6 maggio 2025 | Ufficio federale della cibersicurezza UFCS

Rapporto semestrale 2024/II (luglio – dicembre)

Cibersicurezza

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della cibersicurezza UFCS

Management Summary

Nel suo rapporto semestrale l'Ufficio federale della cibersicurezza (UFCS) illustra gli incidenti e gli sviluppi rilevanti nel contesto delle ciberminacce contro la Svizzera e a livello internazionale. Nel secondo semestre del 2024 l'UFCS ha ricevuto 28 165 segnalazioni di ciberincidenti, un numero leggermente inferiore rispetto a quello registrato nei primi sei mesi dell'anno. Nell'arco dei 12 mesi, tuttavia, il numero è cresciuto di 13 574 unità, per un totale di 62 954 segnalazioni. Le fluttuazioni sono dovute principalmente alla massiccia ondata del fenomeno «telefonate minatorie a nome di false autorità». Il rapporto tra il 90 per cento delle segnalazioni provenienti da privati e il dieci per cento da imprese rimane costante. Le categorie «frode», «phishing» e «spam» si confermano ai vertici della classifica dei fenomeni più segnalati.

Tentativi di frode soprattutto ai danni della popolazione

A quota 18 270 le segnalazioni di frode mantengono il primato, rappresentando due terzi delle segnalazioni pervenute nel secondo semestre del 2024. Nel secondo semestre del 2024 non si sono registrati i picchi di casi relativi alla frode delle telefonate minatorie a nome di false autorità; questo fenomeno era stato trattato in dettaglio nel primo rapporto semestrale del 2024[1]. Per quanto riguarda le «lotterie fraudolente», invece, nell'attuale periodo in esame l'UFCS ha visto triplicare il numero di segnalazioni pervenute. Gli abbonamenti trappola oggetto di queste frodi si inquadrano in zone grigie dal punto di vista legale, che i truffatori fruttano sempre più intenzionalmente in assenza di contromisure efficaci. Sul fronte delle imprese si è osservato un forte aumento di segnalazioni relative alla «truffa del CEO», con cui sono stati presi di mira soprattutto Comuni e parrocchie.

I sovraccarichi portano a guasti, aggiornamenti difettosi e malfunzionamenti

Il 19 luglio 2024 si è verificato il blackout informatico più esteso della storia. Non si è trattato di un ciberattacco, bensì di un aggiornamento software difettoso del fornitore di servizi di cibersicurezza CrowdStrike che ha reso inutilizzabili oltre 8,5 milioni di sistemi Windows – soprattutto di grandi imprese. Oltre agli impatti su organizzazioni come ospedali e industrie, a risentirne è stata soprattutto l'aviazione, rimasta in ginocchio per diverse ore in Svizzera e nel mondo.
Gli attacchi di sovraccarico ai danni dei siti Internet di Cantoni e Comuni, ma anche di piattaforme di servizi finanziari online, ne hanno limitato la disponibilità per un certo periodo di tempo. I cosiddetti attacchi «Distributed Denial of Service[2]» (DDoS) sono resi possibili da un'infrastruttura di attacco distribuita, di solito sotto forma di una botnet come «Gorilla»[3].

---

1 Cfr. Rapporto semestrale 2024/1; cap. 5.

2 Attacchi alla disponibilità (DDoS) (ncsc.admin.ch)

3 Cfr. Analisi tecnica della botnet «Gorilla» (ncsc.admin.ch)

Malware distribuito in maniera creativa – il ransomware mette a repentaglio le imprese

Nell'ambito dei ricatti con ransomware, attori e tecniche d'attacco si adattano costantemente alle circostanze del momento, confermandosi la minaccia più rilevante per le imprese. I cibercriminali legati al collettivo «Black Basta», ad esempio, inondano gli account e-mail con messaggi spam, per poi servirsi di piattaforme di comunicazione digitali per offrire servizi di assistenza attraverso cui compromettere i sistemi delle vittime.
Note aziende svizzere, come assicurazioni malattie e società di recupero crediti, hanno visto il loro nome utilizzato abusivamente per distribuire malware a destinatari di e-mail dannose. Su siti Internet fasulli o compromessi gli utenti vengono indotti tramite falsi «CAPTCHA» a eseguire manualmente script dannosi, infettando così i loro dispositivi. Tramite codici QR stampati su apposite lettere, i cibercriminali hanno cercato di indurre i destinatari a installare un'app «Alertswiss» infetta sui loro cellulari Android.

I phisher cercano nuovi spunti e canali

Il furto di dati d'accesso o informazioni finanziarie attraverso il phishing rimane la seconda categoria di segnalazioni più frequenti. Oltre alle note e-mail di phishing, i cibercriminali cercano sempre più di diffondere le loro richieste fraudolente su altri canali, ad esempio attraverso telefonate di presunti impiegati di banca o l'invio di messaggi tramite il nuovo servizio di messaggistica mobile, successore degli SMS, Rich Communication Services (RCS)[4]. I portali di annunci offrono ai truffatori un facile pretesto per entrare in contatto con le vittime, mentre nel mondo reale i codici QR vengono incollati sui parchimetri per indirizzare altrove i pagamenti degli automobilisti.
Inoltre, nel secondo semestre la popolazione e varie organizzazioni svizzere hanno denunciato 497 096 siti web sospetti tramite la piattaforma di segnalazione «antiphishing.ch»[5]. L'UFCS è riuscito a identificarne 9 355 come veri e propri siti di phishing e ad adottare le contromisure adeguate.

Altri fenomeni

Il tempo che rimane alle organizzazioni per eliminare le vulnerabilità prima che gli aggressori se ne approfittino si sta sempre più riducendo in maniera preoccupante. Lo sfruttamento di queste vulnerabilità non solo porta a continue fughe di dati, ma viene anche utilizzato da attori statali per finalità di spionaggio e, in rari casi, persino per il sabotaggio di sistemi di controllo industriali. Queste tendenze globali devono essere affrontate in modo adeguato dal nostro Paese al fine di garantire la protezione dalle ciberminacce.

---

4 Rich Communication Services (wikipedia.org)

5 Cfr. Rapporto anti-phishing 2024 (ncsc.admin.ch)

Indice

Editoriale

Nel 2024 l'UFCS ha ricevuto in totale 62 954 segnalazioni, 13 500 in più rispetto all'anno precedente. Anche se non tutte le segnalazioni pervenute rappresentano un ciberattacco andato a buon fine, il numero evidenzia in maniera impressionante quanto si sia aggravata la situazione di minaccia nel mondo digitale. Ma non sono soltanto i ciberattacchi a mettere in pericolo la nostra infrastruttura informatica. Anche una manipolazione mal riuscita dei propri sistemi informatici o l'installazione di aggiornamenti difettosi possono causare massicci problemi, talvolta con impatti su scala globale. Un esempio lampante della vasta portata di un simile errore è stato l'episodio del 19 luglio 2024, quando un bug nell'aggiornamento del modulo di sicurezza Falcon dell'azienda CrowdStrike ha causato guasti informatici in tutto il mondo. Secondo le stime, quel giorno il blackout ha interessato circa 8,5 milioni di sistemi a livello globale, per un danno nell'ordine di svariati miliardi di dollari.

Questi episodi evidenziano ancora una volta ciò che gli esperti già sanno da tempo: le misure tecniche, da sole, non bastano. Pur essendo imprescindibili, gli effetti si ripercuotono sul mondo reale, per cui devono essere accompagnate anche da interventi di natura organizzativa. Soltanto la combinazione tra misure tecniche e organizzative, infatti, ci consentirà di massimizzare la resilienza dei nostri sistemi e di reagire rapidamente in caso d'emergenza.
Una gestione efficace delle patch è fondamentale per la sicurezza informatica: garantisce non solo il funzionamento sicuro delle applicazioni, ma anche la loro stabilità. Un patch management scaglionato in base alla criticità e all'esposizione dei sistemi è in ogni caso un'opzione da considerare. L'arte consiste nel trovare un equilibrio tra i test necessari e l'installazione tempestiva degli aggiornamenti.
Altrettanto importante è la formazione regolare del personale addetto su come reagire in caso di guasti e blackout informatici. Le esercitazioni periodiche aiutano a saper agire rapidamente ed efficacemente durante un'emergenza. In caso d'incidente, infatti, ogni secondo è prezioso.

Il presente rapporto semestrale fornisce una panoramica completa delle sfide che la Svizzera ha dovuto affrontare nel campo della cibersicurezza nel secondo semestre del 2024. Oltre agli episodi citati, vengono trattate anche tematiche come gli attacchi DDoS, il ciberspionaggio o la gestione delle vulnerabilità.
Vi auguro di poter trarre dalla lettura di questo rapporto semestrale numerosi spunti e riflessioni utili su come migliorare la sicurezza della vostra infrastruttura informatica e aumentare la resilienza dei vostri sistemi contro attacchi e malfunzionamenti.

Florian Schütz, direttore dell'Ufficio federale della cibersicurezza

1 Ciberminacce in Svizzera – panoramica

Conoscere le minacce che insidiano il ciberspazio è fondamentale per garantire la sicurezza delle tecnologie della comunicazione e dell'informazione a livello nazionale e internazionale. Dietro una percentuale considerevole di minacce si celano attori con motivazioni e capacità tra le più disparate. Il caso dell'aggiornamento software difettoso dell'operatore di cibersicurezza CrowdStrike nel luglio del 2024 ha tuttavia evidenziato chiaramente come anche questi processi debbano essere monitorati con la massima attenzione per il corretto funzionamento delle infrastrutture critiche. Allo stesso tempo, le classiche forme di minaccia continuano ad avere un ruolo rilevante nella valutazione del livello di cibersicurezza, essendo costantemente ottimizzate a livello tattico e metodologico dai loro autori. Gli sviluppi attuali su questo fronte riguardano ad esempio, nei casi di frode, l'uso mirato di specificità locali, come ad esempio la lingua svizzero-tedesca, o il crescente sfruttamento di zone grigie dal punto di vista legale (cfr. cap. 5.4) e di informazioni di dominio pubblico sulla gerarchia aziendale. Tutto ciò rende il ciberspazio un ambiente dinamico sia per gli aggressori che per i difensori. I cibercriminali più inclini alla sperimentazione, ad esempio, lanciano tendenze e si procurano seguaci pronti a emularli nel momento in cui un dato procedimento si rivela efficace.

Il numero di segnalazioni pervenute nel secondo semestre del 2024, 28 165 in totale, segna una lieve diminuzione rispetto al primo (34 789) (cfr. fig. 1). A prescindere da ciò, per il 2024 si rileva un generale aumento annuo di 13 574 unità, per un totale di 62 954[6] segnalazioni. L'incremento è dovuto principalmente al fenomeno delle «telefonate minatorie a nome di false autorità»[7] (cfr. fig. 2). Mentre l'anno precedente tali segnalazioni erano rimaste a quota 7 193, nel 2024 hanno subito un'impennata a 21 903. In controtendenza, invece, le e-mail minatorie[8] in cui, analogamente alle chiamate, le vittime vengono accusate di aver commesso un reato. Mentre nel 2023 le segnalazioni pervenute all'UFCS su questo fenomeno erano ancora 10 120, nel 2024 sono precipitate a quota 3 825, il che evidenzia la tendenza degli ultimi quattro anni a un uso sempre maggiore del telefono come canale di frode. Sebbene la telefonata implichi un impegno individuale maggiore per i criminali, consente di interagire meglio con le vittime e di contrastare immediatamente i dubbi che emergono.
L'UFCS ha osservato un aumento significativo delle segnalazioni nel caso delle «lotterie fraudolente»[9] (3 509 segnalazioni), il cui numero è triplicato rispetto all'anno precedente. Soprattutto nel secondo periodo in esame, le segnalazioni sono cresciute da 744 nel 2023 a 2 398 nel 2024. In molti casi sono stati utilizzati abusivamente i nomi di note catene alimentari o retail, negozi di elettronica o aziende di trasporto svizzere.

---

6 Nelle sue statistiche l'UFCS riporta tutte le segnalazioni pervenute, tra cui anche domande generiche, informazioni e segnalazioni non classificabili. Nel 2024 sono state 1 622 le segnalazioni non attribuibili a un fenomeno o un incidente specifico.

7 Per affrontare più approfonditamente il fenomeno delle «telefonate a nome di false autorità», l'UFCS ha redatto un rapporto che è stato pubblicato contestualmente al rapporto semestrale 2024/1. In esso vengono messi in luce, tra i vari aspetti, gli sviluppi correlati a questo fenomeno, vari modus operandi e le relative tecnologie utilizzate, nonché la situazione giuridica a livello nazionale e internazionale.

8 Finte e-mail minatorie a nome delle autorità (ncsc.admin.ch)

9 Lotterie fraudolente (ncsc.admin.ch)

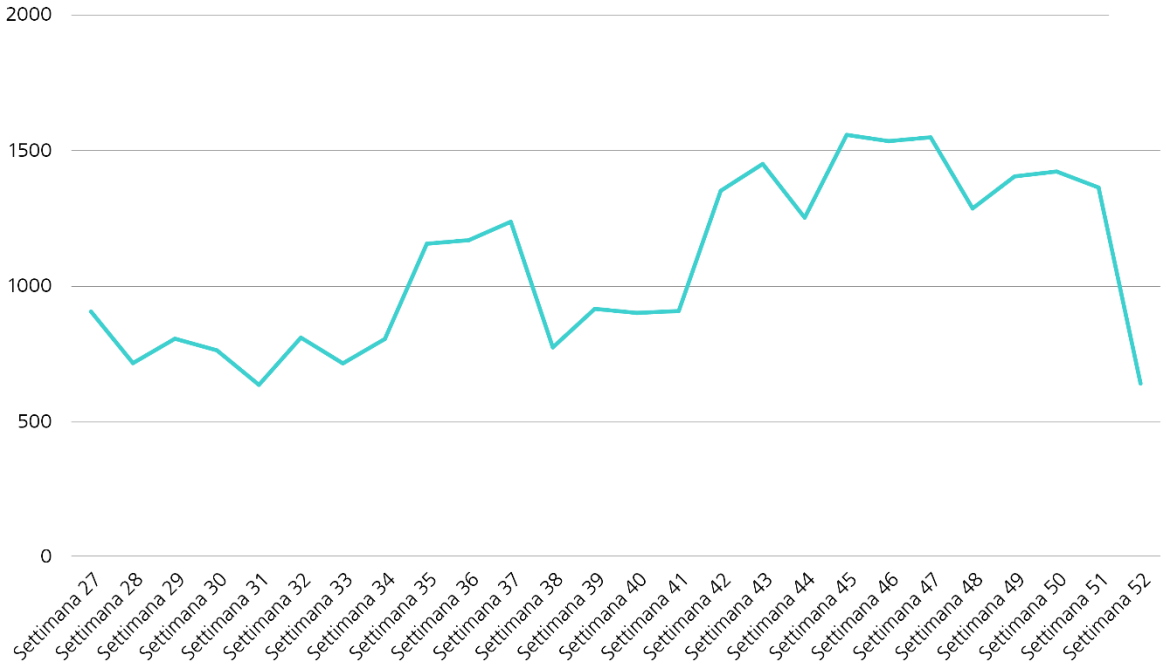

Fig. 1: Segnalazioni settimanali all'UFCS nel secondo semestre 2024, cfr. Numeri attuali (ncsc.admin.ch)

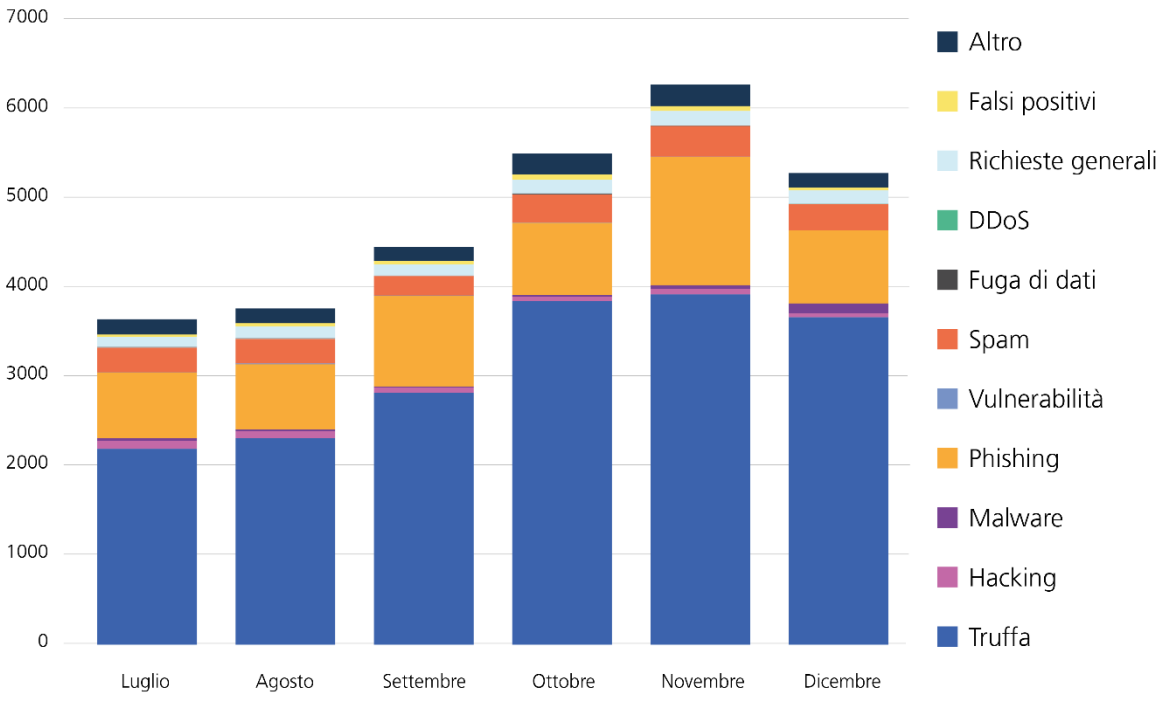

Fig. 2: Segnalazioni all'UFCS nel secondo semestre del 2024 per categoria, cfr. Numeri attuali (ncsc.admin.ch).

Il rapporto tra le segnalazioni provenienti da privati (90%) e quelle da parte di imprese, associazioni e autorità (10%) continua a mantenersi stabile. Tra i reati di frode segnalati più frequentemente dalle imprese, il fenomeno della «truffa del CEO»[10] segna un netto aumento, da 487 a 719 segnalazioni. Ad essere presi di mira, nel 2024, sono stati soprattutto i Comuni e le parrocchie (cfr. cap. 5.3). Per quanto riguarda il «ransomware», la tendenza in lieve diminuzione ha subito una battuta d'arresto. Mentre nel primo semestre erano stati segnalati 20 casi in meno, nel secondo semestre il numero di segnalazioni pervenute è tornato a crescere leggermente di tre unità rispetto allo stesso periodo dell'anno precedente, attestandosi a quota 48. Nel corso dell'anno, le segnalazioni di ransomware pervenute all'UFCS sono state 92. In generale, tuttavia, il numero di casi segnalati non consente di trarre conclusioni sull'entità dei danni. I collettivi di ransomware tendono a concentrarsi sempre più su obiettivi lucrativi, per cui è probabile che il danno atteso per singolo episodio aumenti in futuro. Inoltre, gli attacchi di ransomware sono quasi sempre associati a fughe di dati, il che non solo aggrava i danni per le imprese interessate, ma aumenta anche il rischio di effetti collaterali a carico di terzi, nel momento in cui le loro informazioni sono contenute nei set di dati trafugati.

Le statistiche evidenziano quanto la cibersicurezza e la protezione della Svizzera dai ciberrischi rappresentino una sfida costante per l'economia, lo Stato e la società. Il rapporto semestrale presenta pertanto i principali fenomeni che caratterizzano il panorama delle minacce nel ciberspazio in Svizzera e all'estero: «phishing»[11], «malware»[12], vulnerabilità[13], truffe e ingegneria sociale[14], attacchi alla disponibilità di siti e altri servizi Internet (DDoS)[15], perturbazioni dell'infrastruttura, fughe di dati, ciberspionaggio e sabotaggio. Grazie ai capitoli tematici i lettori possono farsi un'idea generale delle loro forme e declinazioni attuali, nonché di episodi e sviluppi interessanti. Nell'ottica della responsabilità individuale per una Svizzera digitale più sicura, il rapporto formula infine una serie di raccomandazioni per il pubblico su come affrontare queste sfide.

2 Phishing

Subito dopo la frode, i tentativi di phishing rappresentano i secondi ciberincidenti più segnalati all'UFCS. Si tratta di una tecnica con cui i cibercriminali si procurano dati d'accesso, informazioni finanziarie e altri dati riservati sottraendoli a ignari utenti. Una sua tipicità è il fatto che le vittime vengono raggirate con l'inganno (ingegneria sociale), senza utilizzare malware.[16] Sebbene il phishing continui a essere uno dei metodi più comunemente utilizzati per raggiungere un'ampia cerchia di destinatari via e-mail, esistono altri approcci che sfruttano la voce (voice phishing o vishing) o gli SMS (smishing) per raccogliere informazioni sensibili.

---

10 Truffa del CEO (ncsc.admin.ch)

11 Phishing, vishing, smishing (ncsc.admin.ch)

12 Software dannoso (ncsc.admin.ch)

13 Falla di sicurezza (ncsc.admin.ch)

14 Ingegneria sociale (ncsc.admin.ch)

15 Attacco DDoS - E adesso? (ncsc.admin.ch)

16 A livello internazionale il termine phishing non viene utilizzato in maniera univoca, per cui vi sono definizioni che spesso includono anche la diffusione di malware (cfr. Phishing (attack.mitre.org)). L'UFCS, invece, esclude esplicitamente questa dimensione dalla definizione utilizzata.

Nel 2024 l'UFCS ha ricevuto 12 038 segnalazioni di tentativi di phishing, 2 623 in più rispetto all'anno precedente. Pare tuttavia che dal secondo semestre il numero di segnalazioni in arrivo, a quota 5 395, si sia stabilizzato, seppur a un livello elevato. Diverso è invece il quadro che emerge a livello statistico dal punto di vista degli URL di phishing verificati e confermati dall'UFCS[17], dove si osserva un costante aumento a livello sia annuale[18] che semestrale. Se nel secondo semestre del 2023 si erano documentati 5 242 URL di phishing unici, nello stesso periodo del 2024 il loro numero era già raddoppiato a quota 9 355. L'andamento dettagliato a livello settimanale è illustrato alla figura 3. Per rendere i siti di phishing il più possibile affidabili, i criminali continuano ad attirare le loro vittime utilizzando illecitamente sulle loro pagine i nomi di marche e aziende note. Nel periodo in esame sono stati bersaglio di phishing soprattutto il settore finanziario (23%), i servizi postali (22%), i trasporti pubblici (22%), il settore informatico (11%) e le telecomunicazioni (8%). Queste percentuali sono rimaste relativamente costanti di mese in mese (cfr. fig. 4).

Oltre ai classici tentativi di phishing ai danni di operatori finanziari, la casistica ha riguardato come sempre l'invio di messaggi fraudolenti concernenti la consegna di un pacco e di e-mail su presunti rimborsi a nome di fornitori, delle FFS, di SwissPass e di varie amministrazioni delle contribuzioni. Nel periodo in esame i phisher hanno maggiormente tenuto conto di alcune peculiarità locali della Svizzera, spacciandosi ad esempio per la Cassa di compensazione AVS.[19] Continuano anche i tentativi di phishing ai danni di account Microsoft 365. La tecnica attualmente diffusa è l'invio di e-mail di phishing attraverso una sorta di catena di Sant'Antonio, il cosiddetto «chain phishing», con cui – una volta compromessa la casella di posta elettronica – si inviano istantaneamente messaggi di phishing a tutti i contatti della rubrica.

Oltre alle e-mail, un canale sempre più utilizzato per finalità di phishing sono i messaggi di testo. Da questo punto di vista, nel secondo semestre del 2024 l'UFCS ha osservato anche l'uso del sistema RCS o di iMessage da parte dei criminali. Il motivo potrebbe risiedere nel fatto che, dal 2022, i gestori di telefonia mobile Swisscom, Salt e Sunrise hanno implementato un filtro per gli SMS, per cui sono in grado di bloccare con maggiore efficienza anche eventuali SMS fraudolenti. Tramite RCS e iMessage, invece, i phisher riescono ad aggirare questi filtri e raggiungere comunque le loro potenziali vittime. Come in molti ambiti della cibersicurezza, anche in questo caso si evidenzia il classico gioco del gatto e del topo tra truffatori e operatori di servizi di sicurezza.

Mentre l'invio di e-mail e SMS di phishing è un attacco di massa e solo una minima parte di essi va a buon fine, quest'anno si sono ripetutamente registrati anche tentativi d'attacco mirati a gruppi specifici. Ne sono un esempio le telefonate da parte di sedicenti impiegati di banca di una presunta divisione antifrode, i tentativi di phishing ai danni di venditori su piattaforme di annunci o l'applicazione di codici QR sui parchimetri. Queste tre tecniche saranno oggetto di ulteriore approfondimento nei prossimi capitoli.

---

17 L'UFCS riceve segnalazioni di phishing non solo sotto forma di segnalazioni di casi concreti, ma anche tramite la piattaforma antiphishing.ch, che considera ulteriori fonti. Per tale motivo i numeri qui indicati potrebbero differire da quelli relativi alle segnalazioni dirette di phishing.

18 Un'analisi annuale dettagliata del fenomeno del phishing in Svizzera è riportata nel rapporto anti-phishing 2024.

19 Attenzione: e-mail di phishing a nome dell'AVS (ncsc.admin.ch)

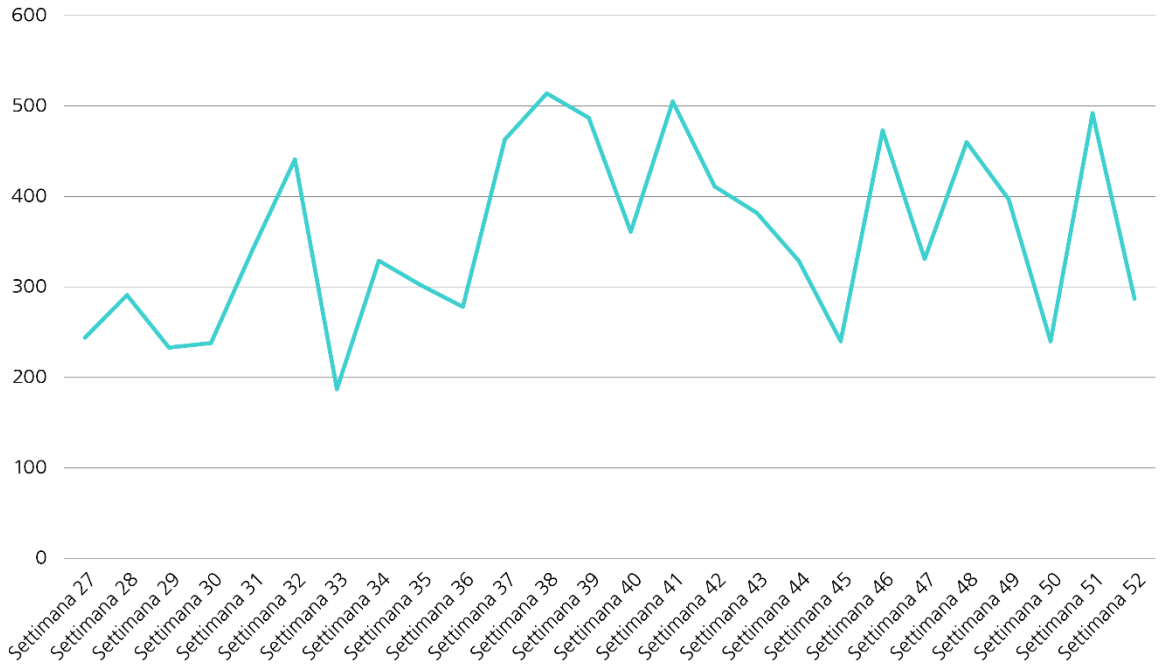

Fig. 3: Numero di URL di phishing verificati e confermati settimanalmente dall'UFCS nel secondo semestre 2024

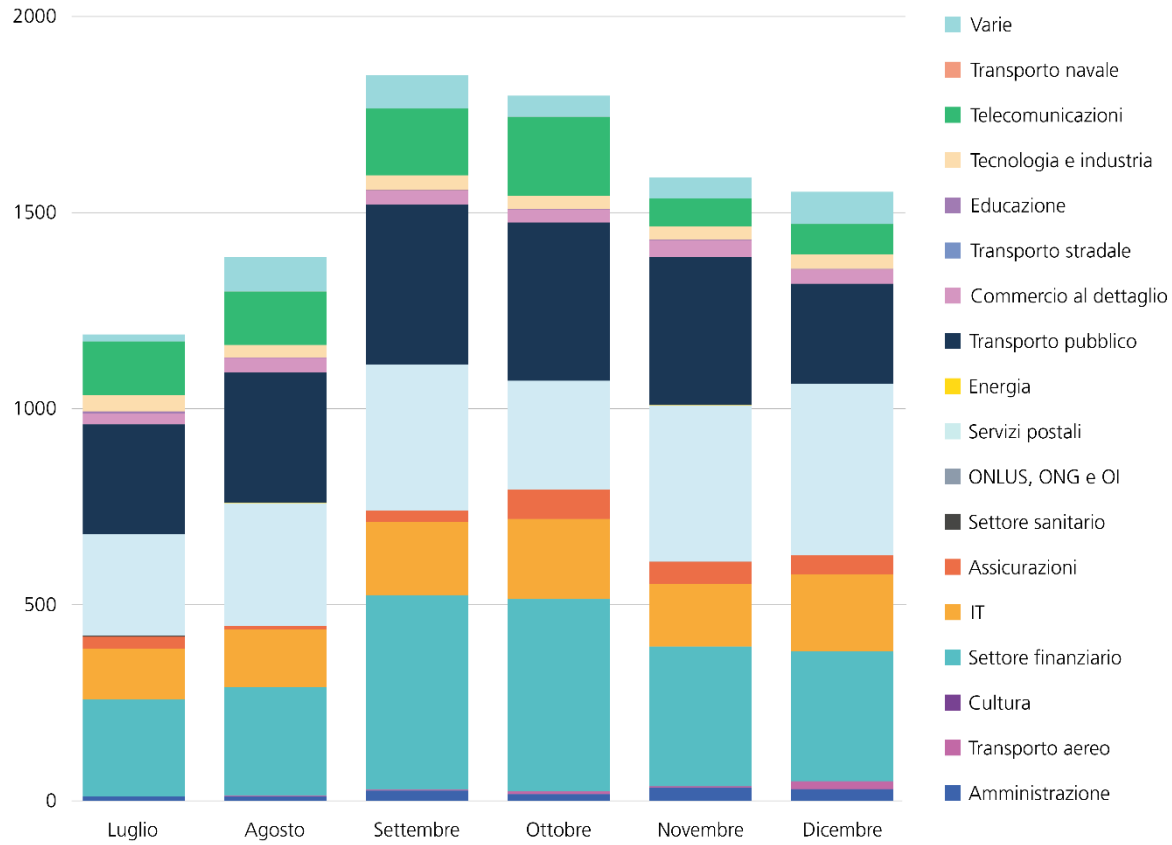

Fig. 4: Numero di URL di phishing verificati e confermati dall'UFCS nel secondo semestre 2024 per settori di marchi sfruttati

Raccomandazioni

Segnalate all'UFCS tentativi di phishing sospetti all'indirizzo reports@antiphishing.ch oppure direttamente sul sito antiphishing (antiphishing.ch). Se desiderate avere un riscontro, potete segnalare il caso di phishing ai nostri specialisti anche tramite l'apposito modulo di segnalazione o all'indirizzo incidents@ncsc.ch. Con il vostro aiuto l'UFCS può allertare in maniera mirata e adottare i provvedimenti del caso affinché questi siti vengano rimossi da Internet.

2.1 Telefonate da parte di presunti impiegati di banca

Nel periodo in esame diverse campagne di phishing hanno nuovamente preso di mira i clienti di varie banche svizzere, sia regionali che grandi istituti di credito. La peculiarità di questa campagna è stata la combinazione di diversi metodi per acquisire credibilità agli occhi delle vittime. Oltre all'impiego di strumenti tecnici, i criminali hanno fatto ricorso all'ingegneria sociale, spacciandosi ad es. per dipendenti di portali di pagamento come PayPal, per impiegati di banca o funzionari di polizia delle rispettive divisioni antifrode.

Le telefonate da parte di presunti impiegati di banca non sono una novità. Già negli anni intorno al 2010 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) aveva messo in guardia da simili attacchi di phishing. All'epoca, alle vittime veniva fatto credere che si dovesse effettuare un aggiornamento dell'e-banking, che successivamente avrebbe dovuto essere testato. I malcapitati venivano dunque convinti a installare un software di accesso remoto, con cui eseguire il presunto aggiornamento del servizio. Mediante un pagamento di prova si sarebbe infine verificata la funzionalità del sistema. Solo più tardi le vittime scoprivano che un importo di diverse migliaia di franchi era stato trasferito sul conto di un complice del truffatore.[20] Ma anche più di recente l'UFCS ha registrato ripetutamente chiamate di questo tipo. Sebbene la procedura di base sia rimasta invariata, nel frattempo i truffatori hanno modificato il loro pretesto. Nei casi attuali si spacciano ad esempio per un tale «Signor Bianchi» che lavora al reparto Sicurezza della banca e sostengono di voler bloccare un pagamento fraudolento. Sebbene il numero di telefono visualizzato corrisponda a quello ufficiale della banca che i truffatori dicono di rappresentare, in realtà si tratta di un numero falsificato mediante una tecnica detta «spoofing»[21]. Mentre in alcuni casi si cerca ancora di far credere che sia stato prelevato un importo per l'acquisto di un televisore a schermo piatto presso un negozio di elettronica, negli episodi più recenti il pretesto è generalmente un presunto addebito fraudolento di CHF 800. I truffatori consigliano alle vittime di chiamare immediatamente la divisione antifrode della Polizia cantonale, e comunicano loro anche il numero a cui telefonare. Per bloccare il pagamento fraudolento, alla vittima viene chiesto di installare un software di accesso remoto sul proprio computer e di autorizzare l'accesso sia al terminale che al conto bancario. Anziché bloccare il pagamento, anche in questo caso vengono prelevate somme illecitamente.

In altre varianti, oltre alla chiamata la vittima riceveva prima un SMS con un codice a quattro cifre che avrebbe dovuto comunicare alla presunta divisione antifrode a fini di verifica. Anche

20 Social Engineering: un nuovo metodo d'attacco orientato contro le imprese (ncsc.admin.ch)

21 Spoofing (ncsc.admin.ch)

in questo caso un sedicente impiegato di banca chiamava successivamente la vittima per assisterla con presunti problemi sul portale e-banking. A incrementare la fiducia era soprattutto la parlata in svizzero-tedesco priva di accento di certi truffatori, oltre a una serie di misure tecniche come ad esempio lo spoofing. Di conseguenza le vittime, credendo di parlare con un impiegato di banca, svelavano anche token di sicurezza come il loro secondo fattore di autenticazione, con cui i criminali si procuravano infine l'accesso all'e-banking dei malcapitati.

I criminali utilizzano questo tipo di tecniche per ottenere in tempo reale i dati d'accesso necessari, prima che questi perdano di validità. Se un'applicazione richiede un'autenticazione a due fattori (MFA), infatti, i truffatori possono effettuare l'accesso soltanto nell'esatto momento in cui la vittima svela i propri dati. Non è possibile utilizzare i dati trafugati in un momento successivo. Questo aspetto è ciò che contraddistingue simili attacchi di vishing da attacchi di phishing tradizionali, come il phishing di SwissPass o in parte anche il phishing con carte di credito, in cui i dati possono essere utilizzati anche in un secondo momento. In questi casi è sufficiente una semplice pagina statica di phishing.

Raccomandazioni

Attivate possibilmente sempre l'autenticazione a più fattori (MFA) come ulteriore meccanismo di sicurezza dei vostri account. Nonostante la MFA riduca enormemente il rischio di compromissione, la si può aggirare con varie tecniche di ingegneria sociale (social engineering)[22]. State dunque attenti alle richieste fasulle – soprattutto via e-mail e SMS – se vi si chiede di confermare accessi o trasmettere a qualcun altro il vostro token di sicurezza. Nessuna banca svizzera si farà mai dettare al telefono un token di sicurezza per verificare la propria clientela. Ricordate anche che i mittenti delle e-mail e i numeri di telefono possono essere facilmente falsificati.

2.2 Phishing tramite annunci

Gli annunci offrono ai truffatori molteplici possibilità d'attacco. Tra le classiche varianti si annoverano la vendita di prodotti inesistenti o il mancato pagamento di merce acquistata e già spedita. Parallelamente hanno preso piede forme di phishing rivolte contro i venditori: i truffatori fingono di mostrare interesse per un prodotto e spingono la vittima a effettuare la spedizione e il trasferimento di denaro tramite un servizio di corriere indicato dal presunto acquirente. Se la vittima acconsente, il sedicente corriere chiede il versamento di importi fittizi da effettuarsi mediante carta di credito. In questi casi gli aggressori mirano soprattutto ai dati della carta di credito. In alcuni casi segnalati all'UFCS si è però anche cercato di creare un account Twint con il numero di telefono della vittima. A quest'ultima veniva innanzitutto chiesto il numero di telefono e il numero del conto, dopodiché con queste informazioni veniva registrato un account Twint. A quel punto la vittima doveva connettersi a un sito su cui inserire il codice di sicurezza di Twint per confermare che il numero di telefono appartenesse effettivamente alla persona che intendeva aprire l'account.

22 Ingegneria sociale (ncsc.admin.ch)

Rispetto alle e-mail di phishing inviate in massa senza indicazioni specifiche, in cui i mittenti sperano che il testo generico faccia cadere in trappola le vittime, negli ultimi episodi osservati i phisher si danno parecchio da fare con una comunicazione diretta e personalizzata con la vittima, adattando il loro scenario alle circostanze del momento. Tra questi casi di phishing, infatti, si riscontrano continuamente tentativi di frode in svizzero tedesco.

Raccomandazioni

Siate cauti nei confronti delle richieste avanzate dagli acquirenti. Insistete sul fatto che le spese amministrative e di spedizione siano pagate dall'acquirente. Scrivetelo esplicitamente anche nell'annuncio.

2.3 Phishing sulle tariffe del parcheggio con falsi codici QR

Le possibilità di pagare il parcheggio online stanno diventando sempre più diffuse tra la popolazione. Le moderne soluzioni di pagamento consentono agli utenti di pagare rapidamente e in maniera efficiente le tariffe del parcheggio tramite varie piattaforme, come app per cellulari, siti web o appositi parchimetri. Di solito utilizzano codici QR per una procedura di pagamento intuitiva.

Questa semplificazione cela tuttavia anche una serie di rischi. Nel periodo in esame, in varie città svizzere i veri codici QR disponibili ai parcheggi sono stati in più casi nascosti incollandovi sopra dei codici manipolati. Se utilizzati, questi ultimi reindirizzavano le vittime a un sito web di pagamento illecito, ma dall'aspetto realistico, sul quale si poteva scegliere se pagare con Twint o con carta di credito.

Fig. 5: Codice QR incollato sopra quello reale su un parchimetro

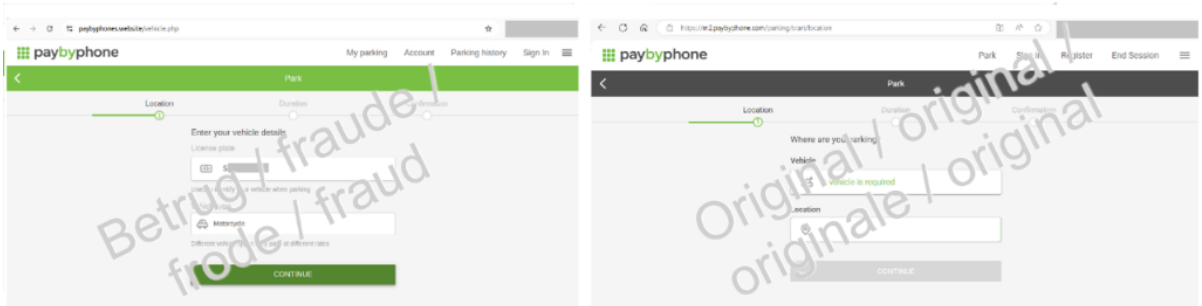

Fig. 6: Sito internet fraudolento, ma apparentemente reale (a sinistra). Solo dall'indirizzo Internet si capisce che non si tratta del sito corretto

Visto che solitamente si è di fretta quando si cerca un parcheggio, è difficile che si controllino i dettagli del pagamento, come l'importo addebitato o il destinatario. Una volta autorizzata l'operazione, svariate centinaia di franchi vengono presto accreditate su un conto fraudolento.

Rispetto ai classici metodi di phishing, in questa variante il truffatore o il suo complice deve essere in loco per applicare l'adesivo, correndo il rischio di essere colto in flagrante. La cosa sorprendente è che questi tentativi non sono stati compiuti una sola volta. Dopo che le frodi

erano state scoperte e gli adesivi rimossi, in alcuni casi non è passato molto tempo prima che i truffatori ne incollassero di nuovi.

Raccomandazioni

Prima di scansionare un codice QR fisico e pubblico, osservatelo e toccatelo per assicurarvi che non si tratti di un adesivo. Accertatevi che l'indirizzo Internet (URL) richiesto corrisponda a quello previsto. Osservatelo con attenzione. Le differenze possono essere minime. Interrompete il processo di pagamento se notate incongruenze.

3 Malware

Per insinuarsi in un dispositivo o in una rete, il software dannoso (il cosiddetto «malware») continua a essere uno degli strumenti principali utilizzati dai cibercriminali. Il capitolo 3.1 spiega l'uso del malware per infettare i sistemi a livello di primo accesso. A finire sotto i riflettori sono stati, in particolare, i tentativi di diffusione di malware con presunti nomi di assicuratori malattie e società di recupero crediti nazionali. L'UFCS ha osservato inoltre l'uso di nuove tecniche che, attraverso «CAPTCHA»[23] fasulli, vogliono indurre i potenziali obiettivi a infettarsi da sé eseguendo codici di programmi dannosi. Per buona parte delle imprese il ransomware continua a rappresentare la minaccia maggiore. Il capitolo 3.2 esamina alcuni episodi avvenuti in Svizzera e gli sviluppi rilevanti di questo fenomeno. Da ultimo il capitolo 3.3 illustra una campagna che, tramite codici QR applicati sulla classica corrispondenza postale, cerca di indurre i destinatari a installare un'app di Android infettata con un malware.

3.1 Accesso iniziale con malware

Per compromettere i sistemi informatici, i cibercriminali utilizzano spesso il malware come porta d'accesso. In molti casi questi attacchi sono accompagnati da cosiddette tecniche di ingegneria sociale, il cui scopo è indurre gli utenti a compiere determinate azioni, come ad esempio l'esecuzione dei malware summenzionati. Qui di seguito vengono illustrate le principali tendenze riguardanti il primo accesso con malware e le relative tecniche di ingegneria sociale riscontrate nella seconda metà del 2024, con particolare attenzione agli sviluppi in Svizzera.

Nel periodo in esame, in Svizzera sono stati registrati numerosi tentativi di infettare i sistemi con malware come «Agent Tesla», «SnakeKeyLogger», «Formbook», «Lumma Stealer», «Vidar Stealer», «Strela Stealer» o il mobile malware «Coper/Octo2». La maggior parte di queste campagne di diffusione non presentava caratteristiche specifiche per la Svizzera. Il modus operandi non si discostava dallo schema internazionale, il che fa pensare a un approccio opportunistico dei criminali, il cui obiettivo è infettare i sistemi senza una selezione mirata a monte. Due campagne registrate a novembre 2024 hanno tuttavia evidenziato alcuni tratti specifici per la Svizzera: la distribuzione del mobile malware Coper/Octo2 tramite invio

[23] Richiesta in moduli online in cui bisogna confermare di essere una persona e non un robot. In questi cosiddetti CAPTCHA bisogna ad esempio svolgere calcoli o selezionare i riquadri di un'immagine dove sono presenti animali, auto, ponti ecc.

postale fisico con un link che rimandava al malware, in cui si è abusato dell'identità aziendale di MeteoSvizzera (cfr. cap. 3.3), e una campagna e-mail in cui è stato sfruttato il nome di diverse aziende svizzere per diffondere Lumma Stealer.

All'UFCS sono pervenute numerose segnalazioni di e-mail sospette, apparentemente provenienti da una società di recupero crediti svizzera o da una cassa malati svizzera. Questi messaggi fanno riferimento a un accredito o un sollecito di pagamento fittizio, invitando il destinatario a cliccare su un link per visualizzare la fattura. Una volta cliccato, viene scaricato un file di collegamento malevolo che, se eseguito su un sistema Windows, attiva uno script. Questo script avvia un primo loader, che varie aziende di sicurezza informatica chiamano «Emmenhtal»[24] o «PEAKLIGHT»[25]. A quel punto viene installato un trojan del tipo Lumma Stealer per il furto delle informazioni («Infostealer»), che raccoglie e invia dati sensibili come credenziali di login, cookie del browser o anche wallet per criptovalute.[26]

In Svizzera sono state osservate anche altre campagne di distribuzione di Lumma Stealer, ma effettuate secondo i metodi comunemente utilizzati a livello internazionale. Uno di questi, noto come «ClickFix», si riscontra sempre più spesso negli ultimi tempi. Consiste nell'ingannare i malcapitati con un CAPTCHA fasullo, che in realtà serve a distinguere tra utenti reali e automatizzati. Cliccando sul pulsante «Non sono un robot», il codice malevolo viene copiato negli appunti e il sito chiede alla vittima di premere la combinazione di tasti «Windows + R», «Ctrl + V» ed «Enter» per terminare la verifica.[27] In realtà questa operazione avvia l'esecuzione di uno script dannoso e l'installazione del malware. Questo metodo, con cui gli utenti eseguono a loro insaputa un codice malevolo, sembra essere molto efficace, essendo state osservate molte varianti che distribuiscono diverse tipologie di malware. Vari canali YouTube, ad esempio, sono stati compromessi o creati appositamente per pubblicare istruzioni fasulle con cui indurre gli utenti a eseguire codici dannosi. In tal caso il pretesto è che questo codice serve a soddisfare una determinata richiesta, ad esempio relativa a criptovalute, licenze software o problemi informatici.[28]

Un altro caso degno di nota in Svizzera ha riguardato uno sviluppatore contattato via LinkedIn. Con il pretesto di un'offerta di lavoro, il malcapitato si è ritrovato con un software da scaricare e installare, ma in realtà si trattava di un malware, il cui obiettivo era rubare dati soprattutto legati al mondo delle criptovalute. A livello internazionale vari operatori nel campo della sicurezza hanno riferito di campagne simili. Questo caso specifico fa probabilmente parte di una campagna internazionale denominata «Contagious Interview», che si rivolgeva specificatamente a sviluppatori informatici via LinkedIn e il cui obiettivo consisteva nell'indurli a installare un malware durante il processo di candidatura.[29] Ciò avveniva, ad esempio, nascondendo il codice malevolo all'interno di un programma che avrebbe dovuto essere sottoposto a un debug, oppure in un installer per il software di videoconferenza necessario per il colloquio di presentazione. In una campagna affine, inoltre, gli aggressori sono riusciti a diffondere sulla piattaforma NPM (Node Package Manager) le copie infette di pacchetti software legali. NPM

---

24 Emmenhtal: A little-known loader distributing commodity infostealers worldwide (orangecyberdefense.com)
25 PEAKLIGHT: Decoding the Stealthy Memory-Only Malware (google.com)
26 Email con malware a nome di società di recupero crediti e di casse malati (ncsc.admin.ch)
27 Quando il malware si nasconde dietro CAPTCHA fraudolenti e presunti aggiornamenti (ncsc.admin.ch)
28 Your Data Is Under New Lummanagement: The Rise of LummaStealer (cybereason.com)
29 Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers (paloaltonetworks.com)

è una piattaforma che consente ai programmatori di condividere cosiddette «librerie» o «pacchetti» da utilizzare per lo sviluppo di programmi. I malfattori sfruttano la fiducia in queste piattaforme per pubblicare copie apparentemente autentiche con nomi simili a quelli originali.[30] In un caso particolarmente sofisticato osservato a fine anno, gli aggressori sono persino riusciti a introdurre un codice malevolo negli aggiornamenti di due pacchetti originali, per cui, una volta installata la versione corrotta di questi pacchetti, i sistemi venivano infettati con il software di mining di criptovalute «XMRig».[31]

Questi casi rappresentano soltanto una piccola parte dei numerosi malware e metodi di attacco utilizzati dai cibercriminali. Affinché la loro attività sia redditizia, questi ultimi devono ottenere un profitto che dipende fondamentalmente da due variabili l'investimento richiesto e il guadagno atteso. Sinora lo sviluppo dell'intelligenza artificiale (IA) non ha avuto un impatto dirompente sull'evoluzione di queste minacce. Si riscontra tuttavia una crescente integrazione dell'IA da parte dei criminali[32] per ottimizzare determinate attività e compensare eventuali deficit, riducendo così l'impegno necessario. La diffusione sempre maggiore delle criptovalute e la loro conservazione su dispositivi privati favorisce la redditività di questi attacchi, per cui si prevede che tali minacce rimarranno un mezzo efficace anche in futuro.

Raccomandazioni

Nei messaggi sospetti non cliccate su link, non aprite file allegati e non scannerizzate codici QR. In caso di dubbio, chiedete al presunto mittente tramite altri canali se ha effettivamente inviato il messaggio in questione.

Quando cercate un software su Internet, prima di scaricarlo verificate di essere sui siti web dei produttori o su un altro sito affidabile – ad esempio una nota rivista di informatica. Quando utilizzate i motori di ricerca, in particolare, controllate se il sito visualizzato è dichiarato come pubblicità a pagamento oppure no. Se si tratta di pubblicità a pagamento, fate attenzione, dal momento che gli aggressori ricorrono spesso a questo metodo per comparire tra i primi risultati di ricerca.

Siate sempre prudenti quando aprite una finestra di download.

Se possibile, impostate sempre la funzione di aggiornamento automatico dei programmi. In alternativa, utilizzate 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.

30 Tenacious Pungsan: A DPRK threat actor linked to Contagious Interview (datadoghq.com)

31 Supply Chain Attack on Rspack npm Packages Injects Cryptojacking Malware (socket.dev)

32 Cfr. Rapporto semestrale 2024/1, cap. 5.1.

3.2 Ransomware

Questo sottocapitolo illustra la situazione attuale sul fronte dei ransomware. Si tratta di un tipo di attacco in cui i cibercriminali criptano, mediante un malware, i dati presenti sui sistemi informatici della vittima, rendendoli inutilizzabili per quest'ultima[33]. In genere i dati vengono contemporaneamente esfiltrati. A seguire chiedono alla vittima il pagamento di un riscatto, Se la vittima paga, i criminali promettono di fornire uno strumento di decodifica (decryptor) e di non diffondere i dati rubati. Il rapporto fornisce innanzitutto un aggiornamento per quanto riguarda la Svizzera, dopodiché evidenzia i casi e le tendenze a livello internazionale.

3.2.1 Attività ransomware in Svizzera

In generale, dopo lo smantellamento di grandi collettivi di ransomware come «LockBit» e «ALPHV» nella prima metà del 2024, alcuni degli sviluppatori e complici dei gruppi di ransomware hanno dovuto cercare altre alleanze. Questa dinamica ha comportato un aumento della concorrenza, dal momento che altri gruppi (come «RansomHub»[34], «Akira», «BlackCat» e «Play»[35]) hanno cercato di convincere questi operatori esperti a instaurare una collaborazione, offrendo loro condizioni più allettanti. Come si vedrà nel prossimo paragrafo relativo agli incidenti in Svizzera, alcuni nomi noti nel mondo del ransomware, come Akira, LockBit e «INC Ransom», figurano in cima alla lista anche tra gli episodi registrati nel Paese.

Il fenomeno ransomware ha interrotto secondo le statistiche la tendenza leggermente al ribasso degli ultimi anni. Mentre nel primo semestre erano stati segnalati 20 casi in meno, nel secondo semestre il numero di segnalazioni pervenute è tornato a crescere leggermente di tre unità rispetto allo stesso periodo dell'anno precedente, attestandosi a 48 casi. Nell'arco del 2024 le segnalazioni sono pertanto diminuite rispetto all'anno precedente di 17 unità, passando da 109 a 92. Si conferma stabile la tendenza che vede il ransomware colpire perlopiù il mondo delle imprese[36]. I casi di ransomware ai danni di privati - in particolare contro i loro dispositivi NAS - sono diminuiti in modo significativo nel secondo semestre. Sono soltanto otto gli episodi che hanno avuto come vittime cittadini privati.
Se si considerano i collettivi di ransomware segnalati più di frequente (cfr. fig. 7), spicca soprattutto Akira, che con 15 casi, il doppio rispetto alla seconda variante di ransomware più diffusa, LockBit. Akira si caratterizza per un comportamento opportunistico e aggressivo, già osservabile nella prima metà del 2024. Ciò si traduce in un numero relativamente elevato di vittime, che coinvolgono diversi settori e aziende di varie dimensioni. Sebbene LockBit sia stato frenato dall'operazione di polizia «Cronos» a metà febbraio 2024, rimane ancora una delle varianti di ransomware più segnalate in Svizzera. Nel corso dell'operazione di polizia, le forze dell'ordine hanno preso il controllo e distrutto le infrastrutture di LockBit, frammentando la rete dei partecipanti e mettendo a disposizione delle vittime strumenti di decodifica gratuiti. Ciononostante, l'attività del ransomware rimane a un livello stabile, come sottolinea il gruppo LockBit con un annuncio di una nuova versione – «LockBit 4.0» – previsto per febbraio 2025

---

33 Ransomware (ncsc.admin.ch)

34 RansomHub Overtakes LockBit as Most Prolific Ransomware Group (infosecurity-magazine.com)

35 Play & LockBit Ransomware Join Hands to Launch Cyber Attacks (gbhackers.com)

36 Cfr. Rapporto semestrale 2024/1; cap. 3.2.1.

nel dicembre 2024.[37] Questa quarta versione era già stata annunciata a inizio 2024 prima dell'intervento della polizia.
Al terzo posto segue il ransomware INC Ransom, con quattro casi segnalati, mentre il resto della classifica si divide tra 14 diverse famiglie di ransomware. A parte alcuni grandi collettivi, l'attività è distribuita su molti gruppi, tra cui anche quelli più piccoli, il che indica uno sviluppo verso un approccio più modulare e decentralizzato. I grandi gruppi di ransomware hanno quindi ceduto il passo a molti piccoli gruppi in cui gli autori degli attacchi ransomware operano alternativamente o contemporaneamente per diverse operazioni.[38]

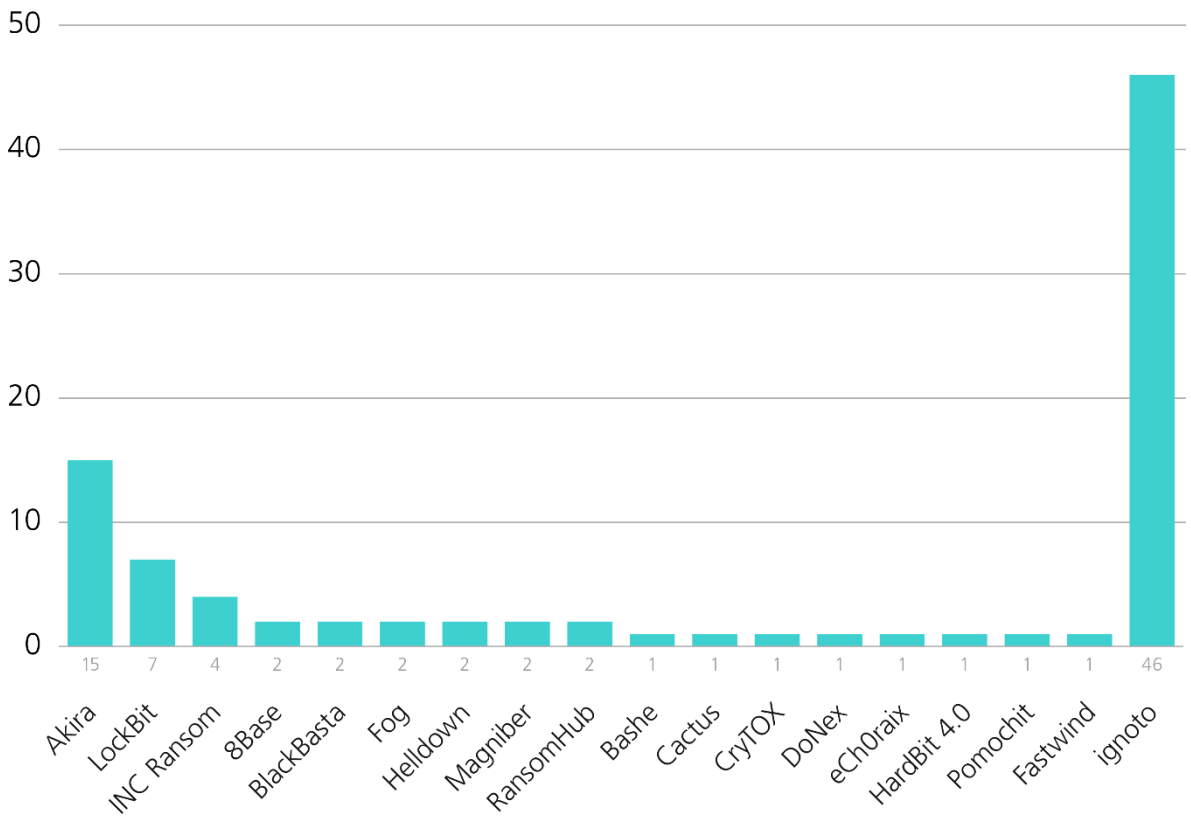

Fig. 7: Numero di casi di ransomware segnalati all'UFCS nel secondo semestre del 2024

Nuova variante di ransomware

Tra le nuove famiglie di ransomware osservate dall'UFCS in Svizzera si annoverano[39]: «RansomHub», «INC Ransom», «Fog», «Helldown», «Pomochit» e «Cicada». Sebbene queste varianti di ransomware siano considerate nuove, presentano , spesso, somiglianze con malware già esistenti, come nel caso di Cicada.[40] Nel caso della variante Helldown comparsa sul finire

37 LockBit Admins Tease a New Ransomware Version (infosecurity-magazine.com)
38 Cfr. rapporto semestrale 2024/1; conclusioni nel cap. 3.2.
39 Neue Ransomware-Banden zielen auch auf Schweizer Firmen (inside-it.ch)
40 Cicada 3301 – Ransomware-as-a-Service – Technical Analysis (truesec.com)

dell'estate, l'omonimo gruppo ha attaccato un operatore di servizi informatici svizzero, sottraendogli 67 GB di dati.[41] Helldown è ancora poco conosciuto e agisce principalmente sfruttando le vulnerabilità per infiltrarsi nelle reti delle vittime e installare il ransomware, in parte derivato dal codice di «LockBit 3.0». Il gruppo si fece notare per la prima volta dopo la diffusione su larga scala di una vulnerabilità nei prodotti Zyxel.[42]
RansomHub è un fornitore di «Ransomware-as-a-Service (RaaS) » comparso nel febbraio del 2024, che annovera nei suoi ranghi ex utenti di ALPHV e LockBit. Dal febbraio del 2024 sono già oltre 210 le vittime attribuite a RansomHub, tra cui anche almeno tre dalla Svizzera: uno studio di architettura d'interni della Svizzera romanda, un'impresa industriale del Canton Zurigo e un'impresa di software del Canton Berna[43]. Il ransomware prende di mira spazi di archiviazione non correttamente configurati sul cloud e backup. Secondo un'analisi a cura della CISA (US Cybersecurity and Infrastructure Security Agency), anche alcune infrastrutture critiche sono nel mirino di RansomHub.[44]
Tra le vittime del malware INC Ransom[45], attivo da luglio 2023, figuravano già la sanità, il settore finanziario, almeno un'associazione e diverse PMI. Il primo accesso può variare nel caso di questo software, con modalità che spaziano dallo spear phishing via e-mail allo sfruttamento di vulnerabilità.

Attività di varianti di ransomware già note

Nel semestre in esame si sono registrati attacchi anche da parte di ransomware già noti, come Akira o Play, che hanno preso di mira i settori dell'industria, degli immobili, dell'istruzione, dei servizi e del commercio, della finanza e il mondo delle PMI. Nel caso di Play la vittima è stata un gestore patrimoniale. Un quarto dei clienti menzionati nei dati trafugati erano clienti ad alto rischio o politicamente esposti di diversi paesi.[46] Questo caso dimostra che la pubblicazione di dati personali sensibili non solo comporta rischi per l'azienda stessa, ma può anche costituire un pericolo per le persone private menzionate nei dati.

Raccomandazioni

Sul sito web dell'UFCS è disponibile un elenco di misure preventive per proteggersi dai ransomware, insieme a istruzioni da seguire in caso di incidente.

3.2.2 Il ransomware come sfida globale

Tecniche diversificate vengono utilizzate nei tentativi di attacco

Il cambio di dinamica nell'ecosistema che circonda il ransomware ha costretto alcuni gruppi di ransomware a diventare più flessibili e a evolversi dal punto di vista tecnico e tattico. Il gruppo ransomware «Black Basta», già oggetto di discussione nella prima metà del 2024, ne è un

41 Ransomware-Angriff auf Schweizer IT-Dienstleister (inside-it.ch)
42 Helldown Ransomware: an overview of this emerging threat (sekoia.io)
43 Aufstrebende Ransomware-Bande attackiert Schweizer Software-Firma (inside-it.ch)
44 #StopRansomware: RansomHub Ransomware (cisa.gov)
45 Ransomware Spotlight: INC (trendmicro.com)
46 Boreal Capital: Hacker erbeuten Daten von Vermögensverwalter (tagesanzeiger.ch)

esempio.[47] Il gruppo, noto per la selezione di obiettivi di alto profilo, ha utilizzato diverse tecniche per le campagne di distribuzione del proprio ransomware nuovi e/o versatili metodi di infezione.[48] Ciò includeva, tra le altre cose:

- E-mail bombing: gli aggressori inondano le caselle e-mail delle vittime con migliaia di messaggi spam per sovraccaricare gli account di posta elettronica dei destinatari o nascondere altre attività illecite.
- Assistenza fittizia: servendosi di account Microsoft 365 compromessi, gli aggressori inviano messaggi o effettuano chiamate tramite la piattaforma di collaborazione Teams, spacciandosi per l'assistenza tecnica dell'organizzazione e inducendo le vittime a scaricare software di monitoraggio e assistenza da remoto (RMM: Remote Monitoring and Management) o inviando loro codici QR malevoli per avere accesso all'ambiente informatico desiderato.
  Una variante dell'assistenza fittizia consiste nel richiedere l'accesso remoto al dispositivo della vittima, anziché indurre quest'ultima a scaricare da sé il contenuto dannoso. Grazie alle funzioni presenti in Microsoft Quick Assist o nella condivisione del controllo in Teams, gli aggressori assumono il controllo del dispositivo della vittima e alla fine, se riescono a ottenere i diritti di amministratore, installano il ransomware.

L'ultima tecnica di distribuzione di Black Basta in ordine di tempo, via Teams tramite codice QR, è stata utilizzata anche ai danni di aziende svizzere.[49] Un motivo del passaggio a questo nuovo metodo di attacco potrebbe essere stato lo smantellamento della botnet «Qakbot» nel 2023, che ha reso necessarie nuove partnership con i procacciatori di primi accessi e nuovi tool personalizzati.[50]
Questa capacità di adattamento e la volontà di diversificare e ottimizzare le proprie operazioni sono emerse anche in altri gruppi come Akira,[51] ora focalizzato prevalentemente sul furto di dati. A monte di questo tipo di attacco gli aggressori effettuano una preselezione e una classificazione dei dati raccolti[52] attraverso una ricerca mirata al fine di estrapolare preziose informazioni sensibili, tra cui ad esempio dati finanziari, cartelle di personale e pazienti, documenti classificati, dati relativi a tecnologie informatiche e reti utilizzate e altri dati degni di particolare protezione.

Tendenze tra le vittime e gli attori di minacce

Secondo uno studio condotto da Semperis nel 2024, le vittime che pagano il riscatto sono più numerose di quanto si pensi.[53] Tra i motivi principali, la necessità di riprendere l'operatività il più rapidamente possibile, la protezione dei dati di pazienti, clienti o aziende o il rischio di danni reputazionali. Un'altra argomentazione è stata l'assicurazione Cyber che ha coperto i costi.

---

47 Cfr. Rapporto semestrale 2024/1; cap. 3.2.1.

48 Sophos MDR tracks two ransomware campaigns using "email bombing," Microsoft Teams "vishing" (sophos.com), ReliaQuest Uncovers New Black Basta Social Engineering Technique (reliaquest.com)

49 Settimana 44: «Black Basta» - Lo spam al servizio della cifratura: variante di attacco sofisticata alle aziende (ncsc.admin.ch)

50 UNC4393 Goes Gently into the SILENTNIGHT (cloud.google.com)

51 Akira ransomware continues to evolve (talosintelligence.com)

52 Ransomware-driven data exfiltration: techniques and implications (sekoia.io)

53 Rapporto sul rischio ransomware (semperis.com)

Raccomandazioni

In generale, l'UFCS e i suoi partner internazionali[54] sconsigliano alle vittime di ransomware di pagare il riscatto. Non vi è alcuna garanzia che i criminali informatici mantengano la parola data. Con il pagamento del riscatto, i criminali informatici ricevono un sostegno finanziario che consente loro di ampliare le proprie strutture e sferrare ulteriori attacchi.

Un'altra tendenza internazionale osservata nel semestre in esame è l'utilizzo del ransomware da parte di cibercriminali spinti da motivazioni non esclusivamente di natura finanziaria. Secondo Microsoft, attori del ciberspionaggio strettamente legati a uno Stato utilizzano il ransomware come ultima fase delle loro operazioni per ottenere vantaggi finanziari, provocare disservizi, distrazioni, falsificare l'attribuzione di prove o ottenerne la cancellazione.[55] È presumibilmente il caso del gruppo cinese «ChamelGang»[56] e di vari collettivi nordcoreani, iraniani o russi[57]. Per quanto riguarda la Corea del Nord, da un rapporto di ricerca emerge una collaborazione tra lo Stato e alcuni membri del gruppo Play.[58]

Alcuni gruppi di hacktivisti, come ad esempio il collettivo «CyberVolk» avente presunti legami con l'India, si servono ora del ransomware anche per attaccare istituzioni statali e pubbliche in Paesi che perseguono altri interessi.[59] Al contrario determinati gruppi mossi da intenti finanziari, come «FunkSec»[60], praticano l'haktivismo.

Sfruttamento di vulnerabilità negli attacchi ransomware

Lo sfruttamento delle vulnerabilità nei sistemi di autenticazione e accesso remoto è una tecnica molto diffusa come primo accesso negli attacchi ransomware (cfr. anche cap. 4).[61] Le vulnerabilità sfruttate, inoltre, sono spesso zero-day, ossia ancora sconosciute. In questo caso le vittime vengono raramente selezionate in modo mirato dai cibercriminali, che tendono piuttosto a scandagliare Internet alla ricerca di reti private virtuali (VPN) e firewall vulnerabili con interfacce di gestione accessibili pubblicamente sul web. Fungendo da punto di accesso alle reti interne, queste soluzioni diventano spesso una porta d'ingresso per attacchi ransomware. I criminali agiscono pertanto in modo opportunistico, senza prendere di mira un settore specifico, ma non appena hanno individuato una potenziale vittima, concentrano tutti i loro sforzi su di essa. Nel semestre in esame è emerso chiaramente che gli autori di ransomware hanno

54 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)
55 Microsoft Digital Defense Report 2024 (microsoft.com)
56 ChamelGang | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware (sentinalone.com)
57 Escalating Cyber Threats Demand Stronger Global Defense and Cooperation (microsoft.com)
58 Jumpy Pisces Engages in Play Ransomware (unit42.paloaltonetworks.com)
59 'CyberVolk' hacktivists use ransomware in support of Russian interests (therecord.media)
60 FunkSec – Alleged Top Ransomware Group Powered by AI (checkpoint.com)
61 Dragos Industrial Ransomware Analysis: Q3 2024 (dragos.com)

sfruttato diverse vulnerabilità per le loro attività. Tra queste figuravano varianti di ransomware consolidate e più recenti come Akira, Black Basta, Fog, Helldown, ma anche LockBit.[62]

Oltre allo sfruttamento delle vulnerabilità, le aziende sono particolarmente insidiate sul fronte della loro catena di fornitura. Il rischio deriva il più delle volte dalle conseguenze che l'azienda si ritrova ad affrontare a seguito di un incidente con un partner esterno o un subappaltatore. La catena di fornitura è spesso complessa, il che rende più difficile l'implementazione delle misure di cibersicurezza. L'industria manifatturiera[63], ad esempio, è considerata particolarmente esposta a causa della complessità dei sistemi e degli impianti connessi a Internet.

Il bilancio al termine del secondo semestre 2024 vede un numero superiore di gruppi, ma inferiore di famiglie di ransomware e un aumento degli attacchi a livello globale[64], il che si riflette anche nel numero crescente di fughe di dati e di siti web su cui vengono offerti. A ciò si aggiunge il fatto che l'impiego sempre più massiccio dell'IA consente a nuovi cibercriminali, come FunkSec, di accedere ancora più facilmente a un maggior numero di potenziali obiettivi.

In Europa e in Svizzera si stanno intensificando gli sforzi a livello legislativo per migliorare la preparazione, l'individuazione e la reazione agli incidenti di cibersicurezza, ad esempio con il «Cyber Solidarity Act» per il settore sanitario nell'Unione europea[65], il «Cyber Security and Resilience Bill» nel Regno Unito[66] e l'ordinanza sulla cibersicurezza (OCS) in Svizzera[67].

Raccomandazioni

L'accesso remoto dev'essere protetto in modo adeguato. Per ogni servizio raggiungibile via Internet andrebbe impostata un'autenticazione a due fattori. Se non è possibile, l'accesso andrebbe limitato a indirizzi IP e porte specifici e dovrebbe essere predisposto un presidio adeguato.

I protocolli di accesso remoto devono essere monitorati onde individuare eventuali schemi d'accesso atipici, in particolare accessi da regioni in cui l'azienda non ha dipendenti, da intervalli IP assegnati a grandi fornitori di hosting, da endpoint VPN noti o dalla rete TOR.

È inoltre importante definire una gestione regolare delle patch per correggere le vulnerabilità in modo tempestivo e verificarle con apposite scansioni. Gli aggiornamenti che eliminano eventuali lacune critiche in materia di sicurezza nei sistemi raggiungibili via Internet dovrebbero poter essere installati nell'arco di 24 ore. I software o i sistemi che non sono più supportati

62 VMware ESXi (CVE-2024-37085) per l'installazione, ad esempio, del Ransomware Akira, Black Basta und LockBit
Veeam Backup & Replication (CVE-2024-40711) e SonicWall SonicOS (CVE-2024-40766) per l'installazione di Akira und Fog
Zywall Zyxel (CVE-2024-11667) per l'installazione di Helldown, cfr. cap. 3.2.1.
Windows Error Reporting Service (CVE-2024-26169) per l'installazione di Black Basta

63 Manufacturing Cyber Risk Report 2024 (blackkite.com)

64 2024-rapid7-ransomware-radar-report (rapid7.com)

65 The EU Cyber Solidarity Act (ec.europa.eu)

66 Cyber Security and Resilience Bill (gov.uk)

67 Il Consiglio federale avvia la procedura di consultazione relativa all'ordinanza sulla cibersicurezza (news.admin.ch)[68] Attenzione: false lettere a nome di MeteoSvizzera - il codice QR scarica un malware invece di un'app d'allerta meteo (ncsc.admin.ch)

dal produttore («End of Life», EOL) dovrebbero essere disattivati o – se possibile – trasferiti in una partizione di rete separata e isolata.

3.3 Malware su dispositivi mobili

Nel novembre 2024 L'UFCS, l'Ufficio federale di meteorologia e climatologia (MeteoSvizzera) e l'Ufficio federale della protezione della popolazione (UFPP) hanno ricevuto segnalazioni relative a lettere cartacee sospette, apparentemente provenienti dall'Ufficio federale di meteorologia e climatologia. Si trattava di lettere false, spedite da truffatori che cercavano di far scaricare software dannosi sugli smartphone.
Nella lettera i destinatari venivano esortati a installare una nuova «app d'allerta meteo», ma non esiste un'app della Confederazione con quel nome. Il codice QR presente nella lettera porta invece al download di un malware denominato «Coper» (noto anche come «Octo2»). Una volta installata la presunta app d'allerta meteo, il malware cerca di rubare dati sensibili, ad esempio i dati d'accesso a oltre 383 app per smartphone (ad es. app di e-banking).
Il malware infetta soltanto gli smartphone con sistema operativo Android. Non appena il malware viene scaricato, sul display del telefono appare una falsa app «AlertSwiss» con logo modificato in cui l'ortografia («AlertSwiss» invece di «Alertswiss») e il logo differiscono dall'app reale. Invece di un logo rotondo come nell'applicazione originale, quella non autentica presenta un logo rettangolare all'interno di un cerchio bianco. La vera app Alertswiss dell'UFPP è un'app per informare, allertare e allarmare la popolazione, che viene utilizzata da diversi enti federali e cantonali.[68]

Raccomandazione

Sul sito dell'UFCS trovate un elenco di nove consigli pratici per un utilizzo sicuro del cellulare (ncsc.admin.ch).

4 Vulnerabilità

Il «Time-To-Exploit» (TTE) è un indicatore fondamentale nella gestione delle vulnerabilità. Misura il tempo che intercorre tra la pubblicazione o la scoperta di una vulnerabilità e il suo sfruttamento attivo (exploit) da parte degli aggressori. Il suo valore indica con quanta rapidità le organizzazioni devono reagire alle vulnerabilità al fine di prevenire potenziali attacchi.
Il TTE è influenzato da diversi fattori. A livello tecnico sono decisivi aspetti quali la disponibilità di dettagli relativi all'exploit e di kit di exploit. Una volta pubblicati i dettagli relativi a una vulnerabilità, come un proof of concept o un codice exploit, il TTE si riduce. Un altro aspetto rilevante è il grado di complessità. Mentre le vulnerabilità facilmente comprensibili e sfruttabili riducono talvolta drasticamente il TTE, le lacune di sicurezza complesse richiedono un lasso di tempo maggiore per essere sfruttate, dal momento che presuppongono più competenze e preparazione da parte dell'aggressore.

[68] Attenzione: false lettere a nome di MeteoSvizzera - il codice QR scarica un malware invece di un'app d'allerta meteo (ncsc.admin.ch)

In passato, inoltre, le lacune di sicurezza venivano ricercate meno sistematicamente, mentre oggi gli aggressori fanno ricorso all'IA e approfittano dell'apprendimento automatico (ML) per individuare i sistemi vulnerabili e quindi sviluppare rapidamente gli exploit. Inoltre, anche le attività dei potenziali aggressori sul dark web contribuiscono a uno sfruttamento più rapido delle vulnerabilità rispetto al passato, potendo scambiare gli exploit più rapidamente in forum e su marketplace digitali.

A lungo termine il TTE dimostra di essersi costantemente ridotto nel corso del tempo. Nel 2018 Mandiant, una società americana di sicurezza informatica, ha iniziato ad analizzare le vulnerabilità rispetto a questo indicatore. I risultati delle indagini sono allarmanti. Mentre nel 2018/2019 si osservava ancora un TTE medio di 63 giorni, nel 2020/2021 il lasso di tempo si era già ridotto a 44 giorni. Nel biennio successivo 2021/2022 il TTE medio è nuovamente sceso di 12 giorni, attestandosi a quota 32 giorni. Nel 2023, infine, dopo una media di soli cinque giorni, si è dovuto fare i conti con un potenziale sfruttamento di una vulnerabilità scoperta o o resa pubblica.[69]
Questa evoluzione è il risultato di progressi tecnologici, organizzativi e criminali grazie ai quali gli aggressori sono in grado alla fine di identificare e sfruttare più rapidamente le vulnerabilità. Il TTE più breve implica che le imprese hanno sempre meno tempo a disposizione per applicare le patch a una vulnerabilità o adottare altre misure di sicurezza necessarie. La pressione sui gestori delle infrastrutture informatiche affinché agiscano in tempi rapidi aumenta in maniera significativa a mano a mano che il TTE diminuisce. Soprattutto in caso di vulnerabilità critiche, spesso passa pochissimo tempo prima che si osservino i primi attacchi.

Nella seconda metà del 2024 l'UFCS ha avvertito le infrastrutture critiche circa la presenza di diverse vulnerabilità. Gli avvisi riguardavano cosiddette vulnerabilità zero-day e n-day. Nel primo caso si tratta di vulnerabilità ancora in gran parte sconosciute al vasto pubblico e anche al produttore stesso. Non esiste dunque ancora una patch da installare, ma la lacuna di sicurezza è già sfruttata attivamente. Questa costellazione è ad alto rischio per le organizzazioni. Tra i vari avvisi, l'UFCS ne ha pubblicati due per CVE-2024-47575 (in FortiManager) e CVE-2024-0012 (in Palo Alto Networks PAN-OS), riguardanti vulnerabilità zero-day in prodotti che in Svizzera godono di un'ampia base di utenti. In entrambi i casi le aziende non hanno di fatto avuto tempo per procedere all'eliminazione.

Diversa è invece la vulnerabilità n-day. In questo caso, al momento della pubblicazione della vulnerabilità esiste già una correzione del software (patch/fix) disponibile agli utenti, in quanto il produttore è stato coinvolto già in una fase precedente e ha quindi avuto un certo margine di tempo per prepararsi a sviluppare le contromisure. In questa categoria l'UFCS ha segnalato attivamente, ad esempio, la vulnerabilità CVE-2024-40766 (in SonicWall SonicOS), riguardante una serie di servizi ampiamente utilizzati di un fornitore nel campo della sicurezza di rete. In questo caso specifico, tra la pubblicazione della lacuna di sicurezza da parte del produttore (21 agosto 2024) e il primo riscontro di un potenziale sfruttamento (6 settembre 2024) sono trascorsi soltanto 16 giorni.

---

69 How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends (cloud.google.com)

Raccomandazioni

Il time-to-exploit (TTE) sensibilmente ridotto pone le organizzazioni e le aziende dinanzi a nuove sfide. Gli aggressori stanno diventando sempre più efficienti nell'identificare e sfruttare rapidamente le vulnerabilità. Per proteggersi efficacemente dai loro attacchi, è dunque fondamentale poter contare su una combinazione tra rapido roll-out degli aggiornamenti, approccio proattivo alla sicurezza e automazione. Molte organizzazioni hanno difficoltà ad adattare la velocità di distribuzione delle patch alle tempistiche TTE sempre più ristrette.

Tenete assolutamente conto degli ultimi sviluppi del TTE e adattate i processi di gestione delle patch della vostra azienda alle tempistiche sempre più ristrette degli exploit. Ottimizzate e accelerate i vostri cicli di patch, soprattutto in caso di vulnerabilità critiche. Date la priorità all'eliminazione delle vulnerabilità nelle parti esposte della vostra infrastruttura. Eseguite regolarmente test di penetrazione e scansioni delle vulnerabilità per individuare proattivamente eventuali lacune di sicurezza. Implementate un sistema di monitoraggio e utilizzate le informazioni disponibili sulle minacce (threat intelligence). Il monitoraggio in tempo reale della vostra infrastruttura, unito alle possibilità di automazione, vi aiuterà a individuare tempestivamente eventuali lacune di sicurezza. Assicuratevi che la vostra azienda abbia un inventario aggiornato dell'infrastruttura e dei prodotti utilizzati.

Anche misure d'accompagnamento come l'impiego del red teaming, controlli di sicurezza regolari o la gestione di un programma «bug bounty» nella vostra azienda possono essere d'aiuto nel valutare l'efficacia dei tempi di reazione rispetto alla risoluzione di vulnerabilità.

5 Truffe e ingegneria sociale

Anche nel secondo semestre del 2024 il fenomeno delle «frodi» ha rappresentato la maggior parte delle segnalazioni pervenute all'UFCS. Quasi due terzi di esse, per un totale di 18 270, rientravano in questa macrocategoria. Mentre i tentativi di frode hanno registrato un forte aumento anno su anno, passando da 30 496 a 41 374, il numero di segnalazioni pervenute nel secondo semestre è risultato inferiore di 1 052 unità rispetto allo stesso periodo dell'anno precedente. Le oscillazioni in questa categoria sono praticamente tutte riconducibili al fenomeno delle «telefonate minatorie a nome di false autorità».[70] Nella primavera del 2024 l'UFCS ha registrato in alcuni momenti un record di segnalazioni in ingresso. Nelle settimane 12 e 14, ad esempio, sono state oltre 1600 alla settimana solo su questo fenomeno. Questi picchi non si sono invece registrati nella seconda metà dell'anno. Dopo che nei mesi estivi si era persino osservato un calo, con volumi di segnalazioni scesi a due cifre, in autunno i numeri sono tornati a crescere e da allora oscillano tra le 500 e le 700 segnalazioni settimanali.
Nel periodo in esame l'UFCS ha osservato un forte aumento dei casi di «lotterie fraudolente». Rispetto al secondo semestre del 2023, le segnalazioni sono passate da 744 a 2 398. Anche rispetto all'intero anno il numero di segnalazioni pervenute è più che triplicato, da 1 025 a oltre 3 509. In molti casi, in questo fenomeno sono stati utilizzati abusivamente i nomi di note catene alimentari o retail, negozi di elettronica o aziende di trasporto. Per riscuotere la presunta vincita, si viene reindirizzati a un sito web in cui inserire dati personali come credenziali della carta

[70] Cfr. Rapporto: Truffe telefoniche nel ciberspazio (ncsc.admin.ch)

di credito, nome, indirizzo e-mail o numero di cellulare. Nascosto nelle CG, scritto a caratteri minuscoli sul sito o addirittura al di fuori dell'area visibile della pagina web viene segnalato che si sta sottoscrivendo un abbonamento pluriennale, il cui canone viene poi immediatamente addebitato sulla carta di credito. La peculiarità di questo modus operandi è lo sfruttamento di zone grigie dal punto di vista legale, che i truffatori cercano di utilizzare sempre più spesso operando al di sotto del diritto penale (cfr. cap. 5.4).
Tra i reati di frode più segnalati dalle aziende, il fenomeno della «truffa del CEO» segna un forte aumento, con i Comuni e le parrocchie tra le organizzazioni più colpite (cfr. cap. 5.3). In lieve discesa, invece, le segnalazioni di «truffe con manipolazione delle fatture», che sull'intero 2024 sono diminuite di 4 unità, scendendo a quota 114.

5.1 Frodi finanziarie online e frodi relative al rimborso

Anche nel semestre in esame la «frode degli investimenti online» si conferma la categoria con il maggior numero di danni finanziari segnalati, il cui ammontare per singolo caso può risultare molto elevato e raggiungere le sei cifre. Una variante è la combinazione con una cosiddetta «romance scam»: si tratta di una frode in cui i truffatori inizialmente si presentano come potenziali partner sentimentali, conquistando la fiducia della vittima e instaurando legami affettivi. Il primo contatto avviene ad esempio tramite siti di incontri. Una volta instaurata e consolidata la fiducia, la presunta fidanzata o il presunto fidanzato convince la vittima a effettuare investimenti apparentemente redditizi, sostenendo di aver personalmente ottenuto cospicui guadagni. In questo modo le vittime sono meno prudenti e meno critiche nei confronti delle proposte d'investimento, provenendo da una persona di cui si fidano.

Tuttavia, anche quando la truffa dell'investimento è alle spalle e la vittima si è rassegnata alla perdita finanziaria, il pericolo non è ancora scongiurato. In molti casi, infatti, i truffatori sfruttano la delusione per ingannare la vittima una seconda volta. A tal fine ricontattano la vittima dopo un certo periodo di tempo, ma questa volta non come «società di investimenti», bensì come «autorità di vigilanza sui mercati finanziari», «autorità di perseguimento penale» o come organizzazioni che dicono di voler aiutare le vittime a recuperare il denaro perduto. Nella disperazione, molti si aggrappano a questa speranza. Alle e-mail sono in genere allegati documenti dall'aspetto ufficiale, provvisti anche di timbri, firme e loghi ufficiali, ma sono tutti falsi. Se una vittima accetta, vengono chiesti tasse o imposte per poter avviare il processo di rimborso, a cui fanno seguito sempre nuove commissioni, finché la vittima non si arrende e smette di pagare.[71]

Raccomandazioni

Più elevato è il rendimento promesso, maggiore è solitamente il rischio. Si raccomanda cautela se improvvisamente vengono contattati presunti avvocati, organizzazioni, autorità di vigilanza dei mercati finanziari o enti simili che promettono di recuperare il denaro perso e richiedono il pagamento anticipato di commissioni. Non pagare mai commissioni. Se le aziende avessero recuperato il denaro, potrebbero detrarre le commissioni direttamente dall'importo recuperato e trasferirle il saldo senza alcuna commissione.

71 Settimana 38: truffa dell'investimento – presunta assistenza dopo una perdita ingente (ncsc.admin.ch)

In caso di richieste da parte di fornitori di servizi finanziari, verifichi che questi siano autorizzati dall'Autorità federale di vigilanza sui mercati finanziari (FINMA). Sul sito della FINMA[72] sono disponibili informazioni sui fornitori di servizi finanziari autorizzati in Svizzera. Se un fornitore di servizi finanziari non è autorizzato, è necessario prestare particolare attenzione. Verifichi il fornitore di servizi finanziari sulla base delle recensioni disponibili su Internet.

5.2 Varianti di fake sextortion

Nella «fake sextortion» i malfattori sostengono di aver hackerato il computer o l'account di posta elettronica e di aver raccolto foto o video che ritraggono il destinatario dell'e-mail durante una presunta visita a siti pornografici. Questi messaggi vengono inviati a caso dai ricattatori. I computer e gli account e-mail in questione non sono stati hackerati né esistono foto compromettenti. Per rendere credibili le loro minacce, gli aggressori utilizzano da anni vari stratagemmi. Falsificano gli indirizzi di posta elettronica dei mittenti (Spoofing) cosicché sembri che l'e-mail sia stata inviata dal proprio account. In un'altra variante vengono citate nell'e-mail vecchie password da precedenti fughe di dati per far credere che l'account sia stato hackerato. In alcuni casi queste password vengono persino utilizzate per impossessarsi di account di social media e caricarvi contenuti illeciti, in maniera tale da provocare il blocco dell'account – il tutto per far credere alla vittima che il truffatore abbia accesso a dati compromettenti. Nel secondo semestre sono comparse in rapida successione due varianti. Questo potrebbe essere un segnale del fatto che il fenomeno non è più così redditizio per i truffatori, che stanno cercando nuovi metodi per mantenere in vita il modello di business.

Inizialmente sono stati segnalati messaggi di «fake sextortion» in cui al destinatario viene mostrato parte del suo numero di telefono (cfr. fig. 8). Dalle ricerche a cura dell'UFCS è risultato che anche queste informazioni potrebbero provenire da una fuga di dati, in questi casi probabilmente dal leak avvenuto sulla piattaforma di criptovalute «Gemini». Pare infatti che tutti i destinatari delle e-mail fraudolente segnalate all'UFCS fossero coinvolti in questa fuga di dati.[73]

Nella seconda nuova variante i truffatori hanno utilizzato anche gli indirizzi di domicilio, anch'essi ottenuti da fughe di dati, per creare un legame con l'indirizzo e-mail della vittima. Dopo che casi simili erano stati inizialmente osservati negli Stati Uniti, nel secondo semestre del 2024 anche l'UFCS ha ricevuto alcune prime segnalazioni dalla Svizzera. Rispetto alle varianti americane, tuttavia, i truffatori si sono spinti oltre e nell'e-mail ricattatoria non si limitano a menzionare l'indirizzo di domicilio della vittima, ma cercano su Google Maps anche immagini della casa o delle immediate vicinanze e le aggiungono all'e-mail (cfr. fig. 9). In questo modo vogliono convincere la vittima di avere il pieno controllo del computer e di conoscere anche il suo ambiente privato. Questa combinazione di informazioni digitali e fisiche rafforza notevolmente la minaccia e può indurre la vittima a esaudire le richieste dei truffatori.[74]

---

72 Autorizzazione della FINMA: il biglietto d'ingresso al mercato finanziario (finma.ch)

73 Settimana 33: «Fake sextortion» e fughe di dati (ncsc.admin.ch)

74 Settimana 39: Ancora una nuova variante di fake sextortion: ora i truffatori sanno dove vive la vittima (ncsc.admin.ch)

I know, 76-XXX- is too personal to reach you.

Let me get straight to the point. You do not know anything about me however I know everything about you and you must be thinking why are you receiving this mail, correct?

I actually installed a Malware on porn website and there's more, you accessed same porn web site to experience fun (you get my drift). And while you were busy enjoying those videos, your browser began functioning as a RDP (Remote Protocol) that has a keylogger which gave me accessibility to your screen as well as your camera access. Just after that, my software program obtained all of your data and every one of your contacts from device including your complete photos.

Exactly what have I done?
It's simply your bad luck that I found your blunder. After that I invested in more days than I should have digging into your life and prepared a split screen sextape. First part shows the video you had been viewing and second part shows the view from your web camera (it is someone doing dirty things). Actually, I am ready to delete all information about you and allow you to move on with your regular life. And I will offer you two options that will achieve it. These two alternatives are either to disregard this e mail (bad for you), or pay me a small amount to close this topic forever.

Exactly what should you do?
Let's explore above two options in more depth. First Option is to turn a deaf ear my email message. Let us see what will happen if you choose this path. I will certainly send out your video to your contacts including members of your family, co-workers, and so forth. It does not protect you from the humiliation you and your family will face when relatives and buddies uncover your sordid videotape from me in their inbox. Other Option is to pay me, and be confidential about it. We will name this my "keep the secret charges". Now Lets discuss what will happen if you go with this choice. Your little secret remains private. I will keep my mouth closed. Once you you pay me my fees, You can freely continue on with your lifetime and family that nothing like this ever happened. You'll make the transfer via Bitcoins.

Amount to be paid: $950
My BTC Address: 1J8Sy8pJFa8Z952qNUumNv3NX31u2VzRKf
(Here's QR code, scan it)

Fig. 8: E-mail di fake sextortion con visualizzato il numero di telefono del destinatario

Important: You got one day to sort this out and I will only accept Bitcoin. I have a special pixel in this e mail, and now I've been notified that you have read through this email message. This email and Bitcoin address are custom-made for you, untraceable. If you are unfamiliar with Bitcoin, google it. You can buy it online or through a Bitcoin ATM in your neighborhood. There's no point in replying to this email or negotiating, it's pointless my price is fixed. As soon as you send the complete payment, my system will inform me and I will wipe out all the dirt I got on you. Remember if I notice that you've shared or discussed this mail with someone else, your video will instantly start getting sent to your contacts and I will post a physical tape to all of your neighborhood next week. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes.

Looks familiar?

Fig. 9: E-mail di fake sextortion con numero di telefono, indirizzo e un'immagine dell'indirizzo di domicilio presa da Google Maps

Raccomandazioni

Ignorate le e-mail di fake sextortion e non lasciatevi intimidire. Ad oggi, all'UFCS non sono noti casi in cui fosse presente materiale fotografico compromettente.

5.3 Truffa del CEO nei comuni, nelle scuole e nelle chiese

Nel secondo semestre si è registrato un forte aumento delle segnalazioni relative al fenomeno della truffa del CEO. Mentre nel 2023 si erano fermate a quota 487, l'anno scorso ne sono pervenute ben 719. La classica truffa del CEO consiste spesso nell'invio di un'e-mail al reparto finanziario da parte del presunto CEO o al tesoriere da parte del presunto presidente dell'associazione. Attraverso una storia credibile, il destinatario viene indotto a effettuare un pagamento. In molti casi viene anche chiesto di acquistare una carta regalo e successivamente di inviare il codice ai truffatori.

Un aspetto particolarmente evidente di questo fenomeno è che alcuni settori sono presi di mira molto più di altri: nel secondo semestre del 2024 scuole, parrocchie e Comuni hanno ricevuto un numero esorbitante di richieste fraudolente di questo tipo. La spiegazione è semplice: nella truffa del CEO le informazioni vengono raccolte principalmente da fonti pubbliche, per poter risalire alle strutture gerarchiche di aziende, organizzazioni o associazioni. Molte imprese presentano pubblicamente il loro team, con relative funzioni e indirizzi e-mail, sul proprio sito, ma decisamente non in maniera così sistematica come Comuni, scuole o parrocchie. In questi ambiti è fondamentale poter garantire alla popolazione una modalità di contatto semplice, per cui i dati vengono pubblicati con estrema trasparenza, tanto che a volte su Internet si trovano persino interi elenchi di collaboratori. Ciò che da un lato è una dimostrazione di vicinanza alla popolazione, dall'altro rappresenta un business lucrativo per i truffatori, che ne fanno ampio uso.[75]

Raccomandazioni

Sensibilizzate tutti i collaboratori sulla truffa del CEO. Informate in merito a queste modalità d'attacco soprattutto chi lavora nei reparti finanziari e chi ricopre posizioni chiave. Nelle associazioni vanno istruiti tutti i membri che ricoprono una funzione nel consiglio direttivo. Definite processi chiari per la gestione dei pagamenti e sincerateVi che vengano rispettati (ad es. principio del doppio controllo, firma congiunta a due ecc.).

5.4 Lo sfruttamento delle zone grigie della legge

In molti siti segnalati all'UFCS la frode è evidente. Le pagine di phishing, ad esempio, sono facili da riconoscere come tali. Nella maggior parte dei casi c'è poco spazio per l'interpretazione, per cui è anche facile far togliere queste pagine dal web. Per molti altri fenomeni si può sospettare che il sito abbia un intento fraudolento, ma lo si può provare solo in pochissimi casi.

[75] Settimana 49: la truffa del CEO colpisce sempre più anche parrocchie, scuole, associazioni e partiti politici (ncsc.admin.ch)

Di conseguenza è difficile, se non impossibile, farli rimuovere dal web. I truffatori, inoltre, tendono sempre più spesso a operare di proposito in questa zona grigia dal punto di vista legale. I cosiddetti abbonamenti trappola sono ormai noti da tempo in tale contesto. Si tratta di siti che pubblicizzano un prodotto gratuito, ma il fatto che l'abbonamento gratis, se non disdetto, viene convertito dopo pochi giorni in uno a pagamento viene scritto in caratteri minuscoli. Non appena si oltrepassa la scadenza, viene addebitato in un'unica soluzione il canone annuo o persino un canone biennale. Questi abbonamenti trappola sono considerati all'origine di tutte le frodi che sfruttano le zone grigie.

Un altro esempio che è stato ripetutamente segnalato nel secondo semestre del 2024 è quello dei negozi online che consegnano deliberatamente merce errata di scarsa qualità. In caso di reclamo il prodotto dev'essere restituito a proprie spese al venditore, che solitamente ha sede in Estremo Oriente. In questi casi i costi di spedizione sono di gran lunga superiori al valore dell'articolo, che pertanto non vale la pena rendere. Avendo tuttavia avuto la possibilità di reso, a questo punto non è chiaro se la procedura possa essere definita una frode.

Ancora più truffaldini sono i siti in cui apparentemente è possibile richiedere estratti del casellario giudiziario. Dopo aver effettuato l'ordine e pagato CHF 20, anziché ricevere l'estratto richiesto ci si vede recapitare soltanto una guida che spiega come ottenere il documento. Queste informazioni sono totalmente inutili, dal momento le si sarebbe potute reperire con una semplice ricerca via Internet. Anche su questo sito, tuttavia, viene specificato a caratteri minuscoli che si tratta semplicemente di una guida per il perfezionamento dell'ordine e non dell'ordine stesso. È evidente, però, che i gestori speculino proprio sul fatto che la vittima non legga queste righe. Nella maggior parte dei casi, quindi, perseguire penalmente questi soggetti diventa molto difficile. Un simile modus operandi si riscontra in diversi siti che fingono di voler aiutare i viaggiatori a ottenere un visto. In questi casi, l'impegno è praticamente lo stesso di quando si richiede il visto sui siti ufficiali dei rispettivi Paesi. L'unica differenza è il costo, notevolmente superiore sui siti di assistenza fasulli.
Anche le presunte offerte per la registrazione in un annuario settoriale più o meno noto rientrano in questa categoria. Vengono inviate alle aziende per posta o via e-mail, spesso camuffate da fattura ufficiale. In piccolo, tuttavia, viene specificato che il vero e proprio contratto viene stipulato soltanto previo pagamento della fattura. Anche in questo caso i mittenti della fattura speculano sul fatto che l'azienda non sappia più esattamente se si tratti di un contratto già stipulato da prorogare, oppure che non legga le righe in cui viene detto che si tratta semplicemente di un'offerta.

Raccomandazioni

Leggete attentamente le fatture che non vi aspettavate di ricevere, anche ciò che è scritto in piccolo. In caso di dubbio chiarite se la fattura sia giustificata o meno. Prima di registrarvi o di inserire i dati della carta di credito, leggete assolutamente le relative condizioni. Prestate particolare attenzione soprattutto in caso di presunte offerte gratuite. Controllate le recensioni dell'operatore su Internet.

6 Attacchi alla disponibilità di siti e servizi online e perturbazione dell'infrastruttura

Con gli attacchi alla disponibilità di siti e servizi online – generalmente sotto forma di «Distributed Denial of Service» (DDoS)[76] – gli aggressori cercano di mettere temporaneamente fuori uso un servizio accessibile via Internet bombardandolo di richieste. Questi attacchi non comportano né un accesso illegittimo ai dati né un furto di informazioni o un danno permanente ai sistemi.
L'infrastruttura può tuttavia essere perturbata anche quando aggiornamenti o modifiche alla configurazione ne compromettono l'operatività. È il caso del tool di login dei media svizzeri OneLog, che nell'autunno del 2024 ha subito un'interruzione della disponibilità dei servizi di registrazione e login presumibilmente a causa di una manipolazione malevola dei suoi sistemi. Questo attacco ha compromesso varie funzioni in cascata, come il paywall o la funzione di commento delle pubblicazioni colpite[77] (cfr. cap. 7). Oltre alle manipolazioni malevole, anche gli effetti di un aggiornamento errato di un componente possono causare malfunzionamenti. Un caso del genere viene illustrato nella seconda parte di questo capitolo utilizzando l'esempio del fornitore di servizi di sicurezza CrowdStrike.

6.1 Attacchi DDoS

All'origine dei blackout temporanei avvenuti nel secondo semestre del 2024 ai danni di vari servizi finanziari[78] e siti web cantonali[79] vi erano attacchi DDoS sferrati contro i sistemi di varie organizzazioni svizzere. Le segnalazioni dirette pervenute nel 2024 all'UFCS su questo tipo di attacchi sono aumentate solo lievemente rispetto al 2023, passando da 41 a 48. L'incremento è stato registrato perlopiù nella seconda metà dell'anno, quando le segnalazioni sono passate da 17 a 25.

Spesso gli attacchi DDoS avvengono tramite infrastrutture che i cibercriminali, pagando, possono indirizzare verso bersagli a loro scelta. Nel mese di settembre del 2024 l'UFCS ha registrato un aumento degli attacchi DDoS effettuati da una botnet chiamata «Gorilla». Si tratta di un servizio «DDoS-as-a-service» offerto su Telegram, che può essere noleggiato a pagamento. Essendo stato colpito un operatore di un'infrastruttura critica in Svizzera, l'UFCS ha pubblicato i risultati tecnici in un rapporto[80]. Gli attacchi DDoS contro le infrastrutture svizzere erano attacchi di amplificazione DNS che, sfruttando il «Domain Name System» (DNS), deviano flussi di dati eccezionalmente elevati sull'infrastruttura della vittima, sovraccaricandola.

La domenica delle elezioni, il 24 novembre 2024, il sito Internet del Canton Svitto è stato vittima di un attacco DDoS[81]. L'attacco è durato a lungo, rendendo indisponibili per diverse ore anche i siti di diversi Comuni di vari Cantoni e una serie di siti web cantonali[82]. Tutti i siti colpiti erano

---

76 Attacchi alla disponibilità (DDoS) (ncsc.admin.ch)
77 OneLog Update: Login-Service wieder verfügbar (onelog.ch)
78 DDoS-Angriff trifft Swisscom und legte Twint lahm (inside-it.ch)
79 Revue des cybermenaces: Septembre 2024 (vd.ch)
80 Cfr. Breve analisi tecnica della botnet «Gorilla» (ncsc.admin.ch)
81 Un attacco DDoS al sito web del Cantone di Svitto causa l'indisponibilità di diversi siti web cantonali e comunali (ncsc.admin.ch)
82 Cyber-Angriff: Websiten von Gemeinden nicht mehr erreichbar (luzernerzeitung.ch)

gestiti dallo stesso provider, per cui hanno subito danni collaterali. Le motivazioni dell'attacco sono rimaste ignote e non è stato stabilito neppure un legame diretto con la domenica di voto.

Se si confrontano le osservazioni a livello nazionale con gli episodi registrati a livello globale, si rileva come la Svizzera non sia stata colpita in modo spropositato da attacchi DDoS.[83] Oltre ai continui attacchi di hacktivisti nel contesto dei conflitti internazionali, anche singoli eventi possono provocare campagne DDoS. In Francia, ad esempio, l'arresto del fondatore e CEO della app di messaggistica Telegram, Pavel Durov, ha scatenato una reazione in parte coordinata di vari collettivi di haktivisti, che con l'hashtag #FreeDurov hanno sferrato attacchi DDoS contro oltre 50 organizzazioni francesi.[84]
In alcuni casi le forze dell'ordine sono riuscite a identificare e arrestare gli artefici della campagna o a neutralizzare l'infrastruttura d'attacco. La polizia spagnola, ad esempio, ha arrestato alcuni soggetti che facevano parte della botnet «DDoSia» del gruppo filorusso «NoName057(16)»[85] e che avevano fornito vari dispositivi per gli attacchi.[86] La giustizia americana è riuscita a incriminare due membri di spicco del gruppo di haktivisti «Anonymous Sudan» e a confiscare buona parte della loro infrastruttura d'attacco.[87] Nell'ambito dell'operazione «PowerOff» le forze dell'ordine tedesche sono riuscite sinora a rimuovere dalla rete 27 servizi stresser. Si tratta di servizi DDoS che possono essere noleggiati da terzi per attaccare qualsiasi obiettivo. L'intervento della polizia ha consentito di identificare oltre 300 utenti di queste offerte, alcuni dei quali sono già stati arrestati.[88]

Nonostante questi interventi repressivi andati a buon fine, gli attacchi DDoS rimangono un mezzo prediletto da vari attori per limitare in breve tempo la disponibilità dei servizi in questione e attirare tra l'altro su di sé l'attenzione. I media possono vanificare questo intento facendo passare in sordina questi episodi. La continua espansione delle infrastrutture d'attacco, come le botnet e le loro tecniche avanzate, richiedono agli operatori di rete di mantenere costantemente aggiornate le loro misure di difesa.

Raccomandazioni

Il sito dell'UFCS contiene, nella sezione Attacchi alla disponibilità (DDoS) (ncsc.admin.ch), un elenco di informazioni e misure di prevenzione e difesa da tali attacchi. Preparatevi a un potenziale attacco in collaborazione con il vostro operatore di servizi o webhoster, in modo tale da arginare le conseguenze. Per i sistemi critici può essere utile attivare a titolo di supporto una protezione DDoS commerciale.

In caso di attacco DDoS con estorsione l'UFCS raccomanda di non cedere al ricatto. Dopo un primo versamento i truffatori potrebbero chiedere ulteriore denaro e proseguire comunque gli attacchi. Segnalate invece il caso all'UFCS e contattate la polizia per sporgere denuncia. Se

83 Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4 (cloudflare.com)
84 Hacktivists Call for Release of Telegram Founder with #FreeDurov DDoS Campaign (blog.checkpoint.com)
85 Rapporto di analisi dettagliata sugli attacchi DDoS «NoName057(16)» (ncsc.admin.ch)
86 Tres detenidos por delitos de daños informáticos con fines terroristas (interior.gob.es)
87 Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks (justice.gov)
88 Operation „Power OFF": weltweiter Schlag gegen Cybercrime-Infrastruktur (bka.de)

siete vittima di un attacco, trovate varie raccomandazioni su Attacco DDoS – E adesso? (ncsc.admin.ch).

6.2 Caso CrowdStrike

Il 19 luglio 2024 si è verificato un guasto globale ai sistemi Windows che è stato descritto come il blackout informatico esteso della storia. All'origine del disservizio non c'è stato un ciberattacco, bensì un bug nell'aggiornamento del modulo di sicurezza Falcon di CrowdStrike, il cui compito è appunto quello di riconoscere e contrastare questo tipo di ciberattacchi. In seguito al citato aggiornamento, su un gran numero di computer Windows è comparsa la cosiddetta «Blue Screen of Death», che comporta il crash del sistema e il blocco del funzionamento.[89] CrowdStrike è riuscita a individuare il bug nell'arco di poche ore e a interrompere immediatamente la distribuzione dell'aggiornamento difettoso, dopodiché CrowdStrike e Microsoft hanno pubblicato le istruzioni per la risoluzione del problema.[90] Per risolverlo è stato necessario avviare in modalità provvisoria tutti i sistemi colpiti e rimuovere manualmente un file specifico. Poiché l'avvio in modalità provvisoria non è in genere disponibile agli utenti normali e in alcuni casi le chiavi Bitlocker necessarie si trovavano su altri sistemi coinvolti nell'incidente, alcune organizzazioni hanno registrato notevoli ritardi nella risoluzione del problema. Si stima che oltre 8,5 milioni di sistemi in tutto il mondo siano stati vittima dell'attacco, con un danno complessivo stimato in diversi miliardi di dollari.[91]

Gli effetti si sono manifestati prima in Australia, poi in India, Europa e Stati Uniti, a seconda del momento in cui è iniziata la giornata lavorativa successiva all'aggiornamento difettoso. Tra le organizzazioni colpite figuravano numerose grandi aziende, autorità governative e istituzioni pubbliche, con ripercussioni eclatanti soprattutto nel settore dell'aviazione – una circostanza dovuta anche all'elevata complessità del traffico aereo e alla massima sincronizzazione dei piani di volo. L'incidente è avvenuto tra l'altro in un venerdì di luglio, che in Europa coincide con un periodo di alta stagione, per cui si sono verificati molti ritardi o cancellazioni di voli in numerosi aeroporti. I principali hub internazionali, come Heathrow a Londra, e compagnie aeree come Delta Airlines sono stati particolarmente colpiti e hanno dovuto posticipare o cancellare migliaia di voli. Anche in Svizzera, all'aeroporto di Zurigo si sono registrati ritardi e cancellazioni.[92]

L'incidente legato alla sicurezza è stato prontamente strumentalizzato da alcuni criminali per compiere attività fraudolente. Tra le tecniche d'attacco utilizzate vi sono state e-mail di phishing che fingevano di offrire assistenza da parte di CrowdStrike, nonché script dannosi che promettevano un ripristino automatico dei sistemi colpiti. CrowdStrike ha reagito a questi episodi pubblicando rapporti e pareri, e in particolare consigliando agli utenti di scaricare esclusivamente aggiornamenti da fonti ufficiali.[93] Vi sono stati anche truffatori opportunistici che si sono finti dipendenti del servizio clienti di varie compagnie aeree. Altri hanno scandagliato i social media

89 CrowdStrike oopsie crashes Windows workstations across the world (therecord.media)

90 KB5042421: CrowdStrike issue impacting Windows endpoints (microsoft.com), Falcon Content Update Remediation and Guidance Hub (crowdstrike.com)

91 What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk (hbr.org)

92 CrowdStrike-Softwarefehler - Der Tag, an dem die IT weltweit verrückt spielte (srf.ch)

93 Falcon Sensor Issue Likely Used to Target CrowdStrike Customers (crowdstrike.com)

alla ricerca di post di viaggiatori arrabbiati per lo spostamento o la cancellazione del loro volo, per poi contattarli tramite account social fasulli e chiedere loro informazioni sensibili come dati anagrafici, numero di conferma della prenotazione o dati della carta di credito.[94]

A seguito del blackout informatico sopra descritto, CrowdStrike ha rivisto e ottimizzato i processi di controllo interni degli aggiornamenti software e ha aggiunto una funzione con cui i clienti possono scegliere se ricevere gli aggiornamenti dei contenuti in tempo reale o in maniera differita. L'obiettivo è minimizzare il rischio che incidenti di questo tipo si verifichino nuovamente in futuro. Una particolarità dei sistemi Windows, che ha consentito un tale blackout, sono i diritti d'accesso estesi che i software degli offerenti di sicurezza come CrowdStrike necessitano a livello del kernel. Microsoft ha preso posizione in merito, sottolineando che l'accesso da parte delle soluzioni di sicurezza a livello del kernel è necessario, ma dev'essere disciplinato meglio, e che vi saranno innovazioni in futuro miranti a limitare tale accesso. Microsoft ha inoltre annunciato che intensificherà la collaborazione con partner come CrowdStrike al fine di contenere tali rischi in futuro.[95]

Raccomandazioni

Una gestione delle patch efficace è fondamentale per preservare la sicurezza e la stabilità. Le organizzazioni devono valutare tra un'installazione immediata, che risolve rapidamente le vulnerabilità, ma comporta il rischio di guasti non testati, e un'installazione ritardata, che consente di eseguire test approfonditi ma lascia i sistemi non protetti più a lungo. Un aggiornamento scaglionato in base all'esposizione e alla criticità dei sistemi può essere una strategia adeguata per minimizzare i rischi.

La formazione e il training del personale dal punto di vista dei guasti informatici sono essenziali per garantire una reazione rapida ed efficace in caso d'emergenza.

7 Gestione, fughe ed estorsioni di dati

Fughe ed esposizioni involontarie di dati sono state un tema rilevante anche nel secondo semestre del 2024, sia in Svizzera che a livello internazionale. Una conservazione sicura e integra dei dati può tuttavia essere garantita soltanto se autorità, aziende e privati considerano la protezione degli accessi e la gestione dei dati una priorità. Questo aspetto è emerso chiaramente nel ciberincidente avvenuto alla fine di ottobre 2024 ai danni della piattaforma svizzera di «Single Sign-On» OneLog. Sebbene un'indagine forense abbia escluso una fuga di dati degli utenti dalla piattaforma[96], diversi media hanno dovuto offrire i loro contenuti senza paywall per dieci giorni.[97] L'artefice della minaccia, infatti, aveva cancellato i dati di autenticazione

94 Scammers impersonate airline customer service representatives (ftc.gov)

95 CrowdStrike tells Congress of two process changes to address July outage incident (therecord.media), Windows Security best practices for integrating and managing security tools (microsoft.com)

96 Cfr. comunicato stampa OneLog provides further information after the security incident: No evidence of data theft, investigation is ongoing (ringier.com)

97 Ein Super-GAU für die Schweizer Medienwelt (republik.ch)

degli utenti su OneLog, impedendo così l'identificazione dei clienti paganti.[98] Altri ciberincidenti hanno ulteriormente evidenziato il valore dei dati, soprattutto quando viene messa in dubbio l'integrità o la disponibilità dei dati stessi. Nell'episodio che ha colpito il gruppo VidyMed a dicembre 2024, la non disponibilità dei dati ha costretto i quattro ambulatori a tornare temporaneamente all'uso di carta e penna pur di continuare a prestare le cure mediche.[99] Un caso simile ha coinvolto numerose scuole in Europa, Nord America e Singapore che utilizzavano una piattaforma digitale per la gestione delle lezioni. Procuratosi l'accesso alla piattaforma, all'inizio di agosto un utente non autorizzato ha cancellato i dati di almeno 13 000 dispositivi degli studenti.[100] A distanza di pochi mesi un altro fornitore globale di software didattico ha subito un simile ciberincidente: in un messaggio ricattatorio l'aggressore comunicava di aver trafugato i dati di circa 62 milioni di alunni e 10 milioni di insegnanti.[101] Pur non essendo stati cancellati dati sui dispositivi degli studenti e del personale docente né criptati i sistemi, il volume immenso di dati sottratti può servire da base per futuri crimini – sia nel mondo digitale che in quello fisico. Anche in questo caso, infatti, sono state esfiltrate informazioni personali sensibili.[102]

Riguardo alle fughe di dati, la conservazione sicura è particolarmente rilevante nel momento in cui i dati trafugati comportano a posteriori un rischio per altre organizzazioni e persone fisiche. Visto che, dopo un data leak subito da un fornitore, può essere che le aziende debbano monitorare gli accessi alla propria infrastruttura informatica, aumenta anche il rischio di cadere vittima di un tentativo di frode (cfr. cap. 5). Analogamente, nel caso dei privati le informazioni sensibili possono essere utilizzate per impossessarsi di account o compiere attività di phishing (cfr. cap. 2), furti d'identità o frodi finanziarie. Da questo punto di vista meritano attenzione soprattutto i criminali attivi sulla scena del ransomware, visto che – in assenza di pagamento del riscatto – solitamente pubblicano i dati e/o li monetizzano, ad esempio vendendoli (cfr. cap. 3.2). Oltre alle attività dei cibercriminali vi sono anche altre cause, come una gestione inadeguata dei dati nella propria infrastruttura, la presenza di vulnerabilità o configurazioni tecniche errate, che possono portare a un'esposizione dei dati, il che in una seconda fase può essere a sua volta sfruttato dai criminali.

Marketplace dedicati su Internet e nel dark web – come ad esempio Breachforums – offrono ai cibercriminali la possibilità di vendere i dati rubati e realizzare un profitto.[103] A farne le spese è stata, nel novembre del 2024, la società Temenos, un fornitore svizzero di software bancari.[104] L'hacker sosteneva che, oltre a informazioni sul personale, i dati contenessero anche dettagli su applicazioni e servizi web per banche e altri clienti. Per dare maggiore credibilità alle proprie affermazioni, ha aggiunto una serie di screenshot. In alcuni casi gli hacker offrono

98 OneLog provides further information after the security incident: No evidence of data theft, investigation is ongoing (ringier.com)

99 Groupe Vidymed: actualites (vidymed.ch); cfr. comunicati stampa del 7.12.2024, 20.12.2024 e 14.01.2025.

100 Mobile Guardian: Security Incident Report (mobileguardian.com), Hacker wipes 13,000 devices after breaching classroom management platform (bleepingcomputer.com)

101 PowerSchool starts notifying victims of massive data breach (bleepingcomputer.com)

102 Powerschool hat offenbar Daten von 62 Millionen Schülern verloren (inside-it.ch)

103 Cfr. anche Rapporto semestrale 2024/1; cap. 7.2.

104 Hacker verkaufen Daten von Temenos Quantum Fabric (inside-it.ch)

anche la possibilità alle organizzazioni colpite di riacquistare i loro dati per impedirne la pubblicazione o la rivendita. Il problema è che, dinanzi a una simile offerta, le vittime non possono mai sapere fino a che punto i cibercriminali manterranno la parola data.

Alcuni hacktivisti utilizzano i dati sensibili dei loro bersagli per diffondere i propri interessi sociali, politici o ideologici. Una delle modalità preferite da questi gruppi è hackerare i sistemi informatici per poi pubblicare le informazioni e i dati personali trafugati. Questo modus operandi è noto anche come «hack-and-leak». Durante i Giochi olimpici estivi in Francia, ad esempio, un gruppo di hacktivisti filopalestinese ha pubblicato sui social media le informazioni personali di alcuni atleti israeliani: non solo nomi, numeri di telefono, indirizzi, password o fotografie, ma anche informazioni mediche come ad esempio il gruppo sanguigno.[105] Queste informazioni diventano problematiche per aziende e persone fisiche soprattutto se facilmente accessibili ai cibercriminali come dati strutturati. In quella forma, infatti, aumenta il rischio che vengano sistematicamente sfruttate per frodi o altre attività illecite. A metà novembre l'utente «Nam3L3ss» ha pubblicato sulla piattaforma dark web «Breachforums» vari set di dati appartenenti a 25 grandi multinazionali, tra cui anche due aziende svizzere.[106] Dopo un mese di continue attività, il numero di set di dati pubblicati da quello stesso utente era già salito a un centinaio.[107] A differenza di altri utenti della piattaforma, Nam3L3ss sosteneva di non aver ottenuto i dati hackerando i sistemi, bensì di averli raccolti e corretti unicamente grazie all'esposizione involontaria dei dati da parte delle imprese. Ciò avveniva, ad esempio, quando in una trasmissione si inviavano dati non criptati o se gli archivi online non erano protetti da password. Anche i dati utilizzati a fini di estorsione da vari collettivi di ransomware facevano parte di questi set di dati, sebbene Nam3L3ss avesse dichiarato di non essere spinto da finalità di vendita. Il suo obiettivo era piuttosto quello di sottolineare, attraverso la distribuzione di set di dati corretti, le proprie opinioni politiche a favore di una maggiore responsabilità nella conservazione dei dati. In Svizzera un comportamento di questo tipo viola la legge sulla protezione dei dati, dal momento che un attore privato come Nam3L3ss può raccogliere, trattare e pubblicare dati personali solo con il consenso degli interessati.[108] Ciò concerne soprattutto dati personali degni di particolare protezione.

Raccomandazioni

I vari incidenti avvenuti nel secondo semestre del 2024 evidenziano quanto la sicurezza dei dati sensibili debba avere la priorità: una volta che un contenuto è stato pubblicato su Internet, è praticamente impossibile ottenerne la cancellazione definitiva. In generale vale pertanto quanto segue:

In base alle 5W della conservazione dei dati stabilite chi archivia ed elabora quali dati, in quale forma e dove e con chi tali dati vengono condivisi. Oltre a un salvataggio conservativo, a intervalli regolari i dati andrebbero verificati e, se non più necessari, cancellati. Archiviate offline i dati da conservare ma non più utilizzati attivamente. Definite processi chiari e fattibili per il trattamento e la protezione dei dati e controllatene l'implementazione. Proteggete inoltre gli

105 Israeli athletes doxed at Olympic Games by Zeus hacking group (bitdefender.com)

106 Amazon, UBS und Firmenich von Breach betroffen (inside-it.ch)

107 Conversation with a "Nam3L3ss" Watchdog: Preface (databreaches.net)

108 Cfr. anche art. 31 LPD (legge sulla protezione dei dati)

accessi a sistemi, account e dati con password forti e, se possibile, con l'autenticazione a più fattori (MFA).[109] Concedete l'accesso soltanto a coloro che ne hanno realmente bisogno.

I dati trafugati in passato possono essere riutilizzati per attacchi successivi. Verificate periodicamente se i vostri dati compaiono in un data leak, ad esempio sul sito Have I Been Pwned (haveibeenpwned.com) o Identity Leak Checker des Hasso Plattner Instituts (hpi.de).

8 Ciberspionaggio e sabotaggio

Gli attori statali o parastatali rappresentano una particolare tipologia di minaccia nel ciberspazio. I cosiddetti gruppi «Advanced Persistent Threat» (APT)[110] conducono operazioni di spionaggio o, più raramente, sabotaggio se funzionali ai loro interessi. A differenza dei cibercriminali mossi da intenti finanziari, questi gruppi selezionano i loro obiettivi ad hoc e investono notevoli risorse per carpire le informazioni desiderate o ottenere l'effetto voluto. Il sistema di difesa delle organizzazioni potenzialmente coinvolte deve pertanto essere progettato in maniera particolarmente robusta per contrastare questo tipo di minaccia.

8.1 Ciberspionaggio

La stagione del «tifone»

A fine settembre 2024 il Wall Street Journal ha riportato che un gruppo chiamato «Salt Typhoon», presumibilmente operante per conto delle autorità cinesi, aveva compromesso l'attività di vari operatori di telecomunicazioni americani.[111] Dopo queste prime rivelazioni, il 25 ottobre 2024 l'agenzia statunitense CISA e il Federal Bureau of Investigation (FBI) hanno comunicato di aver avviato un'indagine sull'accesso non autorizzato alle infrastrutture di telecomunicazione da parte di attori legati alla Repubblica Popolare Cinese.[112]. Questo annuncio è avvenuto in concomitanza con la pubblicazione sui media di diversi articoli, secondo cui Salt Typhoon, infiltrandosi nei sistemi dei colossi delle telecomunicazioni statunitensi, si era impossessato specificatamente dei dati presenti nei telefoni utilizzati dall'allora e odierno presidente Donald Trump, dal politico statunitense J.D. Vance, dai collaboratori dell'ex vicepresidente Kamala Harris e da altre figure del Partito democratico. Vi furono inoltre altre rivelazioni riguardanti una possibile compromissione del sistema utilizzato dal governo degli Stati Uniti per richiedere intercettazioni telefoniche. L'esatta portata di questa campagna è ancora difficile da stimare. Nel dicembre del 2024 la Casa Bianca ha dichiarato di aver identificato tra le vittime nove società di telecomunicazioni, attraverso le quali i criminali potrebbero aver attaccato determinati obiettivi per un periodo di tempo prolungato. In questo caso gli accessi privilegiati permettevano all'aggressore di registrare chiamate, localizzare utenti e accedere ai metadati dei dispositivi mobili[113]. Secondo la società di sicurezza informatica Trend Micro, c'è anche la possibilità che la campagna fosse rivolta contro strutture al di fuori degli Stati Uniti. L'azienda

[109] Cfr. Proteggete i vostri account (ncsc.admin.ch)
[110] APT – Glossary (csrc.nist.gov)
[111] Chinese-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack (wsj.com)
[112] Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications (cisa.gov)
[113] US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage (reuters.com)

ha infatti rilevato alcune somiglianze tra le attività di Salt Typhoon e quelle di un attore che stava monitorando, chiamato «Earth Estries»[114].
Molto probabilmente l'obiettivo di Salt Typhoon è avere accesso a informazioni degne di particolare protezione. In questo ambito, la compromissione di società di telecomunicazioni rappresenta una porta d'ingresso ideale per molti obiettivi altamente interessanti, soprattutto politici di alto livello. Altri attacchi, che le autorità statunitensi attribuiscono anch'essi ad attori statali cinesi, sembrano tuttavia mirare piuttosto al controllo di infrastrutture critiche. È il caso del gruppo «Volt Typhoon», citato nell'ultimo rapporto semestrale dell'UFCS.[115] Le autorità statunitensi temono che questi accessi possano essere utilizzati, in caso di crisi, per azioni di sabotaggio ai danni di infrastrutture statunitensi.[116]

L'attenzione che gli Stati Uniti rivolgono alle presunte attività ostili della Cina si riflette anche nelle reazioni ufficiali. Il 18 settembre 2024, ad esempio, il Dipartimento di Giustizia statunitense ha annunciato lo smantellamento di una botnet che avrebbe operato per conto dell'APT cinese «Flax Typhoon». Nel loro comunicato le autorità statunitensi hanno sottolineato che la botnet era gestita dalla società cinese Integrity Technology Group. Successivamente, il 3 gennaio 2025 il Dipartimento del Tesoro degli Stati Uniti ha comunicato di aver imposto sanzioni contro la stessa impresa per il suo ruolo negli attacchi hacker ai danni di istituzioni statunitensi, la cui paternità era stata attribuita a Flax Typhoon[117]. Con un tempismo eclatante, poco prima il Dipartimento del Tesoro aveva reso nota una compromissione dei suoi sistemi informatici da parte di un attore che, anche in questo caso, aveva presunti legami con lo Stato cinese. Gli aggressori avevano utilizzato una chiave di assistenza rubata a un fornitore terzo con accesso privilegiato.[118]

Nuova campagna di APT29

Il rapporto dell'UFCS relativo al primo semestre del 2024 conteneva già informazioni su numerose attività di spionaggio attribuite al gruppo «APT29», sospettato di operare per conto dei servizi segreti esteri russi. APT29 è stato anche accusato di essere l'artefice di una campagna su vasta scala, probabilmente condotta anch'essa a scopo di spionaggio. Dal 22 ottobre 2024 Microsoft ha osservato come questo attore, che la stessa società chiama «Midnight Blizzard», inviasse una serie di e-mail di spear phishing molto mirate contenenti un file di connessione RDP (Remote Desktop Protocol) firmato. Se eseguito, questo file creava una connessione a un server controllato dall'attore.[119]. Secondo Microsoft, l'obiettivo di questa campagna erano autorità governative, università, organizzazioni operanti nell'ambito della difesa e ONG in decine di Paesi, prevalentemente in Europa, Australia e Asia. Attività simili sono state segnalate anche dal Computer Emergency Response Team ucraino (CERT-UA) con la denominazione «UAC-0215» e da Amazon[120]. Le e-mail di phishing di questa campagna sono state inviate da

---

114 Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions (trendmicro.com)
115 Rapporto semestrale 2024/1 (ncsc.admin.ch)
116 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (cisa.gov)
117 Treasury Sanctions Technology Company for Support to Malicious Cyber Group (treasury.gov)
118 US Treasury says Chinese hackers stole documents in 'major incident' (reuters.com)
119 Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files (microsoft.com)
120 Amazon identified internet domains abused by APT29 (aws.amazon.com)

indirizzi e-mail di organizzazioni legittime, che erano stati raccolti in compromissioni precedenti.

Evoluzione delle tecniche

I gruppi più sofisticati, attivi nel campo del ciberspionaggio, possiedono la capacità di sviluppare e migliorare costantemente il loro arsenale offensivo, consentendo loro di sfruttare nuove opportunità e aggirare misure difensive esistenti. Nel periodo in esame vi sono stati due esempi eclatanti di questo know-how molto specifico.
Nell'ottobre del 2024 il fornitore di software di sicurezza ESET ha attribuito una serie di attacchi ai danni di un'organizzazione governativa europea al gruppo APT «GoldenJackal». Secondo ESET, questo attore ha ideato due diverse fasi per compromettere sistemi fisicamente isolati (air gap) utilizzando una chiavetta USB. In una prima fase la chiavetta USB viene inserita in un sistema connesso a Internet già compromesso in origine. Il metodo utilizzato per questa prima compromissione non è ancora noto. La stessa chiavetta USB viene successivamente utilizzata per infettare il sistema isolato, non appena collegata a quest'ultimo. Infine, i dati vengono nuovamente trafugati dal sistema connesso a Internet nel momento in cui la chiavetta USB viene reinserita in tale sistema. L'air gap viene generalmente utilizzato per le reti critiche, come i sistemi di controllo industriale o le reti ad alta sicurezza. Considerate le risorse necessarie per lo sviluppo di un simile tool, è probabile che vi sia il coinvolgimento di uno Stato. ESET non si sbilancia nell'attribuire la paternità degli attacchi, ma rileva somiglianze a livello operativo con alcuni APT presumibilmente russi, in particolare con «Turla».[121]

Nel novembre 2024 la società di cibersicurezza Volexity ha descritto un nuovo modus operandi molto creativo utilizzato da «GruesomeLarch», un presunto APT russo (noto anche come «APT28» o «Sofacy») sospettato di operare per conto del servizio di intelligence militare russo. Per realizzare i propri obiettivi di ciberspionaggio, il gruppo si è insinuato nelle reti dei suoi obiettivi connettendosi al wi-fi delle rispettive aziende. La strategia consisteva nell'infiltrarsi in un'altra organizzazione ubicata nei pressi dell'obiettivo per poi espandersi all'interno della medesima al fine di trovare sistemi a doppia connessione, ovvero sistemi con connessione di rete via cavo e wireless, e successivamente connettersi da questo sistema compromesso alla rete wi-fi aziendale della vera vittima.[122]

Conclusioni

L'alta propensione di tali aggressori a investire tempo e risorse in strumenti ausiliari consente loro di penetrare nelle reti più sicure in assoluto. In generale, non dovrebbe essere consentito inserire chiavette USB in sistemi protetti e fisicamente isolati. Dovrebbero essere consentite solo connessioni esterne ben definite e monitorate. Anche la compromissione di un'azienda vicina può rappresentare un rischio per la sicurezza. Nel caso del Wi-Fi, è inoltre importante distinguere tra la rete ospite e la rete aziendale più protetta.

121 Mind the (air) gap: GoldenJackal gooses government guardrails (welivesecurity.com)
122 The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access (volexity.com)

Presunti collaboratori informatici

Alcuni attori sospettati di lavorare per conto del governo nordcoreano rivestono ormai da tempo una posizione particolare tra i ciberattori statali offensivi, dal momento che non si limitano al ciberspionaggio, ma svolgono gran parte delle loro attività per scopi finanziari. Questa tendenza è in linea con le priorità del regime di Pyongyang, che a causa delle numerose sanzioni economiche necessita di valuta estera.

Da presunti attori affiliati alla Corea del Nord, in particolare, giungono spesso attacchi a piattaforme di scambio di criptovalute. Negli ultimi giorni del periodo in esame, le autorità statunitensi e giapponesi hanno individuato un attore statale della Corea del Nord dietro il furto di 308 milioni di USD avvenuto nel maggio del 2024 sulla piattaforma di scambio DMM[123]. In questo e in molti altri casi, il vettore d'attacco è un presunto processo di assunzione di collaboratori informatici, nel quale si cerca di trasmettere al bersaglio un codice malevolo[124]. Negli ultimi tempi, tuttavia, i criminali hanno più volte fatto ricorso a un altro metodo, che consiste nello spacciare i propri agenti come collaboratori informatici e nel farli assumere da aziende occidentali come personale operante da remoto. A tal fine utilizzano identità fasulle e una serie di strumenti tecnici (in particolare VPN) per mascherare la loro posizione. Non esitano nemmeno a utilizzare l'IA per generare foto o video[125]. Questo metodo si è rivelato molto redditizio. In un atto d'accusa pubblicato il 12 dicembre 2024, il Dipartimento di Giustizia statunitense ha dichiarato 14 cittadini nordcoreani responsabili di aver organizzato una frode di questo tipo durata sei anni, nella quale risulta che siano stati trasferiti nelle casse del regime nordcoreano ben 88 milioni di USD.[126].

Questa minaccia ha molte sfaccettature, e l'accesso da parte di questi collaboratori alle reti di aziende occidentali può essere sfruttato a fini lucrativi in vari modi. Da un lato questi personaggi guadagnano incassando lo stipendio per il lavoro che svolgono nelle aziende. Dall'altro, tuttavia, sono stati osservati anche casi in cui hanno sottratto dati sensibili per poi ricattare i loro ex datori di lavoro. Questi attori sembrano perseguire non solo obiettivi finanziari, in quanto il loro accesso alle reti aziendali può, in determinate circostanze, essere utilizzato anche per scopi di spionaggio.

---

123 FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com (fbi.gov)

124 Su questo metodo si vedano in particolare i dettagli di una campagna denominata «contagious interview»: Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware (unit42.paloaltonetworks.com)

125 In tale contesto, la società Knowbe4 ha condiviso un esempio concreto di processo di assunzione con un candidato avente simili intenti malevoli:
How a North Korean Fake IT Worker Tried to Infiltrate Us (blog.knowbe4.com)

126 Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions (justice.gov)

Raccomandazioni

La difesa contro questo tipo di minaccia deve avvenire su diversi livelli. In primo luogo, è importante identificare comportamenti o elementi sospetti durante il processo di assunzione. Inoltre, durante il processo di assunzione dovrebbero essere effettuati controlli per verificare l'identità dei candidati.[127]

8.2 Minaccia a sistemi di controllo industriali e tecnologie operative

La digitalizzazione non solo porta all'impiego via via più massiccio delle tecnologie informatiche nell'ambito dei dati e delle informazioni, ma coinvolge e controlla sempre più anche i processi fisici. La tecnologia operativa (OT) utilizzata, come i sistemi di controllo industriale (ICS) – che in passato era perlopiù isolata – ora è sempre più interconnessa alla restante architettura, il che la espone anche ai rischi derivanti da questo ecosistema.

Chi non opera in ambito industriale entra tendenzialmente in contatto con questa evoluzione attraverso i progressi nel campo dell'automazione degli edifici, con i progetti di domotica «smart home». Non sorprende quindi che gli specialisti della sicurezza in ambito industriale abbiano osservato un aumento dei tentativi di attacco ai danni dell'automazione degli edifici.[128]

Gli attacchi andati a buon fine contro questi sistemi di matrice industriale, con pesanti ripercussioni sul mondo fisico, continuano a essere registrati quasi esclusivamente nell'ambito di conflitti già in corso. Alla fine di luglio del 2024, ad esempio, è stato reso noto che dietro un blackout di due giorni di un impianto di riscaldamento che alimentava circa 600 edifici residenziali in Ucraina vi era un attacco di sabotaggio. Il malware «FrostyGoop», sviluppato ad hoc per l'attacco, è stato dispiegato tramite Modbus, il protocollo che viene utilizzato in sistemi industriali ciberfisici.[129] Il secondo conflitto, che sta imperversando in Medio Oriente, vede anch'esso il continuo susseguirsi di ciberattacchi, seppur con un ruolo secondario. Alcuni soggetti già associati ai Guardiani della Rivoluzione iraniani in precedenti attacchi, ad esempio, hanno utilizzato il malware «IOCONTROL» per manipolare dispositivi IoT e OT.[130] Sul fronte opposto, un gruppo di hacktivisti che si fa chiamare «Red Devil» ha affermato di aver sabotato alcuni impianti di depurazione delle acque nel sud del Libano.[131]
Oltre ai ciberattacchi, anche gli interventi fisici hanno un impatto sulle tecnologie dell'informazione e della comunicazione. Alcuni pager e ricetrasmittenti di Hezbollah, ad esempio, sono stati manipolati all'interno della catena di produzione e distribuzione e fatti esplodere dopo la

---

127 The latest in North Korea's fake IT worker scheme: Extorting the employers (therecord.media)
Questo documento dettagliato delle autorità britanniche contiene una serie di raccomandazioni:
Advisory on North Korean IT Workers (gov.uk)

128 2024 Global Threat Roundup (forescout.com)

129 Impact of FrostyGoop ICS Malware on Connected OT Systems (dragos.com)

130 Inside a New OT/IoT Cyberweapon: IOCONTROL (claroty.com)

131 Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks (securityweek.com)

consegna.[132] Nel Mar Baltico, la distruzione di una grande quantità di cavi sottomarini ha indotto gli Stati costieri interessati a rafforzare le misure di sicurezza per la loro protezione.[133]

Al di fuori delle zone di guerra si registrano anche tentativi di sabotaggio isolati da parte di hacktivisti legati alle parti in conflitto. Il gruppo filorusso «Z-Pentest», ad esempio, ha manomesso alcuni sistemi di controllo di pompe danesi, i cui effetti sono stati tuttavia contenuti.[134]

In futuro il «Cyber Resiliency Act» (CRA), entrato in vigore a livello europeo il 10 dicembre 2024, potrebbe fornire un contributo importante al miglioramento della protezione dei sistemi OT e IoT, imponendo ai produttori l'obbligo di approntare una quantità minima di funzioni di sicurezza.[135]

Raccomandazioni

Mettete al sicuro i vostri sistemi industriali onde evitare gli attacchi descritti in questo capitolo. A tale proposito l'UFCS propone alcune Misure di protezione dei sistemi di controllo industriali (ICS). Lievemente più complessi sono gli standard minimi per diversi settori, che l'Ufficio federale per l'approvvigionamento economico del Paese UFAE ha definito in collaborazione con le rispettive organizzazioni di settore.

132 Lebanon pager and walkie-talkie explosions: What we know so far (apnews.com)
133 We assume damage to Baltic Sea cables was sabotage, German minister says (theguardian.com)
134 »Koden var 1234«: For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere (jyllands-posten.dk)
135 Cyber Resilience Act (digital-strategy.ec.europa.eu)