18 novembre 2025 | Ufficio federale della cibersicurezza UFCS

Rapporto semestrale 2025/I (gennaio – giugno)

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 primo semestre del 2025 l'UFCS ha ricevuto 35 727 segnalazioni di ciberincidenti, a conferma di una tendenza che si è ormai stabilizzata a un livello elevato. Il 58 per cento di esse riguarda il fenomeno delle «truffe». Anche se le principali forme di minaccia in Svizzera sono rimaste invariate, il modus operandi degli aggressori si è distinto per innovazione e ha mostrato alcuni sviluppi interessanti.

La sfida del ransomware e dell'estorsione di dati
Il «ransomware»[1], con relativa estorsione di dati, continua a rappresentare una seria minaccia per qualsiasi organizzazione in Svizzera. Gli attacchi segnalati all'UFCS – principalmente da imprese e organizzazioni – sono stati 57, in lieve aumento rispetto ai 44 registrati nello stesso periodo dell'anno precedente. La maggior parte delle segnalazioni relative alla variante di ransomware conteneva nuovamente «Akira», seguita a breve distanza dalle crittografie di dati di LockBit. Una delle principali sfide per le organizzazioni sono i ciberattacchi all'interno della catena di fornitura che, colpendo un'impresa informatica, possono avere conseguenze negative anche sui rispettivi clienti.

Pubblicità fraudolenta come vettore d'attacco
Uno dei temi rilevanti emersi nella diffusione di «phishing in tempo reale»[2], «software dannosi»[3] e prodotti d'investimento fraudolenti è stato il crescente abuso di pubblicità a pagamento in motori di ricerca e social media. Si tratta di annunci che vengono utilizzati per indurre le vittime a prendere decisioni avventate, soprattutto nel caso delle «truffe degli investimenti online»[4]. Un altro fenomeno ormai affermatosi anche in Svizzera è il modello della truffa di rimborso dopo che una truffa dell'investimento online è andata a buon fine.

Phishing: nel mirino i clienti bancari
Nel primo semestre del 2025 varie campagne di phishing in tempo reale e phishing in due fasi hanno preso di mira soprattutto i clienti bancari svizzeri. Attraverso annunci pubblicitari a pagamento che comparivano nei motori di ricerca prima delle vere pagine di login, le vittime venivano reindirizzate verso siti di e-banking fasulli. Sempre tramite annunci sono stati diffusi siti di phishing per sottrarre dati delle carte di credito, credenziali d'accesso Twint e login a piattaforme di e-banking. Un altro fenomeno segnalato sempre più frequentemente sono stati gli attacchi di phishing in due fasi: i clienti bancari vengono inizialmente indotti a inserire su un sito di phishing dati meno sensibili, come il loro numero di telefono, dopodiché i truffatori utilizzano quelle informazioni per contattare la vittima, fingendo pagamenti sospetti e ottenendo così l'accesso all'e-banking.

---

1 Ransomware (ncsc.admin.ch)
2 Phishing, vishing, smishing (ncsc.admin.ch)
3 Malware (ncsc.admin.ch)
4. Truffa dell'investimento (ncsc.admin.ch)

Hacktivismo: gli attacchi DDoS si confermano uno strumento consolidato

Anche nel periodo in rassegna la Svizzera è stata vittima di attacchi alla disponibilità (DDoS)[5]. Oltre a gruppi filo-palestinesi, anche vari collettivi di hacktivisti filo-russi[6] hanno sferrato attacchi DDoS con l'intento di bloccare temporaneamente servizi accessibili via Internet, come i siti web. Tuttavia, sia durante il «World Economic Forum» (WEF) che all'«Eurovision Song Contest» (ESC) si è riusciti a evitare conseguenze significative grazie a misure di prevenzione e difesa mirate. Gli attacchi DDoS non comportano accessi al sistema, ma sovraccaricano i servizi con richieste, causando disturbi temporanei. Durante eventi di risonanza internazionale rappresentano dunque uno strumento allettante per gli hacktivisti per ottenere visibilità mediatica e generare incertezza nell'opinione pubblica.

Altri fenomeni

A causa della sua forte interdipendenza a livello internazionale dovuta all'utilizzo di software ampiamente diffusi, anche il panorama informatico svizzero è interessato da vulnerabilità di rilevanza globale. Tali vulnerabilità vengono sfruttate dagli aggressori per ottenere un primo accesso ai sistemi informatici delle aziende, con conseguenti potenziali fughe di dati. Anche attori statali possono servirsi di questo mezzo per compiere attività di spionaggio e sabotaggio. Per quanto riguarda le ciberminacce, ad oggi la Svizzera ha mantenuto una situazione relativamente stabile, benché risulti sempre più difficile muoversi in un contesto internazionale segnato da tensioni ed escalation geopolitiche.

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

6 Cfr. Rapporto semestrale 2023/1, cap. 2.

Indice

Editoriale **4**
1 Ciberminacce in Svizzera – panoramica **6**
2 Phishing **8**
3 Malware **13**
3.1 Accesso iniziale con malware 13
3.2 Ransomware 15
3.3 Malvertising: abuso di annunci pubblicitari in motori di ricerca 18
4 Vulnerabilità **19**
5 Truffe e ingegneria sociale **20**
6 Attacchi alla disponibilità di siti e servizi online **24**
7 Gestione, fughe ed estorsioni di dati **25**
8 Ciberspionaggio e sabotaggio **27**
8.1 Ciberspionaggio 28
8.2 Minaccia a sistemi di controllo industriali e tecnologie operative 30

Editoriale

Nel primo semestre del 2025 la Svizzera ha ospitato due grandi eventi di rilevanza internazionale: a gennaio il «World Economic Forum» (WEF) a Davos, a maggio l'«Eurovision Song Contest» (ESC) a Basilea. Queste manifestazioni finiscono spesso nel mirino degli hacktivisti, che ne sfruttano la visibilità mediatica globale per diffondere messaggi politici alterando o disturbando il funzionamento di siti web e guadagnandosi così l'attenzione dei media. Grazie a una prevenzione mirata, a misure tecniche di protezione e a una stretta collaborazione con gli organizzatori e le autorità di sicurezza, gli attacchi DDoS verificatisi in Svizzera nel contesto di questi due eventi sono stati respinti con successo. Decisiva è stata la collaborazione coordinata e lungimirante, che dimostra il giusto percorso intrapreso dalla Svizzera in materia di cibersicurezza, così come auspicato con la Ciberstrategia nazionale (CSN).

Allo stesso tempo, tuttavia, emerge anche un'altra dimensione della minaccia: a finire nel mirino dei cibercriminali non sono solo gli eventi, sfruttati come palcoscenico, ma anche personalità famose. L'Ufficio federale della cibersicurezza (UFCS) sta ricevendo dalla popolazione numerose segnalazioni di annunci pubblicitari fasulli, in cui viene fatto credere, ad esempio, che la presidente della Confederazione Karin Keller-Sutter promuove una piattaforma d'investimento. I truffatori utilizzano la tecnologia deepfake per imitare il volto e la voce della presidente della Confederazione e quindi infondere fiducia. Queste manipolazioni apparentemente reali mirano a inibire la capacità di giudizio delle vittime. Perfida è soprattutto la tattica di abbinare un volto noto a una voce falsificata e alla promessa di lauti guadagni per aumentare notevolmente la credibilità della truffa. L'UFCS informa regolarmente in merito a come riconoscere questi deepfake e a quali precauzioni adottare, invitando alla massima cautela.

Anche la situazione delle minacce in generale rimane tesa: nel primo semestre del 2025 l'UFCS ha ricevuto circa 36 000 segnalazioni – un valore stabile, ma sempre elevato. Oltre la metà (58%) riguardava tentativi di truffa. I criminali perfezionano costantemente i loro metodi: di recente, ad esempio, si è osservata una tecnica di phishing in due fasi, in cui le vittime sono state prima attirate su siti web fraudolenti e poi contattate per telefono. L'obiettivo era ottenere dati sensibili, come le credenziali di accesso all'e-banking, tramite stratagemmi psicologici.

Nell'ambito delle imprese cresce l'attenzione verso gli attacchi ai danni dei fornitori di servizi informatici. Questi episodi non colpiscono soltanto i diretti interessati, ma anche i loro clienti, ad esempio in caso di pubblicazione di dati riservati sul darknet. La cibersicurezza nella catena di fornitura sta dunque diventando un tema rilevante. L'UFCS assiste le imprese con strumenti e raccomandazioni per difendersi più efficacemente da questi attacchi indiretti.

Un altro passo importante per rafforzare la ciberresilienza è stato compiuto con l'introduzione dell'obbligo di segnalare i ciberattacchi contro le infrastrutture critiche. Dal 1° aprile 2025 i gestori di queste infrastrutture sono tenuti per legge a segnalare all'UFCS gli incidenti gravi, garantendo in tal modo la trasmissione rapida di informazioni rilevanti, l'individuazione tempestiva dei rischi e l'attivazione di misure coordinate.
La cibersicurezza è un tema onnipresente sia sulla scena politica che in occasione di grandi eventi o nella vita di tutti i giorni. È quindi fondamentale che tutti i soggetti coinvolti –

dall’amministrazione all’economia e alla popolazione – si assumano le proprie responsabilità nei confronti della cibersicurezza: la resilienza, infatti, si costruisce dove collaborazione, vigilanza e tecnologia vanno di pari passo.

Florian Schütz, direttore dell’Ufficio federale della cibersicurezza

1 Ciberminacce in Svizzera – panoramica

Nel ciberspazio sono diversi gli attori che, con motivazioni e capacità differenti, influenzano il panorama delle minacce per imprese, organizzazioni e privati. Mentre altri Paesi occidentali sono stati indotti ad apportare significativi cambiamenti al loro sistema di analisi dei rischi per quanto concerne le infrastrutture critiche, soprattutto a causa delle tensioni e dell'escalation sulla scena geopolitica internazionale, sinora la Svizzera ha goduto di una situazione relativamente stabile in ambito ciber. Sebbene gli esperti di sicurezza registrino costantemente cambiamenti e sviluppi complessi dovuti a tecniche di attacco sempre più innovative, le principali minacce osservate e le relative conseguenze sono rimaste relativamente costanti nel tempo.
Affinché in futuro si possa avere una valutazione più ampia della situazione delle ciberminacce e allertare con dovuto anticipo i gestori di infrastrutture critiche, il Parlamento svizzero ha introdotto l'obbligo di segnalare i ciberattacchi contro tali infrastrutture.[7] Dal 1° aprile 2025 l'UFCS riceve le segnalazioni tramite il «Cyber Security Hub» (CSH). Poiché l'obbligo è stato introdotto a metà del periodo in esame, l'arco di tempo considerato è ancora troppo breve, per cui i casi soggetti all'obbligo di segnalazione verranno analizzati sistematicamente soltanto a partire dal secondo rapporto semestrale del 2025. Come avvenuto finora, il presente rapporto si basa dunque prevalentemente su segnalazioni volontarie provenienti dalla popolazione e dal settore economico.

Il numero di segnalazioni pervenute nel primo semestre del 2025, pari a 35 727 in totale[8], segna un lieve aumento di 938 unità rispetto al primo semestre dell'anno precedente (cfr. fig. 1). Anche in questo semestre, la categoria «truffa» si conferma la modalità di attacco più segnalata (cfr. fig. 2). Due fenomeni, in particolare, sono mutati rispetto al passato: mentre le segnalazioni di «telefonate minatorie a nome di false autorità»[9] sono drasticamente diminuite rispetto all'anno scorso, passando da 13 730 a 10 578, mentre quelle relative alla «truffa della pubblicità per investimenti» sono risultate in aumento. In quest'ultima casistica spicca in particolare il mese di marzo con ben 851 segnalazioni, un numero cresciuto di quasi otto volte rispetto allo stesso periodo dell'anno precedente (112 segnalazioni). Anche sul fronte del ransomware l'UFCS ha registrato un aumento dei casi, che da 44 nella prima metà del 2024 sono passati a 57 nel primo semestre del 2025. Ad aprile, in particolare, si è osservato un picco di segnalazioni, probabilmente riconducibile all'attenzione mediatica e al dibattito crescenti sull'introduzione dell'obbligo di segnalazione dei ciberattacchi. Da maggio 2025 il numero di segnalazioni è tornato a oscillare tra zero e due casi alla settimana.

Il rapporto tra le segnalazioni provenienti da privati (90%) e quelle da parte di imprese, associazioni e autorità (10%) è rimasto costante. Come i privati, anche le imprese sono vittime di «telefonate minatorie a nome di autorità» e di tentativi di «phishing».

---

7 Informazioni sull'obbligo di segnalare (ncsc.admin.ch)

8 Nelle sue statistiche l'UFCS riporta tutte le segnalazioni pervenute, tra cui anche domande generiche, informazioni e segnalazioni non classificabili. Nel primo semestre del 2025 sono state 1430 le segnalazioni non attribuibili a un fenomeno o un incidente specifico.

9 Per affrontare più approfonditamente il fenomeno delle telefonate minatorie a nome di false autorità, l'UFCS ha redatto un rapporto che è stato pubblicato contestualmente al rapporto semestrale 2024/1.

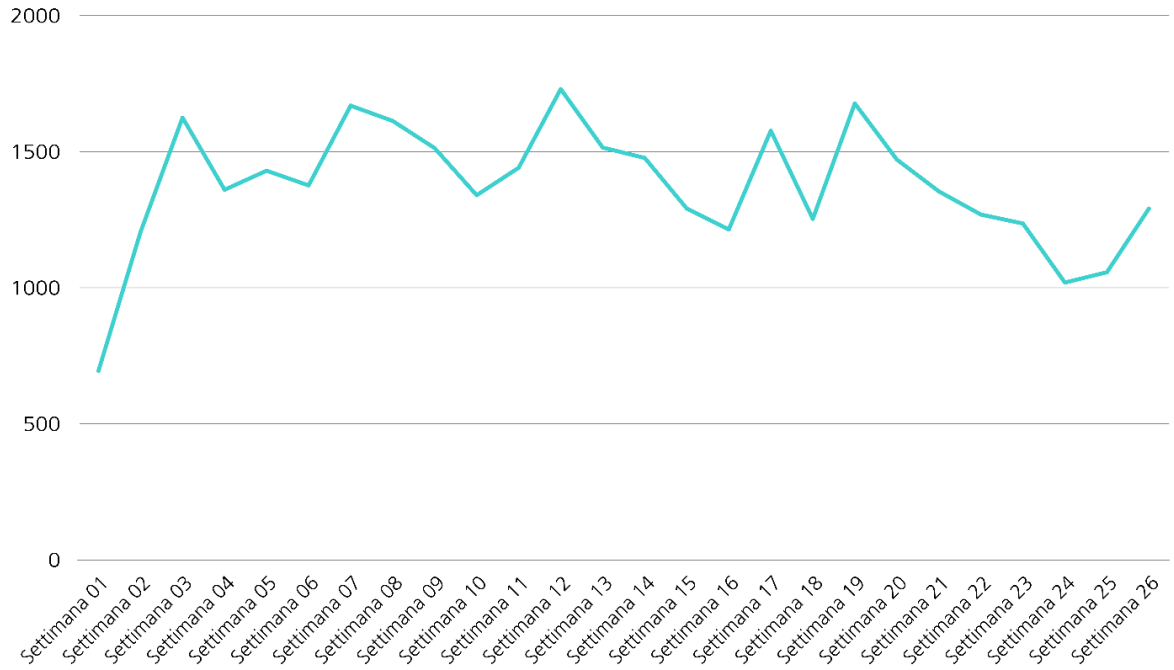

Fig. 1: Segnalazioni settimanali all'UFCS nel primo semestre 2025, cfr. numeri attuali (ncsc.admin.ch).

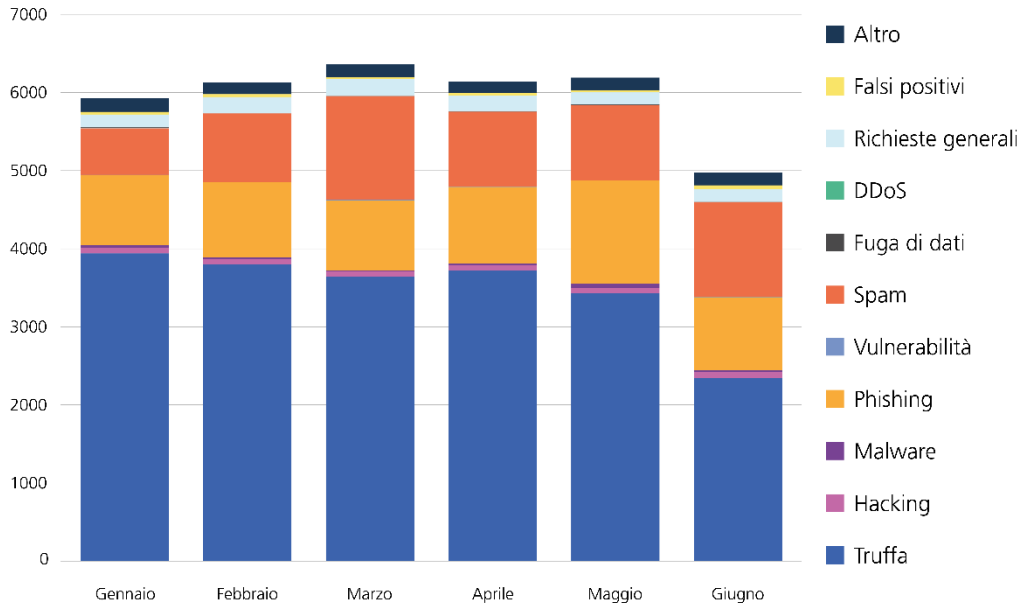

Fig. 2: Segnalazioni all'UFCS nel primo semestre del 2025 per categoria, cfr. numeri attuali (ncsc.admin.ch).

Due tipologie di attacco tipicamente rivolte contro le organizzazioni sono state invece il cosiddetto «Business E-Mail Compromise»[10] e la «truffa del CEO»[11] (cfr. cap. 5). Quest'ultimo fenomeno, in particolare, è risultato in forte aumento, a conferma della tendenza già osservata nell'ultimo anno.[12] I 605 tentativi di truffa del CEO segnalati nel periodo in esame equivalgono alla quasi totalità dei casi registrati in tutto il 2024. Tra le vittime si contano ancora una volta soprattutto Comuni, scuole e parrocchie.

Le statistiche evidenziano quanto la cibersicurezza e la protezione della Svizzera dai cyber-rischi 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 per la Svizzera nel ciberspazio: phishing, malware, vulnerabilità, truffe e ingegneria sociale[13], attacchi alla disponibilità di siti web e altri servizi Internet (DDoS), fughe di dati, ciberspionaggio e sabotaggio informatico. L'attenzione è rivolta in particolare agli eventi e agli sviluppi in territorio svizzero, mentre le evoluzioni a livello internazionale vengono citate soltanto se utili a illustrare il panorama delle minacce in Svizzera (cfr. cap. 8). Grazie ai capitoli tematici i lettori possono farsi un'idea generale delle loro forme e declinazioni attuali, nonché di episodi interessanti e dell'evoluzione dei principali fenomeni. 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

Il phishing consente ai ciberattori di raccogliere credenziali di accesso, informazioni finanziarie e altri dati riservati all'insaputa degli utenti. Ciò che contraddistingue questo tipo di attacco è il fatto di far leva sulla manipolazione psicologica (ingegneria sociale) dei destinatari senza diffondere malware.[14] La procedura classica consiste nell'invio di un messaggio contenente un link a un vasto numero di destinatari. Il link rimanda a un sito di phishing all'apparenza legittimo. Se il sito viene ritenuto credibile, la vittima vi inserisce dati sensibili – ad esempio credenziali di accesso o dati della carta di credito – che finiscono così nelle mani dei truffatori. Sebbene il phishing via e-mail continui a essere uno dei metodi più comunemente utilizzati, esistono altri approcci che sfruttano la voce (voice phishing o «vishing») o gli SMS («smishing») e altre forme di messaggistica mobile per estorcere informazioni. Se invece il phishing è mirato a una persona o un'organizzazione specifica, si parla di «spear phishing». Rispetto alla variante più diffusa, questa forma è molto più difficile da individuare, essendo confezionata su misura in funzione dei rispettivi bersagli.

---

10 Business E-Mail Compromise (BEC) (ncsc.admin.ch)

11 Truffa del CEO (ncsc.admin.ch)

12 Cfr. anche Rapporto semestrale 2024/2, cap. 5.3.

13 Ingegneria sociale (ncsc.admin.ch)

14 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 primo semestre del 2025 l'UFCS ha ricevuto 5981 segnalazioni di tentativi di phishing tramite l'apposito modulo, 662 in meno rispetto allo stesso periodo dello scorso anno. Un andamento simile emerge dalle statistiche delle segnalazioni pervenute tramite la piattaforma antiphishing.ch[15] gestita dall'UFCS, in cui, anche in questo caso, dopo mesi di continua crescita si osserva una riduzione. Mentre nel primo semestre del 2024 gli URL di phishing unici documentati sono stati 11 505, nello stesso periodo del 2025 sono scesi a quota 7412. Per rendere i siti di phishing il più affidabili possibile, 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 i servizi postali (23%), il settore finanziario (22%), i trasporti pubblici (19%), il settore informatico (9%) e le telecomunicazioni (7%). Dall'inizio del 2025 si è registrato un continuo aumento, pari a una media del sei per cento, delle segnalazioni di siti di phishing unici che simulavano siti di compagnie assicurative, tra cui ad esempio le casse malati. Opposta, invece, la dinamica sul fronte del settore informatico, dove nel periodo in esame si è registrata una contrazione del fenomeno. Una drastica riduzione delle segnalazioni si è osservata in particolare nei mesi di marzo e aprile, dovuta principalmente ai minori attacchi di phishing subiti dai trasporti pubblici (cfr. fig. 3).
La maggior parte delle segnalazioni riguardava il classico phishing con carte di credito. Anche in questo caso, tuttavia, i criminali hanno cercato di migliorare le loro chance di successo limitando, ad esempio, l'accesso ai siti di phishing agli utenti di dispositivi mobili. Poiché le autorità lavorano prevalentemente con i computer, la probabilità di essere scoperti in breve tempo si riduce. Si continua inoltre a osservare un numero elevato di attacchi ai danni di Microsoft 365 sotto forma di «chain phishing»[16], talvolta in abbinamento a tecniche di elusione dell'autenticazione a più fattori (MFA). L'UFCS ha registrato anche tentativi di phishing più sofisticati ai danni di account di Twint o e-banking, in cui i criminali hanno utilizzato come pretesto, ad esempio, piattaforme di annunci o una procedura in due fasi in combinazione con voice-phishing. Pur essendo più complessi delle classiche e-mail di phishing, questi metodi infondono fiducia e quindi aumentano le probabilità di successo per i truffatori. La loro credibilità è favorita soprattutto dal contatto personale – a volte protratto per diversi giorni – che consente ai criminali di reagire prontamente a eventuali sospetti delle vittime.

---

[15] 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.

[16] Il chain phishing consiste nell'invio di spam o messaggi di phishing attraverso una sorta di catena di Sant'Antonio, con cui – una volta compromessa la casella di posta elettronica – si inviano istantaneamente messaggi di phishing a tutti i contatti della rubrica.

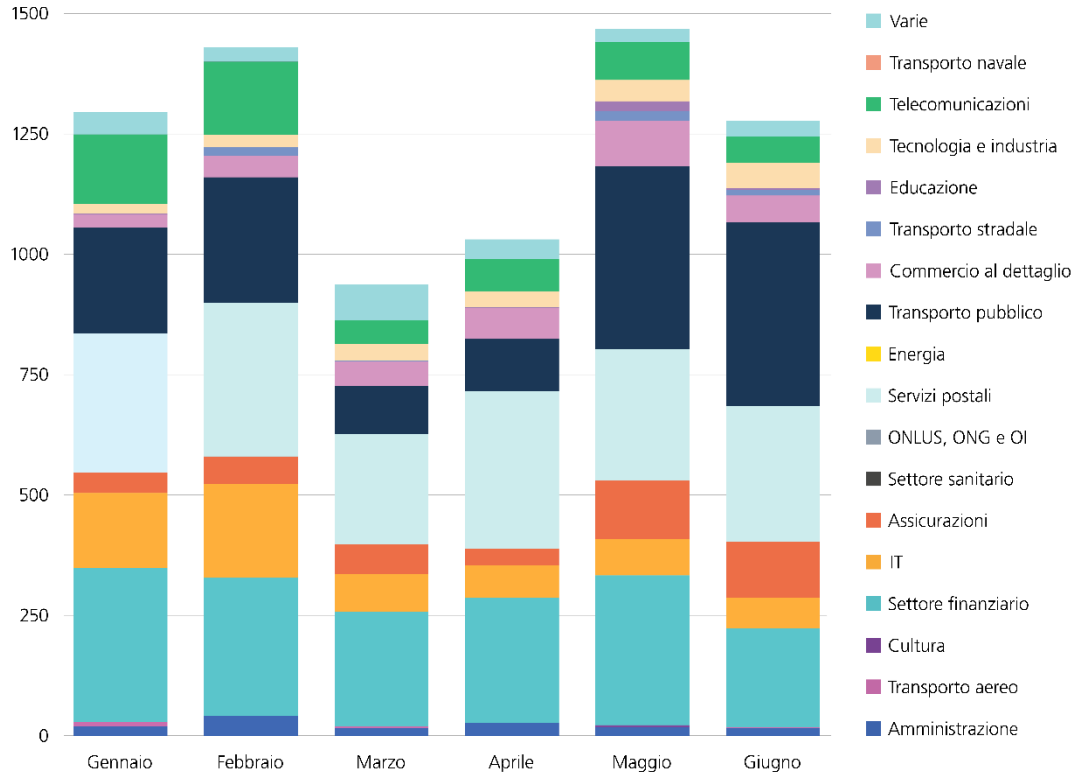

Fig. 3: Numero di URL di phishing verificati e confermati dall'UFCS nel primo semestre 2025, per settore di marchi sfruttati.

Raccomandazioni

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

Phishing in tempo reale: nel mirino le applicazioni bancarie

Per garantire una maggiore protezione nell'accesso all'e-banking e nell'autorizzazione dei pagamenti, le banche svizzere fanno in genere ricorso alla MFA (Multi Factor Authentification), richiedendo codici SMS o una conferma push. In questo modo si evita che si possa accedere ad applicazioni bancarie attraverso credenziali d'accesso rubate. Solo fino a un decennio fa, per aggirare i meccanismi di sicurezza delle applicazioni bancarie i criminali utilizzavano prevalentemente malware, come ad esempio «Retefe» nel caso dell'«Operazione Emmental»[17]. Oggi, invece, i malware bancari sono pressoché scomparsi in Svizzera. Gli attacchi ai danni di conti correnti online sono avvenuti perlopiù mediante ingegneria sociale e il phishing in tempo reale, soprattutto verso la fine di giugno del 2025. A differenza del classico

[17] Cfr. Retefe –presunti attacchi a clienti bancari svizzeri (ncsc.admin.ch)

phishing, nel cosiddetto real-time phishing gli aggressori rubano le credenziali in tempo reale per poi sfruttarle immediatamente prima che perdano di validità.
Attraverso annunci pubblicitari a pagamento pubblicati nei motori di ricerca prima delle vere pagine di login, le vittime vengono reindirizzate verso siti di e-banking fasulli. Queste campagne di phishing, che emulavano soprattutto le banche cantonali, contenevano spesso domini[18] con le estensioni «.app», «.digital» o «.help».[19] Nel momento in cui qualcuno inserisce i propri dati di accesso nella pagina contraffatta, in background i truffatori si connettono al vero sito di e-banking, creando un accesso parallelo. Nel frattempo si tiene occupata la vittima simulando un ritardo nel processo di login, ad esempio visualizzando una clessidra. Quando il vero sito di e-banking chiede il secondo fattore di autenticazione, i phisher inoltrano la richiesta al dispositivo della vittima. Una volta che quest'ultima ha inserito il secondo fattore, i malviventi accedono al suo conto online. Per non destare sospetti, successivamente i truffatori inviano alla vittima un messaggio di errore che la invita a effettuare nuovamente l'accesso.

Appropriazione di account Twint tramite annunci

Anche con gli annunci si utilizza spesso il phishing in tempo reale, tanto che dal mese di agosto del 2024 questi tentativi di attacco si sono quintuplicati (cfr. fig. 4). Gli attacchi iniziano spesso discretamente: un presunto acquirente contatta il venditore poco dopo la pubblicazione dell'annuncio e propone di organizzare la consegna e il pagamento anticipato, ad esempio tramite la Posta Svizzera. A quel punto la vittima riceve un link per ritirare il denaro apparentemente già versato. Il sito fraudolento a cui si viene indirizzati chiede a tal fine i dati della carta di credito, le credenziali di accesso a Twint o il login all'e-banking. Questi siti hanno tutte le carte in regola per essere credibili perché sono studiati appositamente per l'offerta commerciale specifica, con tanto di prezzo corretto e foto del prodotto.

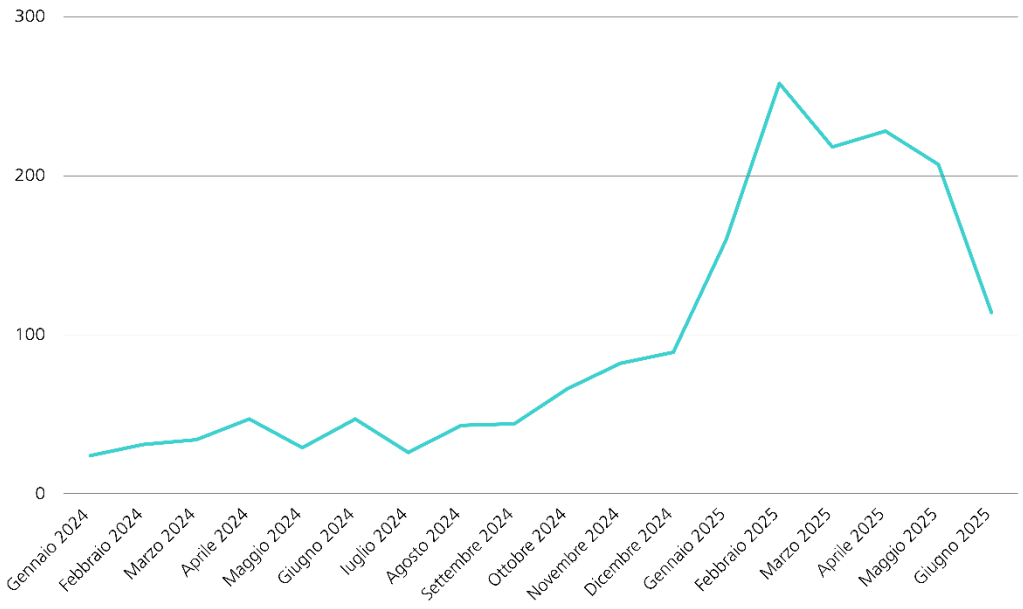

Fig. 4: Aumento del phishing tramite annunci da gennaio 2024

[18] Cfr. Glossario (ncsc.admin.ch), voce Domini.
[19] Cfr. Attenzione: Phishing in tempo reale a nome delle banche cantonali (ncsc.admin.ch)

Una volta inseriti i dati, i criminali tengono occupata la vittima così da potersi connettere in background al suo e-banking. Pare che l'obiettivo primario dei truffatori non siano tanto i conti online, quanto invece gli account Twint ad essi collegati. Anziché effettuare un pagamento fraudolento tramite e-banking, collegano uno dei loro dispositivi all'account Twint della vittima, così da poter eseguire istantaneamente transazioni irrevocabili. Spesso, inoltre, la truffa non viene rilevata dalle banche se non dopo un certo periodo di tempo, consentendo potenzialmente ai criminali di prelevare ulteriori somme. Le tracce del furto vengono cancellate trasferendo il denaro rubato su più conti, alcuni dei quali hackerati.

Attacchi di phishing in due fasi e voice phishing

Una sottovariante del phishing in tempo reale è il voice phishing. La novità di questa forma di attacco è l'utilizzo crescente di una procedura in due fasi. Inizialmente i truffatori sfruttavano siti di phishing per ottenere dalle vittime informazioni meno sensibili, ossia non i dati di accesso all'e-banking, ma ad esempio il numero di telefono e l'istituto bancario di riferimento.

In una seconda fase, la procedura segue il classico schema del voice phishing: i truffatori telefonano alla vittima fingendosi spesso «il signor Bianchi» del reparto Sicurezza della banca indicata nel phishing. Di solito il numero visualizzato corrisponde effettivamente a un numero ufficiale di quella banca, che viene falsificato mediante tecniche di spoofing[20] – come si fa ad esempio anche per gli indirizzi e-mail. I truffatori fanno credere alle vittime di voler bloccare un addebito fraudolento, che in numerose segnalazioni viene quantificato in CHF 800. Per impedire la truffa, alla vittima viene chiesto di installare sul computer un software di accesso remoto e di autorizzare l'accesso sia al proprio terminale che al conto bancario. In questo modo i criminali possono effettuare operazioni di nascosto nell'e-banking della vittima. Questi casi evidenziano l'importanza di una solida formazione del personale bancario a contatto con la clientela. In caso di domande da parte di clienti scettici, spetta loro avvertirli tempestivamente di potenziali tentativi di truffa commessi a nome della banca.

Raccomandazioni

Attivate dove possibile l'autenticazione a più fattori (MFA) come ulteriore meccanismo di sicurezza dei vostri account. Nonostante la MFA riduca enormemente il rischio di compromissione, anch'essa può essere aggirata con varie tecniche di ingegneria sociale (social engineering)[21]. Fate dunque attenzione alle richieste fasulle – soprattutto via e-mail e SMS – quando vi viene chiesto di confermare accessi o trasmettere a qualcun altro il vostro token di sicurezza. Ricordate anche che i mittenti delle e-mail e i numeri di telefono possono essere facilmente falsificati per dare maggiore credibilità ai messaggi. Non inserite mai le credenziali della carta di credito o altri dati sensibili in un sito che avete aperto da un link inviato tramite e-mail o un messaggio di testo.

20 Spoofing (ncsc.admin.ch)

21 Ingegneria sociale (ncsc.admin.ch)

3 Malware

I software dannosi (i cosiddetti «malware») sono uno dei principali strumenti utilizzati dai criminali per procurarsi l'accesso a un dispositivo o una rete. Di norma si tratta di programmi che, all'insaputa degli utenti, eseguono funzioni indesiderate e perlopiù maligne ai danni di sistemi informatici[22], come ad esempio il furto, la manipolazione e/o la distruzione di dati. L'infezione da malware può avvenire attraverso diverse modalità e canali, e può colpire qualsiasi tipo di dispositivo e infrastruttura.

3.1 Accesso iniziale con malware

Per accesso iniziale s'intendono tutte le azioni necessarie a un aggressore per compromettere un sistema estraneo. Le tecniche generalmente utilizzate a tal fine sono, ad esempio, la conoscenza delle credenziali d'accesso (ad es. nome utente e password) attraverso ingegneria sociale e phishing (cfr. cap. 2), lo sfruttamento di vulnerabilità (cfr. cap. 4) o anche il ricorso a malware, ad esempio trojan. Quest'ultima modalità richiede di norma un'azione da parte degli utenti che, attraverso vari meccanismi di inganno (ingegneria sociale), vengono indotti a installare il software dannoso sui propri sistemi. Il malware, ad esempio, può essere nascosto in un altro programma o in un allegato o un link ricevuto via e-mail, che a primo acchito può sembrare innocuo.

Anche nel primo semestre del 2025 l'UFCS ha osservato varie campagne di diffusione di malware finalizzate a infettare i sistemi. Oltre all'abuso di file immagine «.svg», gli aggressori hanno fatto ricorso, ad esempio, all'invio di fatture false per installare malware sui terminali delle vittime. La maggior parte di queste campagne di diffusione, tuttavia, non presentava caratteristiche specifiche per la Svizzera, bensì era in linea con i modelli internazionali.
Secondo i dati in possesso dell'UFCS, la diffusione di malware via e-mail («malspam») riveste un ruolo tendenzialmente secondario negli attacchi alle reti aziendali, mentre l'utilizzo di siti compromessi[23] o l'attivazione di pubblicità malevola («malvertising») sui motori di ricerca[24] sono tecniche sempre più diffuse tra i cibercriminali (cfr. cap. 3.3).

Tra questi modus operandi si è registrato un crescente utilizzo del metodo «ClickFix»[25], un fenomeno osservato soprattutto in relazione a siti che imitano noti portali di prenotazione alberghiera. In pratica, tramite siti malevoli o apparentemente affidabili, ma compromessi si copia uno script negli appunti, dopodiché viene chiesto all'utente di eseguire la combinazione di tasti «Windows + R», «Windows + X» o «CTRL + V» per una presunta operazione

22 Software dannoso (ncsc.admin.ch)
23 ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery (sekoia.io)
24 University site cloned to evade ad detection distributes fake Cisco installer (malwarebytes.com)
25 Cfr. Rapporto semestrale 2024/2, cap. 3.1.

necessaria. Con il pretesto di un CAPTCHA[26] o dell'accettazione di cookie[27] gli aggressori inducono le vittime a compiere l'azione desiderata. In realtà, tuttavia, quest'ultima provoca l'esecuzione dello script malevolo copiato negli appunti e quindi l'installazione di un malware, ad esempio tramite PowerShell.[28]

«Lumma Stealer» è un malware che, documentato ormai da tempo e spesso osservato in associazione alla tecnica ClickFix, sembra essersi progressivamente affermato come strumento prediletto dai cibercriminali.[29] La sua infrastruttura è stata sequestrata nel maggio del 2025 nell'ambito di un'operazione congiunta tra aziende informatiche e autorità di perseguimento penale, ostacolando almeno temporaneamente la diffusione del malware.[30] Nello stesso mese è andata in scena un'ulteriore collaborazione internazionale tra forze di sicurezza: l'«Operazione Endgame», con cui è stata smantellata l'infrastruttura di sette varianti di malware.[31] Sebbene questi interventi disturbino le attività dei provider illegali di accessi iniziali e quindi l'economia criminale, è prevedibile che questi operatori cercheranno subito di ripristinare la loro infrastruttura. Altri criminali non direttamente colpiti dalle operazioni, inoltre, sfrutteranno il vuoto creatosi sul mercato per soddisfare la domanda con i propri prodotti. Uno di essi potrebbe essere, ad esempio, il malware «Rhadamanthys», anch'esso osservato in relazione a «ClickFix» e riscontrato in campagne di diffusione via e-mail in Svizzera e in Europa. Nelle e-mail i criminali si spacciano per studi legali e minacciano la vittima di conseguenze giudiziarie per una presunta violazione dei diritti d'autore. I dettagli del reato – affermano – sarebbero contenuti in un file PDF da scaricare. Quest'ultimo, in realtà, si rivela essere un file eseguibile malevolo, che alla fine infetta il sistema con il malware «Rhadamanthys».[32]

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 consolidati se ha effettivamente inviato il messaggio in questione. Siate sempre prudenti quando aprite una finestra di download.

Quando cercate un software su Internet, prima di scaricarlo verificate di essere sui siti web dei produttori o su un altro sito affidabile. Quando utilizzate i motori di ricerca, in particolare, controllate se il sito visualizzato sia dichiarato come pubblicità a pagamento oppure no. Se si tratta di pubblicità a pagamento, occorre essere cauti. Gli aggressori utilizzano spesso questo metodo per posizionarsi ai primi posti nei risultati di ricerca.

Eseguite regolarmente le patch dei vostri sistemi e limitate per quanto possibile gli accessi. In caso di sospetta infezione, fate tempestivamente controllare e, se necessario, ripulire il

---

26 Settimana 9:Gli hotel e i loro ospiti sempre più nel mirino dei cibercriminali (ncsc.admin.ch)

27 Abuse.ch: Booking themed ClickFix campaign using a fake cookie banner (linkedin.com)

28 Cfr. Rapporto semestrale 2024/2, cap. 3.1.

29 Cfr. Rapporto semestrale 2024/2, cap. 3.1.

30 Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool (microsoft.com)

31 Operation ENDGAME strikes again: the ransomware kill chain broken at its source (europol.europa.eu)

32 Copyright Phishing Lures Leading to Rhadamanthys Stealer Now Targeting Europe (cybereason.com)

computer da uno specialista. L'opzione più sicura è quella di resettare completamente il computer, ma non dimenticate di salvare prima tutti i dati personali.

3.2 Ransomware

Il ransomware è un tipo di attacco in cui gli aggressori utilizzano un malware per crittografare i dati presenti sui sistemi informatici della vittima, rendendoli inutilizzabili per quest'ultima.[33] Prima di agire, solitamente gli aggressori realizzano una copia dei dati per poi chiedere un riscatto. In caso di pagamento i criminali promettono di fornire un tool di decodifica (decryptor). Se invece la vittima non reagisce alle loro richieste, minacciano di pubblicare i dati trafugati. Spesso, inoltre, i gruppi di ransomware cercano di aumentare ulteriormente la pressione sulla vittima per indurla a pagare, ad esempio contattando alcuni suoi clienti e fornitori per ricattarli a loro volta con la pubblicazione dei dati rubati.

Nel primo semestre del 2025 il servizio nazionale di contatto per i ciber-rischi dell'UFCS ha ricevuto 57 segnalazioni di attacchi ransomware – prevalentemente da imprese (cfr. fig. 5). La tendenza è in lieve aumento rispetto al primo semestre del 2024, quando i casi segnalati erano stati 44. È probabile che il numero effettivo di casi di ransomware in Svizzera sia lievemente superiore, dal momento che non tutte le organizzazioni colpite effettuano una segnalazione. Nella prima metà dell'anno i gruppi di ransomware più attivi nel nostro Paese si confermano i medesimi dell'anno precedente: le varianti Akira e LockBit hanno criptato i dati rispettivamente in otto e sette casi.[34] Da marzo 2023 Akira rappresenta anche a livello internazionale uno dei gruppi più attivi, minacciando organizzazioni di ogni dimensione e settore. LockBit, invece, è stato uno dei collettivi di ransomware più devastanti e influenti a livello mondiale fino a febbraio 2024. Nonostante all'inizio del 2025 sia stata sviluppata la nuova variante «LockBit 4.0», la sua attività è calata drasticamente a seguito di varie operazioni internazionali di perseguimento penale e fughe di dati interne.[35] In un numero relativamente elevato di segnalazioni (21) non vengono fornite indicazioni circa la variante di ransomware, per cui nel grafico vengono rappresentate come sconosciute.

33 Ransomware (ncsc.admin.ch)

34 Cfr. Rapporto semestrale 2024/1 e 2024/2, cap. 3.2 sulle varianti di ransomware.

35 What the LockBit 4.0 Leak Reveals About RaaS Groups (darkreadings.com)

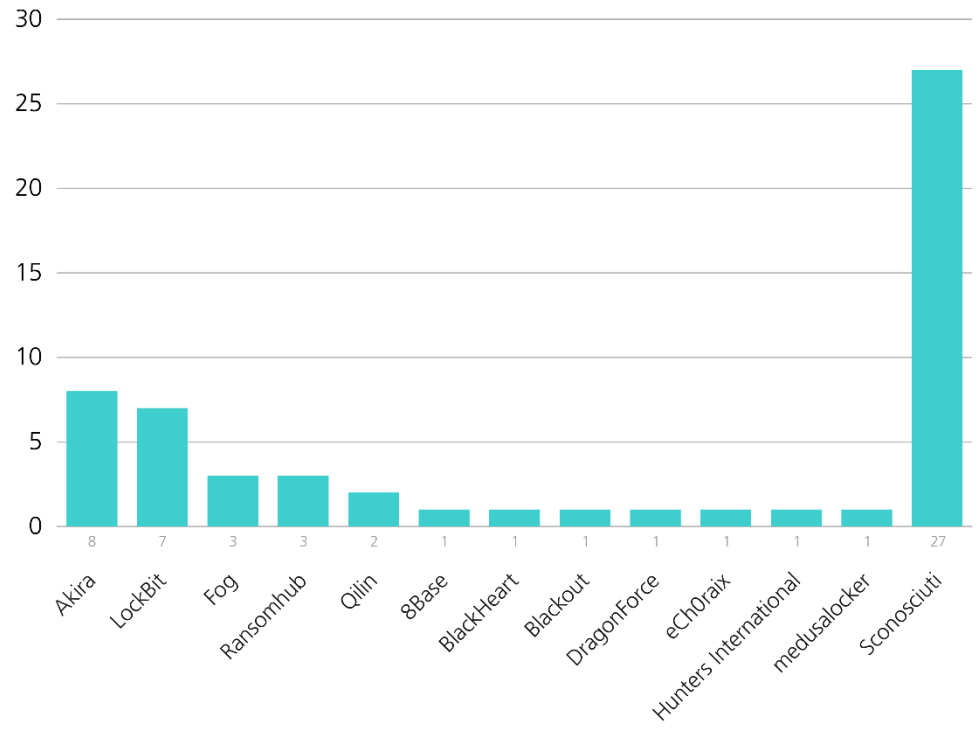

Fig. 5: Numero di casi di ransomware segnalati all'UFCS nel primo semestre del 2025

Come mostrano le statistiche, la minaccia del ransomware persiste a un livello elevato. La scena continua a essere caratterizzata dall'emergere di nuovi collettivi e dalla scomparsa o trasformazione di gruppi esistenti, una dinamica spinta tra l'altro da ristrutturazioni interne[36], fughe di dati[37] o operazioni delle autorità di perseguimento penale.[38] Nonostante nessuno dei gruppi noti abbia come bersaglio specifico le organizzazioni svizzere, gli attacchi opportunistici sono ormai diventati la norma e colpiscono pertanto anche il nostro Paese. Il loro modus operandi si basa principalmente su un accesso iniziale con malware, sullo sfruttamento di vulnerabilità o sul furto delle credenziali d'accesso tramite campagne di phishing e «Infostealer»[39]. Questa evoluzione sta prendendo forma nel contesto di un'economia criminale caratterizzata da suddivisione del lavoro e specializzazione: mentre certi attori si concentrano sull'acquisizione di accessi, altri sviluppano ad esempio nuovi software ransomware. Questo spiega il successo di modelli di business quali «Ransomware-as-a-service» (RaaS), che consentono anche a soggetti con competenze tecniche limitate di sferrare attacchi. Su piattaforme pronte all'uso gli sviluppatori mettono a disposizione gli strumenti necessari per le diverse fasi di un attacco ransomware (ad esempio esfiltrazione dei dati, cifratura, comunicazione e pagamento), provvedendo alla loro manutenzione. Il collettivo «DragonForce», attivo anche in Svizzera, è un esempio di tale tendenza: l'attività già osservata

36 Lynx Ransomware: A Rebranding of INC Ransomware (paloaltonetworks.com)

37 LockBit Ransomware Gang Hacked, Operations Data Leaked (darkreading.com)

38 Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown (europol.europa.eu)

39 Un Infostealer è un malware che raccoglie informazioni sensibili (ad esempio dati d'accesso) e le trasmette agli hacker.

nel 2023[40] offre ora, dall'inizio del 2025, una piattaforma completa che i partner possono gestire con il proprio nome. In cambio gli sviluppatori del ransomware trattengono per sé una percentuale del riscatto.[41]

Oltre all'infrastruttura utilizzata, i gruppi più abili perfezionano costantemente le loro tecniche per aggirare le misure di difesa in continuo aggiornamento. Alcuni di essi, ad esempio, impiegano ora i cosiddetti «EDR Killer», che possono essere sia malware che software legittimi, ma utilizzati in modo illecito.[42] Grazie a essi i gruppi di ransomware possono modificare o disattivare del tutto il software di sicurezza all'inizio dell'attacco, per evitare di venire scoperti troppo presto, il che dà loro il tempo di individuare i dati sensibili prima dell'esfiltrazione e della codifica. Per massimizzare l'impatto, operano principalmente in orari marginali, come di notte, nei giorni festivi o nei fine settimana.

Diversi episodi in Svizzera avvenuti nella prima metà del 2025 hanno messo in luce i rischi che gli attacchi ransomware possono comportare anche per organizzazioni terze. Una volta compromesso un fornitore, infatti, gli accessi potenzialmente sottratti possono fungere da vettori d'attacco. Si pensi ad esempio al ransomware che ha colpito Cistec, un'azienda svizzera che sviluppa software per i sistemi informatici delle cliniche: gli accessi remoti di Cistec ai sistemi ospedalieri per la manutenzione del software avrebbero potuto essere sfruttati per sferrare ulteriori attacchi contro gli stessi ospedali.[43] Altri episodi ai danni di fornitori di servizi informatici evidenziano l'impatto diretto che possono subire i clienti di un'organizzazione colpita. Nell'attacco alla filiale di Ilem, circa il 15 per cento dei clienti ha perso temporaneamente l'accesso ai servizi cloud dell'azienda.[44] Nel caso di 2sic, la società è riuscita a respingere preventivamente un attacco mettendo offline i propri sistemi, il che tuttavia ha causato un'interruzione di due o tre giorni durante i quali i clienti non hanno potuto lavorare con i sistemi.[45] Certi casi, infine, sottolineano il rischio di fughe di dati, se la vittima direttamente colpita è in possesso di informazioni relative a clienti aziendali e terzi (cfr. cap. 7). Nel caso Radix, una fondazione attiva nel campo della promozione della salute, dopo l'attacco sono stati pubblicati i dati rubati. Tra i clienti di Radix figuravano anche diverse unità amministrative dell'Amministrazione federale. Sebbene Radix non avesse accesso diretto ai sistemi di quest'ultima, non si può escludere che tra i dati compromessi vi fossero anche informazioni correlate all'Amministrazione federale.[46]

---

40 Cfr. Rapporto semestrale 2023/2, cap. 3.4.2.

41 DragonForce expands ransomware model with white-label branding scheme (bleepingcomputer.com)

42 Ransomware crews add EDR killers to their arsenal – and some aren't even malware (theregister.com)

43 Ransomware-Angriff auf KIS-Anbieter Cistec (inside-it.ch); «An einer Katastrophe vorbeigeschlittert» (inside-it.ch)

44 Ransomware-Angriff auf Genfer IT-Gruppe Ilem (inside-it.ch)

45 Ransomware Angriff auf 2sic Hosting abgewehrt (2sic.com)

46 Ciberattacco contro la fondazione Radix: Nel mirino anche i dati dell'Amministrazione federale (ncsc.admin.ch)

Raccomandazioni

Sul sito dell'UFCS è disponibile un elenco di misure preventive per proteggersi dal ransomware e varie istruzioni operative su come procedere in caso di attacco. 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 di emergenza. In generale l'UFCS e i suoi partner internazionali[47] sconsigliano alle vittime di ransomware di pagare il riscatto, non essendovi alcuna garanzia che i cibercriminali mantengano la parola data. Pagare significa finanziare i cibercriminali, consentendo loro di continuare ad ampliare le loro strutture e sferrare ulteriori attacchi.

3.3 Malvertising: abuso di annunci pubblicitari in motori di ricerca

Nel 2025 l'UFCS ha osservato diversi casi in cui gli annunci sui motori di ricerca sono stati utilizzati in modo improprio sia per il phishing (cfr. cap. 2) che per la diffusione di malware («malvertising»). I cibercriminali sfruttano in modo mirato pubblicità a pagamento che imitano siti web legittimi o marchi noti e le posizionano in evidenza sopra i risultati organici, aumentando così la probabilità che le vittime clicchino sull'annuncio malevolo. Gli utenti che giudicano erroneamente il link come affidabile vengono reindirizzati verso un sito fraudolento, il quale scarica direttamente il codice malevolo[48] o induce le vittime a eseguire il download di file d'installazione infetti. Spesso queste campagne sfruttano termini di ricerca popolari come «download», «aggiornamento» o «assistenza», oltre a software diffusi come ad esempio «Chrome». Gli aggressori possono ad esempio pubblicare un annuncio relativo a un software apparentemente ufficiale, ma che in realtà nasconde un trojan o un ransomware.
Il rischio è dato dal fatto che questa truffa funziona anche su motori di ricerca noti come Google o Bing. Gli annunci vengono prenotati e pubblicati in tempo reale, il che consente ai criminali di adattare rapidamente le loro campagne e aggirare eventuali contromisure.

Raccomandazioni

Scaricate software soltanto dai siti dei produttori ufficiali o da portali affidabili, anche se i motori di ricerca visualizzano un annuncio apparentemente veritiero. Verificate se i risultati di ricerca visualizzati sono pubblicità («sponsored») oppure se si tratta di siti normalmente indicizzati. L'utilizzo di ad blocker, patch di sicurezza aggiornate e soluzioni di protezione degli endpoint, inoltre, possono ridurre sensibilmente il rischio di infezione. Nelle aziende può essere opportuno che gli utenti consultino preventivamente i loro servizi informatici prima di scaricare di loro iniziativa software e quindi potenziali malware.

47 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)
48 What Is a Drive by Download Attack? (kaspersky.com)

4 Vulnerabilità

Per vulnerabilità s'intende una lacuna di sicurezza in un sistema informatico. Può trattarsi di una vulnerabilità a livello di software o di design, ma anche di una protezione non adeguatamente configurata, come nel caso di password standard.[49] Particolarmente critiche sono le vulnerabilità «zero day», ovvero vulnerabilità già scoperte, ma per le quali il produttore non ha ancora messo a disposizione una patch di sicurezza ufficiale, per cui potrebbero essere sfruttate dagli aggressori. La crescente digitalizzazione e l'interconnessione dei dispositivi, in particolare, possono amplificare i danni derivanti dallo sfruttamento di singole vulnerabilità o dalla loro concatenazione, compromettendo dati e sistemi.

A causa della sua forte interdipendenza a livello internazionale, il panorama informatico svizzero è direttamente esposto a vulnerabilità globali. Economia, amministrazione e infrastrutture critiche fanno perlopiù affidamento su prodotti di marchi leader a livello mondiale, motivo per cui anche nel primo semestre del 2025 la Svizzera è stata colpita da lacune di sicurezza critiche presso produttori consolidati e attivi a livello mondiale come Fortinet, Microsoft o Ivanti. Il ciberspazio e le minacce che ne derivano sono fondamentalmente indipendenti dai confini politici. Ciò che rappresenta un problema a livello globale può dunque avere ripercussioni negative anche sulla Svizzera.

Il modus operandi è noto e utilizzato ormai da tempo: in generale le categorie di sistemi con le vulnerabilità più critiche e numerose sono rimaste invariate. L'attenzione degli aggressori e degli esperti di sicurezza si concentra pertanto su due ambiti principali: da un lato i terminali degli utenti, come laptop, workstation e dispositivi mobili, dall'altro l'infrastruttura esposta a Internet. Componenti come firewall o accessi VPN rappresentano la prima linea di difesa e allo stesso tempo la principale porta d'ingresso per le compromissioni. Se gli aggressori riescono a sfruttare una vulnerabilità in questa periferia, ottengono un accesso iniziale con cui insinuarsi nella rete e compiere altre azioni.
Per le imprese e le autorità svizzere questa dinamica implica la necessità di gestire un volume costantemente elevato di aggiornamenti di sicurezza per questi componenti essenziali. Un patch management tempestivo e completo è indispensabile per proteggere gli asset digitali e garantire la resilienza contro i ciberattacchi.

Raccomandazioni

Se possibile, aggiornate automaticamente i programmi. In alternativa, utilizzate la funzione di aggiornamento integrata o scaricate la versione più recente direttamente dal produttore.
Per le imprese, in particolare, è importante allestire un solido sistema di gestione delle patch con cui eliminare tempestivamente eventuali vulnerabilità. Un presupposto fondamentale a tal fine è disporre di un inventario aggiornato delle infrastrutture e dei prodotti utilizzati. Date la priorità soprattutto alle lacune di sicurezza presenti nelle parti esposte a Internet della vostra

[49] Falla di sicurezza (ncsc.admin.ch)

infrastruttura. Eseguite regolarmente test di penetrazione e scansioni delle vulnerabilità per individuare proattivamente potenziali lacune di sicurezza. I software o i sistemi che non sono più supportati dal produttore («End of Life», EOL) dovrebbero essere disattivati o – se possibile – trasferiti in una partizione di rete separata e isolata. Utilizzate inoltre un sistema di monitoraggio e le informazioni disponibili sulle minacce («threat intelligence») per poter reagire in tempi rapidi a eventuali sviluppi rilevanti. Il monitoraggio in tempo reale della vostra infrastruttura, unito alle possibilità di automazione, vi aiuterà a individuare tempestivamente tentativi di attacco e anomalie. Anche misure d'accompagnamento come l'impiego del «red teaming»[50], controlli di sicurezza regolari o la gestione di un programma «bug bounty» possono essere di aiuto nel valutare e migliorare costantemente l'efficacia dei propri processi di sicurezza.

5 Truffe e ingegneria sociale

La truffa consiste nell'ingannare intenzionalmente una persona allo scopo di arricchire illegalmente se stessi o altri, procurando un danno materiale alla vittima.[51] Nel mondo digitale, la sfida principale risiede nel fatto che i criminali possono operare a distanza. Spesso, infatti, agiscono da Paesi in cui il sistema di perseguimento penale è particolarmente complicato. In genere i truffatori informatici non utilizzano tecniche sofisticate di attacco, bensì cercano di manipolare psicologicamente le potenziali vittime (ingegneria sociale[52]) inducendole a compiere di loro iniziativa alcune delle azioni necessarie per portare a termine la truffa.

Come negli anni precedenti, anche nella prima metà del 2025 i casi di truffa sono stati il fenomeno più segnalato all'UFCS (20 878 segnalazioni, 58%), anche se in calo di circa 2000 unità rispetto allo stesso periodo dell'anno scorso. A diminuire sono state soprattutto le segnalazioni di telefonate minatorie a nome di autorità (cfr. fig. 6). I picchi record di oltre 1000 segnalazioni a settimana registrati lo scorso anno in questo stesso periodo non si sono verificati nel secondo trimestre in esame. Sulla base delle informazioni disponibili all'UFCS non è possibile valutare in che misura questo calo sia persistente e riconducibile alle misure adottate dagli operatori di telecomunicazione.

---

50 Il «red team» è un gruppo indipendente che, nei panni di un potenziale aggressore, attacca un'organizzazione per testare l'infrastruttura e i suoi processi in condizioni reali. L'obiettivo è individuare e quindi eliminare tempestivamente una lacuna di sicurezza esistente prima di un vero ciberattacco (cfr. Red team (wikipedia.org)).

51 Cfr. per una definizione legale art. 146 CP (codice penale)

52 Ingegneria sociale (ncsc.admin.ch)

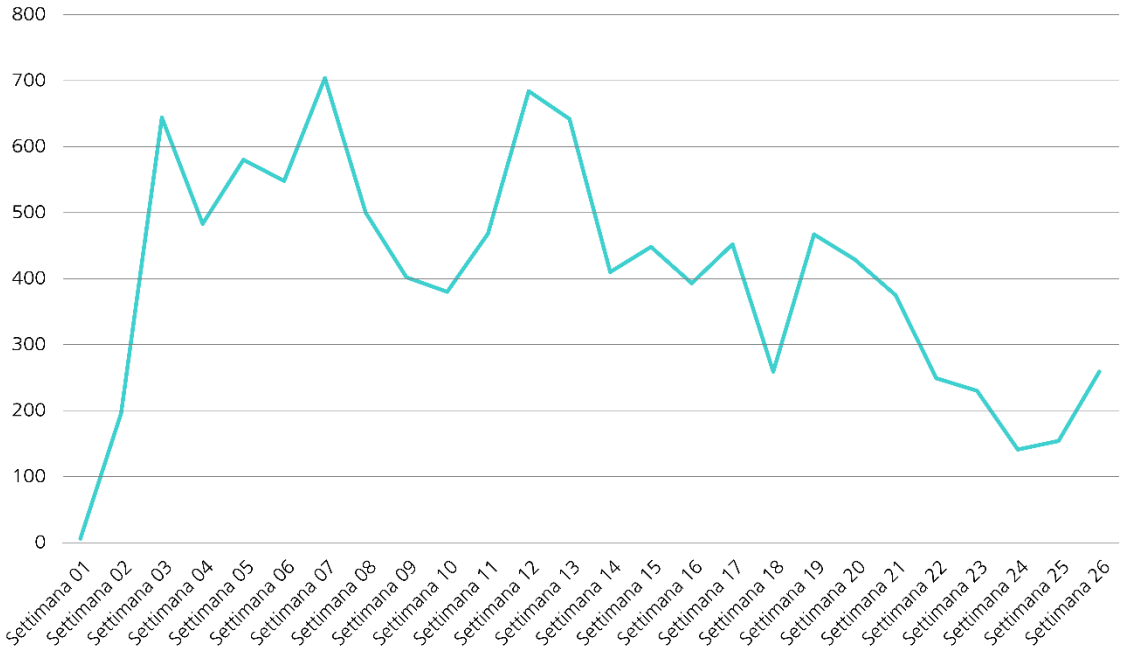

Fig. 6: Calo delle segnalazioni pervenute nel secondo trimestre del 2025 rispetto al fenomeno delle telefonate minatorie a nome di autorità

Un trend analogo a quello delle truffe telefoniche ha riguardato anche il fenomeno delle e-mail intimidatorie inviate da presunte autorità, in cui le vittime vengono accusate di un reato. Con 1487 segnalazioni, la loro diffusione in Svizzera è calata rispetto al medesimo periodo dell'anno precedente (2'252). Anche le lotterie fraudolente, che solitamente portano ad abbonamenti trappola o a siti di phishing, sono stati segnalati in misura minore. Dopo aver raggiunto un picco di 2398 segnalazioni nel secondo semestre del 2024, il numero di segnalazioni ricevute è ora sceso a quota 1916. In questi casi sono stati utilizzati abusivamente i nomi di note catene alimentari o retail, negozi di elettronica e aziende di trasporto pubblico. Pressoché invariato, invece, è il numero di segnalazioni pervenute per episodi di «fake sextortion»[53] (1136).

In linea con la tendenza del secondo semestre del 2024,[54] l'UFCS ha registrato un nuovo aumento del fenomeno «truffa del CEO». Rispetto ai 719 casi registrati complessivamente nel 2024, a fine giugno le segnalazioni avevano già raggiunto quota 605. A essere maggiormente colpite sono state ancora una volta le realtà con un alto grado di trasparenza a livello di struttura organizzativa e possibilità di contatto, come Comuni, scuole e parrocchie. Sul fronte delle truffe con manipolazione delle fatture[55] («Business-E-Mail-Compromise», BEC) – una variante di truffa dai contenuti analoghi ma tecnicamente più complessa – si è registrata una lieve diminuzione da 65 a 59 casi rispetto allo stesso periodo dell'anno precedente. Oltre al

---

53 Cfr. Rapporto semestrale 2024/2, cap. 5.2.

54 Cfr. Rapporto semestrale 2024/2, cap. 5.3.

55 A livello internazionale, il fenomeno del «Business Email Compromise» (BEC) non è utilizzato in modo uniforme, motivo per cui in altre definizioni, ad esempio, la frode del CEO è intesa come una sottocategoria del BEC (cfr. Business Email Compromise (fbi.gov)). L'OFCS distingue tuttavia esplicitamente i due fenomeni e segue la definizione dell'Ufficio federale di polizia (fedpol).

BEC, anche la truffa dell'investimento è spesso causa di ingenti danni finanziari. Associato a questo fenomeno si è osservato un sensibile aumento di pubblicità ingannevoli che rimandavano tra l'altro a questo tipo di siti. Rispetto alle 729 segnalazioni pervenute nello stesso periodo dell'anno precedente, nella prima parte del 2025 se ne contano già 3485. Sempre nel contesto delle «truffe degli investimenti online», in Svizzera ha preso piede la variante della «truffa di recupero», a quota 145 segnalazioni. In questo caso i criminali contattano le vittime di una truffa dell'investimento affermando di poterle aiutare a recuperare i soldi rubati, ma solo a condizione che paghino di ulteriori somme per il presunto servizio. I paragrafi che seguono forniscono un'analisi più dettagliata delle pubblicità ingannevoli per le truffe degli investimenti online, della truffa di recupero e un confronto tra BEC e truffa del CEO.

Pubblicità ingannevole prima della truffa dell'investimento

Tramite inserzioni e link sui social media, sui portali di streaming o in annunci a pagamento vengono costantemente pubblicizzati siti web sospetti. Secondo le segnalazioni pervenute all'UFCS, questo fenomeno è cresciuto di ben cinque volte nella primavera del 2025. Si tratta di siti che, emulando i classici portali di notizie, pubblicano interviste fittizie con personaggi famosi per promuovere presunte offerte di investimento che promettono rendimenti da capogiro a fronte di un rischio ridotto e a partire da un capitale minimo, ad esempio, di soli 250 CHF/euro (cfr. fig. 7). Questi portali di notizie sono molto simili a noti media svizzeri come Blick, 20min, SRF o RTS. Per le interviste i truffatori utilizzano figure di spicco dello sport, dei media o della politica.[56] Ultimamente, oltre agli articoli di cronaca vengono pubblicati anche video deepfake[57], che simulano ad esempio le edizioni del telegiornale. Una volta effettuato un primo investimento e quindi attivato il meccanismo della truffa, alla vittima viene fatto credere, in un portale appositamente creato, che la somma investita si moltiplicherà rapidamente. Le vittime vengono così indotte a trasferire ulteriori somme di denaro ai truffatori. Il problema è che i criminali sono in grado di pubblicare sui siti in breve tempo e in modo del tutto automatizzato un gran numero di contenuti fraudolenti, senza che questi debbano essere sottoposti a un controllo minimo da parte dei gestori dei siti in fase di caricamento. Viceversa, l'individuazione, la segnalazione e la disattivazione richiedono molto più tempo, per cui le autorità sono costantemente in ritardo rispetto alle attività dei truffatori.

Truffa di recupero dopo la truffa dell'investimento online

In Svizzera sono in aumento le segnalazioni relative a queste false richieste di rimborso – dalle 31 del primo semestre del 2024 il fenomeno è cresciuto, registrando nel 2025 ben 145 segnalazioni. Dopo aver subito una truffa di investimento, infatti, le vittime nutrono ancora la speranza di recuperare in qualche modo il denaro perduto. Ai truffatori non resta che cogliere questa opportunità per far loro credere, fingendosi autorità o aziende apparentemente serie, di aver rintracciato le somme sottratte. Per rientrare in possesso dei soldi «ritrovati», tuttavia, le vittime devono prima pagare una serie di imposte, tasse o costi di altra natura. I truffatori cercano di aumentare la loro credibilità agli occhi delle vittime, fornendo documenti falsi dall'aspetto ufficiale, spesso a nome di autorità britanniche o cipriote.

56 Settimana 35: Truffe con personaggi famosi – il volto nascosto dell'intelligenza artificiale (ncsc.admin.ch)

57 Deepfake (wikipedia.org)

Confronto tra Business E-Mail Compromise (BEC) e truffa del CEO

Nel periodo in esame si è osservato un forte aumento dei casi di tentata truffa del CEO, mentre la variante correlata del Business E-Mail Compromise (BEC) ha segnato solo una lieve diminuzione. Tra gli scenari tipici che contraddistinguono entrambe le tipologie di truffa vi sono e-mail fasulle inviate da un partner commerciale alla contabilità con richieste urgenti di bonifici, fatture fittizie di fornitori o finte lettere di avvocati relative a presunte acquisizioni segrete. Mentre nella truffa del CEO le informazioni utilizzate provengono da fonti pubbliche, nel caso del BEC i criminali violano prima di tutto gli account di posta elettronica aziendali per poi sfruttare le informazioni interne che sono riusciti a estrapolare. Nel BEC i criminali riescono dunque a formulare le loro richieste in maniera più credibile, adattandole specificatamente alle vittime. Anziché avanzare richieste generiche, ad esempio, citano dettagli quali coordinate bancarie o numeri di fattura e adeguano lo stile di scrittura all'azienda che fingono di rappresentare. Ciò implica un maggiore sforzo per i criminali, dal momento che gli attacchi mirati richiedono competenze tecniche sofisticate e una preparazione più accurata – ad esempio spiando modelli di comunicazione o procedure interne. In genere, tuttavia, anche il danno finanziario subito dalla vittima è di conseguenza più elevato.

Fondamentale ai fini della buona riuscita del BEC è l'accesso all'account aziendale, come dimostrano i numerosi attacchi di phishing ai danni di account Microsoft 365 svizzeri (cfr. cap. 2). Questi ultimi vengono, da un lato, utilizzati scrivendo a tutti i contatti allo scopo di diffondere ulteriori attacchi di phishing – ad esempio tramite il chain phishing – e quindi ottenere potenziali accessi ad account e-mail. Dall'altro, i criminali esaminati preventivamente tali account per individuare i contenuti monetizzabili. Se i truffatori trovano ad esempio una comunicazione relativa a una fattura non ancora saldata, si inseriscono nella corrispondenza. Nonostante un BEC possa essere effettuato direttamente dall'account e-mail compromesso, spesso i truffatori registrano un dominio simile a quello dell'azienda colpita, con il quale creare appositi indirizzi e-mail e riuscire a ingannare più facilmente le vittime – i clienti aziendali. A quel punto si rivolgono ai clienti con fatture insolute, chiedendo loro di versare gli importi su un altro conto. Questi credono di continuare a interagire con l'interlocutore legittimo, dato che lo stile e gli estremi delle fatture corrispondono alla cronologia delle comunicazioni precedenti. Da ultimo, questo tipo di truffa via e-mail è causa, oltre che di perdite finanziarie, anche di danni reputazionali: in alcuni casi, infatti, i criminali possono sottrarre anche informazioni sensibili, come i dati dei clienti, compromettendo la fiducia dei partner verso l'organizzazione (cfr. cap. 7).

Raccomandazioni

Siate scettici nei confronti di e-mail, messaggi di testo e telefonate in cui si minacciano conseguenze e viene esercitata pressione temporale (ad es. perdita di denaro, denuncia penale, blocco del conto o della carta). Tenete presente che i truffatori possono falsificare facilmente la loro identità mediante lo spoofing[58]. In generale, quindi, siate cauti in caso di richieste di pagamento insolite e promesse di guadagni. Nelle imprese tutti i processi riguardanti il traffico di pagamenti dovrebbero essere chiaramente regolamentati a livello interno. Inoltre, nessuna banca svizzera e nessun istituto di carte di credito vi chiederà mai via

[58] Spoofing (ncsc.admin.ch)

e-mail di modificare password o verificare i dati della carta di credito. Analogamente, il personale delle banche non vi chiederà mai token di sicurezza né altri dati d'accesso personali al vostro account e-banking o TWINT come criterio per verificare la vostra identità durante una telefonata.

6 Attacchi alla disponibilità di siti e servizi online

Con gli attacchi alla disponibilità di siti e servizi online – generalmente sotto forma di «Distributed Denial of Service» (DDoS) – gli aggressori cercano di mettere temporaneamente fuori uso un servizio accessibile via Internet inviando un numero elevato di richieste. Questi attacchi non comportano direttamente né un accesso illegittimo ai dati né un furto di informazioni o un danno permanente ai sistemi. Si tratta di una modalità di attacco utilizzata in particolare per finalità di attivismo nel ciberspazio (hacktivismo), per mascherare un'altra attività o, nel caso dei criminali, per ricattare le vittime.

Il 2025 è iniziato con una serie di attività sospette nell'ambito degli attacchi DDoS. Il 10 gennaio un attacco DDoS ha interrotto per circa 45 minuti servizi vari, tra cui telefonia, Outlook e alcuni siti e applicazioni specialistiche della Confederazione. Grazie alle contromisure adottate, la situazione è tornata rapidamente alla normalità.[59] Già alcuni giorni prima, varie banche svizzere avevano dovuto fare i conti con una serie di anomalie ad alcuni loro servizi online.[60] Il gruppo di hacktivisti filo-palestinesi «RooTDoS» ha rivendicato la paternità degli attacchi, adducendo come motivazione l'entrata in vigore del divieto di dissimulare il viso.[61]
Come previsto, verso la fine di gennaio sono andati in scena vari attacchi DDoS contro siti web svizzeri legati al World Economic Forum (WEF), che tuttavia non hanno influito sui lavori del WEF.[62] Gli attacchi sono stati rivendicati dal gruppo hacktivista filo-russo «NoName057(16)», che già in passato aveva cercato di attirare l'attenzione sullapropria causa in occasione di altri grandi eventi nazionali e internazionali.[63] L'obiettivo primario di questi attacchi è diffondere tra la popolazione un clima intimidatorio che non si basa su una reale minaccia.
Il 19 marzo 2025 vari servizi informatici dell'Amministrazione federale sono stati temporaneamente compromessi da una serie di intensi attacchi DDoS,[64] di cui non è stato possibile accertare l'origine né la motivazione. Come già accaduto durante il WEF, a metà maggio vi sono stati attacchi DDoS contro vari siti web svizzeri anche in concomitanza con l'Eurovision Song Contest (ESC) di Basilea.[65] Grazie anche alle misure preventive adottate

59 Interruzione dei sistemi informatici dell'Amministrazione federale a causa di un attacco DDoS (ncsc.admin.ch)
60 Massive technische Störung bei der Migros Bank (watson.ch)
61 CyberKnow: "Pro-palestine hacktivists, RootDos are targeting Migros bank in Europe (x.com)
62 Gli attesi attacchi DDoS sono iniziati (ncsc.admin.ch)
63 Plusieurs sites web suisses touchés par une cyberattaque (swissinfo.ch)
64 Interruzione dei sistemi informatici dell'Amministrazione federale a causa di un attacco DDoS (ncsc.admin.ch)
65 Gli attacchi DDoS previsti nel contesto dell'ESC sono iniziati (ncsc.admin.ch)

dagli organizzatori, queste attività non hanno però avuto ripercussioni sullo svolgimento dell'evento.[66]

Oltre agli hacktivisti si sono sporadicamente osservati anche attacchi DDoS legati a tentativi di estorsione. In questi casi, gli estorsori hanno dapprima lanciato un breve attacco dimostrativo, dopodiché – presumibilmente a nome del già noto collettivo «NoName057(16)» – hanno annunciato un imminente attacco su larga scala. Quest'ultimo, tuttavia, non è mai stato confermato.[67] L'estorsione DDoS non rientra nei tipici schemi d'attacco di questo collettivo di hacktivisti, il che lascia presumere che si tratti molto probabilmente di un'emulazione.
In genere, comunque, nella maggior parte degli attacchi DDoS non è possibile risalire né agli autori né alle motivazioni. L'infrastruttura d'attacco sottostante, infatti, può essere utilizzata – spesso a pagamento – dai soggetti più disparati contro qualsiasi obiettivo, e sta diventando sempre più performante.[68] Secondo un'analisi settoriale specifica per il comparto finanziario, la minaccia nei confronti dei servizi esposti a Internet è una sfida strategica in costante crescita.[69] Il continuo miglioramento delle competenze dei ciberattori richiede un'analisi consapevole dei rischi al fine di tutelare le funzioni critiche.

Raccomandazioni

Il sito dell'UFCS contiene, nella sezione Attacchi alla disponibilità (DDoS), 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 attacchi DDoS legati a tentativi di estorsione l'UFCS raccomanda di non cedere alle richieste. Dopo un primo versamento i criminali potrebbero chiedere ulteriore denaro e proseguire comunque gli attacchi. Potete invece segnalare il caso all'UFCS e contattare la polizia per sporgere denuncia. Se siete vittima di un attacco DDoS, trovate varie raccomandazioni sul sito dell'UFCS Attacco DDoS - E adesso?

7 Gestione, fughe ed estorsioni di dati

Fughe di dati ed esposizioni involontarie di dati continuano a essere un tema ricorrente sia in Svizzera che a livello internazionale. Oltre a violare la privacy, le fughe di dati possono causare ulteriori danni, soprattutto nei casi in cui a valle può insorgere 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,

66 Ciber-resilienza durante grandi eventi e conferenze internazionali (ncsc.admin.ch)
67 Cfr. Rapporto semestrale 2024/1, cap. 6 per una campagna analoga.
68 Defending the Internet: How Cloudflare blocked a monumental 7.3 Tbps DDoS attack (cloudflare.com)
69 From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector (fsisac.com)

aumenta anche il rischio di cadere vittima di un tentativo di truffa (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 truffe finanziarie. Le fughe di dati rivestono particolare importanza soprattutto negli attacchi ransomware e a scopo di estorsione, visto che – in assenza di pagamento del riscatto – i dati vengono solitamente pubblicati e/o monetizzati, ad esempio vendendoli (cfr. cap. 3.2). Anche altre cause, come una carente gestione dei dati all'interno della propria infrastruttura, la presenza di vulnerabilità (cfr. cap. 4) o configurazioni tecniche errate, possono causare un'esposizione dei dati.

Un incidente legato alla sicurezza presso un fornitore di servizi cloud ha coinvolto la sua clientela commerciale sia in Svizzera che all'estero. Il 20 marzo 2025 una persona ha pubblicato un post con lo pseudonimo «rose87168» sul forum di hacker «BreachForum»,[70] sostenendo di aver violato i server di Oracle e di aver anche sottratto informazioni relative a circa sei milioni di utenti.[71] Tra le varie richieste, l'hacker ha offerto alle aziende colpite di cancellare i loro dati in cambio di un riscatto. Per i clienti di Oracle la situazione è diventata un problema poiché l'azienda si è mostrata titubante e cauta nella comunicazione. Di conseguenza, sia le imprese coinvolte che le autorità hanno avuto difficoltà a valutare la reale portata della fuga di dati.[72] Soltanto il 16 aprile l'agenzia statunitense per la cibersicurezza CISA è riuscita a fare chiarezza sul caso, individuando un accesso non autorizzato al vecchio sistema cloud «Oracle Classic».[73] L'accesso e il furto delle credenziali hanno messo a rischio soprattutto le aziende e gli utenti che, dopo la migrazione a «Oracle Cloud», avevano mantenuto invariati password e login.

A differenza del primo incidente, Chain IQ – una società svizzera specializzata negli acquisti per conto di terzi – è stata direttamente vittima di un'estorsione di dati da parte del gruppo «World Leaks». Il 12 giugno quest'ultimo ha pubblicato circa 900 GB di dati appartenenti a Chain IQ, tra cui anche dati dei clienti di altre società svizzere del settore finanziario, del commercio retail e del comparto edilizio.[74] Tra essi figuravano ad esempio i numeri di telefono interni di contatti aziendali, nonché altre informazioni su progetti d'acquisto.[75] Chain IQ ha comunicato che nell'attacco era stato impiegato un malware ancora sconosciuto, che aveva consentito agli aggressori di muoversi inosservati all'interno del sistema aziendale.[76] Tra il primo accesso iniziale e la denuncia dell'estorsione, inoltre, è trascorso circa un mese. L'intento dei criminali era verosimilmente quello di ostacolare l'analisi tecnica dell'attacco dopo la sua scoperta.

---

70 Cfr. Rapporto semestrale 2024/1, cap. 7.2 per maggiori informazioni su BreachForum e il commercio di dati.

71 Oracle denies breach after hacker claims theft of 6 million data records (bleepingcomputer.com)

72 Oracle attempt to hide serious cybersecurity incident from customers in Oracle SaaS service (doublepulsar.com)

73 CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise (cisa.gov)

74 Plus de 100 000 employés d'UBS touchés par un vol massif de données sensibles, affectant aussi Pictet (letemps.ch)

75 Cyber-Attack Chain IQ Group AG (chainiq.com)

76 Cyberattacks pose security risks for all companies (chain iq.com)

World Leaks è un nuovo gruppo che ha raccolto il testimone dal gruppo ransomware «Hunters International».[77] A differenza dell'attività ransomware – che tra le sue vittime ha colpito anche realtà svizzera[78] – con World Leaks gli hacker sostengono di esfiltrare dati a fini estorsivi, ma di non ricorrere alla crittografia dei sistemi. Contrariamente a questa affermazione, tuttavia, ci sono vittime di World Leaks note a livello internazionale i cui dati sono stati comunque criptati con un software.[79]

I data leak possono però colpire anche i privati, che si vedono pubblicare le loro informazioni su siti del dark web[80] e del web sommerso.[81] Tali informazioni possono finire in reti criminali nel momento in cui, ad esempio, vi è una fuga di dati dei clienti in seguito a un ciberincidente o un'esposizione di dati – come evidenziano i due incidenti verificatisi nel primo semestre del 2025.

Raccomandazioni

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 al principio fondamentale 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. Codificate soprattutto i dati sensibili. 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.

I dati trafugati in passato possono essere riutilizzati per attacchi successivi. Verificate periodicamente se i vostri dati d'accesso compaiono in un data leak, ad esempio sul sito Have I Been Pwned[82] o su Identity Leak Checker dell'Hasso Plattner Institut[83].

8 Ciberspionaggio e sabotaggio

Gli attori statali o parastatali rappresentano una particolare tipologia di minaccia nel ciberspazio. I cosiddetti gruppi «Advanced Persistent Threat» (APT)[84] conducono operazioni di spionaggio o, più raramente, sabotaggio se funzionali agli interessi del loro Stato. Mentre le

77 The beginning of the end: the story of Hunters International (group-ib.com)

78 Cfr. attacco informatico alla Cassa di compensazione Swissmem – Gestione dell'incidente, conclusioni tratte, preparazione per il futuro (ak-swissmem.ch)

79 World Leaks: An Extortion Platform (blog.lexfo.blog.fr)

80 Web sommerso (wikipedia.org), Dark web (wikipedia.org),

81 Leaked: Politicians' emails and passwords on the dark web (proton.me); cfr. Datenleck: Parlamentarier-Daten landen im Darknet (srf.ch)

82 Cfr. Have I Been Pwned (haveibeenpwned.com)

83 Cfr. Identity Leak Checker (sec.hpi.de)

84 APT – Glossary (csrc.nist.gov)

prime rappresentano una sfida continua per il controspionaggio svizzero, il cibersabotaggio mirato si osserva generalmente solo in situazioni di conflitto o di elevate tensioni geopolitiche.[85] A differenza dei cibercriminali mossi da intenti finanziari, gli APT selezionano i loro obiettivi ad hoc e investono notevoli risorse per carpire le informazioni desiderate o ottenere l'effetto voluto. Di conseguenza, le organizzazioni potenzialmente coinvolte devono progettare un sistema di difesa a 360 gradi per contrastare questo tipo di minaccia. Grazie alle risorse tecniche, finanziarie e di personale degli APT, infatti, le attività preparatorie possono essere avviate anni prima dell'attacco effettivo.

8.1 Ciberspionaggio

Già nella seconda metà del 2024 l'APT cinese «Salt Typhoon» era finito sotto i riflettori per i suoi attacchi contro alcuni operatori di telecomunicazioni statunitensi ed europei.[86] Nel febbraio del 2025 una società di sicurezza informatica ha segnalato una serie di recenti attività da parte dello stesso attore ai danni di dispositivi di rete vulnerabili di CISCO.[87] A solo un mese di distanza sono state rilevate attività da parte di un altro gruppo di ciberspionaggio, presumibilmente anch'esso operante in Cina. A questo APT, denominato «Silk Typhoon», vengono attribuiti numerosi attacchi su scala internazionale in diversi settori, caratterizzati dall'impiego di metodi sofisticati come lo sfruttamento di vulnerabilità zero-day. In particolare, il gruppo si è tuttavia distinto anche per i suoi attacchi contro le catene di fornitura (attacchi alle «supply chain») in cui, servendosi di operatori informatici compromessi, ha cercato di accedere ai sistemi di clienti di loro interesse.[88]
Come molti altri APT, anche Silk Typhoon utilizza reti d'attacco costituite da dispositivi sotto il suo controllo, le cosiddette reti ORB (Operational Relay Boxes)[89]. Fondamentale, in questo caso, è la compromissione di apparecchiature di rete non sufficientemente protette. Questi cosiddetti «edge device», infatti, fungono da punti d'accesso alle reti aziendali. Gli esempi più recenti riguardano l'infezione di firewall[90], di soluzioni VPN per l'accesso remoto[91] e di router[92].

Tra i gruppi di spionaggio che presumibilmente operano per conto della Russia se ne è aggiunto uno nuovo denominato «Laundry Bear». Le autorità olandesi[93] hanno attribuito a questo APT una serie di attacchi contro varie organizzazioni del loro Paese – tra cui anche la

---

85 Cfr. anche comunicato stampa relativo al rapporto sulla situazione «La sicurezza della Svizzera 2025»: il confronto globale ha effetti diretti sulla Svizzera (vbs.admin.ch)

86 Cfr. Rapporto semestrale 2024/2, cap. 8.1.

87 RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers (recordedfuture.com)

88 Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

89 Cfr. Rapporto semestrale 2024/1, cap 8.1.2.

90 Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls (arcticwolf.com)

91 Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation (cloud.google.com), Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

92 Tracking AyySSHush: a Newly Discovered ASUS Router Botnet Campaign (censys.com)

93 Dutch intelligence unmasks previously unknown Russian hacking group 'Laundry Bear' (therecord.media)

polizia nazionale. Secondo Microsoft il gruppo – che il colosso informatico statunitense identifica col nome «Void Blizzard» – è attivo almeno da aprile 2024 ed è prevalentemente interessato a obiettivi legati alla Nato e all'Ucraina. Anche di altri gruppi già consolidati, ritenuti parte dell'ambiente di spionaggio russo, si sono osservate attività nella prima metà del 2025. A maggio, ad esempio, le autorità americane hanno accusato «APT28» di avere nel mirino aziende logistiche e high-tech occidentali, in particolare quelle operanti a supporto dell'Ucraina.[94] Anche le autorità francesi hanno riferito di attacchi ai danni di organizzazioni da parte di questo APT, a cui hanno attribuito ufficialmente la paternità.[95] Questo atteggiamento evidenzia come soprattutto i Paesi occidentali siano sempre più propensi, dopo ciberattacchi spinti da interessi statali, a denunciarne pubblicamente le responsabilità politiche. A fine maggio 2025, ad esempio, la Repubblica Ceca ha ufficialmente attribuito alla Cina un ciberattacco contro il suo Ministero degli Esteri.[96]

Mentre in genere gli attori statali o parastatali svolgono perlopiù attività di spionaggio, quelli legati al regime nordcoreano, in particolare, paiono essere coinvolti anche in attività finanziarie, come ad esempio il furto di criptovalute[97]. Nell'ambito dell'operazione «Contagious Interview» alcuni soggetti probabilmente nordcoreani si sono nuovamente spacciati per reclutatori su LinkedIn . Ai candidati per lo sviluppo di software venivano assegnati compiti che dovevano svolgere sul loro computer in un ambiente non protetto. Il codice fornito, tuttavia, conteneva pacchetti dannosi che installavano un malware.[98] Un'altra variante, legata a ClickFix (cfr. cap. 3.1), consisteva nel far credere ai candidati, durante il processo di assunzione, che un software non funzionasse e che pertanto doveva essere nuovamente scaricato.[99] Un altro esempio tipico è l'utilizzo di tecnici informatici nordcoreani sotto copertura. Su incarico della Corea del Nord, da un lato generano valuta estera e dall'altro trafugano dati per attività di spionaggio e successive estorsioni ai danni delle aziende.[100] Queste attività sono state osservate con maggiore frequenza in Europa, così come in Svizzera.[101] Per non perdere la copertura e poter operare con successo all'estero, spesso gli attori nordcoreani necessitano di un certo grado di supporto nel Paese di destinazione. A tal fine cercano di coinvolgere persone locali, che in genere non sono del tutto consapevoli del loro ruolo. Una possibile spiegazione di questo spostamento dalle aziende statunitensi a quelle europee può essere intesa come conseguenza della maggiore attenzione e delle contromisure adottate sul territorio americano per contrastare queste campagne.

---

94 Russian GRU Targeting Western Logistics Entities and Technology Companies (cisa.gov)

95 Russia – Attribution of cyber attacks on France to the Russian military intelligence service (APT28) (April 29th 2025) (diplomatie.gouv.fr)

96 Czech Republic says China behind cyberattack on ministry, embassy rejects accusations (reuters.com)

97 Bybit loses nearly $1.5 billion in crypto hack – What we know so far (economictimes.indiatimes.com)

98 Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages (socket.dev)

99 Lazarus ClickFake Interview Campaign: From Contagious to ClickFix Malware Tactics (blog.sekoia.io)

100 Cfr. Rapporto semestrale 2024/2, cap. 8.1.

101 DPRK IT Workers Expanding in Scope and Scale (cloud.gloogle.com)

Raccomandazioni

La difesa contro questa tipologia di minaccia deve avvenire su più livelli attraverso una strategia «defence-in-depth»[102]. L'elevata propensione di questi aggressori a investire tempo e risorse in strumenti consente loro di individuare e sfruttare nuove vulnerabilità in ognuno dei loro obiettivi. L'efficacia o meno di una strategia di difesa dipende pertanto dalla misura in cui si considerano vari componenti dell'infrastruttura informatica, tra cui ad esempio il perimetro, la rete, gli endpoint, ma anche il fattore umano e l'organizzazione stessa. A tale proposito è importante sapere che un'intrusione da parte di un APT, con le sue immense risorse e capacità, non può mai essere esclusa del tutto, nemmeno se in un'organizzazione si è definito e adottato un piano di sicurezza a più livelli. Una segmentazione della rete, in cui vengono isolati ad esempio i sistemi critici o i dati sensibili, può ostacolare un'infezione totale dei sistemi in caso di compromissione. Per ulteriori raccomandazioni si rimanda agli standard minimi per le TIC.

8.2 Minaccia a sistemi di controllo industriali e tecnologie operative

La digitalizzazione non solo porta a un crescente impiego 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 ad esempio i sistemi di controllo industriali (ICS) – che in passato era perlopiù isolata – è sempre più interconnessa con il resto dell'ambiente di sistema ed è quindi esposta anche ai rischi derivanti da tale ambiente. 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».

Gli attacchi contro i sistemi di controllo industriali con intento sabotatorio avvengono soprattutto nel contesto di escalation geopolitiche, come la guerra in Ucraina o il conflitto mediorientale tra Israele e Iran di metà giugno 2025. Oltre alla manipolazione abusiva degli stessi sistemi, in questi casi si utilizza anche un malware cosiddetto «wiper» che, mettendo fuori uso i sistemi, impedisce il funzionamento di sistemi di approvvigionamento o produzione. Ne è un esempio l'impiego di «PathWiper» contro infrastrutture critiche ucraine nel giugno del 2025.[103]. Per quanto riguarda la Svizzera, ad oggi simili atti di sabotaggio da parte di ciberattori statali non sono stati osservati e vengono ritenuti altamente improbabili. Non si escludono, invece, ripercussioni sotto forma di danni collaterali in seguito a un attacco in territorio estero.[104]

---

[102] Cfr. standard minimi per le TIC (ncsc.admin.ch), cpv. 1.6 sulla strategia «defence-in-depth».

[103] Newly identified wiper malware "PathWiper" targets critical infrastructure in Ukraine (blog.talosintelligence.com)

[104] «La sicurezza della Svizzera 2025»: il confronto globale ha effetti diretti sulla Svizzera (vbs.admin.ch)

Più frequenti rispetto a questi attacchi mirati sono i tentativi opportunistici di manipolare sistemi di controllo industriali esposti a Internet e non sufficientemente protetti. Attraverso queste attività i gruppi di hacktivisti cercano di attirare su di sé quanta più attenzione possibile. Alcuni di essi agiscono su incarico di servizi statali. Gli aggressori non possiedono competenze particolarmente avanzate, bensì si limitano ad attivare i primi circuiti a cui riescono ad accedere. I loro bersagli sono quindi di natura non particolarmente critica, ad esempio una diga che regola il deflusso dell'acqua in un allevamento ittico[105] o mini-centrali elettriche al servizio di mulini[106].
Oltre alle diverse tipologie di attacco summenzionate, anche il perimetro dei sistemi potenzialmente esposti continua ad ampliarsi con l'ingresso di numerosi nuovi operatori, la maggior parte dei quali privati. Con lo sviluppo del fotovoltaico e il crescente numero di impianti solari collegati alla rete elettrica, ad esempio, aumenta il numero di sistemi controllabili. Molti inverter – un componente fondamentale per l'allacciamento alla rete – presentano tuttavia una serie di vulnerabilità che potrebbero consentire l'accesso a soggetti non autorizzati.[107] Per ridurre le probabilità che questi utenti della rete subiscano manipolazioni abusive, è necessario attribuire la necessaria importanza alla cibersicurezza.

Raccomandazioni

Proteggete i vostri sistemi industriali per 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 del settore. Ulteriori indicazioni sono disponibili nelle raccomandazioni relative all'OT[108] dell'Information Security Society Switzerland (ISSS).

105 Cyberattack on Norwegian Dam Highlights Password Exposure Risks (claroty.com)
106 Hacktivists Target France Over Diplomatic Moves (cyble.com)
107 SUNDOWN A Dark Side to Solar Energy Grids (forescout.com)
108 ISSS Operational Technology (OT) Empfehlungen (cybernavi.ch)