente protetto.[14] Un altro caso degno di nota ha visto soggetti associati al collettivo di hacker Anonymous pubblicare dati del fornitore di servizi Internet russo Convex, i quali dimostravano un controllo illegale sui cittadini da parte del governo russo.[15] È invece leggermente diverso il metodo adottato dagli hacktivisti del gruppo di ransomware denominato «MalasLocker». Analogamente ai gruppi di ransomware tradizionali (cfr. n. 4.2), gli hacktivisti si procurano innanzitutto una copia dei dati dai sistemi delle loro vittime, quindi lanciano un ransomware, ossia un software malevolo di crittografia. Invece di chiedere un riscatto, però, pretendono che le vittime facciano una donazione a un'organizzazione benefica, se desiderano ottenere la chiave di crittografia per accedere ai loro dati e scongiurare che questi siano pubblicati.[16]

2.4 Sabotaggio

Tra le varie modalità con cui gli hacktivisti tentano di attirare l'attenzione sulle loro istanze, le più pericolose sono senza dubbio i tentativi di sabotaggio a sistemi produttivi. Anche se nella maggior parte dei casi le ripercussioni effettivamente da attribuirsi alle attività informatiche degli hacktivisti siano minori rispetto a quanto si afferma, si tratta di un genere di minaccia che merita comunque attenzione.[17]

---

14 Cfr. EXCLUSIVE: Leaked TSA No Fly List: File Found on Airline Server (dailydot.com); Schweizer Hackerin stellt USA bloss: Geheime Flugverbots-Liste erbeutet (watson.ch)

15 128GB Of Russian ISP Convex Data Leaked By Anonymous Hacker (informationsecuritybuzz.com)

16 MalasLocker ransomware targets Zimbra servers, demands charity donation (bleepingcomputer.com); Dark Web Profile: MalasLocker Ransomware (socradar.io)

17 We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems (mandiant.com)

Un gruppo degno di nota in questo ambito, emerso dall'ambiente dell'hacktivismo classico che gravita intorno ad Anonymous, si chiama GhostSec.[18] Nel gennaio del 2023 il gruppo ha annunciato di aver sferrato il primo attacco ransomware specifico per sistemi di tecnologia industriale contro sistemi di controllo bielorussi. Il sistema attaccato si basa su un tipo di distribuzione Linux che già in passato era stato compromesso da ransomware. Anche se l'attacco ha avuto conseguenze sul piano operativo, non è comunque riuscito a intervenire direttamente sul processo fisico controllato.[19]

Gli hacktivisti che attuano operazioni di sabotaggio agiscono soprattutto nell'ambito di conflitti geopolitici. Nel quadro della guerra russa di aggressione all'Ucraina, per esempio, è nato il gruppo OneFist[20], che ha rivendicato numerose azioni con conseguenze fisiche, principalmente in territorio russo.[21] Nel contesto dei conflitti in Medio Oriente sono invece attivi già da diverso tempo collettivi come Predatory Sparrow[22], che hanno rivendicato per esempio danni concreti ad acciaierie iraniane.[23]

Per ora, le capacità degli hacktivisti in questo ambito si limitano alla manipolazione di sistemi di controllo non protetti e raggiungibili da Internet o all'impiego di strumenti di attacco pubblicamente accessibili, come moduli Metasploit[24], concepiti per i sistemi industriali.

Nel caso di attacchi più complessi, si sospetta talvolta che dietro ai gruppi di hacktivisti si celi anche un sostegno statale. Ad esempio, sono stati presi in esame possibili legami tra il servizio informativo militare russo e gruppi di hacktivisti filorussi.[25] Si pensa inoltre che dietro le azioni di sabotaggio ai sistemi governativi albanesi ad opera di presunti hacktivisti del gruppo Homeland Justice vi siano forze di sicurezza iraniane.[26] Oppure si pensi al recente attacco mosso a un gestore della rete satellitare russa[27] da parte di presunti hacktivisti appartenenti alla cerchia della Wagner, che stando a quanto documentato da alcuni ricercatori nel campo della cibersicurezza avrebbe coinvolto operazioni ucraine.

Riuscire in un tentativo di sabotaggio consente di richiamare su di sé una forte attenzione mediatica. Ci si deve dunque aspettare che in futuro anche altri collettivi di hacktivisti cerchino di acquisire questo genere di capacità. L'NCSC britannico ha addirittura emanato un'esplicita allerta circa il rischio di attacchi informatici distruttivi a infrastrutture critiche occidentali da parte di hacktivisti filorussi[28], che acquisirebbero le relative competenze grazie al supporto di organizzazioni statali o di unità consolidate di gruppi cibercriminali.

---

18 Ghost Security (wikipedia.org)

19 Hacker group discloses ability to encrypt an RTU device using ransomware, industry reacts (industrialcyber.co)

20 About Us | Cyber Security (onefist.org)

21 Meet the hacker armies on Ukraine's cyber front line (bbc.com)

22 Predatory Sparrow (Threat Actor) (fraunhofer.de)

23 Predatory Sparrow massively disrupts steel factories while keeping workers safe (malwarebytes.com)

24 Metasploit | Penetration Testing Software, Pen Testing Security (metasploit.com) – Metasploit Framework è uno strumento pensato per gli addetti alla sicurezza, in grado di individuare e verificare vulnerabilità nei sistemi informatici. Come ogni strumento, può essere anche sfruttato per finalità malevole.

25 GRU: Rise of the (Telegram) MinIOns (mandiant.com)

26 Microsoft investigates Iranian attacks against the Albanian government (microsoft.com)

27 Hackers claim to take down Russian satellite communications provider (therecord.media)

28 NCSC warns of emerging threat to critical national infrastructure (ncsc.gov.uk)

Conclusione / raccomandazioni

Lo standard minimo per le TIC e gli standard TIC minimi per diversi settori definiti dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), in collaborazione con il settore economico, fungono da raccomandazione e da guida per difendersi in modo adeguato dagli attacchi di hacktivisti.

3 Segnalazioni provenienti da imprese e privati

3.1 Segnalazioni di ciberincidenti ricevute

Segnalazioni settimanali pervenute all'NCSC nel primo semestre del 2023

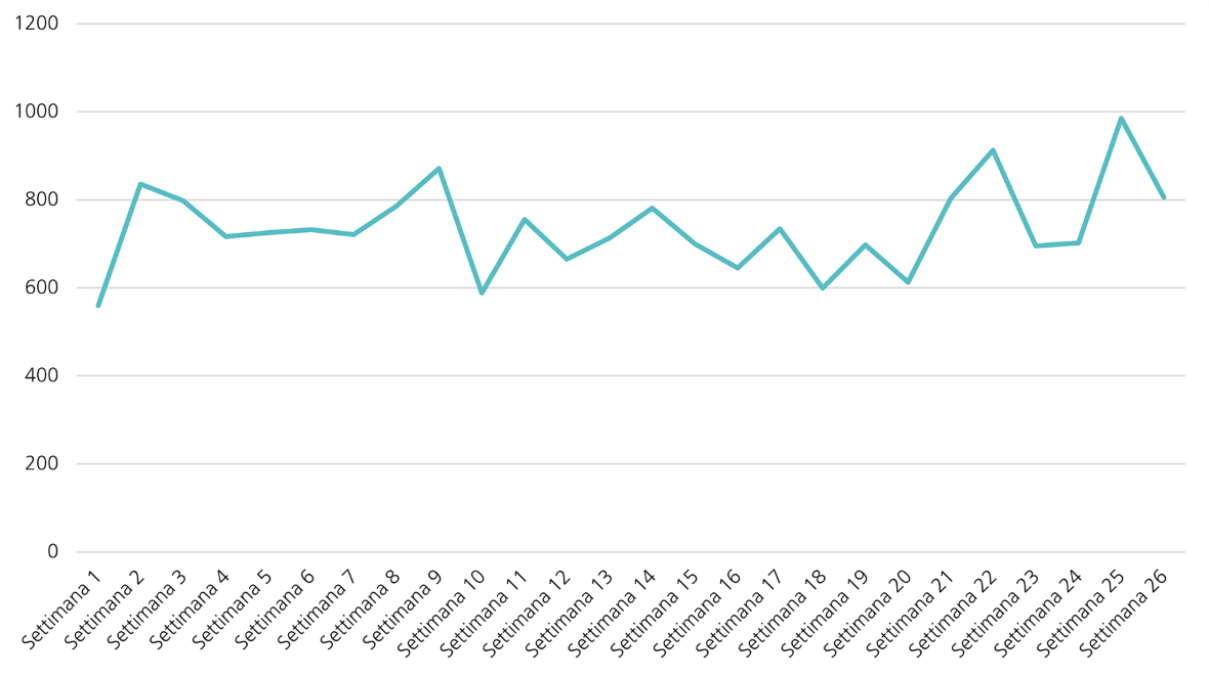


Fig. 3: Segnalazioni settimanali all'NCSC tra gennaio e giugno 2023, vedi anche Numeri attuali (ncsc.admin.ch).

Segnalazioni pervenute all'NCSC nel primo semestre del 2023 per categoria

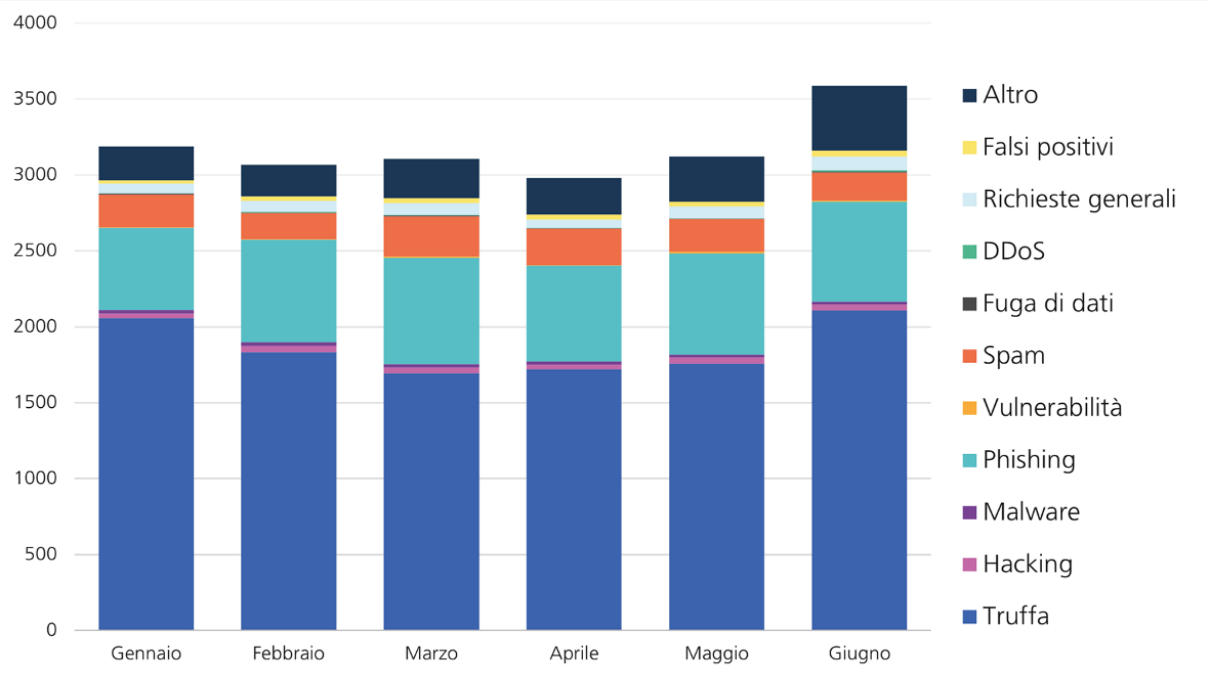


Fig. 4: Segnalazioni all'NCSC nel primo semestre del 2023 per categoria, vedi anche Numeri attuali (ncsc.admin.ch).

Nel primo semestre del 2023, l'NCSC ha ricevuto 19 048 segnalazioni di ciberincidenti, ossia circa 2000 in più sia rispetto al semestre precedente (16 951), che rispetto allo stesso periodo dell'anno precedente (16 844). L'aumento risulta tuttavia più contenuto di quello registrato un anno prima. La quota di finte e-mail minatorie inviate da presunte autorità (5511) e quella di segnalazioni di «spoofing» telefonico (543) sono pressoché inalterate e si confermano allo stesso livello dello scorso semestre. La percentuale di segnalazioni di truffe (11 168) sul totale delle segnalazioni ricevute è scesa lievemente, passando dal 62 al 59 per cento. A registrare invece un notevole aumento, pari a circa 1700 segnalazioni rispetto al semestre scorso, sono state le segnalazioni di phishing. Nel periodo attualmente in esame, sono state depositate 3875 segnalazioni classificabili come phishing. L'aumento è da attribuirsi essenzialmente a una campagna di phishing attuata contro clienti di SwissPass, che si è protratta per tutto il primo semestre. Il numero di segnalazioni in proposito è salito a circa 1000 ed è quasi dieci volte maggiore rispetto al semestre precedente.

Fig. 5: Esempio di tentativo di phishing riguardante un rimborso fasullo di un biglietto delle FFS.

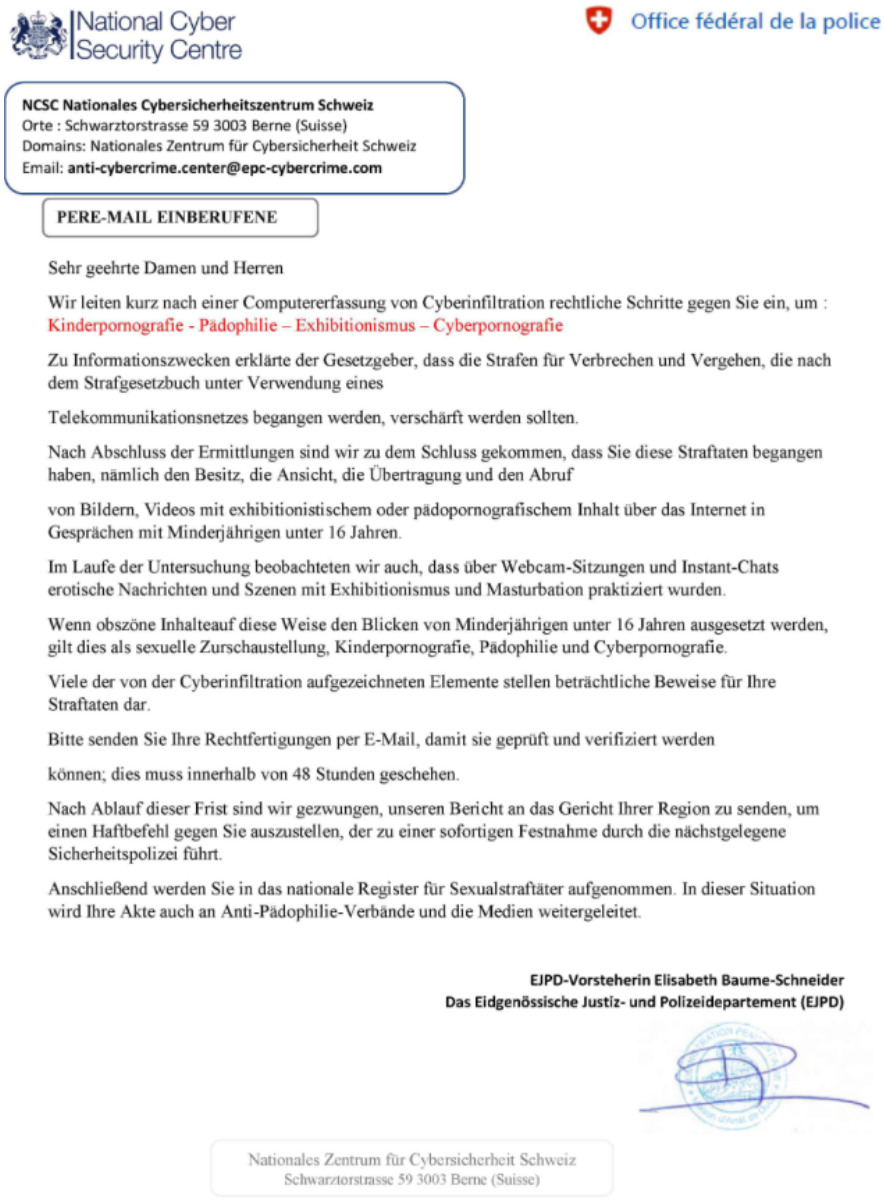
Sono stati segnalati inoltre sempre più tentativi di phishing legati ad annunci, in cui veniva chiesto di pagare delle commissioni correlate a una vendita o di confermare una transazione. L'obiettivo è quello di indurre il venditore a fornire i dati della sua carta di credito. Anche il phishing tramite messaggi di testo (il cosiddetto «smishing») ha registrato un lieve aumento. Resta invece inalterato il livello di tentativi di phishing correlati a false notifiche di consegne di pacchi, che con 600 segnalazioni copre il 15 per cento delle segnalazioni totali di phishing.

Il rapporto tra le segnalazioni da parte di privati (86 %) e quelle di imprese, associazioni e autorità si mantiene stabile. Tra le segnalazioni più frequenti da parte delle imprese, hanno subito un lieve calo sia il numero di truffe del CEO (116 segnalazioni) sia quello di «business e-mail compromise» (BEC), in cui la vittima viene truffata mediante la manipolazione di una fattura (36). Gli attacchi con ransomware (56) e gli attacchi DDoS (24) sono invece aumentati. Le imprese segnalano per lo più finte e-mail minatorie inviate da presunte autorità, le cosiddette «fake extortions» (346), tra cui rientrano per esempio anche numerosi tentativi di estorsione ai danni di amministratori web. Gli aggressori, in questi casi, fanno credere che il sito web presenti delle vulnerabilità, insinuando che vi sia stata una fuga di dati. Le imprese segnalano regolarmente anche tentativi di phishing, finalizzati per lo più ad acquisire le credenziali di accesso a Microsoft Office 365.

3.2 La truffa rimane il tipo di incidente più segnalato

3.2.1 Ancora numerose le finte e-mail minatorie inviate da presunte autorità

Il 30 per cento delle segnalazioni pervenute riguarda ancora finte e-mail minatorie inviate da presunte autorità («fake extortion»). Nella larga maggioranza dei casi, le e-mail minatorie accusano la vittima di aver compiuto un presunto reato. Tali minacce sono inviate a nome di autorità nazionali o internazionali. Nell'ultimo semestre, è stato utilizzato con frequenza sempre maggiore il nome dell'NCSC svizzero, affiancato però al logo dell'ente omologo britannico. Nelle comunicazioni fraudolente figurava il più delle volte la firma falsificata della direttrice dell'Ufficio federale di polizia, Nicoletta della Valle, di un consigliere federale o di una consigliera federale. I truffatori sembrano essere aggiornati sulla politica svizzera, perché sei giorni dopo l'insediamento della consigliera federale Baume-Schneider sono emerse e-mail fasulle a suo nome.



National Cyber Security Centre

Office fédéral de la police

NCSC Nationales Cybersicherheitszentrum Schweiz
Orte : Schwarztorstrasse 59 3003 Berne (Suisse)
Domains: Nationales Zentrum für Cybersicherheit Schweiz
Email: **anti-cybercrime.center@epc-cybercrime.com**

PERE-MAIL EINBERUFENE

Sehr geehrte Damen und Herren

Wir leiten kurz nach einer Computererfassung von Cyberinfiltration rechtliche Schritte gegen Sie ein, um : Kinderpornografie - Pädophilie – Exhibitionismus – Cyberpornografie

Zu Informationszwecken erklärte der Gesetzgeber, dass die Strafen für Verbrechen und Vergehen, die nach dem Strafgesetzbuch unter Verwendung eines

Telekommunikationsnetzes begangen werden, verschärft werden sollten.

Nach Abschluss der Ermittlungen sind wir zu dem Schluss gekommen, dass Sie diese Straftaten begangen haben, nämlich den Besitz, die Ansicht, die Übertragung und den Abruf

von Bildern, Videos mit exhibitionistischem oder pädopornografischem Inhalt über das Internet in Gesprächen mit Minderjährigen unter 16 Jahren.

Im Laufe der Untersuchung beobachteten wir auch, dass über Webcam-Sitzungen und Instant-Chats erotische Nachrichten und Szenen mit Exhibitionismus und Masturbation praktiziert wurden.

Wenn obszöne Inhalteauf diese Weise den Blicken von Minderjährigen unter 16 Jahren ausgesetzt werden, gilt dies als sexuelle Zurschaustellung, Kinderpornografie, Pädophilie und Cyberpornografie.

Viele der von der Cyberinfiltration aufgezeichneten Elemente stellen beträchtliche Beweise für Ihre Straftaten dar.

Bitte senden Sie Ihre Rechtfertigungen per E-Mail, damit sie geprüft und verifiziert werden

können; dies muss innerhalb von 48 Stunden geschehen.

Nach Ablauf dieser Frist sind wir gezwungen, unseren Bericht an das Gericht Ihrer Region zu senden, um einen Haftbefehl gegen Sie auszustellen, der zu einer sofortigen Festnahme durch die nächstgelegene Sicherheitspolizei führt.

Anschließend werden Sie in das nationale Register für Sexualstraftäter aufgenommen. In dieser Situation wird Ihre Akte auch an Anti-Pädophilie-Verbände und die Medien weitergeleitet.

EJPD-Vorsteherin Elisabeth Baume-Schneider
Das Eidgenössische Justiz- und Polizeidepartement (EJPD)

Nationales Zentrum für Cybersicherheit Schweiz
Schwarztorstrasse 59 3003 Berne (Suisse)

Fig. 6: E-mail di «fake extortion» a nome dell'NCSC con il logo dell'ente omologo inglese, apparentemente firmata da Elisabeth Baume-Schneider. L'e-mail è stata segnalata all'NCSC il 6 gen. 2023, poco dopo l'insediamento della nuova consigliera federale.

3.2.2 Altri fenomeni della categoria delle truffe

L'NCSC riceve anche molte segnalazioni concernenti truffe dell'anticipo (1660). Oltre alle classiche promesse di un'eredità o di un baule pieno d'oro, esistono varianti moderne. Il destinatario riceve via e-mail un nome utente e una password e al link indicato può vedere una notevole somma in criptovaluta depositata su un conto apparentemente suo. Viene invitato a pagare ripetute commissioni sempre più elevate per ottenere il versamento delle somme promesse, che naturalmente non saranno mai veramente erogate.

I fenomeni di «fake sextortion», abbonamenti trappola e truffe relative ad annunci sono stati segnalati nella stessa misura dello scorso semestre. Per quanto riguarda gli annunci, si è passati dalla truffa al phishing. Nel corso della procedura di pagamento, infatti, la vittima riceve un link di phishing.

Nell'ambito delle truffe dell'investimento online, l'NCSC ha registrato 245 segnalazioni, rilevando un lieve aumento rispetto alle 219 del semestre precedente. L'entità delle perdite segnalate, però, è più che raddoppiata, attestandosi a 9,5 milioni di franchi. I truffatori sembrano investire una quantità enorme di risorse in termini di personale, perché approcciano le vittime in modo estremamente reattivo e mirato. Oltre a entrare «personalmente» in contatto con le future vittime mediante vari canali dei social media, conquistando la loro fiducia nel tempo, sono ad esempio in grado di offrire sui siti web creati per la truffa un'assistenza via chat o telefono, disponibile sette giorni su sette e ventiquattr'ore su ventiquattro. Offrono altresì video didattici in cui sono spiegate le funzioni delle presunte piattaforme di investimento.

Ancora una volta, i truffatori hanno dimostrato di saper reagire molto rapidamente alle novità. Basti pensare che in occasione del lancio del razzo Starship è circolata una truffa «give away» con un video «deepfake» che ritraeva Elon Musk.[29]

Fig. 7: Video «deepfake» con Elon Musk. Oltre all'immagine, anche la voce è stata creata con la tecnica «deepfake».

[29] Settimana 17: video promozionale falso per una truffa «give away» (ncsc.admin.ch)

3.3 Segnalazioni di phishing

Al secondo posto tra gli incidenti più segnalati vi è il fenomeno del phishing, che ha registrato un aumento di oltre il 40 per cento arrivando a rappresentare, nello scorso semestre, ben un quinto delle segnalazioni pervenute.

In generale si osserva che i tentativi di phishing diventano sempre più complessi e gli hacker sperimentano nuovi metodi per dissimulare i link di phishing.

Sono diventati più frequenti anche i messaggi di phishing inviati tramite SMS (il cosiddetto «smishing»). In particolare, sono state segnalate false notifiche di consegne di pacchi. Il destinatario riceve un messaggio che sembra provenire da La Posta, DHL, DPD o Fedex e annuncia che non è stato possibile recapitare un pacco perché mancano dei dati o vanno pagate delle commissioni. La pagina di phishing è impostata in modo da essere visualizzata solo quando la si apre da cellulare (ad es. con il browser Chrome su sistema operativo Android). Se invece la si apre da computer, si viene reindirizzati direttamente al sito web corretto (ad es. quello de La Posta). In questo modo gli hacker cercano di far credere alle autorità di sicurezza che il messaggio e il link ivi contenuto non siano fraudolenti e che non sia dunque necessario intervenire. Fino ad ora sono invece piuttosto rari i casi segnalati di phishing con codice QR.

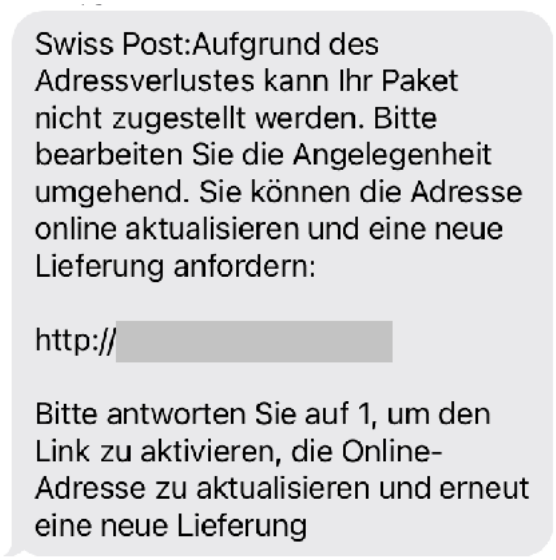


Fig. 8: Tipico tentativo di «smishing» con una falsa notifica di consegna di un pacco a nome de La Posta Svizzera. Dopo aver cliccato sul link viene chiesto di inserire i dati della carta di credito.

È stata riscontrata anche un'ondata di phishing telefonico (il cosiddetto «voice phishing» o «vishing»), in cui gli aggressori si fingevano collaboratori di una compagnia di telecomunicazioni e con una serie di stratagemmi cercavano di ottenere il secondo fattore inviato tramite SMS. In seguito venivano acquistate PaySafeCard sui negozi online della compagnia di telecomunicazioni.[30]

Nel primo trimestre del 2023 sono stati segnalati casi frequenti di phishing in tempo reale riguardanti Microsoft Office 365 soprattutto da parte di aziende. Spesso veniva utilizzato un documento HTML allegato a un'e-mail. La pagina di phishing aperta in locale dal browser ri-

30 Settimana 5: phishing complesso via telefono (ncsc.admin.ch)

portava addirittura loghi aziendali corretti, scaricati in background dal sito ufficiale reale attraverso script dinamici. Non appena una vittima inseriva nome utente e password sulla pagina di phishing, veniva il momento di intercettare, sempre mediante la stessa pagina, il secondo fattore, valido per un periodo di tempo limitato. Con l'intento di ottenere più tempo per le successive attività in background, dopo l'accesso gli hacker fanno credere alla vittima che ci sia un problema temporaneo alla rete.[31]

Pagine di phishing per settimana

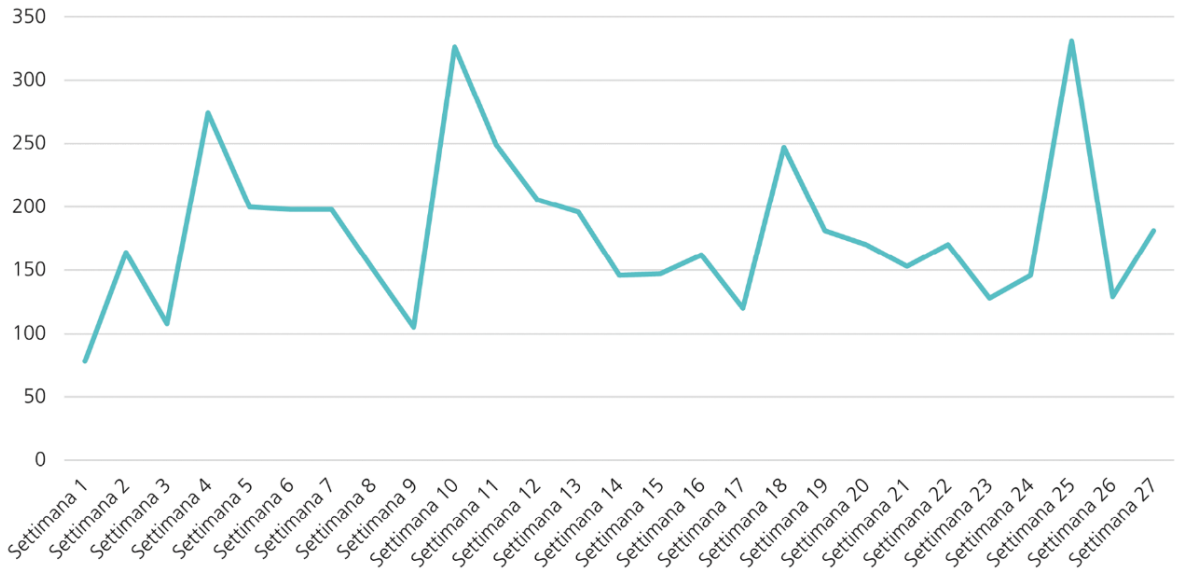


Fig. 9: URL di phishing verificati e confermati dall'NCSC ogni settimana nel primo semestre del 2023.

3.4 Segnalazioni di malware e hacking

3.4.1 Incidenti di ransomware: sviluppi differenti per aziende e privati

Nel primo semestre del 2023 sono state registrate 124 segnalazioni di malware. La tendenza è sempre in calo rispetto al periodo precedente (155 segnalazioni). Come già riscontrato nel semestre scorso, non si sono verificate importanti ondate di diffusione di software dannosi inviati via e-mail.

Sebbene anche le segnalazioni di ransomware siano diminuite da 76 a 64, non si può assolutamente abbassare la guardia. Il calo delle segnalazioni, infatti, non è da attribuirsi alle aziende, ma ai privati (diminuzione da 27 a 8 casi). I sistemi NAS di privati, pur essendo particolarmente esposti, sono ormai colpiti solo sporadicamente.[32] Si è registrato invece un incremento delle segnalazioni da parte di imprese, autorità amministrative e associazioni, che sono passate da 49 a 56. Come dimostrano numerosi esempi relativi al primo semestre del 2023, vengono prese di mira anche imprese di dimensioni maggiori (cfr. in proposito n. 4.2.1). Nel periodo in esame si è confermato particolarmente attivo il ransomware Lockbit. Altre famiglie

[31] Settimana 6: attacchi di phishing in tempo reale ai danni di account protetti di Office 365 (ncsc.admin.ch)

[32] Cfr. Settimana 4: vulnerabilità in dispositivi NAS dell'azienda QNAP e nuova variante di phishing (ncsc.admin.ch)

di ransomware segnalate sono state Play, BlackCat, Medusalocker, Phobos, BlackByte, BlackBasta, Babuk, ECh0raix e Akira. In molti casi, al momento della segnalazione la famiglia di ransomware interessata non è ancora nota, perciò l'NCSC non è in grado di fornire dati attendibili al riguardo. Per questo motivo, attualmente l'NCSC sta elaborando un modulo di feedback da inviare alle aziende in seguito a ogni incidente per rilevare sistematicamente tali informazioni.

3.4.2 Segnalazioni di hacking

Le segnalazioni di hacking sono diminuite, passando da 276 a 225. Quasi la metà di esse riguarda la violazione di account dei social media. Le segnalazioni attribuibili a questa categoria sono rimaste pressoché invariate, attestandosi a 101 segnalazioni contro le 108 del semestre precedente. I truffatori continuano a sfruttare gli account dei social media violati anche nell'ambito della «fake sextortion» per avvalorare i loro tentativi di falsa estorsione. Un altro frequente utilizzo degli account hackerati consiste nell'inserimento di annunci pubblicitari di truffe dell'investimento. Soprattutto nel caso di account con molti follower, questa è una trappola molto diffusa per trasmettere informazioni su offerte dubbie al maggior numero possibile di potenziali vittime.

3.5 Diverse segnalazioni

3.5.1 Ottimizzazione per motori di ricerca con domini abbandonati e siti web hackerati

Quando si fa una ricerca su determinati argomenti utilizzando i motori di ricerca comuni, in genere si clicca solo sui risultati che appaiono nella prima pagina. Se i risultati non sono soddisfacenti, si preferisce di solito modificare le parole chiave piuttosto che prendersi il tempo di verificare se vi siano soluzioni migliori nella seconda o la terza pagina.

Lo hanno notato anche le persone che gestiscono siti sospetti, che tentano con ogni stratagemma possibile di manipolare le ricerche a loro vantaggio, in modo da posizionare le loro offerte nella prima pagina di risultati. In questo modo aumentano le possibilità che le potenziali vittime aprano i risultati della ricerca manipolati e finiscano su siti Internet fasulli.

Nel primo semestre, l'NCSC ha ricevuto, tra le altre, segnalazioni sulle due procedure descritte di seguito.

Nel primo caso, vengono sfruttati domini abbandonati. Molti proprietari di domini sono a conoscenza del problema: si possiedono domini che in realtà non servono più e si sta pensando di disdirne il contratto perché generano tasse annuali. Tuttavia, solo pochi pensano al fatto che, dopo la cessazione, chiunque può registrare nuovamente il dominio e inserirvi contenuti a piacimento. In passato, l'NCSC ha ricevuto ripetutamente segnalazioni, in cui ex proprietari di domini si lamentavano del fatto che shop online sospetti o siti web con contenuti per adulti venivano in seguito visualizzati all'indirizzo del vecchio sito Internet. I domini principalmente presi di mira sono quelli che hanno un gruppo di visitatori piccolo, ma comunque di particolare interesse per gli aggressori. In questo modo, l'aggressore sfrutta il posizionamento ottenuto sui motori di ricerca dal sito Internet originale. Se viene inserito un termine di ricerca corrispondente, non è il dominio originale a comparire nel posizionamento del motore di ricerca, ma il dominio che è stato riutilizzato con i nuovi contenuti dall'aggressore.

Nel secondo caso, gli aggressori tentano di manipolare i risultati dei motori di ricerca servendosi di siti web hackerati. All'inizio dell'anno l'NCSC ha riscontrato che cercando su Google alcuni siti web segnalati all'NCSC come hackerati, tra i risultati veniva visualizzato il titolo corretto. L'estratto dei contenuti riportato sotto il titolo non aveva però nulla a che fare con il sito web, ma conteneva vari link celati dietro combinazioni di lettere e numeri. Anche aprendo il sito web dalla cache di Google, ossia una copia del sito web salvata provvisoriamente da Google, veniva visualizzato l'elenco sospetto di link. Se si accedeva al sito digitando l'URL, il contenuto era corretto. Probabilmente vengono visualizzati contenuti diversi in base allo «user agent». Quando si visita un sito vengono inviati i dati concernenti il tipo di user agent, che includono informazioni riguardanti il sistema operativo e il browser utilizzati. Tali informazioni possono essere utilizzate, oltre che per rilevazioni statistiche, anche per ottimizzare i contenuti di siti web su un particolare tipo di browser. Google scansiona la rete per lo più con lo user agent «Googlebot» per cui è possibile individuare le ricerche di Google. Tale funzione può tuttavia anche essere manipolata per presentare a Google un contenuto web appositamente preparato. Dal momento che nei diversi siti Internet hackerati vengono inseriti sempre gli stessi link, Google li considera interessanti e più rilevanti di quanto non siano in realtà. I link finiscono così in cima ai risultati e ottengono una maggiore visibilità. Tutti gli altri visitatori del sito web hackerato, quindi anche il proprietario, visualizzano il contenuto normale. Di conseguenza, la manipolazione risulta meno evidente e può persistere nel tempo.

4 Situazione

4.1 Accesso iniziale

Ottenere l'accesso ai sistemi informatici da remoto o agli account degli utenti è la prima tappa nella maggior parte dei ciberattacchi. L'accesso iniziale può avvenire in vari modi[33] e, una volta ottenuto, può essere trasmesso ad altri aggressori.

4.1.1 Nome utente / password

I truffatori si impossessano delle credenziali per l'accesso perlopiù tramite attacchi di phishing (cfr. n. 3.3). In altre parole, gli utenti vengono ingannati e indotti a fornire agli hacker le loro credenziali di accesso. La qualità dei messaggi di phishing è in costante miglioramento, pertanto è sempre più difficile riconoscerli.[34] Al tempo stesso, gli autori di attacchi informatici reagiscono alle nuove misure di sicurezza e hanno elaborato strategie per accedere persino ad account protetti da metodi di autenticazione a due o più fattori.[35]

---

[33] Si veda anche Initial Access, Tactic TA0001 (mitre.org)

[34] Settimana 25: riconoscere il phishing è sempre più difficile (ncsc.admin.ch); si veda anche il n. 3.3.

[35] Settimana 6: attacchi di phishing in tempo reale ai danni di account protetti di Office 365 (ncsc.admin.ch); Settimana 8: Un presunto SMS del Consiglio federale e altre nuove varianti di phishing (ncsc.admin.ch); Settimana 9: e-mail minatorie a nome dell'NCSC e phishing in tempo reale (ncsc.admin.ch); Settimana 19: «SIM swapping» – come rubare una scheda SIM online (ncsc.admin.ch)

Conclusione / raccomandazioni

Sebbene le misure di sicurezza non garantiscano una protezione assoluta, vale la pena ostacolare il più possibile l'operato di eventuali aggressori. Si consiglia pertanto di scegliere password complesse e, laddove possibile, proteggere gli account importanti con metodi di autenticazione a due o più fattori.[36]

Verificate sempre l'indirizzo che si cela dietro un link e l'URL.[37] Un logo o comunque un'immagine non provano l'autenticità di un'e-mail o di un sito web. Prestate estrema attenzione quando vi viene chiesto di inserire password o altre informazioni.

4.1.2 Malware (trojan)

L'installazione di trojan apre un varco agli aggressori per penetrare nel sistema target. È inoltre un metodo comune per ottenere l'accesso al sistema della vittima. Di norma, l'installazione non avviene automaticamente ma richiede un'azione da parte dell'utente, perciò quest'ultimo deve essere indotto a effettuarla. Per riuscirci, gli hacker adottano vari stratagemmi. Spesso il codice che installa il malware è integrato in un altro programma o camuffato in altro modo, cosicché l'utente non si accorga della sua esecuzione.

È molto frequente che la diffusione di software dannosi avvenga via e-mail. Il codice per l'infezione può essere contenuto direttamente nell'allegato oppure in un link che figura nell'e-mail. Il contesto dell'e-mail induce l'utente a eseguire il file contenente il codice dannoso. Può fare riferimento, ad esempio, ad attività quotidiane come offerte, consegne e fatture, o rimandare a informazioni esclusive su eventi di attualità. Per rendere ancora più credibile l'e-mail contenente il malware, alcuni hacker sfruttano addirittura scambi di e-mail passati e reali, ottenuti tramite accessi non autorizzati ad altre organizzazioni. È ciò che può accadere ad esempio con «QakBot», un malware la cui prima infezione provoca sistematicamente infezioni di ransomware.[38] Molte volte accade anche che al destinatario venga messa pressione in termini di tempo, in modo da indurlo a compiere azioni non meditate. In una sua retrospettiva settimanale l'NCSC ha descritto un esempio concreto in cui vengono messi in pratica questi vari elementi (diffusione via e-mail, installazione del software nascosta in un altro programma, pressione nei confronti dell'utente affinché reagisca immediatamente).[39]

Capita altresì che gli utenti siano indotti a installare software dannosi mediante l'acquisto di spazi pubblicitari online o la visualizzazione di risultati di ricerca sponsorizzati («malvertising»). Tali annunci fanno credere che il software che si sta cercando sia disponibile alla pagina corrispondente, ma insieme al software desiderato (per lo più gratuito) viene installato anche il malware.[40]

---

36 E per «Elaborare password complesse» (s-u-p-e-r.ch); Proteggete i vostri account (ncsc.admin.ch)

37 Cibermito: quando clicco su un link si collega effettivamente al sito Internet specificato (ncsc.admin.ch)

38 Settimana 24: il malware «QakBot» è ancora attivo e utilizza nuovi stratagemmi (ncsc.admin.ch)

39 Settimana 18: il lupo travestito da agnello: quando il malware si nasconde nell'aggiornamento (ncsc.admin.ch)

40 Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals (trendmicro.com)

Infine, i criminali si servono anche di chiavette USB per diffondere i loro malware, innanzitutto perché le chiavette USB possono essere elaborate specificatamente per avviare l'infezione in un ambiente target[41], in secondo luogo perché un malware, nel momento in cui una chiavetta USB viene inserita in un computer già infetto, può copiarsi su di essa e contagiare poi i sistemi in cui viene successivamente inserita. Si tratta di una procedura che si tende a non prendere più in considerazione, eppure continua a essere praticata.[42]

Conclusione / raccomandazioni

Non cliccate mai su link inviati con e-mail sospette e non aprite mai gli allegati. In caso di dubbio, chiedete al presunto mittente se ha effettivamente inviato l'e-mail in questione.

Quando cercate un software su Internet, verificate di essere sul sito web del produttore o su un altro sito affidabile (ad es. in una rivista di informatica). Siate prudenti quando si apre una finestra di download. Se possibile, impostate la funzione di aggiornamento automatico dei programmi. In alternativa, utilizzate sempre la funzione di aggiornamento integrata o scaricate la versione più recente direttamente dal produttore.

Non collegate mai al computer dispositivi USB sconosciuti o trovati casualmente.

4.1.3 Sfruttamento delle vulnerabilità

Non appena viene individuata una vulnerabilità in un prodotto, vari attori iniziano a cercare su Internet i sistemi esposti. Dopo qualche ora o giorno la falla inizia a essere sfruttata. Anche le vulnerabilità note da tempo e per le quali sarebbe disponibile una patch vengono sfruttate regolarmente.[43] Talvolta gli hacker sfruttano anche le cosiddette vulnerabilità zero-day[44]: all'inizio di giugno, il gruppo di ransomware Cl0p ha iniziato a servirsi di una vulnerabilità «SQL injection» fino ad allora sconosciuta nel programma di scambio di file «MOVEit Transfer». Applicazioni web raggiungibili da Internet sono state infettate con una «shell web»[45] per mezzo della quale si riusciva poi ad accedere a banche dati di «MOVEit Transfer» ad esse collegate.[46]

Oltre a errori di programmazione da parte degli sviluppatori, risolvibili tramite una patch o un aggiornamento, anche le configurazioni scelte per l'implementazione di prodotti possono comportare vulnerabilità. Diversi produttori forniscono istruzioni per configurare i loro prodotti in modo sicuro o potenziarli.

---

41 Ciberdritta: chiavette USB infette come vie di accesso per i ciberattacchi (ncsc.admin.ch)

42 Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives (checkpoint.com)

43 Si veda ad es. Settimana 7: sistemi VMware ESXi criptati (ncsc.admin.ch)

44 Una vulnerabilità zero-day è una vulnerabilità per cui non esistono ancora né aggiornamenti né patch in grado di risolverla.

45 Una «shell web» è un'interfaccia che consente l'accesso da remoto a un server web mediante un browser web.

46 Vulnerabilità critica nel programma di scambio di file «MOVEit» (ncsc.admin.ch); CL0P Ransomware Gang Exploits MOVEit Vulnerability (cisa.gov); si veda anche i n. 4.4.1, 4.5.1 e 4.5.2.

Raccomandazioni

Quando utilizzate nuovi prodotti verificate la relativa configurazione per gli aspetti concernenti la sicurezza e la protezione dei dati. Assicuratevi che siano attivate soltanto le funzionalità di cui avete bisogno.

Privati e aziende dovrebbero quindi mantenere sempre aggiornati i software su tutti i loro dispositivi, possibilmente attraverso la funzione di aggiornamento automatico.[47] Si raccomanda vivamente di procurarsi un sistema efficace di gestione dei software, con un inventario e procedure per gli aggiornamenti.[48]

I software che hanno raggiunto la fine del loro ciclo di vita e non presentano più aggiornamenti da parte del produttore vanno sostituiti.

4.2 Ransomware

Anche nel primo semestre si sono verificati numerosi casi di ransomware in vari settori, dalle piccole attività locali fino alle grandi aziende multinazionali. Gli esempi qui di seguito riguardano sia la Svizzera che l'estero e, oltre a illustrare la situazione nel ciberspazio, delineano l'evoluzione dei gruppi e dei metodi di azione nel primo semestre del 2023.

4.2.1 Ciberincidenti in Svizzera: alcuni esempi

In Svizzera il ransomware più diffuso si conferma «Lockbit». Gli aggressori che ne fanno uso lanciano campagne di phishing ben architettate o sfruttano vulnerabilità per penetrare nei sistemi. Ad attirare particolare attenzione da parte dell'NCSC in questo semestre sono state soprattutto le attività dei gruppi Play e BlackBasta.

Attacchi eclatanti mossi dal gruppo Play

Il gruppo Play si è mostrato molto attivo: tra i soggetti presi di mira vi sono stati, ad esempio, Pool Energia Svizzera a febbraio del 2023[49], due grandi aziende mediatiche come CH Media ed NZZ a marzo[50], il Comune vallesano di Saxon ad aprile[51] nonché il fornitore di servizi informatici Unico[52] e il fornitore di software Xplain[53] a maggio. I problemi causati dagli attacchi e la successiva pubblicazione dei dati sottratti alle vittime hanno conferito grande visibilità al gruppo Play.

---

47 Si veda U per «usare gli aggiornamenti» (s-u-p-e-r.ch)

48 Si veda il rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.2.

49 Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)

50 Daten von CH Media nach Cyberangriff veröffentlicht (chmedia.ch);
Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch);
Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch)

51 Saxon: Cyberattacke auf die Vormundschaftsbehörde (polizeiwallis.ch)

52 Ransomware-Attacke auf IT-Dienstleister Unico Data: viele Betroffene (watson.ch)

53 Attacco hacker alla ditta Xplain: colpita anche l'Amministrazione federale (ncsc.admin.ch)

BlackBasta danneggia l'attività industriale

Anche gli hacker di BlackBasta si sono fatti notare nel primo semestre. Tra le loro vittime vi sono state aziende come ABB[54] e il fornitore di macchine e servizi industriali Bobst[55]. In entrambi i casi gli attacchi hanno compromesso le attività industriali.

BlackBasta funziona fondamentalmente come un «ransomware as a service» (RaaS), ma non vi sono indizi circa interventi del gruppo su forum specifici del dark web o su piattaforme di negoziazione illegali per farsi pubblicità o comunque reclutare nuovi complici. Le informazioni più recenti fanno pensare che gli autori del software sviluppino autonomamente la loro toolbox. Se così fosse, è possibile che il gruppo collabori solo con un numero limitato di complici di fiducia.

Evoluzione del gruppo BianLian

Nel precedente rapporto semestrale, l'NCSC ha riportato il caso del gruppo BianLian[56]. A settembre del 2022, a soli due mesi dai suoi primi attacchi, il gruppo ha preso di mira la sua prima vittima svizzera. Allora l'NCSC aveva comunicato che, come molti altri autori di malware, BianLian agiva secondo il principio della doppia estorsione, in base al quale, prima di essere crittografati, i dati vengono esfiltrati, ossia copiati indebitamente dai sistemi della vittima. Dal gennaio del 2023, però, il gruppo sembra aver smesso di crittografare i dati, limitandosi a sottrarli. Va osservato che, proprio in quel periodo, era stato rilasciato un programma gratuito di decrittazione per il ransomware di BianLian.

Ciò non ha tuttavia impedito al gruppo di portare avanti le proprie operazioni. Nella primavera del 2023, il Dipartimento dell'educazione del Cantone di Basilea Città è stato oggetto di un attacco di BianLian, in seguito al quale i dati sottratti sono stati pubblicati sul dark web.[57] Anche altri gruppi di ransomware abituati ad attuare pratiche di doppia estorsione, come BlackCat o Cl0p, hanno iniziato ad abbandonare la fase di crittografia.[58] Vi sono poi gruppi di estorsori, come ad esempio Karakurt, che non hanno mai messo in atto la crittografia.

4.2.2 La situazione all'estero

Sotto il profilo dei ransomware, la situazione svizzera è piuttosto in linea con quella internazionale. I gruppi con il maggior numero di attacchi sono «Lockbit», «BlackCat/AlphV» e «Royal», mentre ad essere colpiti sono soprattutto imprese industriali e fornitori di servizi.[59] Tra gli incidenti più eclatanti vi è stato quello subìto dalla Royal Mail britannica, che a gennaio del 2023 ha dovuto sospendere temporaneamente le spedizioni internazionali in seguito a un'infezione con il ransomware «LockBit».[60]

---

54 Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com); ABB provides details about IT security incident (abb.com)

55 Cyberattaques ciblées: Bobst résiste à deux piratages informatiques (24heures.ch); Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)

56 Rapporto semestrale 2022/2 (ncsc.admin.ch), n. 5.2.2.1.

57 Grosser Cyberangriff - Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

58 Cfr. n. 4.5.1.

59 March 2023 broke ransomware attack records with 459 incidents (bleepingcomputer.com); Ransomware Trends 2023, Q2 Report (cyberint.com)

60 LockBit leaks more Royal Mail data after ransomware attack (techmonitor.ai)

Oltre ai costanti attacchi da parte di gruppi noti, sono emersi anche nuovi ransomware (ad es. «Akira») e nuovi gruppi (ad es. MalasLocker, cfr. n. 2.1.1); altri gruppi si sono invece sciolti (Hive) o sono tornati alle cronache, come nel caso di Cl0p.[61]

4.2.3 Panoramica degli attori più attivi e dei vettori d'infezione più frequenti

Capacità di cavalcare l'onda

Nel semestre in esame la maggior parte degli incidenti è stata attribuibile a Lockbit, BlackCat/AlphV e Cl0p. I vettori d'infezione utilizzati cambiano nel tempo, con la stessa rapidità con cui vengono scoperte nuove vulnerabilità e rilasciate nuove patch per la loro risoluzione. I cibercriminali sanno adeguarsi molto rapidamente alle nuove tendenze tecnologiche, come ad esempio con l'utilizzo dei linguaggi di programmazione «Go» e «Rust»[62], lo sfruttamento di vulnerabilità in server VMware ESXi[63] o la diffusione di malware attraverso file OneNote[64]. Talvolta non è neppure necessario modificare la procedura tecnica, poiché sono sufficienti i metodi già in uso basati sull'ingegneria sociale. Gli errori umani rimangono il punto debole più fruttuoso per i cibercriminali.

Attacchi a fornitori di servizi informatici

Anche fornitori di servizi informatici sono stati oggetto di attacchi ransomware. Se questo genere di attacchi viene mosso contro un'azienda del settore informatico, infatti, ciò può avere ripercussioni su molti clienti contemporaneamente. I fornitori di servizi informatici costituiscono un'interfaccia o uno snodo per molte reti di clienti e, proprio per questo effetto moltiplicatore, sono particolarmente interessanti per gli hacker, che vi scorgono l'opportunità di chiedere riscatti più numerosi e/o più elevati. Per un fornitore di servizi informatici è dunque fondamentale disporre di un piano d'emergenza per il proseguimento dell'attività operativa (che comprenda il backup dei dati e la replicazione dell'infrastruttura dei server attraverso l'immagine di sistema e il cloud computing), in modo da poter riprendere rapidamente le proprie attività in caso di attacco ransomware.

Tendenza ad abbandonare la crittografia

Per molto tempo, la doppia estorsione è stata in un certo senso il metodo standard adottato dai gruppi di ransomware e dai relativi complici. In casi specifici si è giunti addirittura a una tripla estorsione: oltre ad esfiltrare e successivamente crittografare i dati, infatti, gli aggressori attaccavano terze parti e persone appartenenti alla cerchia della vittima, ricattandole sulla base dei dati sottratti. Ora, invece, l'NCSC osserva una tendenza ad abbandonare la crittografia da parte di vari gruppi, che si limitano a esfiltrare i dati e a ricattare le vittime minacciando di pubblicarli (cfr. n. 4.5.1).

---

61 Si veda i n. 4.4.1 e 4.5.2.

62 Si veda il rapporto semestrale 2022/2 (ncsc.admin.ch), n. 5.2.2.

63 Settimana 7: sistemi VMware ESXi (ncsc.admin.ch)

64 Qakbot evolves to OneNote Malware Distribution (trellix.com)

Conclusioni, previsioni e raccomandazioni

Nell'ambito dei ransomware, i gruppi e i loro modi di procedere si evolvono e cambiano sempre più velocemente. È dunque tanto più essenziale, se possibile, attuare misure preventive a livello tecnico e umano.[65]

Sul sito web dell'NCSC sono riassunti alcuni suggerimenti per la gestione di questi incidenti:

«Sono vittima di un attacco ransomware. E adesso?» (ncsc.admin.ch) e «C'è stata una fuga di dati. E adesso?» (ncsc.admin.ch)

4.3 Sistemi di controllo industriali (ICS) e tecnologia operativa (OT)

Nel primo semestre del 2023, gli attacchi opportunistici ai danni di reti di organizzazioni che gestiscono anche sistemi di controllo industriali e tecnologie operative si sono confermati essere la minaccia più grave per il funzionamento sicuro di tali sistemi. Gli attacchi attribuiti al ransomware «BlackBasta» attuati in Svizzera contro l'azienda industriale ABB[66] e il produttore romando di macchinari Bobst[67] hanno compromesso almeno temporaneamente l'attività operativa dei relativi impianti industriali. Nel settore energetico, l'azienda Pool Energia[68] è finita nel mirino del ransomware «Play» (cfr. n. 4.2.1).

Sul piano internazionale, dall'inizio dell'anno si è registrato un incremento delle attività con software malevoli finalizzati alla cancellazione dei dati (i cosiddetti «wiper»), che hanno provocato interruzioni dell'esercizio a organizzazioni sul territorio ucraino.[69] Tra gli altri, è stato utilizzato il «NikoWiper»[70] ai danni di un'impresa del settore energetico. L'aumento dell'incidenza dei wiper è riconducibile anche a un nuovo attore, denominato Cadet Blizzard[71] o Frozen Vista[72], che, tra le altre cose, all'inizio del conflitto ha attuato una serie di attacchi con il wiper «WhisperGate». Al di fuori del territorio di guerra, invece, è stato mosso un ciberattacco a un gasdotto canadese che ha provocato interruzioni al trasporto di energia.[73] Dai «Pentagon leaks» emergerebbe che l'attacco è stato rivendicato dal gruppo di hacktivisti filorusso Zarya. Altre attività potenzialmente distruttive ad opera di hacktivisti sono riportate nel paragrafo dedicato (n. 2.4).

Alla fine di maggio, la società di sicurezza informatica Mandiant ha pubblicato alcune scoperte sul malware «CosmicEnergy», specifico per colpire ICS.[74] Questo attacca infatti i dispositivi che funzionano in base allo standard di alimentazione elettrica IEC 104. Sia Mandiant che altri

---

65 Cfr. metodi e misure di cui al n. 4.1.

66 Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com); ABB provides details about IT security incident (abb.com)

67 Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)

68 Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)

69 Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever (wired.com)

70 New Report Reveals NikoWiper Malware That Targeted Ukraine Energy Sector (thehackernews.com)

71 Cadet Blizzard emerges as a novel and distinct Russian threat actor (microsoft.com)

72 Fog of war: how the Ukraine conflict transformed the cyber threat landscape (blog.google)

73 Russian hacktivist threat on Canada's pipelines is 'call to action,' top cyber official says (therecord.media)

74 CosmicEnergy: New OT Malware Possibly Related To Russian Emergency Response Exercises (mandiant.com)

specialisti di sicurezza degli ICS[75] ipotizzano che si tratti di uno strumento utilizzato per scenari di esercitazione. Non presenta il potenziale distruttivo di software malevoli come «Industroyer 2.0» o «Pipedream», resi noti nel primo semestre del 2022.[76]

Il rischio di attacchi mirati a processi controllati da tecnologie operative resta elevato soprattutto nel quadro dei conflitti esistenti, come ad esempio la guerra in Ucraina e le tensioni in Medio Oriente. L'autorità statunitense per la cibersicurezza (CISA)[77] mette in guardia dalle attività di Volt Typhoon, un attore sponsorizzato dallo stato cinese, il quale secondo Microsoft[78] sta sviluppando anche capacità dirompenti impiegabili, ad esempio, in caso di escalation delle tensioni con Taiwan[79].

In tutto il mondo si punta a mettere al sicuro i sistemi che controllano processi di infrastrutture critiche. Per questo l'UE ha emanato la direttiva NIS2, che impone agli esercenti l'adozione di misure di sicurezza adeguate.[80] Negli Stati Uniti, la CISA ha pubblicato un white paper su come incrementare la resilienza delle infrastrutture ciberfisiche critiche.[81] Nel mondo industriale, il comparto economico privato ha dato vita al progetto «ETHOS» con l'intento di promuovere la condivisione di avvisi specifici sulla sicurezza OT e di informazioni sulle minacce.[82]

Conclusione / raccomandazioni

Le considerazioni sulla resilienza dei sistemi e delle organizzazioni sono essenziali per preservare l'esercizio degli impianti industriali anche in situazioni critiche. Ciò include anche la formazione e la formazione continua dei collaboratori.

Misure appropriate sono contenute negli standard minimi per le TIC, pubblicati dall'UFAE e aggiornati nel 2023, o nei relativi standard settoriali: Standard minimi per le TIC (ncsc.admin.ch)

L'NCSC sul proprio sito raccomanda una serie di misure di protezione dei sistemi di controllo industriali (ICS) (ncsc.admin.ch).

4.4 Vulnerabilità

4.4.1 «MOVEit» (CVE-2023-34362 | CVE-2023-35036 | CVE-2023-35708)

Alla fine di maggio del 2023 Progress Software ha individuato una vulnerabilità zero-day critica (CVE-2023-34362) nei propri software di trasmissione dei dati «MOVEit Transfer» e «MOVEit Cloud», che riguardano tutte le versioni dell'applicazione. Sono numerose le aziende in tutto il mondo che si servono dell'applicazione per la condivisione e lo scambio di file.

---

75 COSMICENERGY Malware Is Not an Immediate Threat to Industrial Control Systems (dragos.com)
76 Si veda il rapporto semestrale 2022/1 (ncsc.admin.ch), n. 5.4.1.
77 People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (cisa.gov)
78 Volt Typhoon targets US critical infrastructure with living-off-the-land techniques (microsoft.com)
79 Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target? (nytimes.com)
80 Direttiva sulle misure per un livello comune elevato di cibersicurezza in tutta l'Unione (NIS2) (ec.europa.eu)
81 Research, Development, and Innovation for Enhancing Resilience of Cyber-Physical Critical Infrastructure: Needs and Strategic Actions (cisa.gov)
82 ETHOS | Emerging Threat Open Sharing (ethos-org.io)

Il 31 maggio 2023 il produttore ha pubblicato un avviso sulla sicurezza («advisory»)[83] in cui descrive dettagliatamente la vulnerabilità e spiega le misure necessarie per risolverla. In quel momento, però, alcuni soggetti criminali stavano già sfruttato attivamente la falla di sicurezza.

La vulnerabilità colpisce i server Windows su cui è attiva una versione vulnerabile del software «MOVEit». Un eventuale aggressore può individuare in modo relativamente semplice questi sistemi, servendosi di servizi di indicizzazione pubblici su Internet o di port scanning, e identificare così degli obiettivi di attacco.

L'applicazione web «MOVEit», che consente agli utenti di gestire e condividere file in modo semplice e pratico, è esposta a una cosiddetta «SQL injection». Sfruttando tale falla di sicurezza, un hacker può penetrare nel sistema target (nel caso specifico, in particolare nella banca dati di «MOVEit Transfer»), eseguire comandi di sistema e accedere indebitamente a informazioni dell'azienda colpita. Un attacco di questo tipo permette innanzitutto di rubare dati e quindi di sfruttarli per chiedere un riscatto alle vittime. In più, offre a terzi la possibilità di modificare i dati esistenti nel sistema o di introdurvi nuovi file, dunque anche malware.

Poco dopo la scoperta della vulnerabilità zero-day, il gruppo di ransomware Cl0p ha rivendicato centinaia di attacchi a organizzazioni di tutto il mondo. Lo scenario di attacco descritto è stato attuato dai cibercriminali anche nei confronti di aziende svizzere di vari settori, ancor prima che riuscissero a installare sui sistemi le apposite patch create dal produttore.

Il 31 maggio 2023 il produttore Progress Software, pubblicando l'«advisory» relativo alla vulnerabilità CVE-2023-34362, ha fornito istruzioni dettagliate e ha messo a disposizione delle patch per risolvere immediatamente la vulnerabilità. Contestualmente, nell'ambito delle ricerche su CVE-2023-34362, ha incaricato un'azienda terza di sottoporre a verifica il codice software per l'applicazione «MOVEit». Dalla revisione del codice, pochi giorni più tardi, è emersa la presenza di altre due vulnerabilità critiche, per le quali sono state pubblicate ulteriori patch, una il 9 giugno 2023 (CVE-2023-35036) e una il 15 giugno 2023 (CVE-2023-35708).

Entrambe le falle di sicurezza identificate in un secondo momento (CVE-2023-35036 e CVE-2023-35708) appartengono alla stessa categoria individuata per CVE-2023-34362. Tutte e tre le patch create dal produttore sono finalizzate alla rimozione delle cosiddette «SQL injection».

Conclusione / raccomandazioni

Se, nel momento in cui viene pubblicata una vulnerabilità, questa risulta essere già stata sfruttata, oltre ad attuare subito le misure immediate suggerite dal produttore nonché un processo efficiente di gestione delle patch all'interno dell'azienda, è fondamentale verificare in modo attivo e accurato che i sistemi potenzialmente esposti non presentino segni di aver già subìto attacchi. Individuare rapidamente i cosiddetti indicatori di compromissione può infatti aiutare a contenere una serie di attacchi in fase precoce, in modo da ridurre al minimo l'impatto negativo sull'attività e sui processi aziendali.

83 MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362) (progress.com)

4.4.2 Fortinet (CVE-2022-39952 | CVE-2021-42756)

Il 16 febbraio 2023 Fortinet ha comunicato due vulnerabilità critiche individuate dal Product Security Incident Response Team (PSIRT) dell'azienda.

Mentre CVE-2021-42756[84] riguarda «FortiWeb», CVE-2022-39952[85] descrive una falla di sicurezza di «FortiNAC».

«FortiNAC» riconosce e protegge i dispositivi collegati in una rete aziendale utilizzando varie funzioni, che gli permettono di controllare l'accesso alle risorse di rete e di reagire automaticamente agli eventi riguardanti la sicurezza. «FortiWeb» è invece progettato per proteggere applicazioni web e API da attacchi DDoS, dalle minacce riportate dalla OWASP Top 10[86] e da attività di bot malevoli.

In entrambi i casi, in determinate circostanze un hacker può eseguire sul sistema target vulnerabile codici o comandi di sistema e avviare pertanto una «remote code execution» (RCE).

Fino al momento in cui sono state rese note le falle di sicurezza, nessuna delle due vulnerabilità risultava essere stata sfruttata attivamente o, perlomeno, essere nota. Tuttavia già il 21 febbraio 2023, vale a dire pochi giorni dopo che Fortinet aveva comunicato pubblicamente le vulnerabilità, alcuni ricercatori in materia di cibersicurezza hanno pubblicato un codice exploit su CVE-2022-39952, aumentando così in maniera esponenziale la probabilità che cibercriminali vi facessero ricorso. Infatti, solo poche ore dopo la comparsa di tale codice exploit, sono stati segnalati a più riprese tentativi di attacco che sfruttavano attivamente tale vulnerabilità.

Le due vulnerabilità critiche attirano l'attenzione di potenziali aggressori e risultano per loro particolarmente interessanti poiché i prodotti di Fortinet sono estremamente diffusi e utilizzati in tutto il mondo. Fortinet dispone di un'ampia gamma di soluzioni di cibersicurezza e ha fornito oltre 10 milioni di dispositivi. Pertanto i prodotti Fortinet che presentano risapute vulnerabilità sono di grande interesse per gli hacker. Se il numero di prodotti utilizzati a livello mondiale è molto elevato, vi è un'alta probabilità di identificare dispositivi non aggiornati e dunque attaccabili.

Il 21 febbraio 2023, contestualmente alla pubblicazione dei due «advisory» per CVE-2021-42756 e CVE-2022-39952, Fortinet ha comunicato anche le misure necessarie per riparare le vulnerabilità critiche. In entrambi i casi è necessario aggiornare i prodotti «FortiWeb» e «FortiNAC» utilizzati per proteggersi a lungo termine dalla minaccia.

Conclusione / raccomandazioni

Le vulnerabilità in genere iniziano a essere sfruttate subito dopo la loro scoperta, se non addirittura prima. È pertanto essenziale aggiornare i prodotti e i servizi il più rapidamente possibile e installare le patch seguendo le raccomandazioni e le disposizioni del produttore. Adoperatevi anche attivamente per essere sempre aggiornati sulla scoperta di eventuali nuove vulnerabilità. Molti produttori mettono a disposizione dei loro clienti vari canali per ottenere le informazioni rilevanti. Oltre alle informazioni pubblicate sul sito web, è possibile ad esempio abbonarsi

84 PSIRT Advisories FG-IR-21-186 (fortiguard.com)
85 PSIRT Advisories FG-IR-22-300 (fortiguard.com)
86 OWASP Top Ten (owasp.org)

a feed RSS o a newsletter tramite e-mail. In questo modo è possibile integrare tempestivamente le conoscenze relative a ogni nuova vulnerabilità nel relativo processo di gestione aziendale e colmare così eventuali falle di sicurezza.

4.5 Fughe di dati / gestione dei dati

Anche nel 2023, la sicurezza dei dati si conferma una sfida cruciale per imprese e privati. Ciò vale sia per i responsabili dei dati (che sono in possesso dei dati e li archiviano o li fanno archiviare), sia per tutti i fornitori in qualche modo coinvolti nella loro archiviazione, sia per le persone sulle quali vertono i dati. Sebbene la tematica diventi sempre più rilevante e di conseguenza vi sia una crescente consapevolezza in proposito, continua ad accadere che si verifichino fughe di dati in occasione di attacchi informatici. Sempre più spesso, i cibercriminali rinunciano alla classica procedura che prevedeva la crittografia dei dati e la successiva estorsione, per passare a un'estorsione basata solo sull'acquisizione dei dati e la conseguente minaccia con richiesta di denaro per evitare che questi siano pubblicati (cfr. n. 4.2). Anche gli attacchi a fornitori terzi possono dare adito a fughe critiche di dati. In casi di questo tipo, per il cliente del fornitore terzo può essere difficile ricevere informazioni dettagliate sull'incidente e sulle esatte ripercussioni della fuga di dati.

4.5.1 Dagli attacchi basati sulla crittografia alla semplice estorsione basata sui dati

Alla fine di gennaio del 2023, il Dipartimento dell'educazione del Cantone di Basilea Città ha subìto un ciberattacco per opera del gruppo di ransomware BianLian.[87] A maggio, a fronte del mancato pagamento del riscatto richiesto, quasi 1,2 terabyte di dati indebitamente acquisiti sono stati pubblicati sul dark web. Al contrario della consueta procedura messa in atto da BianLian, i sistemi del dipartimento non sono stati crittografati.

Questo caso è esemplificativo di un cambio di strategia da parte di determinati gruppi di ransomware che, anziché attuare la tattica della doppia estorsione[88] (in inglese «double extortion») finora maggiormente diffusa, tendono a puntare sempre più spesso sulla semplice estorsione basata sui dati. Una volta esfiltrati i dati, rinunciano a crittografare i sistemi e, per indurre le vittime a pagare un riscatto, si limitano a speculare sul fatto che la pubblicazione dei dati provocherebbe di per sé danni sufficientemente ingenti. Nel primo semestre del 2023, infatti, si è riscontrato che sempre meno persone sono disposte a pagare un riscatto dopo un attacco di ransomware che sfrutta solo la crittografia.[89] Tale tendenza è rafforzata, tra l'altro, da una più diffusa consapevolezza sulla sicurezza, che porta ad adottare opportune misure

87 Grosser Cyberangriff - Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

88 In un ciberattacco con doppia estorsione, dopo aver rubato i dati, questi vengono crittografati, al fine di estorcere denaro ai loro proprietari e/o di vendere i dati. Viene richiesto un riscatto sia per ottenere la decodifica dei dati e/o dei backup che l'eliminazione o la mancata pubblicazione dei dati rubati.

89 Big Game Hunting is back despite decreasing Ransom Payment Amounts (coveware.com)

(p. es. «backup offline»)[90], e dall'impegno da parte dei fornitori di servizi informatici per mettere a disposizione software di decodifica[91].

I gruppi di ransomware sono attori mossi da intenti finanziari. I ciberattacchi che sfruttano la crittografia sono molto impegnativi, proprio perché le vittime vanno in un certo senso «seguite»: i criminali devono coltivare il contatto con le vittime, condurre delle trattative e, dopo il pagamento, assisterle nella fase di decodifica. Semplificando il modello aziendale, i cibercriminali possono ridurre i propri costi e investire più tempo in altri attacchi. Un esempio significativo del cambio di paradigma è l'operazione che ha visto Cl0p sfruttare una vulnerabilità del programma di scambio di file «MOVEit»[92] per realizzare una compromissione massiccia (cfr. n. 4.4.1). Fino alla fine di giugno del 2023, sul data leak site di Cl0p sono stati pubblicati i nomi di circa 500 organizzazioni colpite. I dati rubati comprendono informazioni su circa 30 milioni di persone in tutto il mondo. Gestire un attacco di tale portata con una crittografia sarebbe estremamente oneroso per i cibercriminali. La nuova procedura risulta per loro comunque vantaggiosa sotto il profilo finanziario, anche se sono relativamente poche le vittime a versare il riscatto richiesto.

Nei casi in cui i dati vengono acquisiti ma non crittografati, la vittima tecnicamente può continuare ad usarli. Tuttavia, una fuga di dati sensibili aziendali e personali può ledere la reputazione e violare le norme sulla protezione dei dati. Gli stessi dati, oltretutto, possono essere utilizzati per altri scopi criminali. Una volta pagato il riscatto non si ha la garanzia che i dati vengano effettivamente eliminati e non pubblicati, e che non siano invece venduti a terzi. Nonostante ciò, molte vittime pagano il riscatto nella speranza di tenere nascosta la questione.

Conclusione / raccomandazioni

Alcuni attori tendono sempre più ad abbandonare la crittografia dei dati a vantaggio di un semplice furto di dati finalizzato all'estorsione. Adottando attente misure, è possibile contenere i danni. Gli utenti devono essere sensibilizzati e formati di conseguenza in base a direttive interne. Una cultura positiva dell'errore consente di ottimizzare i processi interni in collaborazione con il personale, prima che avvenga una fuga di dati.

Gestione corretta dei dati

Regola generale: classificare i dati in base al grado di protezione necessario e proteggerli adeguatamente in conformità a tale classificazione. I dati degni di protezione devono essere possibilmente archiviati in forma crittografata.

Regole di conservazione: stabilire **chi** archivia ed elabora **quali** dati, in **quale forma** e **dove**, e **con chi** sono condivisi. Vanno conservati solo i dati necessari per l'attività aziendale. Verificare periodicamente che vengano eliminati i dati obsoleti o non più necessari. Si può prendere in considerazione anche un'archiviazione di dati digitale offline.

---

90 Improved Security and Backups Result in Record Low Number of Ransomware Payments (coveware.com)

91 BianLian, ad esempio, ha cambiato strategia passando al semplice furto di dati dopo che, all'inizio del 2023, una società di sicurezza informatica aveva rilasciato un programma di decodifica gratuito per il software di crittografia di BianLian.

92 Vulnerabilità critica nel programma di scambio di file MOVEit: Installare con urgenza una Patch (ncsc.admin.ch)

Misure statistiche

Record di dati: i record di dati statistici, ad esempio ottenuti da rilevamenti, o anche i dati finalizzati a condurre test devono essere anonimizzati o pseudonimizzati. È consigliabile conservare separatamente e in forma crittografata anche gli identificatori. Idealmente, i dati grezzi devono essere archiviati separatamente in un supporto di backup offline.

Misure tecniche / igiene informatica

Gestione delle password: introdurre direttive sulle password e l'autenticazione a più fattori.

Osservare il principio del privilegio minimo.

Attuare la segmentazione della rete.

Gestione delle patch: non appena vengono rese note delle vulnerabilità, installare il prima possibile le patch necessarie, considerando i cicli di vita dei prodotti.

Misure organizzative

Definire e testare un piano d'emergenza per la gestione degli incidenti, definendo chiaramente le responsabilità.

In caso di fuga di dati è necessario attuare il più rapidamente possibile misure d'emergenza tecniche e coinvolgere eventualmente specialisti esterni. Si raccomanda una comunicazione coerente e trasparente sia verso l'interno che verso l'esterno. L'ideale sarebbe elaborare preventivamente una strategia comunicativa appropriata.

Verificare inoltre con quali tempistiche è necessario informare persone e organizzazioni sulla fuga di dati. A tal proposito, osservare la nuova legge federale sulla protezione dei dati (in vigore dall'1.9.2023). In caso di violazione della sicurezza dei dati, è necessario inviare tempestivamente una notifica all'incaricato federale della protezione dei dati e della trasparenza (IFPDT).

4.5.2 Fughe di dati provocate da ciberattacchi *attraverso* e *all'interno* della catena di fornitura

Per realizzare beni e servizi, spesso le organizzazioni e le aziende ricorrono a loro volta a servizi e beni di produzione di fornitori terzi. In questo contesto, possono verificarsi ciberattacchi *all'interno*[93] della catena di fornitura (in inglese «supply chain») o *attraverso*[94] la stessa. Data la crescente interconnessione tra i processi aziendali e l'incessante processo di digitalizzazione, tali attacchi possono compromettere o interrompere le attività operative. Tra le conseguenze più disastrose, oltre ai problemi provocati all'attività principale, possono esservi anche le fughe di dati. Spesso i ciberattacchi contro fornitori causano anche la fuoriuscita di informazioni di accesso e dati dei relativi clienti. D'altro canto, i sistemi o i software danneggiati del fornitore possono essere sfruttati per prelevare dati direttamente ai clienti.

---

93 Nei ciberattacchi *all'interno* della catena di fornitura, l'artefice si concentra innanzitutto su un fornitore terzo; anche i clienti di tale fornitore possono tuttavia subire danni collaterali.

94 Un ciberattacco *attraverso* la catena di fornitura, noto anche come attacco alla supply chain, combina due attacchi che però hanno come target principale i clienti del fornitore. Mentre nella prima fase l'attacco è rivolto a un fornitore, nella seconda si sfrutta il danno arrecato all'infrastruttura del fornitore per compromettere l'obiettivo principale, ossia il cliente.

Nel primo semestre del 2023 si sono verificati numerosi casi di fuga di dati di terzi o su terzi, sia sul piano nazionale che su quello internazionale. In Svizzera, in diversi casi[95] i cibercriminali hanno esfiltrato dati di fornitori terzi per poi venderli sul dark web e/o sfruttarli come mezzo di estorsione su data leak site (cfr. n. 4.2.1). Tra questi dati non vi erano solo informazioni sul fornitore stesso ma anche dati dei relativi clienti, ai quali forniva servizi informatici per l'infrastruttura informatica, in toto o in parte. Anche sul panorama internazionale vi sono stati aggressori mossi da intenti finanziari che si sono appropriati di dati al fine di estorcere denaro sia ai fornitori che ai loro clienti.[96] Il numero dei clienti coinvolti, in particolare in relazione alle vulnerabilità di software per il trasferimento di documenti, è stato molto elevato.[97]

Conclusione / raccomandazioni

Le catene di fornitura rappresentano una sfida cruciale per la cibersicurezza e richiedono una gestione attiva del rischio. Quantificare l'impatto di una fuga di dati richiede un notevole dispendio di risorse. Oltre ad adottare misure per una gestione sicura dei dati e per una buona igiene informatica (cfr. raccomandazioni di cui al n. 4.5.1), in generale le organizzazioni e le aziende dovrebbero condividere dati con terzi solo nella misura strettamente necessaria. È inoltre importante che conoscano il loro specifico panorama di minacce informatiche, individuino i rischi critici, li sintetizzino in un piano di riduzione dei rischi e aggiornino quest'ultimo con regolarità. Nel farlo, è necessario controllare tutti i settori operativi esaminando i rapporti di dipendenza nei confronti di determinati fornitori e servizi secondo il loro grado di criticità. Sulla base di questo profilo di rischio, in particolare nei casi di elevata criticità, andrebbero stabiliti per contratto un diritto di audit presso i fornitori terzi e un obbligo di notifica degli incidenti. Le organizzazioni e le aziende più piccole possono rivolgersi ad associazioni o consulenti specializzati per ottenere una verifica indipendente.

È altresì fondamentale monitorare i propri sistemi in modo da poter analizzare gli accessi e le attività di altro tipo nonché, in caso di anomalie, adottare contromisure. Rientra in questo aspetto una protezione ottimale dei canali di connessione e di comunicazione tra i fornitori e la propria organizzazione. Le organizzazioni devono anche elaborare un piano d'emergenza, aggiornarlo costantemente e testarlo. Gli scenari di esercitazione devono tenere conto anche dei rapporti con i fornitori e degli effetti indiretti di eventuali fughe di dati.

---

95 Tra gli incidenti avvenuti sul piano nazionale ricordiamo:
- CH Media/NZZ: Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch); Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch)
- tipografia della «Schweizer Revue»: La fuga di dati riguarda fino a 425'000 svizzere e svizzeri all'estero (swissinfo.ch)
- Xplain AG: Attacco hacker alla ditta Xplain: colpita anche l'Amministrazione federale (admin.ch)

96 Tra gli incidenti avvenuti sul piano internazionale ricordiamo:
- Capita: UK pension funds warned to check on clients' data after Capita breach (therecord.media)
- Alliance Healthcare: Cyberattack cripples Spanish drug giant Alliance Healthcare (cybernews.com); Un ciberataque impide […] medicamentos […] a las farmacias (elpais.com)
- Managed Care of North America: Nearly 9 million people affected by data breach from cyberattack on dental insurer (therecord.media)

97 Cfr. Progress Software e la vulnerabilità di «MOVEit» (cfr. n. 4.4.1) nonché Fortra e la vulnerabilità di «GoAnywhere»: Summary of the Investigation Related to CVE-2023-0669 (fortra.com)

4.6 Hacking di siti web

I siti web hackerati possono essere sfruttati in vari modi. Oltre a inserirvi messaggi politici (cfr. n. 2.2), contenuti per la SEO (cfr. n. 3.5.1) o pagine di phishing, è possibile utilizzarli anche per diffondere malware. Se ricercatori nel campo della cibersicurezza o altre persone riscontrano modifiche illecite di questo tipo, di norma cercano di informare il gestore del sito web affinché vi ponga rimedio. Spesso, però, i contatti per raggiungerlo non sono semplici da trovare sul sito web, oppure non sono del tutto disponibili. Per affrontare al meglio il problema, l'Internet Engineering Task Force (IETF) ha elaborato uno standard in base al quale chi gestisce un sito web dovrebbe inserire i contatti più importanti in un file di testo denominato «security.txt» e salvarlo nella directory predefinita «/.well-known».[98]

Raccomandazioni

Pubblicate sul vostro sito web il contatto della persona responsabile della sicurezza.[99]

Proteggete il vostro sito Internet seguendo le raccomandazioni dell'NCSC.

Notifiche a gestori di siti web per settimana

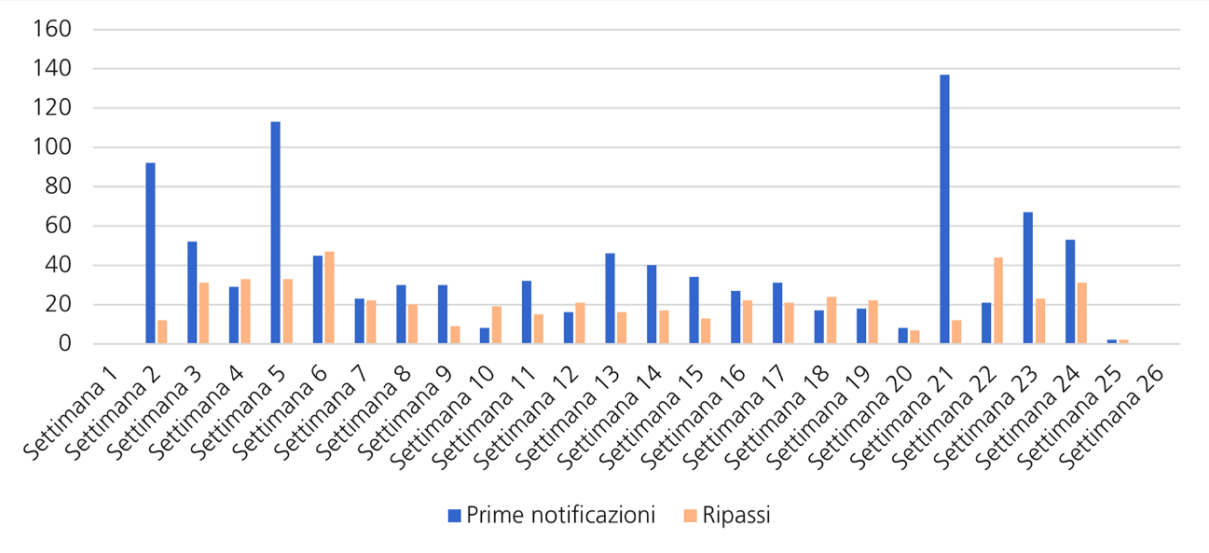


Fig. 10: Notifiche dell'NCSC a gestori di siti web in merito a siti hackerati e modificati illecitamente.

98 RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure (ietf.org)

99 Pubblicate sul vostro sito web il contatto della persona responsabile della sicurezza (ncsc.admin.ch)

4.7 Aggiornamento sulla guerra in Ucraina

Nel primo semestre del 2023 è trascorso un anno dall'attacco mosso dalla Russia nei confronti dell'Ucraina il 24 febbraio 2022. Gli ultimi due rapporti semestrali hanno riportato una serie di ciberattacchi avvenuti nel contesto di questa guerra fino alla fine del 2022.[100]

Principali sviluppi dall'inizio del 2023

Gli aggressori legati allo Stato russo operano in particolare nell'ambito dello spionaggio e del sabotaggio, soprattutto diffondendo tramite e-mail malware in grado di aprire un primo varco per penetrare nei sistemi. Anche le campagne di phishing sono finalizzate ad acquisire dalle vittime i dati di accesso a determinati sistemi. Attività di questo tipo sono state osservate soprattutto in Ucraina, ma anche altri Paesi, per lo più alleati dell'Ucraina o membri della NATO, hanno denunciato campagne di spionaggio.

I gruppi di hacktivisti conducono principalmente attacchi finalizzati a compromettere la disponibilità di siti web (attacchi DDoS). I gruppi di hacktivisti filorussi prendono di mira in particolare i Paesi che offrono sostegno all'Ucraina o che impongono sanzioni alla Russia. Sono state infatti riportate numerose attività al di fuori del territorio ucraino, specialmente in Paesi dell'UE e/o in membri della NATO. All'inizio di giugno, anche la stessa Svizzera è finita per una settimana nel mirino del gruppo di hacktivisti filorusso NoName057(16), proprio poco prima che il presidente ucraino tenesse un discorso in videocollegamento di fronte all'Assemblea federale il 15 giugno 2023.[101] Pur provocando solo danni marginali, gli attacchi di questi collettivi hanno scopi di propaganda.

Sviluppi futuri

Non vi è nulla che faccia pensare che i ciberattacchi malevoli correlati al conflitto in Ucraina possano diminuire. Finché la guerra si protrarrà è molto probabile che la Russia continui a sferrare attacchi informatici e a sfruttare ogni occasione per raggiungere i propri obiettivi, sia con operazioni associate ad altri piani operativi, che con singole iniziative. Le azioni dei gruppi di hacktivisti rappresentano pertanto un notevole fattore di rischio per il futuro. Diversi gruppi hanno dichiarato l'intenzione di passare dagli attacchi DDoS finora osservati a operazioni ancora più distruttive. Sebbene al momento ancora nessun gruppo sembri disporre delle competenze necessarie per portare a termine questi nuovi obiettivi, qualora questa situazione cambiasse potrebbero verificarsi danni collaterali più ingenti.

---

[100] Si veda il rapporto semestrale 2022/1 (ncsc.admin.ch), n. 3 e il rapporto semestrale 2022/2 (ncsc.admin.ch), n. 5.6.

[101] Si veda il n. 2.1.