

7 novembre 2024 | Ufficio federale della cibersecurity UFCS



Rapporto semestrale 2024/I (gennaio – giugno)

# Cybersicurezza

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 cibersecurity UFCS**

## Management Summary

Il rapporto semestrale dell'Ufficio federale della cibersecurity (UFCS) presenta i principali ciberfenomeni che caratterizzano l'attuale panorama delle minacce in Svizzera. Sulla base dei ciberincidenti e degli sviluppi registrati nel nostro Paese nel primo semestre del 2024 si illustrano le tecniche e le metodologie con cui i vari criminali che popolano il ciber spazio cercano di raggiungere i loro obiettivi.

Nel primo semestre del 2024 l'UFCS ha ricevuto 34 789 segnalazioni di ciberincidenti, ben 15 740 in più rispetto allo stesso periodo dello scorso anno. Questa cifra, pressoché raddoppiata, è dovuta soprattutto alla crescita delle «chiamate fasulle a nome della polizia», delle «lotterie fraudolente», degli «abbonamenti trappola» e del fenomeno del «phishing». Circa il 90 per cento delle segnalazioni pervenute all'UFCS è stato trasmesso da privati, il 10 per cento dalle imprese. Come negli anni precedenti la maggior parte di esse era riferita alle categorie «truffa», «phishing» e «spam».

### **Truffa – primato di segnalazioni**

A quota 23 104 le segnalazioni di truffa mantengono il primato, rappresentando due terzi delle segnalazioni pervenute nel primo semestre del 2024. Rispetto allo stesso periodo dello scorso anno (11 174) il numero è più che raddoppiato. 13 730 di esse, ossia quasi il 40 per cento, riguardano finte telefonate da parte delle autorità. Questo fenomeno consiste nell'effettuare telefonate a tappeto a numeri casuali, facendo credere alle vittime di essere coinvolte in un procedimento penale e inducendole a premere il tasto «1» per procedere alle fasi successive. A quel punto le vittime vengono messe in contatto con un truffatore e convinte a scaricare un software di accesso remoto, che consente ai criminali di insinuarsi nei loro computer ed effettuare a loro insaputa pagamenti tramite e-banking.

### **Massiccio aumento delle segnalazioni di phishing**

Nel primo semestre del 2024 l'UFCS ha ricevuto 6643 segnalazioni di phishing, registrando un massiccio aumento di circa 2800 segnalazioni rispetto allo stesso periodo dello scorso anno (3879 segnalazioni). La maggior parte dei tentativi di phishing 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. In particolare continuano le segnalazioni all'UFCS di tentativi di phishing ai danni di account Microsoft 365. Una 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 tutta la rubrica.

### **Attacchi DDoS in occasione di grandi eventi e conferenze internazionali**

Con gli attacchi alla disponibilità di siti e servizi online – noti anche come «Distributed Denial of Service» (DDoS) – gli aggressori cercano di mettere temporaneamente fuori uso un sito web o un servizio online bombardandolo di richieste. Nel corso del semestre in esame si sono osservate in particolare tre campagne DDoS: ad aprile 2024 varie organizzazioni svizzere del settore finanziario hanno segnalato una serie di attacchi DDoS abbinati a un tentativo di estorsione, che pare siano stati rivendicati dal gruppo «Armada Collective» o «Alpha Jackal». Oltre a moventi di carattere finanziario gli attacchi DDoS sono stati nuovamente utilizzati per finalità

politiche nell'ambito di grandi manifestazioni e conferenze internazionali sul territorio svizzero. A gennaio 2024 il collettivo di hacktivisti filorusi «NoName057(16)» ha preso di mira vari siti legati al World Economic Forum (WEF), mentre a giugno 2024 è stata la volta dei siti di organizzazioni connesse alla «Conferenza sulla pace in Ucraina» tenutasi al Bürgenstock. Nel complesso gli attacchi si sono mantenuti entro i limiti previsti e hanno compromesso solo minimamente l'infrastruttura informatica. In nessun momento i sistemi informatici e i dati di queste manifestazioni o delle organizzazioni coinvolte sono risultati in serio pericolo.

### **Ransomware – una sfida nazionale e globale**

Il numero di segnalazioni all'UFCS relativo ad attacchi ransomware ai danni delle imprese segna un lieve calo, con i tre collettivi «Akira», «8Base» e «Black Basta» tra i principali artefici in Svizzera di questi episodi nel corso del periodo in esame. Gli attacchi ransomware colpiscono vittime di ogni settore e dimensione aziendale. I privati, invece, sono sempre meno presi di mira dai cybercriminali, in linea con la tendenza registrata sinora. Visto il tipico comportamento opportunistico dei gruppi di ransomware, questa flessione potrebbe essere stata influenzata dal sempre maggior numero di attacchi mirati contro bersagli molto remunerativi. Anche a livello internazionale gli attacchi di ransomware mettono a dura prova imprese e autorità.

### **Altri fenomeni**

Il rapporto evidenzia inoltre le tendenze e gli sviluppi sul fronte delle vulnerabilità e dei malware per dispositivi mobili e accesso iniziale. Anche il tema della gestione dei dati richiede attenzione. Dopo un data leak, infatti, spesso i dati trafugati vengono sfruttati per compromettere sistemi informatici e sferrare attacchi di ingegneria sociale nell'ambito di truffe. Da ultimo, il documento fornisce un quadro generale delle attività di ciberspionaggio e sabotaggio nel contesto di tensioni geopolitiche e di questo anno record per le elezioni. Sebbene questo capitolo si basi perlopiù su osservazioni provenienti dall'estero, anche questo aspetto è fondamentale per poter valutare a 360 gradi la situazione delle minacce in Svizzera.

## Contenuto

|   |           |
|---|-----------|
| Editoriale .....  | 4         |
| <b>1</b> <b>Ciberminacce in Svizzera – panoramica</b> .....                           | <b>6</b>  |
| <b>2</b> <b>Phishing</b> .....  | <b>8</b>  |
| <b>2.1 Prende piede il chain phishing</b> .....                                       | <b>11</b> |
| <b>2.2 Preso di mira il secondo fattore</b> .....                                     | <b>11</b> |
| <b>3</b> <b>Malware</b> .....   | <b>12</b> |
| <b>3.1 Accesso iniziale con malware</b> .....   | <b>13</b> |
| <b>3.2 Ransomware</b> .....   | <b>15</b> |
| 3.2.1 <i>Attività ransomware in Svizzera</i> .....                                    | 16        |
| 3.2.2 <i>Ransomware, una sfida globale</i> .....                                      | 17        |
| <b>3.3 Malware su dispositivi mobili</b> .....  | <b>20</b> |
| <b>4</b> <b>Vulnerabilità</b> .....   | <b>21</b> |
| <b>5</b> <b>Truffe e ingegneria sociale</b> .....                                     | <b>23</b> |
| <b>5.1 Tecniche di intelligenza artificiale nei tentativi di truffa</b> .....         | <b>24</b> |
| <b>5.2 Pubblicità per truffa dell'investimento</b> .....                              | <b>24</b> |
| <b>6</b> <b>Limitazione della disponibilità di siti e servizi online (DDoS)</b> ..... | <b>25</b> |
| <b>7</b> <b>Gestione, fughe ed estorsioni di dati</b> .....                           | <b>27</b> |
| <b>7.1 Fughe di dati presso i fornitori</b> .....                                     | <b>27</b> |
| <b>7.2 Commercio legale e illegale di dati</b> .....                                  | <b>29</b> |
| <b>8</b> <b>Ciberspionaggio e sabotaggio</b> .....                                    | <b>32</b> |
| <b>8.1 Ciberspionaggio</b> .....  | <b>33</b> |
| 8.1.1 <i>Istituzioni politiche sotto pressione</i> .....                              | 33        |
| 8.1.2 <i>Sviluppi internazionali nel ciberspionaggio</i> .....                        | 34        |
| <b>8.2 Minaccia a sistemi di controllo industriali e tecnologie operative</b> .....   | <b>36</b> |

## Editoriale

L'Ufficio federale della cibersicurezza UFCS traccia un bilancio dei suoi primi 182 giorni di attività. Sono stati sei mesi interessanti, fatti di progetti impegnativi, decisioni visionarie e del consolidamento di nuove strutture con altre di ormai comprovata efficacia. La strada intrapresa non è sempre facile, ma l'obiettivo di rendere la Svizzera più resiliente alle cyberminacce rimane la priorità assoluta per tutto il personale dell'UFCS.

Il processo di crescita e sviluppo dell'UFCS è un cammino incessante, di cui alcuni traguardi sono già stati raggiunti. A metà giugno, ad esempio, in occasione della «Conferenza di alto livello sulla pace in Ucraina» l'UFCS ha dimostrato di avere le competenze per fornire in breve tempo servizi particolari insieme ai propri partner. Quale responsabile del coordinamento generale della Rete integrata della situazione ciber nazionale, il nostro Ufficio è stato in grado di garantire in qualunque momento la (ciber)sicurezza di tutti i soggetti coinvolti e delle infrastrutture necessarie allo svolgimento della conferenza. La chiave per mettere in sicurezza un evento così esposto in breve tempo è stata una pianificazione sistematica basata sui rischi, nonché la garanzia che tutte le forze d'intervento perseguissero i medesimi obiettivi. Altrettanto fondamentale, tuttavia, è stato anche far sì che le organizzazioni coinvolte avessero sempre il livello di informazioni necessarie, così da poter agire in modo coordinato. Tutto questo è stato possibile poiché il personale dell'UFCS, grazie al solido bagaglio di conoscenze specialistiche e alla profonda comprensione dei ciber-rischi, è stato in grado di interfacciarsi a pari livello con tutti i partner e gli stakeholder, a livello sia nazionale che internazionale. Oltre al coordinamento, a monte dell'evento l'UFCS era anche responsabile dell'Attack Surface Management delle infrastrutture minacciate e della sensibilizzazione delle organizzazioni potenzialmente interessate, ed è stato inoltre coinvolto nell'attività di gestione degli incidenti. In questa sede vorrei cogliere l'occasione per ringraziare tutti i partner per l'eccellente collaborazione. Un ringraziamento particolare va alla Polizia cantonale di Lucerna e di Nidvaldo, che hanno integrato il nostro personale nelle loro organizzazioni d'intervento. Io e i miei colleghi siamo fieri che questa esperienza ci abbia avvicinato e fatto crescere insieme ancora di più. È solo rimanendo uniti che aumenteremo la cibersicurezza in Svizzera.

Nel mio ultimo editoriale ho affrontato, tra i vari temi, la questione dell'elevata vulnerabilità dei sistemi informatici e della reattività a tratti ancora carente in caso di ciberincidenti rilevanti per la sicurezza. A inizio giugno 2024 la società Synovis, che fornisce servizi a numerosi ospedali londinesi, è caduta vittima di un attacco ransomware. A causa dei conseguenti black-out dei sistemi, per circa cinque settimane si sono dovuti spostare più di 6000 appuntamenti per interventi chirurgici e trasfusioni di sangue. Questo episodio mostra ancora una volta quanto la cibersicurezza sia da considerare una priorità. Ma non devono per forza essere sempre eventi di questa portata a causare grandi problemi. Anche i ciberincidenti che di per sé non rappresentano una minaccia diretta per lo Stato possono scatenare forte ansia e ingenti perdite finanziarie per le vittime e, in alcuni casi, portare un'azienda al fallimento. L'accumularsi di tali episodi può far sì che, per via della loro grande quantità, alla fine nasca realmente una minaccia nazionale. Ecco perché è importante che, quando si parla di cibersicurezza, non si pensi soltanto alle infrastrutture critiche, ma si contribuisca anche a fare in modo che tutte le imprese della Svizzera – dalle ditte individuali alle aziende che operano in settori di rilevanza sistemica – possano svolgere la loro attività con meno restrizioni possibili.

Guardo con trepidazione alle sfide che ci attendono nella seconda metà del 2024 e spero che, leggendo questo rapporto semestrale, possiate trarre molti nuovi spunti su come migliorare ulteriormente la vostra cibersecurity.

**Florian Schütz, direttore dell'Ufficio federale per la cibersecurity**

# 1 Ciberminacce in Svizzera – panoramica

Le ciberminacce sono diventate parte integrante della costellazione di minacce che incombono non solo sulla Svizzera, ma anche sul mondo intero. Sebbene gli ormai noti fenomeni come il phishing, la diffusione di malware o le attività di spionaggio nel ciber spazio siano una costante da anni, le metodologie e le tattiche impiegate dai cybercriminali nell'ambito di tali attività vengono continuamente perfezionate. Nel primo semestre del 2024, ad esempio, questo ambiente dinamico ha visto un intensificarsi dell'uso dell'apprendimento automatico, o machine learning (ML)<sup>1</sup>, nei tentativi di truffa<sup>2</sup> o nel phishing<sup>3</sup>. I cybercriminali, inoltre, ampliano costantemente la gamma di canali utilizzati per sferrare i loro attacchi: servizi come Google Ads, ad esempio, vengono sempre più spesso sfruttati per compiere frodi sugli investimenti. A seconda del calcolo costi-benefici, questi nuovi approcci finiscono per diventare di routine oppure rimangono un esperimento una-tantum.

Nel primo semestre del 2024 l'UFCS ha ricevuto in tutto 34 789 segnalazioni, con un significativo aumento di ben 15 740 rispetto al medesimo periodo dell'anno scorso. Questa cifra pressoché raddoppiata è dovuta soprattutto alla crescita delle «chiamate fasulle a nome della polizia»<sup>4</sup>, delle «lotterie fraudolente»<sup>5</sup>, degli «abbonamenti trappola»<sup>6</sup> e del fenomeno del «phishing». Per quanto riguarda le chiamate fasulle a nome della polizia<sup>7</sup>, le segnalazioni hanno registrato un'impennata soprattutto tra le settimane 10 e 18, il che a sua volta ha fatto chiaramente lievitare il numero di segnalazioni totali (cfr. fig. 1). Grazie alle misure introdotte dalle compagnie di telecomunicazione, entro giugno 2024 si è riusciti ad arginare questa ondata di chiamate fasulle, per cui da quel momento in poi fino alla fine del periodo di riferimento, il numero complessivo delle segnalazioni è progressivamente diminuito.

La maggior parte delle segnalazioni è effettuata dalla popolazione (90 %) e il restante 10 per cento dalle imprese<sup>8</sup>, per cui non c'è da meravigliarsi che vengano segnalati soprattutto casi di frode, phishing e spam (cfr. fig. 2). Per quanto riguarda gli attacchi ransomware<sup>9</sup> ai danni delle imprese, le segnalazioni hanno registrato un lieve calo: mentre negli ultimi sei mesi del 2023 l'UFCS ne aveva ricevute 56, nel periodo in esame sono state soltanto 39. Ai danni dei privati, negli ultimi mesi il fenomeno si è stabilizzato a un livello basso, con valori a una cifra. Nonostante non si possa escludere una discrepanza tra il numero di casi segnalati e quelli reali, pare che i criminali si stiano allontanando dagli attacchi a tappeto, ma poco redditizi, per puntare invece a pochi obiettivi, ma estremamente lucrativi.

---

<sup>1</sup> [Apprendimento automatico \(wikipedia.org\)](https://it.wikipedia.org/wiki/Apprendimento_automatico)

<sup>2</sup> Cfr. [Lotterie fraudolente \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/lotterie-fraudolente), [Offerte di lavoro fraudolente \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/offerte-di-lavoro-fraudolente), [Fake-Support \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/fake-support), o anche [Truffa del CEO \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/truffa-del-ceo)

<sup>3</sup> [Phishing, vishing, smishing \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/phishing-vishing-smishing)

<sup>4</sup> [Chiamate a nome di false autorità \(polizia, dogana\) \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/chiamate-a-nome-di-false-autorita)

<sup>5</sup> [Lotterie fraudolente \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/lotterie-fraudolente)

<sup>6</sup> [Abbonamenti trappola \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/abbonamenti-trappola)

<sup>7</sup> Per esaminare più da vicino il fenomeno delle “chiamate fasulle a nome della polizia”, l'UFCS ha redatto un rapporto che è stato pubblicato in concomitanza con la relazione semestrale. Il rapporto fa luce, tra l'altro, sugli ultimi sviluppi del fenomeno, sui vari approcci e tecnologie utilizzati a questo scopo e sulla situazione giuridica nazionale e internazionale.

<sup>8</sup> La categoria «imprese» comprende anche associazioni e autorità.

<sup>9</sup> [Ransomware \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ransomware)



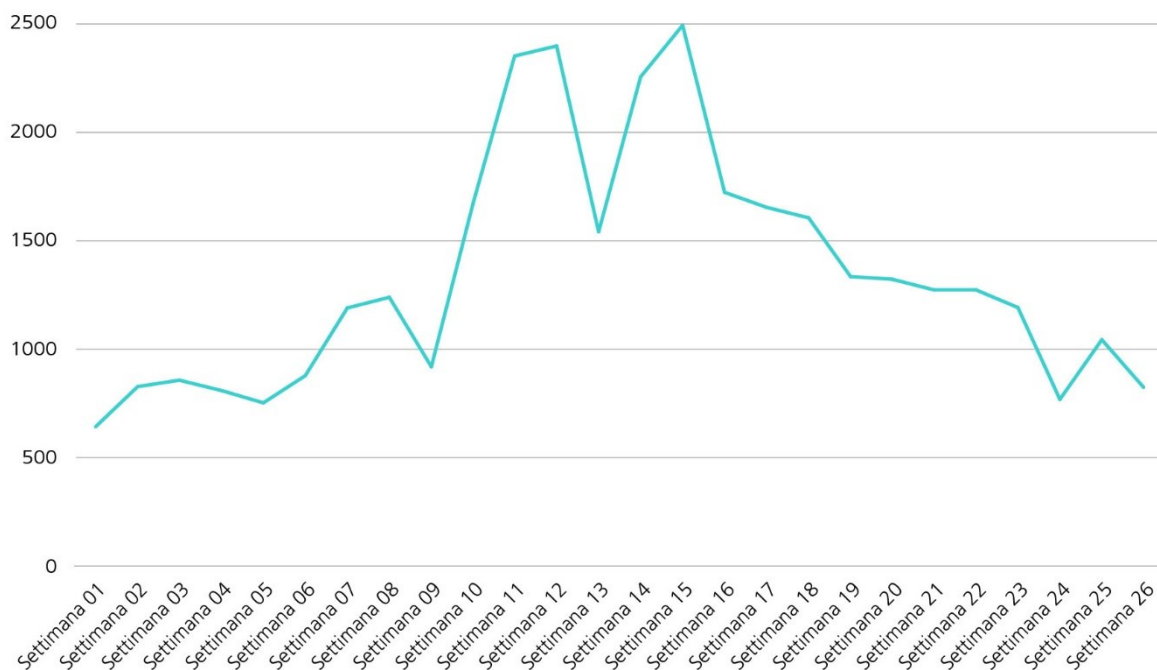


Fig. 1: Segnalazioni settimanali all'UFCS nel primo semestre 2024, cfr. [Numeri attuali \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/numeri-attuali).

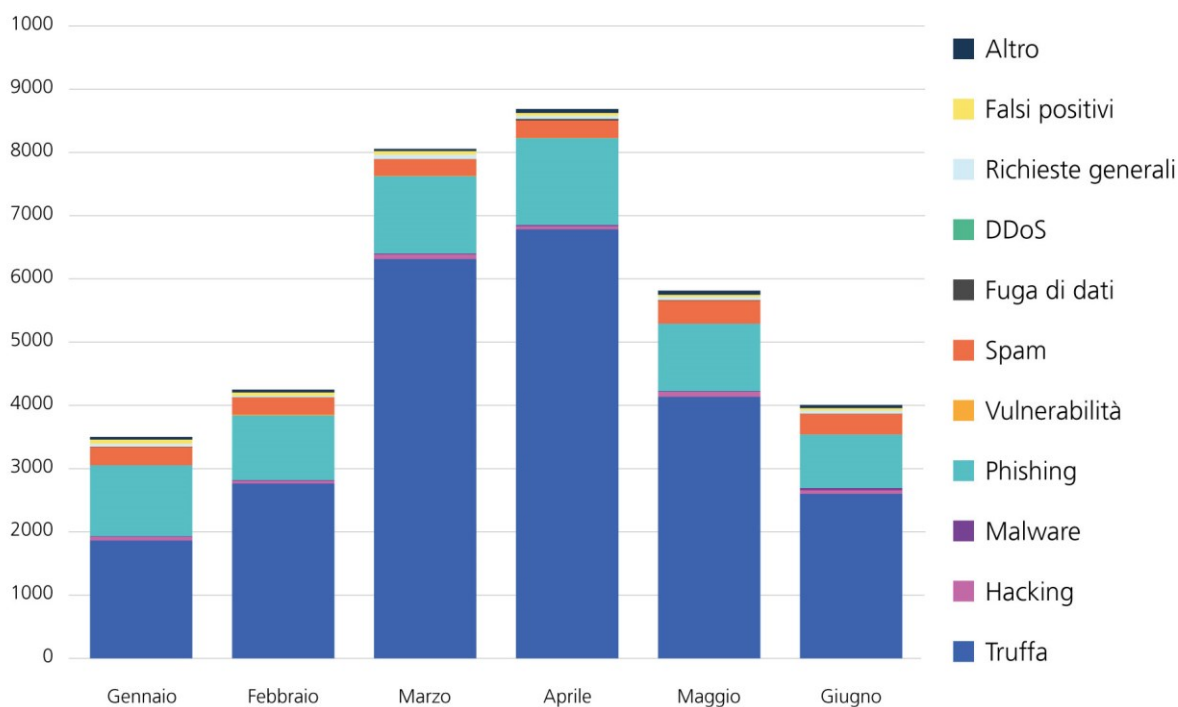


Fig. 2: Segnalazioni all'UFCS nel primo semestre del 2024 per categoria, cfr. [Numeri attuali \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/numeri-attuali).

Le statistiche evidenziano quanto la cibersicurezza e la protezione della Svizzera dai ciber-rischi rappresentino una sfida costante per l'economia, lo Stato e la società. Con la creazione



dell'Ufficio federale della cibersicurezza (UFCS) il 1° gennaio 2024, anche il rapporto semestrale pubblicato due volte all'anno<sup>10</sup> è stato rivisto nella sua struttura. Ora ciascun capitolo è dedicato a un fenomeno specifico che contraddistingue in maniera particolare il panorama delle minacce in Svizzera: phishing, malware, vulnerabilità, truffe e ingegneria sociale<sup>11</sup>, attacchi alla disponibilità di servizi esposti sulla rete Internet (DDoS), fughe di dati, ciberspionaggio e sabotaggio informatico. Resta invece invariato l'obiettivo principale – informare l'opinione pubblica sul tema della cibersicurezza. Il rapporto semestrale vuole essere uno strumento con cui evidenziare, attraverso episodi reali, le cyberminacce e le sfide del momento, ricavando consigli e raccomandazioni per la popolazione. Secondo il principio della responsabilità personale, infatti, tutti sono chiamati a contribuire in base alle proprie capacità e possibilità a garantire la sicurezza della Svizzera nello spazio digitale.

## 2 Phishing

I siti di phishing figurano, insieme ai casi di truffa, in cima alla classifica dei ciberincidenti più segnalati all'UFCS. Nello specifico si tratta di una tecnica con cui i cybercriminali si procurano credenziali d'accesso, informazioni finanziarie e altri dati riservati sottraendoli a ignari utenti del ciber spazio. Una sua tipicità è il fatto che le vittime vengono raggirate con l'inganno (ingegneria sociale), per cui non si basa in primo luogo sull'utilizzo di malware.<sup>12</sup> 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.

Nel primo semestre del 2024, le segnalazioni<sup>13</sup> di siti di phishing pervenute all'UFCS tramite l'apposito modulo sono state superiori (6643) a quelle dello scorso anno (3879). I tentativi di raggio più frequenti non sono cambiati: continuano a essere inviati migliaia di messaggi fraudolenti concernenti la consegna di un pacco. Anche le e-mail che annunciano un presunto rimborso a nome di fornitori, da parte delle FFS, di SwissPass o varie amministrazioni delle contribuzioni rientrano nel repertorio standard dei phisher. Un quadro analogo si ritrova anche in altri dati statistici che documentano le campagne di phishing in Svizzera. Un altro valore in crescita riguarda gli URL di phishing verificati e confermati dall'UFCS. Mentre nel primo semestre dello scorso anno gli URL di phishing unici documentati sono stati 4765, nello stesso periodo del 2024 sono più che raddoppiati, raggiungendo quota 11 505. L'andamento settimanale è illustrato alla figura 3. Per rendere i siti di phishing quanto più credibili possibile, i criminali continuano a servirsi di marche e imprese note. Nel periodo in esame sono stati bersaglio di phishing soprattutto il settore finanziario (26 %), i servizi postali (24 %), i trasporti pubblici (23 %), le telecomunicazioni (11 %) e il settore informatico (8 %). Queste percentuali sono rimaste relativamente costanti nel corso dei mesi (cfr. fig. 4).

---

<sup>10</sup> Ulteriori rapporti semestrali sono disponibili in [Rapporti di situazione \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/rapporti-di-situazione)

<sup>11</sup> [Ingegneria sociale \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ingegneria-sociale)

<sup>12</sup> 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 \(attack.mitre.org\)](https://attack.mitre.org/phishing/)). L'UFCS, invece, esclude esplicitamente questa dimensione dalla definizione utilizzata.

<sup>13</sup> L'UFCS riceve segnalazioni di phishing non solo in forma diretta, ma anche tramite l'iniziativa [antiphishing.ch](https://www.antiphishing.ch), che considera ulteriori fonti. Per tale motivo i numeri qui indicati potrebbero differire da quelli relativi alle segnalazioni dirette di phishing.

Per tutelare dal phishing il maggior numero possibile di potenziali vittime, l'UFCS si adopera per disattivare al più presto questi siti. I malfattori, invece, fanno di tutto per impedire che ciò avvenga. Ecco perché i phisher sono costantemente alla ricerca di nuovi metodi per evitare per più tempo possibile che le autorità di sicurezza scoprano i siti di phishing e possano quindi chiuderli. Ad oggi esistono parecchi siti di phishing che è possibile raggiungere soltanto con specifiche configurazioni di rete. Una variante tra le più utilizzate è quella di consentire l'accesso ai siti fraudolenti soltanto tramite smartphone. Tutti gli altri accessi da PC o altri dispositivi connessi a Internet vengono invece reindirizzati a siti legittimi. Il motivo è presto spiegato: la maggior parte degli utenti di Internet utilizza praticamente solo ancora lo smartphone, mentre le autorità di sicurezza lavorano con i PC.

Nel corso del periodo in esame è comparso un altro tipo di approccio con meccanismo di auto-selezione.<sup>14</sup> Anziché inviare direttamente un'e-mail di phishing con il link al sito fraudolento, la vittima riceve un'e-mail innocua a cui le si chiede di rispondere. Soltanto in un secondo passaggio, una volta pervenuta tale risposta, viene spedito via e-mail il link di phishing attraverso un messaggio preconfezionato, che viene automaticamente inoltrato al mittente senza alcun nesso con la comunicazione precedente. Con questo procedimento si vuole soprattutto evitare che il link al sito di phishing venga inoltrato troppo rapidamente da un numero eccessivo di destinatari ad autorità di sicurezza come ad esempio l'UFCS. A ricevere il link, infatti, sono soltanto coloro che non hanno riconosciuto il tentativo di truffa e che presumibilmente non lo segnaleranno neppure. Aumenta così la probabilità che il sito rimanga online per più tempo e riesca a raggiungere un maggior numero di potenziali vittime a cui sottrarre dati delle carte di credito o password.

Un ultimo episodio di rilievo che ha catturato l'attenzione dei media è stata la campagna di phishing ai danni dei clienti di PostFinance, che ha sfruttato un canale raramente utilizzato.<sup>15</sup> In questo caso, nel maggio 2024 i phisher hanno inviato per posta delle lettere contenenti un codice QR che rimandava a un sito di phishing. Nel testo si affermava che fosse necessario riattivare l'accesso all'e-banking per poter continuare a utilizzare il servizio in sicurezza. Nel suo comunicato PostFinance ha dichiarato di non inviare mai questo tipo di lettere, che pertanto andavano cestinate.<sup>16</sup>



## Raccomandazioni

Segnalate all'UFCS phishing sospetti all'indirizzo [reports@antiphishing.ch](mailto:reports@antiphishing.ch) oppure direttamente sul [sito antiphishing \(antiphishing.ch\)](https://www.antiphishing.ch). Se desiderate avere un riscontro, potete segnalare il caso di phishing ai nostri specialisti anche tramite l'apposito [modulo](#) o all'indirizzo [incidents@ncsc.ch](mailto: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.

<sup>14</sup> [Settimana 11: riciclare va bene, ma non le password! \(ncsc.admin.ch\)](#)

<sup>15</sup> Cfr. anche [Phishing: Brief von PostFinance entpuppt sich als Betrugsversuch \(srf.ch\)](#), [Phishing: PostFinance warnt vor neuer Masche \(blick.ch\)](#)

<sup>16</sup> [Sono in circolazione lettere di phishing con codice QR falsificato \(postfinance.ch\)](#)



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

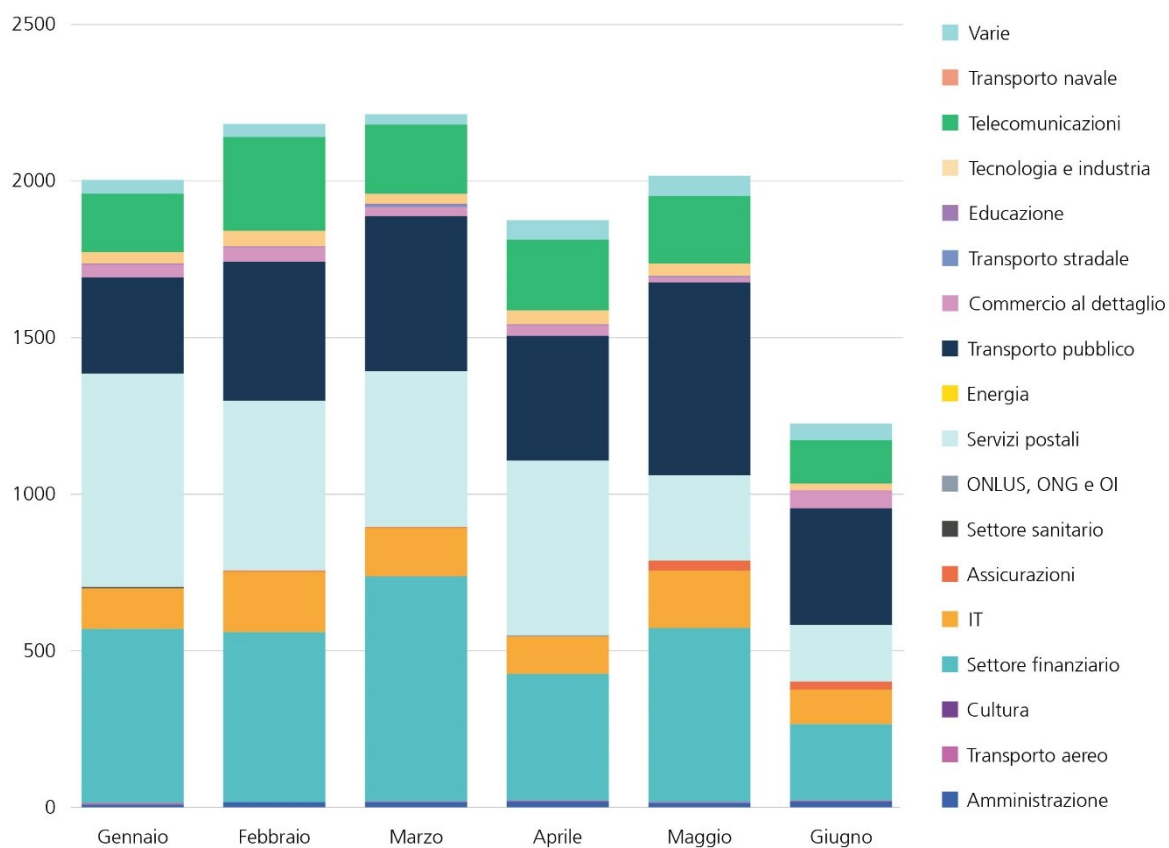


Fig. 4: Numero di URL di phishing verificati e confermati dall'UFCS nel primo semestre 2024 per settori di marchi sfruttati.



fattore si utilizzano anche telefonate fasulle (cfr. cap. 5). Nello stesso istante in cui la vittima si connette al proprio account, gli aggressori si insinuano nel suo computer e quindi anche nell'account. Essendo precedentemente riusciti a convincere la vittima a scaricare un software per l'accesso remoto, ora riescono a vedere tutte le azioni che essa compie sul computer e a effettuare manipolazioni al suo interno senza essere smascherati. Questi casi sono un esempio di come, in generale, l'ulteriore fattore non sia in grado di proteggere da attacchi indesiderati. Serve soprattutto a limitare il tempo a disposizione dell'aggressore per agire. Se viene implementata la MFA, infatti, l'hacker può accedere all'account soltanto in quell'esatto istante o se la vittima stessa è connessa, ma non in un momento successivo. Se invece un account è protetto soltanto da password, l'aggressore può utilizzarlo per i propri scopi finché quest'ultima non verrà modificata.

Nonostante ogni giorno si acceda a un'infinità di servizi digitali – dall'e-mail ai conti bancari e ai social network – per molti la MFA rimane ancora una scocciatura. Più gli utenti vengono esortati ad attivare ulteriori opzioni di autenticazione, più in alcuni aumenta il fastidio per l'ulteriore mole di lavoro percepita, il che li può indurre a diventare meno cauti e a trascurare le prassi di sicurezza opportune. Questo trend è noto anche come «MFA fatigue». Le continue richieste di aprire app per l'autenticazione, digitare codici ricevuti via SMS o utilizzare token hardware possono alla lunga diventare sfiananti. Come se non bastasse, alcuni metodi MFA potrebbero non essere affidabili.<sup>19</sup> I codici SMS, ad esempio, potrebbero arrivare in ritardo o le app di autenticazione avere problemi tecnici. Nel frattempo, purtroppo, i truffatori hanno imparato a sfruttare la «MFA fatigue» per i loro interessi criminali, bombardando i titolari degli account di richieste di verifica fino a portarli allo sfinimento. L'obiettivo, infatti, è stressare le vittime a tal punto da indurle, per esaurimento o per fretta, a confermare per sbaglio il login da parte degli hacker.



### 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)<sup>20</sup>. Prestate dunque attenzione 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. Ricordate anche che i mittenti delle e-mail e i numeri di telefono possono essere facilmente falsificati.

## 3 Malware

Rispetto ad altre fonti di diffusione dei malware in Svizzera<sup>21</sup>, l'UFCS ha ricevuto relativamente poche segnalazioni (92) con riferimento diretto a un software dannoso (malware)<sup>22</sup>. I malware

<sup>19</sup> Cfr. [Second Factor SMS: Worse Than Its Reputation \(ccc.de\)](https://www.ccc.de)

<sup>20</sup> [Ingegneria sociale \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

<sup>21</sup> Cfr. [Statistics \(abuse.ch\)](https://www.abuse.ch)

<sup>22</sup> [Software dannoso \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

vengono sviluppati per eseguire, attraverso programmi, funzioni indesiderate e perlopiù dannose su sistemi informatici, in genere all'insaputa dell'utente.<sup>23</sup> Questa circostanza spiega anche il numero tendenzialmente basso di segnalazioni da parte della popolazione – soprattutto nel caso dei malware associati all'invio di e-mail. Chi non sa che il sistema è infettato da un malware, non segnalerà nulla. D'altro lato, i filtri sviluppati dai produttori di software hanno raggiunto nel frattempo livelli di sofisticazione tali che soltanto una minima percentuale di e-mail con contenuto malevolo arriva a destinazione. Negli ultimi anni, inoltre, anche i meccanismi di sicurezza implementati sui terminali sono talmente migliorati che solo dopo molteplici interazioni con l'utente e svariati avvisi si riesce a installare un file dannoso. Si presume che i criminali stiano puntando a nuovi canali per installare malware sui dispositivi. Li si nasconde ad esempio in freeware, plugin o applicazioni che per l'utente risultano meno trasparenti e che quindi generano anche un minor numero di segnalazioni. Nel corso del periodo in esame si è comunque osservata, con «Poseidon Stealer», un'ondata di malware di vasta portata ai danni degli utenti MacOS (cfr. cap. 3.1). A fine giugno 2024 molti cittadini svizzeri hanno ricevuto un'e-mail con l'oggetto «Da luglio 2024 accesso AGOV obbligatorio per tutti i servizi pubblici».<sup>24</sup> Nell'e-mail veniva chiesto ai destinatari di installare un software, essendo presumibilmente l'unico modo per continuare a garantire l'accesso ai servizi della pubblica amministrazione. Come nel caso del phishing, spesso è il fattore umano che determina il successo di una campagna di malware. Più il pretesto sembra credibile, maggiori sono le probabilità per i cybercriminali di riuscire a diffondere il loro malware su vasta scala.

### 3.1 Accesso iniziale con malware

Per procurarsi un primo accesso a un sistema informatico, spesso i cybercriminali fanno ricorso a malware, come ad esempio i trojan. In genere questi software richiedono un'azione da parte dell'utente, per cui fanno ricorso a una serie di meccanismi di inganno. Il malware, ad esempio, può essere nascosto in un altro programma o in un allegato o un link ricevuto via e-mail, che a un utente poco attento può sembrare innocuo. Molti malware attivi a livello internazionale sono presenti anche in Svizzera, come «AgentTesla», «DarkGate», «FakeUpdates», «Formbook», «Gootloader», «GuLoader», «PikaBot» o anche «Poseidon Stealer»<sup>25</sup>. Di seguito ci si soffermerà in dettaglio sugli ultimi due che, per quanto riguarda la Svizzera, evidenziano a titolo esemplificativo i metodi di diffusione e i fattori che influiscono sull'effetto sortito.

A inizio anno si sono osservati casi in cui si è cercato di diffondere il malware «PikaBot» attraverso il dirottamento di conversazioni via e-mail (ingl. *e-mail thread hijacking*). In questo caso, i criminali si sono serviti di vecchie corrispondenze e-mail sottratte dalle caselle di posta di altre vittime (cfr. cap. 2.1) per ingannare la persona presa di mira (cfr. fig. 5).

---

<sup>23</sup> [BSI - Malware \(bsi.bund.de\)](https://www.bsi.bund.de)

<sup>24</sup> [Criminali informatici diffondono un malware per macOS apparentemente proveniente da AGOV \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/press-releases/2024/06/06-criminals-distribute-malware-for-macos-apparently-originating-from-ago.html)

<sup>25</sup> [Breve analisi tecnica del malware «Poseidon Stealer» \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/press-releases/2024/06/06-poseidon-stealer.html)



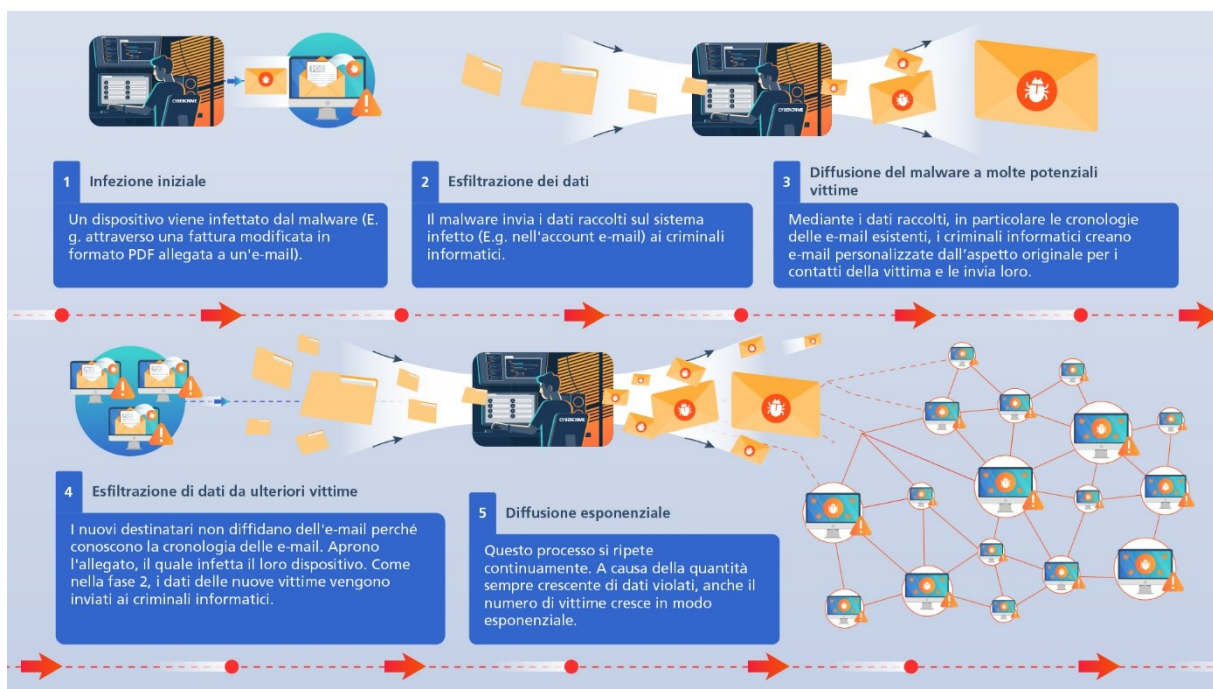


Fig. 5: Dirottamento di conversazioni via e-mail per la diffusione di malware

Il documento allegato, ad esempio un file Excel, informava l'utente che determinati file erano disponibili online e che, per visualizzarli, occorreva cliccare su un pulsante presente in quel file.<sup>26</sup> Dietro quel pulsante si cela tuttavia uno script che causa un'infezione da PikaBot. Quest'ultima può avere conseguenze di notevole portata, soprattutto considerato che dal secondo semestre del 2023 si è osservato un uso sempre più massiccio di questo malware associato a gruppi di ransomware.<sup>27</sup> Per contrastarlo, con l'operazione «Endgame» partita a maggio 2024 le autorità di perseguimento penale sono riuscite, nell'ambito della collaborazione internazionale, a minare l'infrastruttura di vari provider criminali che offrono accessi iniziali (Initial Access Broker) e malware (malware-as-a-service).<sup>28</sup> Questo attacco era rivolto anche all'infrastruttura di PikaBot. Sebbene nell'immediato si presuma che l'operazione riduca le attività di queste minacce nel nostro Paese, questi effetti difficilmente permangono a lungo termine, dal momento che gli autori dei malware – se non sono stati arrestati – ricostruiscono ex-novo la loro infrastruttura, e i criminali che utilizzano questi servizi si rivolgono rapidamente ad altri provider.

A fine giugno 2024 l'UFCS ha comunicato che in Svizzera era in corso una campagna di malspam<sup>29</sup> con «Poseidon Stealer» rivolta contro gli utenti MacOS, nella quale si utilizzava AGOV per indurre le vittime a non dubitare della veridicità del contenuto.<sup>30</sup> Il link presente nell'e-mail indirizzava a un sito in cui ai destinatari veniva chiesto di scaricare un file .dmg, sostenendo che fosse un'applicazione desktop di AGOV. In realtà, invece, il programma proposto era il malware Poseidon Stealer che, non appena eseguito, sottraeva informazioni dal

<sup>26</sup> [TA577 introduced a rather interesting new approach to distribute their Pikabot malware \(x.com\)](#)

<sup>27</sup> [The Emerging Threat of PikaBot Malware \(flashpoint.io\)](#)

<sup>28</sup> [Largest ever operation against botnets hits dropper malware ecosystem \(europol.europa.eu\)](#)

<sup>29</sup> [Was ist Spam? Seine Arten und wie Sie sich schützen \(avast.com\)](#)

<sup>30</sup> [Criminali informatici diffondono un malware per macOS apparentemente proveniente da AGOV \(ncsc.admin.ch\)](#)





sui sistemi informatici della vittima, rendendoli inutilizzabili per quest'ultima. In genere i dati vengono contemporaneamente esfiltrati. A seguire chiedono alla vittima il pagamento di un riscatto per ottenere un tool di decodifica (decryptor) e impedire che i dati rubati vengano pubblicati e rivenduti. L'esperienza dimostra che l'entità dei danni varia di caso in caso. Mentre per alcune vittime gli attacchi non hanno pressoché alcuna conseguenza grazie alle misure di «ciberigiene» adottate, per altre i danni possono risultare potenzialmente fatali.<sup>35</sup> Oltre ai costi di ripristino le imprese devono mettere in conto che i loro servizi informatici saranno parzialmente o completamente fuori uso per giorni o settimane. Dopo la pubblicazione dei dati, inoltre, si può essere esposti al rischio, ad esempio, di un danno reputazionale.

### 3.2.1 Attività ransomware in Svizzera

Il numero di segnalazioni all'UFCS relative ad attacchi ransomware ai danni delle imprese segna un lieve calo, fermandosi a quota 39 nel primo semestre del 2024. Nello stesso periodo dello scorso anno l'UFCS ne registrava ancora 56. I privati, invece, sono sempre meno presi di mira dai cibercriminali, in linea con la tendenza registrata sinora: attualmente sono soltanto cinque le segnalazioni provenienti da privati, contro le otto dello stesso periodo dell'anno precedente. Una maggiore sensibilizzazione degli utenti e l'allestimento di backup (offline) potrebbero aver contribuito a questa flessione. Non è da escludere, inoltre, che abbia inciso anche il maggior numero di attacchi mirati contro bersagli molto remunerativi. Se l'obiettivo è fare quanta più pressione possibile per ottenere il pagamento del riscatto, considerato l'onere ulteriore che ne consegue i criminali potrebbero tendenzialmente attaccare, con le stesse risorse, un numero inferiore di vittime. Le vittime ritenute non interessanti, ma ai danni delle quali gli aggressori si sono comunque procurati ad esempio l'accesso ai sistemi, possono essere monetizzate a parte con la vendita delle informazioni sul dark web (cfr. cap. 3.2).

I tre gruppi di ransomware «Akira», «8Base» und «Black Basta» sono responsabili, nel periodo in esame, di svariati attacchi ai danni di imprese svizzere. A colpire è stato il numero relativamente elevato di segnalazioni da parte di aziende nazionali infettate dal ransomware «Akira», di cui tre soltanto a marzo. Questo gruppo di ransomware si contraddistingue per il suo comportamento opportunistico, visto il numero proporzionalmente elevato di vittime, comprendente diversi settori e differenti dimensioni d'impresa. Nonostante il gruppo sia attivo soltanto da marzo 2023, a inizio 2024 si stima che avesse già attaccato 250 organizzazioni in Europa, America settentrionale e Australia.<sup>36</sup> Akira ha un modus operandi innovativo: secondo l'NCSC finlandese, il collettivo sfrutta ad esempio una vulnerabilità VPN di CISCO per criptare sistematicamente sistemi NAS (dispositivi di archiviazione collegati alla rete) e backup di backup.<sup>37</sup>

Diversamente da Akira, le segnalazioni relative al ransomware 8Base sono lievemente calate, fermandosi a quota tre. In Svizzera, 8Base è diventato famoso dopo che nel novembre del 2023 il gruppo era riuscito a infettare la società informatica svizzera Concevis AG.<sup>38</sup> Il collettivo utilizza una combinazione tra criptaggio dei dati e tecniche di ricatto «name-and-shame» per

---

ransomware di Play del 2023: [L'IFPDT conclude le inchieste nei confronti della ditta Xplain e degli uffici federali fedpol e UDSC \(edoeb.admin.ch\)](#)

<sup>35</sup> Cfr. ad esempio Akumin Inc., CloudNordic, KNP Logistics, MediSecure, Travelex, United Structures

<sup>36</sup> [#StopRansomware: Akira Ransomware \(cisa.gov\)](#)

<sup>37</sup> [Finland warns of Akira ransomware wiping NAS and tape backup devices \(bleepingcomputer.com\)](#)

<sup>38</sup> [Attacco hacker alla società Concevis: interessata anche l'Amministrazione federale \(ncsc.admin.ch\)](#)

indurre le vittime, operanti in diversi settori, a pagare un riscatto.<sup>39</sup> Alcuni campioni di questo ransomware mostrano che si tratta di una versione adattata del ransomware «Phobos v2.9.1»<sup>40</sup>, caricata tramite il software «SmokeLoader».<sup>41</sup> Due casi svizzeri sono stati anche discussi pubblicamente, visto che i dati trafugati erano stati pubblicati sul sito di data leak del gruppo. Uno di essi riguardava la società di telecomunicazioni Nexus Telecom Switzerland AG.<sup>42</sup> Le conseguenze della pubblicazione di 23 gigabyte (GB) di dati sono state contenute, essendo stati sottratti soprattutto dati di archivio e non avendo la società clienti svizzeri. Nell'altro caso, invece, 8Base ha attaccato l'azienda Microna, fornitrice di ortodontisti, dentisti e odontoiatri. Secondo le dichiarazioni della società, l'incidente non ha causato interruzioni alla produzione. Essendovi le copie di sicurezza disponibili, la funzionalità dei sistemi operativi interessati è stata completamente ripristinata nell'arco di qualche giorno. Nonostante la pronta reazione di Mikrona, si presume che alcuni dati siano stati compromessi.<sup>43</sup>

Il gruppo di ransomware Black Basta<sup>44</sup> si è fatto notare in Svizzera per le sue attività soprattutto nel periodo tra febbraio e aprile 2024: a finire contemporaneamente nel mirino dei criminali sono state tre grandi imprese svizzere – tra cui un fornitore per infrastrutture critiche. Nei mesi di febbraio e marzo del 2024, sul sito di data leak di Black Basta sono comparsi i nomi della società di somministrazione di personale Il Team SA e del negozio di giocattoli Franz Carl Weber. Dopo che le due aziende hanno evidentemente respinto ogni tentativo di ricatto, i loro dati – in parte sensibili – sono stati pubblicati.<sup>45</sup> A differenza ad esempio di Akira o 8Base, Black Basta utilizza spesso un approccio più selettivo nella scelta dei suoi obiettivi. Il suo ransomware colpisce sistematicamente imprese e organizzazioni di alto livello, a cui possono essere avanzate richieste di riscatto corpose. Lo dimostra l'attacco di aprile 2024 ai danni di una terza vittima, la società Swisspro.<sup>46</sup> Black Basta ha ammesso la paternità dell'attacco e, stando alle sue dichiarazioni, ha pubblicato 700 GB di dati dopo che Swisspro non ha risposto al ricatto e si è rifiutata di pagare. Avendo colpito vecchie infrastrutture informatiche, le conseguenze dell'attacco sono state minime e Swisspro è stata in grado di fornire i propri servizi in ogni momento.<sup>47</sup>

### 3.2.2 Ransomware, una sfida globale

Anche le infrastrutture critiche sono costantemente nel mirino dei collettivi di ransomware. La loro estrema rilevanza per la vita quotidiana della società e il rischio che da un black-out dei sistemi si scatenino effetti a cascata su altre funzioni critiche aumenta ulteriormente la pressione per trovare una soluzione rapida. È quanto ha osservato anche il Federal Bureau of Investigation (FBI), riscontrando un generale incremento degli attacchi ransomware ai danni

---

<sup>39</sup> [Ransomware Spotlight: 8Base \(trendmicro.com\)](#)

<sup>40</sup> [#StopRansomware: Phobos Ransomware \(cisa.gov\)](#)

<sup>41</sup> [8Base \(sentinelone.com\)](#)

<sup>42</sup> [Daten von Nexus Telecom im Darkweb veröffentlicht \(inside-it.ch\)](#)

<sup>43</sup> [Cyberangriff auf Schweizer Medtech-Firma \(inside-it.ch\)](#)

<sup>44</sup> [#StopRansomware: Black Basta \(cisa.gov\)](#)

<sup>45</sup> [Haufenweise Kundendaten von Schweizer Personalvermittler gestohlen \(inside-it.ch\)](#), [Cyberkriminelle stehlen schützenswerte Daten von Franz Carl Weber \(inside-it.ch\)](#)

<sup>46</sup> [Basta bekennt sich zum Angriff auf BKW-Tochter Swisspro \(inside-it.ch\)](#)

<sup>47</sup> [Russischer Hackerangriff: Attacke auf Schweizer Stromkonzern wirft Fragen auf \(bernerzeitung.ch\)](#)

di infrastrutture critiche.<sup>48</sup> Sebbene alcuni gruppi affermino di seguire determinati standard etici nella scelta delle loro vittime, la maggioranza di essi prende di mira appositamente le infrastrutture critiche perché più inclini a pagare un riscatto. Sono state colpite da attacchi ransomware, ad esempio, le società operanti nell'approvvigionamento e smaltimento delle acque Veolia North America<sup>49</sup> e Southern Water<sup>50</sup>. Analogamente, una software house tedesca che sviluppa prodotti per i sistemi di controllo delle infrastrutture critiche è caduta vittima di un attacco di crittografia dei dati.<sup>51</sup> A parte questi, anche il settore sanitario è un bersaglio prediletto dai criminali. Le autorità statunitensi, infatti, hanno messo in guardia specificatamente il settore sanitario americano dalle attività ransomware di Phobos e Akira (cfr. cap. [3.2.1](#)).<sup>52</sup>

Un caso sensazionale che ha suscitato scalpore a inizio giugno 2024 ha riguardato vari ospedali londinesi, dopo l'attacco sferrato dal ransomware «Qilin» ai danni di Synnovis – uno dei loro fornitori di servizi. A causa del ciberattacco e dei conseguenti black-out dei sistemi informatici, gli ospedali si sono visti costretti a spostare circa 6000 appuntamenti, tra cui interventi chirurgici e trasfusioni di sangue, nell'arco delle cinque settimane successive.<sup>53</sup> Il pronto soccorso, invece, è rimasto sempre operativo. Qualche settimana più tardi il gruppo di ransomware ha pubblicato 400 GB di dati sanitari sensibili.<sup>54</sup> In un'intervista successiva i criminali hanno dichiarato di essere consapevoli delle conseguenze delle loro azioni e di non essere pentiti di nulla.<sup>55</sup>

Per contrastare la crescente minaccia globale delle attività ransomware, varie autorità di perseguimento penale hanno introdotto diverse misure di mitigazione. Degna di nota, in particolare, è la «Operation Cronos» di metà febbraio 2024. Coordinate dalla National Crime Agency (NCA) britannica, le autorità di polizia hanno condotto una manovra di disturbo contro il collettivo di ransomware «LockBit», all'epoca ancora influente.<sup>56</sup> Basti pensare che nel 2023, ad esempio, gli sono stati attribuiti dal 25 al 33 per cento di tutti gli attacchi ransomware a livello mondiale.<sup>57</sup> Oltre ad aver arrestato alcuni membri del collettivo<sup>58</sup> e sequestrato criptovalute, le autorità di perseguimento penale coinvolte hanno sviluppato un decryptor con cui le vittime hanno potuto ripristinare gratuitamente i loro dati crittografati. Il momento clou dell'operazione è stata l'acquisizione dei server dei cybercriminali e il sequestro del loro sito di data leak. Quest'ultimo è stato immediatamente utilizzato dalla polizia come piattaforma di comunicazione per pubblicare aggiornamenti sul caso, come ad esempio l'identità di uno degli amministratori di LockBit<sup>59</sup>.<sup>60</sup> In seguito all'intervento della polizia la leadership di LockBit ha perso la

---

<sup>48</sup> [Federal Bureau of Investigation: Internet Crime Report 2023 \(ic3.gov\)](#)

<sup>49</sup> [Veolia Responds to Cyber Incident \(mywater.veolia.us\)](#)

<sup>50</sup> [Black Basta claims hack on Southern Water \(computing.co.uk\)](#)

<sup>51</sup> [Critical infrastructure software maker confirms ransomware attack \(bleepingcomputer.com\)](#)

<sup>52</sup> Cfr. [CISA, FBI, and MS-ISAC Release Advisory on Phobos Ransomware \(cisa.gov\)](#), [Feds Warn Health Sector About Akira Again, Amid New Attacks \(bankinfosecurity.com\)](#)

<sup>53</sup> [NHS Trusts cancelled over 6,000 appointments after Qilin cyber attack \(computerweekly.com\)](#), [Cyber-attack on London hospitals declared critical incident \(bbc.com\)](#)

<sup>54</sup> [NHS England confirm patient data stolen in cyber attack \(bbc.com\)](#)

<sup>55</sup> [Qilin has 'no regrets' over the healthcare crisis it caused \(theregister.com\)](#)

<sup>56</sup> [The NCA announces the disruption of LockBit with Operation Cronos \(nationalcrimeagency.gov.uk\)](#)

<sup>57</sup> [Auswirkungen der Operation Cronos auf LockBit \(trendmicro.com\)](#)

<sup>58</sup> [LockBit administrator sentenced to almost four years in prison after guilty plea \(therecord.media\)](#)

<sup>59</sup> [LockBit leader unmasked and sanctioned \(nationalcrimeagency.gov.uk\)](#)

<sup>60</sup> [Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption \(trendmicro.com\)](#)

fiducia di molti dei suoi affiliati,<sup>61</sup> tanto che il collettivo è diventato l'ombra di sé stesso. Ciò nonostante, anche dopo la «Operation Cronos» si continuano a registrare casi di infezioni da parte di LockBit. Anche l'UFCS ha ricevuto tre segnalazioni da parte di vittime svizzere, tutte successive all'operazione internazionale.

Il panorama delle cyberminacce è dinamico anche sul fronte dei gruppi di ransomware ed è soggetto a continui cambiamenti. Lo dimostra, da un lato, il caso del gruppo LockBit, che con un'operazione di perseguimento penale mirata è stato di fatto condannato all'irrelevanza. Dall'altro, si registrano sempre nuovi casi di gruppi che scelgono volontariamente di abbandonare la scena, nel momento in cui si rendono conto che vale più la pena svignarsela col bottino (exit scam) o ripartire da zero piuttosto che continuare l'attività. È quanto ha deciso di fare, nel primo semestre del 2024, il gruppo di ransomware «BlackCat» – noto anche come «ALPHV». Dopo che nel dicembre 2023 BlackCat era finito nel mirino di un'operazione di perseguimento penale,<sup>62</sup> a marzo 2024 gli amministratori hanno deciso di tenere tutti per sé i 22 milioni di USD di riscatto incassati, lasciando a bocca asciutta l'affiliato.<sup>63</sup> Una decisione del genere implica anche la definitiva chiusura endogena dell'attività. Altri collettivi di ransomware, come Black Basta, Akira, Hunters International o BianLian, hanno approfittato del vuoto lasciato da BlackCat e sono riusciti successivamente a incrementare il volume delle loro attività. Si presume che molti degli affiliati di BlackCat si siano avvicinati ad altri gruppi. Non è da escludere, inoltre, che gruppi di ransomware destabilizzati rinascano dalle proprie ceneri per riprendere la loro attività sotto un nuovo nome. Un'altra possibilità è che i collettivi più grandi tendano a mano a mano a scomparire per lasciare il posto a tanti gruppi più piccoli. Questo consentirebbe agli sviluppatori di ransomware di lavorare alternativamente o addirittura allo stesso tempo per più operazioni ransomware.



## Raccomandazioni

Effettuate regolarmente delle copie di sicurezza archiviando i vostri dati (anche) su un supporto esterno.<sup>64</sup> Per i dati estremamente importanti seguite la famosa **regola del 3-2-1**: conservate almeno tre copie di sicurezza in due luoghi diversi, di cui almeno una completamente offline.<sup>65</sup> Le strategie di backup più moderne si basano ancora su questa regola, ma migliorano i parametri relativi a ridondanza, accesso e distanza geografica, integrando tra l'altro provider che offrono servizi cloud corrispondenti.<sup>66</sup>

Sul sito dell'UFCS è disponibile un [elenco di altre misure preventive](#) per proteggersi dal ransomware e varie [istruzioni operative su come procedere in caso di attacco](#). In generale l'UFCS sconsiglia alle vittime di ransomware di pagare il riscatto, non essendovi alcuna garanzia che

<sup>61</sup> [Ransomware Talent Surges to Akira After LockBit's Demise \(bankinfosecurity.com\)](#)

<sup>62</sup> [Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant \(justice.gov\)](#)

<sup>63</sup> [BlackCat ransomware turns off servers amid claim they stole \\$22 million ransom \(bleepingcomputer.com\)](#)

<sup>64</sup> [S-U-P-E-R.ch – Cosa tenere a mente quando si effettua il backup dei dati \(ncsc.admin.ch\)](#)

<sup>65</sup> O. Hönö cit. in [Finland warns of Akira ransomware wiping NAS and tape backup devices \(bleepingcomputer.com\)](#)

<sup>66</sup> [What's the Diff: 3-2-1 vs. 3-2-1-1-0 vs. 4-3-2 \(backblaze.com\)](#)

i cybercriminali mantengono la parola data. Una volta pagato il riscatto, in particolare, si accresce la propria attrattiva per ulteriori attacchi.

### 3.3 Malware su dispositivi mobili

Da alcuni anni i dispositivi mobili – smartphone e tablet – sono diventati i nostri compagni di vita quotidiana. Portatili, potenti e costantemente connessi, contengono sempre più dati personali, come foto, contatti ed e-mail, e applicazioni con contenuti sensibili – ad esempio e-banking e software MFA. Per consentire queste funzioni, la maggior parte dei dispositivi mobili utilizza i sistemi operativi Android o iOS. Proprio per questi motivi esiste una categoria di malware a sé che prende di mira i sistemi operativi dei dispositivi mobili, i cosiddetti «mobile malware». Nel periodo in esame, in questo ambito si sono osservati vari incidenti e sviluppi, nessuno dei quali riferiti esclusivamente alla Svizzera.

In Finlandia, nel maggio del 2024 l'agenzia Traficom ha messo in guardia da una campagna di diffusione di malware ai danni degli utenti Android e dei loro account di online banking.<sup>67</sup> Le vittime ricevevano un SMS che chiedeva loro di installare un'applicazione antivirus fasulla. Per ingannare i destinatari, l'SMS avvisava di una sospetta attività bancaria o di una richiesta di incasso e faceva credere di essere stato inviato da banche o servizi di pagamento. I criminali hanno spedito gli SMS in finlandese e hanno utilizzato lo spoofing<sup>68</sup> per dare l'impressione che provenissero da operatori di telecomunicazioni locali. Ai destinatari, inoltre, veniva chiesto di chiamare un numero. Durante la telefonata le vittime venivano convinte a scaricare un'applicazione antivirus fasulla al di fuori dell'app store ufficiale. In realtà, l'app in questione era il malware per dispositivi mobili «Vultur»<sup>69</sup> che, una volta installato, consente tra l'altro l'accesso ad applicazioni presenti sul telefono infetto. Tra queste c'erano anche le applicazioni di e-banking, il che ha consentito ai criminali di svuotare i conti correnti delle vittime.

Oltre a Vultur esiste una miriade di altri malware che infettano i sistemi operativi dei dispositivi mobili e che vengono costantemente perfezionati. Nell'aprile 2024, ad esempio, alcuni ricercatori nel campo della sicurezza hanno analizzato un nuovo malware per cellulari chiamato «Brokewell». Questo software malevolo attacca i sistemi operativi Android spacciandosi per un aggiornamento di Google Chrome, disponibile per il download in un sito web apparentemente innocuo al di fuori dell'app store ufficiale. Una volta installato, consente ai cybercriminali di rubare informazioni sensibili sovrapponendo alle app di e-banking finestre di login fasulle e quindi intercettando le credenziali d'accesso degli utenti. Brokewell è inoltre in grado di registrare altre interazioni degli utenti con i loro dispositivi, ad esempio inserimenti di dati e conversazioni attraverso il microfono, nonché raccogliere e inoltrare informazioni come la posizione geografica, l'elenco delle chiamate e i dettagli tecnici del dispositivo.<sup>70</sup>

Anche gli utenti iOS non sono immuni a questa minaccia. Nel febbraio 2024 alcuni ricercatori nel campo della sicurezza hanno scoperto un malware chiamato «GoldPickaxe.iOS», che

---

<sup>67</sup> [The National Cyber Security Centre Finland's weekly review – 18/2024 \(kyberturvallisuuskeskus.fi\)](#)

<sup>68</sup> [Spoofing \(ncsc.admin.ch\)](#)

<sup>69</sup> [Android Malware Vultur Expands Its Wingspan \(fox-it.com\)](#)

<sup>70</sup> [Brokewell: do not go broke from new banking malware! \(threatfabric.com\)](#)



prende specificatamente di mira il sistema operativo iOS. Questo malware è in grado, ad esempio, di raccogliere dati sul riconoscimento facciale e documenti d'identità e di intercettare SMS. Secondo il rapporto, i criminali avevano utilizzato i dati biometrici trafugati per realizzare un deepfake<sup>71</sup>. Grazie ai documenti d'identità rubati e alla possibilità di captare telefonate e SMS, hanno potuto accedere ai conti bancari delle loro vittime e confermare transazioni di grandi somme di denaro utilizzando il riconoscimento facciale. Per indurre le vittime a installare il software sul loro dispositivo mobile, gli sviluppatori di GoldPickaxe.iOS hanno utilizzato tecniche di ingegneria sociale<sup>72</sup>. Sono stati due i canali di diffusione utilizzati: in un primo momento hanno fatto circolare il malware sulla piattaforma TestFlight di Apple, sulla quale gli utenti possono testare le app prima del loro lancio ufficiale. Quando il malware è stato tolto dalla piattaforma TestFlight, i criminali hanno cambiato metodo, puntando sull'installazione di un profilo di gestione dei dispositivi mobili (MDM)<sup>73</sup> tramite un sito web fraudolento. Dopo l'installazione da parte della vittima, il profilo ha consentito ai criminali di acquisire il pieno controllo del dispositivo, per cui hanno potuto scaricare il malware.<sup>74</sup>



### Raccomandazione

Sul sito dell'UFCS trovate un [elenco di nove consigli pratici per un utilizzo sicuro del cellulare \(ncsc.admin.ch\)](https://ncsc.admin.ch).

## 4 Vulnerabilità

Chi segue attentamente il susseguirsi di articoli e avvisi pubblicati in merito alle vulnerabilità potrebbe avere l'impressione che i prodotti di celebri software house – come ad esempio Cisco, Citrix, Fortinet, Ivanti e VMware – sembrano essere fin troppo spesso bersaglio di vulnerabilità. Parecchie volte all'anno i loro nomi finiscono sulle pagine della stampa specializzata perché vittime di gravi lacune di sicurezza. Ne è un esempio la lacuna di sicurezza scoperta nell'aprile 2024 nella soluzione firewall del produttore di software Palo Alto, che ha consentito ai criminali di attaccare dispositivi vulnerabili ed eseguire da remoto un codice che ha compromesso i sistemi.<sup>75</sup>

A parte questo caso, nel corso del periodo in esame l'UFCS ha allertato più volte i gestori di infrastrutture critiche in merito a varie vulnerabilità presenti nei prodotti. Nell'85 per cento dei casi in cui l'UFCS ha diramato segnalazioni relative a lacune di sicurezza nei prodotti, gli sviluppatori erano aziende attive a livello globale. Soltanto il 15 per cento degli avvisi di vulnerabilità pubblicati, ossia un numero notevolmente inferiore, si riferiva a lacune di sicurezza in applicazioni di fornitori meno conosciuti – e quindi anche molto meno diffusi in Svizzera. In

<sup>71</sup> [Deepfake \(wikipedia.org\)](https://it.wikipedia.org/wiki/Deepfake)

<sup>72</sup> [Ingegneria sociale \(ncsc.admin.ch\)](https://ncsc.admin.ch)

<sup>73</sup> [Mobile-Device-Management \(wikipedia.org\)](https://it.wikipedia.org/wiki/Mobile-Device-Management)

<sup>74</sup> [Face Off: Group-IB identified iOS trojan stealing facial recognition data \(group-ib.com\)](https://group-ib.com)

<sup>75</sup> [CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect \(security.paloaltonetworks.com\)](https://security.paloaltonetworks.com), [Vulnerabilità critica nei firewall di Palo Alto \(ncsc.admin.ch\)](https://ncsc.admin.ch)



generale, comunque, si può dire che le aziende svizzere sono sostanzialmente alle prese con le stesse vulnerabilità, che devono assicurarsi di eliminare, delle loro controparti internazionali. Qui di seguito, ecco spiegati i motivi per cui sono i prodotti di questi rinomati fornitori a essere continuamente bersaglio di vulnerabilità – a volte con un livello di criticità molto elevato. Da un lato i prodotti software più articolati tendono a essere molto complessi. Contengono numerose funzioni e interdipendenze nel codice e all'interno del software, ma anche verso l'esterno, ad esempio con il sistema operativo. Questa complessità può generare errori difficili da diagnosticare ed eliminare all'interno del codice. Ogni nuova funzione o integrazione può, passando inizialmente inosservata, introdurre nuove vulnerabilità. In più, molti grandi sviluppatori di software devono continuamente mettere a punto i loro prodotti per rimanere competitivi sul mercato. Questo costante perfezionamento va spesso di pari passo con la pressione per lanciare rapidamente sul mercato nuovi prodotti e aggiornamenti. Anche questo aspetto può far sì che eventuali vulnerabilità createsi nel processo di sviluppo rimangano inizialmente nascoste. D'altro lato, i software commercialmente più diffusi vengono utilizzati da una miriade di utenti, il che li rende sostanzialmente appetibili ai cybercriminali. Se andato a buon fine, un attacco a un software particolarmente popolare può arrivare a colpire milioni di dispositivi e utenti, massimizzando la potenzialità di danno di un attacco. Questi e altri fattori contribuiscono in maniera determinante al fatto che, nel contesto della gestione delle vulnerabilità, si sentano spesso nomi di grandi e rinomati produttori di software e che per i loro prodotti si rendano note, apparentemente senza sosta, sempre nuove vulnerabilità.



### Conclusione / raccomandazioni

Per i software più diffusi e utilizzati, la probabilità di scoprire a cadenza regolare nuove lacune di sicurezza è notevolmente maggiore: tra i motivi vi sono l'ampia base di utenti e la complessità del software.

I produttori di software commercialmente molto diffusi devono pertanto, da parte loro, promuovere una solida cultura della sicurezza e assumersi la responsabilità della sicurezza dei loro prodotti. Sono varie le misure da parte dei fornitori di software che contribuiscono a rendere un prodotto per quanto possibile sicuro: ad esempio l'esecuzione di test, l'implementazione di best practice per lo sviluppo di prodotti sicuri e soprattutto anche una reazione rapida ed efficiente alla diagnosi di nuove vulnerabilità.

Se utilizzate software di famosi fornitori globali, ciò non significa necessariamente che siano più sicuri da utilizzare e gestire rispetto a un prodotto meno conosciuto. Anche i software di rinomati produttori presentano lacune di sicurezza.

Le lacune di sicurezza risolte di recente non garantiscono che da quel momento in poi il prodotto possa essere utilizzato in sicurezza per lungo tempo. Nuove vulnerabilità possono emergere **in qualsiasi momento**, anche **subito** dopo l'ultimo patch ai vostri sistemi. Ricordate quindi che è necessario effettuare aggiornamenti periodici.

Vale dunque quanto segue: non perdetevi tempo – **aggiornate** il software quando ci sono aggiornamenti di sicurezza disponibili. Anticipate la **fine del ciclo di vita** di un software, sostituendolo per tempo.



## 5.1 Tecniche di intelligenza artificiale nei tentativi di truffa

Già l'ultimo rapporto semestrale<sup>79</sup> si è occupato a fondo dell'impiego dell'intelligenza artificiale (IA) nei tentativi di truffa. Il trend non ha subito sostanziali cambiamenti negli ultimi sei mesi. Nel singolo caso è difficile stabilire in che misura siano stati utilizzati, ad esempio, l'apprendimento automatico (machine learning, ML)<sup>80</sup> e i modelli linguistici di grandi dimensioni (large language model, LLM)<sup>81</sup>, per cui in genere si può soltanto supporre se si sia fatto ricorso o meno a un tool di traduzione. In qualche raro caso, invece, il loro impiego è evidente. L'episodio ad oggi più eclatante e clamoroso di utilizzo di questi strumenti è stata una truffa del CEO<sup>82</sup>. Questa variante di frode consiste nell'inviare al reparto finanziario una richiesta di pagamento apparentemente urgente da parte del CEO. In genere i truffatori non si prendono la briga di rivolgersi in modo specifico alla vittima e di personalizzare accuratamente la richiesta. I testi utilizzati sono infatti generici e perlopiù identici. In questi casi, inoltre, si cerca di evitare che la vittima contatti direttamente il capo. Ma non è stato così in questo episodio: all'inizio, il responsabile finanziario è stato contattato telefonicamente da un sedicente avvocato e invitato a una videoconferenza con il suo capo di lì a pochi minuti.<sup>83</sup> La vittima ha ricevuto un'e-mail con le credenziali per l'incontro. Quando il responsabile finanziario si è collegato alla riunione online, ha effettivamente potuto vedere il suo capo sullo schermo e parlarci. Durante la conversazione, il presunto capo ha poi cercato di ottenere il numero di cellulare del responsabile finanziario e di convincerlo a effettuare transazioni finanziarie. In questo caso, i truffatori hanno creato il video del CEO servendosi di algoritmi deepfake. Non è chiaro dove i criminali abbiano trovato il materiale di partenza per creare i video falsi. L'UFCS presume tuttavia che per creare questi video deepfake sia stato utilizzato materiale video disponibile pubblicamente.

## 5.2 Pubblicità per truffa dell'investimento

Per indurre utenti online a effettuare un investimento su un sito web ambiguo<sup>84</sup>, i criminali si servono di personaggi famosi attraverso cui pubblicizzare offerte d'investimento apparentemente redditizie, promettendo lautissimi guadagni nell'arco di brevissimo tempo. Celebrità svizzere e internazionali del calibro di Sandra Boner, Beatrice Müller, Roger Federer, Nemo o Alain Berset vedono loro malgrado comparire i loro volti su numerosi annunci pubblicitari fasulli che, a volte di pessimo gusto, stanno diventando sempre più fastidiosi. Ogni giorno ne compaiono di nuovi, catturando l'attenzione con false promesse.

Sinora la pubblicità per la truffa dell'investimento ha sempre seguito i medesimi schemi: si esordisce dicendo che al personaggio famoso non è concesso di parlare di un investimento altamente redditizio e sicuro, pena il licenziamento. Un'altra variante afferma che è stata fatta inavvertitamente una dichiarazione che non avrebbe mai dovuto essere resa pubblica. Succede anche che venga persino annunciata la morte di un personaggio famoso. La prima tranche d'investimento è in genere pari a CHF 250. Dopo i primi giorni la vittima riceve resoconti di profitti alle stelle, che hanno lo scopo di indurla a investire ulteriormente. I 250 franchi iniziali

---

<sup>79</sup> Cfr. [Rapporto semestrale 2023/2 \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/0/0/0/0/0/0/rapporto-semestrale-2023-2)

<sup>80</sup> [Apprendimento automatico \(wikipedia.org\)](https://it.wikipedia.org/wiki/Apprendimento_automatico)

<sup>81</sup> [Modello linguistico di grandi dimensioni \(wikipedia.org\)](https://it.wikipedia.org/wiki/Modello_linguistico_di_grandi_dimensioni)

<sup>82</sup> [Truffa del CEO \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/0/0/0/0/0/0/truffa-del-ceo)

<sup>83</sup> [Settimana 14: Riunione online con il deep fake del capo: truffa del CEO 2.0 \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/0/0/0/0/0/0/settimana-14-riunione-online-con-il-deep-fake-del-capo-truffa-del-ceo-2.0)

<sup>84</sup> [Truffa dell'investimento \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/0/0/0/0/0/0/truffa-dell-investimento)



Ad aprile 2024 varie organizzazioni svizzere del settore finanziario hanno segnalato una serie di attacchi DDoS abbinati a un tentativo di estorsione.<sup>87</sup> Questi attacchi, apparentemente rivendicati dal gruppo «Armada Collective»<sup>88</sup> o «Alpha Jackal», utilizzavano il seguente schema: l'organizzazione presa di mira riceve innanzitutto un'e-mail minatoria in cui le si dice che i suoi servizi online verranno compromessi se non pagherà un riscatto. A questa minaccia fa immediatamente seguito un breve attacco DDoS, comunque già in grado di causare un sovraccarico e un'interruzione di tali servizi. Successivamente l'aggressore continua a fare pressione sull'organizzazione affinché paghi il riscatto, minacciandola via e-mail di intensificare i suoi attacchi. In parte dei casi segnalati si è poi visto realizzarsi la minaccia, con un incremento della durata e dell'intensità degli attacchi. In alcuni di essi, gli indirizzi IP sorgente legittimi delle organizzazioni finanziarie sono stati utilizzati abusivamente per attaccare altri istituti. Nella stragrande maggioranza dei casi segnalati, tuttavia, l'impatto è stato limitato e ha potuto essere mitigato con le consuete misure implementate per contenere gli attacchi DDoS. In Svizzera l'ultima attività dell'Armada Collective – o di qualcuno che sostiene di far parte del gruppo – è stata registrata nel 2020.

Oltre a moventi di carattere finanziario, gli attacchi DDoS sono stati nuovamente utilizzati per finalità politiche<sup>89</sup> nell'ambito di grandi manifestazioni e conferenze internazionali sul territorio svizzero. A gennaio 2024 il collettivo di hacktivisti filorusi «NoName057(16)» ha preso di mira vari siti legati al World Economic Forum (WEF), mentre a giugno 2024 è stata la volta dei siti di organizzazioni connesse alla «Conferenza sulla pace in Ucraina» tenutasi al Bürgenstock. A monte di questi eventi l'UFCS aveva pubblicato un compendio delle misure raccomandate agli organizzatori con infrastrutture particolarmente esposte.<sup>90</sup> Durante questi due eventi l'UFCS ha analizzato la selezione degli obiettivi da parte degli hacktivisti e ha lavorato fianco a fianco dei gestori delle infrastrutture interessate. Nel complesso gli attacchi si sono mantenuti entro i limiti previsti e hanno compromesso solo minimamente l'infrastruttura informatica. In nessun momento i sistemi informatici e i dati di queste manifestazioni o delle organizzazioni coinvolte sono risultati in serio pericolo.<sup>91</sup> Si è trattato principalmente di attacchi DDoS al livello di applicazione del modello OSI (il cosiddetto «layer 7»)<sup>92</sup>, ossia nello specifico di un bombardamento di richieste HTTP/s GET.<sup>93</sup> La maggior parte degli indirizzi IP utilizzati appartenevano a operatori di VPN privati, di cui NoName057(16) si è servito per sferrare l'attacco DDoS.

---

<sup>87</sup> [Attacchi DDoS e estorsione: una combinazione molto attuale \(ncsc.admin.ch\)](#)

<sup>88</sup> Il gruppo Armada Collective è stato individuato con lo stesso modus operandi nel 2015 e 2016 da MELANI, un predecessore dell'UFCS. Non esistono tuttavia indizi tecnici a conferma del fatto che dietro questa attività del 2024 si nascondano ancora gli stessi attori.

<sup>89</sup> Cfr. [Rapporto semestrale 2023/2](#), cap. 3.6.1; [Rapporto semestrale 2023/1](#), cap. 2.

<sup>90</sup> [Misure per la ciber-resilienza nel contesto di grandi manifestazioni e conferenze internazionali \(ncsc.admin.ch\)](#)

<sup>91</sup> [Conferenza di alto livello sulla pace in Ucraina: primo bilancio dell'UFCS sui lavori della Rete integrata della situazione ciber \(ncsc.admin.ch\)](#)

<sup>92</sup> [Application layer DDoS attack \(cloudflare.com\)](#)

<sup>93</sup> [HTTP flood DDoS attack \(cloudflare.com\)](#)



## Raccomandazioni

Il sito dell'UFCS contiene, nella sezione [Attacchi alla disponibilità \(DDoS\) \(ncsc.admin.ch\)](https://ncsc.admin.ch), un elenco di 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 siete vittima di un attacco, trovate varie raccomandazioni su [Attacco DDoS – E adesso? \(ncsc.admin.ch\)](https://ncsc.admin.ch).

## 7 Gestione, fughe ed estorsioni di dati

I data leak e l'esposizione involontaria di dati sensibili continuano a fare notizia: a maggio 2024, ad esempio, circa 500 GB di dati biometrici e altri dati sensibili di cittadini indiani, tra cui militari e membri delle forze dell'ordine, sono diventati di pubblico dominio. Il database in questione non era configurato correttamente e non era protetto da password.<sup>94</sup> Una gestione efficace dei dati e della protezione degli accessi è dunque imprescindibile tanto per le imprese quanto per le autorità e i privati, al fine di garantire una conservazione sicura dei dati. Ne sono un esempio, in particolare, le fughe di dati, che non solo hanno conseguenze per i diretti interessati, ma rappresentano anche una potenziale arma d'attacco nei confronti di altre organizzazioni. Ma nemmeno i privati e le loro informazioni sensibili sfuggono all'attenzione dei cybercriminali. Dopo una fuga di dati le vittime sono esposte a un maggiore rischio di subire attacchi successivi, ad esempio sotto forma di sottrazioni di account, phishing (cfr. cap. 2), furto d'identità o truffe finanziarie (cfr. cap. 5). Lo scenario attuale delle cyberminacce mostra che, per quanto riguarda il fenomeno dei data leak, la maggior parte delle informazioni pubblicate abusivamente da collettivi di ransomware vengono sfruttate per estorcere dati (cfr. cap. 3.2). Parallelamente si riscontrano anche altre cause, come una carente gestione dei dati all'interno delle proprie infrastrutture o presso i fornitori. Infine, anche la presenza di vulnerabilità e di configurazioni tecniche errate può portare a un'esposizione involontaria dei dati ed essere sfruttata dai cybercriminali.

### 7.1 Fughe di dati presso i fornitori

A livello nazionale e internazionale le fughe di dati sono una problematica a cui l'opinione pubblica guarda con sempre maggiore attenzione – soprattutto quando sono coinvolte intere catene di fornitura. Uno degli incidenti più clamorosi in Svizzera è l'attacco ransomware di Play ai danni della software house Xplain AG del 2023. Tra i dati dei clienti pubblicati dai criminali ve ne erano anche alcuni dell'Amministrazione federale svizzera, provenienti tra l'altro

---

<sup>94</sup> [Data Leak Exposes 500GB of Indian Police, Military Biometric Data \(hackread.com\)](https://hackread.com)



dall'area della sicurezza interna. A inizio marzo 2024 l'UFCS ha pubblicato un rapporto in cui ha illustrato in sintesi l'elaborazione dell'evento da parte dell'Amministrazione federale, analizzato i dati pubblicati e tratto le conclusioni di tale verifica.<sup>95</sup> Dall'esercizio di classificazione è risultato che circa il 5 per cento del volume complessivo di dati pubblicati riferiti a circa 1,3 milioni di oggetti erano determinanti per l'Amministrazione federale. Nonostante la maggior parte dei dati sia di proprietà della società Xplain AG, 9040 (circa il 14 per cento) di questi oggetti erano attribuibili all'Amministrazione federale. Poco più della metà degli oggetti conteneva informazioni sensibili come dati personali e informazioni tecniche e/o classificate. La classificazione e l'analisi effettuate hanno evidenziato quanto, dopo una fuga di dati, una disamina esatta dei dati trafugati – soprattutto se non strutturati<sup>96</sup> – richieda una mole di lavoro sproporzionata. Una prima sfida è stata quella di predisporre in tempi rapidi gli strumenti adatti per l'elaborazione e l'analisi dei dati, nonché le risorse di personale in grado di svolgere la complessa consultazione e classificazione manuale dei dati. Questo iter assorbe un gran numero di risorse ed è di conseguenza costoso, soprattutto se la consultazione non può essere completamente automatizzata.

L'incidente ha fatto scaturire altre inchieste a livello federale: da un lato il Ministero pubblico della Confederazione (MPC) ha avviato due procedimenti penali in relazione al ciberattacco. Dall'altro l'Incaricato federale della protezione dei dati e per la trasparenza (IFPDT) ha avviato di sua iniziativa un'inchiesta indipendente sulla fuga di dati.<sup>97</sup> Da essa è emerso che, a causa di accordi inadeguati tra il fornitore e due uffici federali, una quantità sproporzionatamente elevata di dati personali era stata trasmessa, attraverso alcuni processi di supporto, al fornitore, presso cui era stata memorizzata. Nell'estate del 2023 il Consiglio federale ha deciso inoltre di istituire uno stato maggiore di crisi politico-strategico «Fuga di dati» e di ordinare un'inchiesta amministrativa.<sup>98</sup> Alla luce delle conclusioni tratte dall'inchiesta amministrativa<sup>99</sup> la Confederazione ha adottato una serie di misure volte a migliorare in maniera persistente e sistematica la sicurezza dei dati. La legge sulla sicurezza delle informazioni (LSIn), entrata in vigore il 1° gennaio 2024, riflette e integra il pacchetto di misure.<sup>100</sup>

Incidenti di natura analoga si osservano anche sulla scena internazionale. Una vasta campagna di attacchi mirati contro clienti della multinazionale Snowflake ha approfittato intenzionalmente del grande parco clienti della società, sfruttandone gli account non sufficientemente protetti. Il core business di Snowflake è l'approntamento di una piattaforma cloud-based<sup>101</sup> per dati strutturati e non, che consente ai clienti di salvare i dati ed elaborarli per analisi approfondite.

---

<sup>95</sup> [Attacco hacker contro Xplain: l'Ufficio federale della cibersicurezza pubblica un rapporto sull'analisi dei dati \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/press-releases/2024/03/03-01-2024-ufcs-report.html)

<sup>96</sup> [Dati non strutturati \(wikipedia.org\)](https://en.wikipedia.org/wiki/Unstructured_data)

<sup>97</sup> Un rapporto con le risultanze dell'inchiesta riguardante il trattamento dei dati da parte di Xplain AG e le relative raccomandazioni è stato pubblicato in data 1° maggio 2024, cfr. [L'IFPDT conclude le inchieste nei confronti della ditta Xplain e degli uffici federali fedpol e UDSC \(edoeb.admin.ch\)](https://www.edoeb.admin.ch/edoeb/en/press-releases/2024/05/01-01-2024-ifpdt-report.html).

<sup>98</sup> [Attacco hacker contro Xplain: il Consiglio federale istituisce uno stato maggiore di crisi politico-strategico per la fuga di dati \(admin.ch\)](https://www.admin.ch/gov/de/press-releases/2023/07/23-01-2023-crisis.html)

<sup>99</sup> Le risultanze dell'inchiesta amministrativa sono state pubblicate in data 1° maggio 2024, cfr. [Conclusione dell'inchiesta amministrativa concernente l'attacco hacker contro Xplain: il Consiglio federale decide misure \(admin.ch\)](https://www.admin.ch/gov/de/press-releases/2024/05/01-01-2024-conclusion.html)

<sup>100</sup> [Il Consiglio federale mette in vigore la legge sulla sicurezza delle informazioni \(admin.ch\)](https://www.admin.ch/gov/de/press-releases/2024/01/01-01-2024-ls-in.html).

<sup>101</sup> [Cloud computing \(wikipedia.org\)](https://en.wikipedia.org/wiki/Cloud_computing)



dite mediante tecniche di apprendimento automatico. Su questa piattaforma, inoltre, è integrato un marketplace in cui si vendono e si scambiano dati e si possono utilizzare gratuitamente dati di terzi. A fine maggio 2024 il gruppo di hacker «ShinyHunters» ha annunciato di aver esfiltrato i dati della società Ticketmaster servendosi di un malware per l'acquisizione di dati (Infostealer).<sup>102</sup> I circa 1.3 terabyte (TB) di dati riguardanti quasi 560 milioni di utenti di Ticketmaster sono stati trafugati dai criminali sulla piattaforma di Snowflake. Spinti da un movente finanziario, gli hacker hanno seguito uno schema simile a quello dei collettivi di ransomware (cfr. cap. 3.2), ma senza criptare i dati alla vittima.

L'incidente accaduto a Ticketmaster, tuttavia, non è il solo. Anche altre imprese, tra cui AT&T<sup>103</sup> e Santander<sup>104</sup>, sono cadute vittima di questa campagna di estorsione dei dati da parte dello stesso gruppo. Un'inchiesta approfondita condotta in collaborazione con la società di sicurezza informatica Mandiant ha concluso che gli accessi non autorizzati ai database erano iniziati già ad aprile 2024. Mandiant, inoltre, non ha trovato prove del fatto che le esfiltrazioni dei dati da istanze di Snowflake fossero dovute a una configurazione errata, una vulnerabilità o un'altra violazione dell'infrastruttura generale di Snowflake, ma ha riscontrato che erano avvenute a seguito di precedenti fughe di dati dei clienti ad opera di Infostealer.<sup>105</sup> La fuga di password risaliva in alcuni casi al 2020. Vista inoltre l'assenza dell'autenticazione a due fattori (2FA) sugli account degli utenti, i criminali sono riusciti a procurarsi sistematicamente l'accesso a istanze di Snowflake. La portata della campagna e anche il possibile danno potenziale si quantificano facilmente se si considera che Mandiant e Snowflake hanno dovuto informare ben 165 possibili vittime dell'esposizione delle infrastrutture di Snowflake.<sup>106</sup>



### Raccomandazioni

Salvate soltanto i dati di cui avete realmente bisogno (economia dei dati). **Cancellate rapidamente** quelli non più necessari e **archivate offline** i dati da conservare, ma non più utilizzati attivamente. Definite in maniera vincolante con fornitori e partner le condizioni e le modalità con cui possono gestire le diverse tipologie di dati. Implementate meccanismi di controllo per garantire il rispetto di questi accordi. Proteggete inoltre gli accessi a sistemi, account e dati con password forti e, se possibile, con l'**autenticazione a più fattori (MFA)**.<sup>107</sup>

## 7.2 Commercio legale e illegale di dati

I dati sono il nuovo oro nell'era della digitalizzazione. Sono un bene prezioso, che li rende interessanti per le attività commerciali sia legali che illegali. Ecco che allora i cybercriminali

<sup>102</sup> [Live Nation confirms Ticketmaster breach after hackers hawk stolen info of 560 million \(therecord.media\)](#)

<sup>103</sup> Cfr. [Toll of Snowflake Hack Widens With Theft of AT&T Text, Calling Data \(bloomberg.com\)](#), [AT&T Addresses Illegal Download of Customer Data \(att.com\)](#)

<sup>104</sup> [More than 12,000 Santander employees in US affected by Snowflake customer breach \(therecord.media\)](#)

<sup>105</sup> [Detecting and Preventing Unauthorized User Access \(snowflake.discourse.group\)](#)

<sup>106</sup> [UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion \(cloud.google.com\)](#)

<sup>107</sup> Cfr. [Proteggete i vostri account \(ncsc.admin.ch\)](#)

fanno ricorso, ad esempio, alle armi del phishing (cfr. cap. 2), a Infostealer e a piattaforme d'acquisto illegali per procurarsi i dati. La costante domanda ha fatto nascere un vero e proprio ecosistema di marketplace illeciti nel dark web e nel web sommerso<sup>108</sup>, alcuni persino nel clear web<sup>109</sup>, che consentono ai criminali scambio, suddivisione del lavoro e specializzazione.<sup>110</sup> Mentre gli uni, ad esempio, raccolgono e vendono vecchie corrispondenze via e-mail soprattutto attraverso il chain phishing (cfr. cap. 2.1) o un malware, gli altri comprano queste informazioni per sfruttarle a fini di truffa.

Un mercato attualmente in voga tra l'opinione pubblica e i media è «BreachForums». La piattaforma in lingua inglese è nata dopo che i precedenti marketplace tanto amati dagli hacker, come ad esempio «RaidForums», erano stati chiusi nel 2022 in seguito a operazioni di polizia.<sup>111</sup> A solo un anno di distanza, tuttavia, le autorità di perseguimento penale statunitensi arrestarono il fondatore, per cui anche la nuova piattaforma aveva subito chiuso i battenti.<sup>112</sup> Eppure, sotto la guida del gruppo ShinyHunters «BreachForums» è riuscita a rinascere dalle proprie ceneri e la piattaforma si è affermata come uno dei forum principali per la vendita e la condivisione gratuita di dati e credenziali d'accesso rubati. I dati scambiati spaziano da quelli di pubblico dominio a contenuti altamente sensibili: un esempio inquietante è il tentativo, nell'aprile 2024, di vendere circa 5 milioni di fototessere ad alta risoluzione – con impressi i numeri delle carte d'identità – di altrettanti cittadini di El Salvador. In aggiunta l'acquirente riceveva anche un set di dati con informazioni personali quali nome, numero della carta d'identità, data di nascita e informazioni di contatto. Si presume che circa l'80 per cento della popolazione salvadoregna sia inclusa in questo data leak.<sup>113</sup>

A maggio di quest'anno le autorità di perseguimento penale sono nuovamente intervenute contro «BreachForums». Con la partecipazione della Polizia cantonale di Zurigo, l'FBI è riuscita ad acquisire temporaneamente il dominio.<sup>114</sup> Purtroppo, dopo due sole settimane gli ex amministratori sono stati in grado di ripristinare il sito sul dark web e di recuperare persino l'accesso al sito originale sul clear web.<sup>115</sup> Pare che il registrar di domini abbia restituito agli amministratori il sito sequestrato dall'FBI sul clear web.<sup>116</sup> Le due piattaforme sono dunque tornate pienamente operative, come hanno chiaramente dimostrato i leak ai danni di Snowflake (cfr. cap. 7.1). Per quanto le autorità di perseguimento penale riescano costantemente a smembrare reti e marketplace di questo tipo e a compromettere le loro attività illecite, la domanda e le infrastrutture di backup sono così robuste che si creano sempre nuove piattaforme.

---

<sup>108</sup> [Web sommerso \(wikipedia.org\)](#), [Dark web \(wikipedia.org\)](#)

<sup>109</sup> [Surface web \(wikipedia.org\)](#)

<sup>110</sup> [Top 10 Deep Web and Dark Web Forums \(socradar.io\)](#)

<sup>111</sup> [One of the world's biggest hacker forums taken down \(europol.europa.eu\)](#)

<sup>112</sup> [Justice Department Announces Arrest of the Founder of One of the World's Largest Hacker Forums and Disruption of Forum's Operation \(justice.gov\)](#)

<sup>113</sup> [Threat Actor Claims to Have Leaked Database Containing Personal Information of 5 Million Salvadoran Citizens \(dailydarkweb.net\)](#)

<sup>114</sup> [Breachforum: FBI und Kapo Zürich gelingt Schlag gegen Hacker \(nzz.ch\)](#)

<sup>115</sup> [BreachForums returns just weeks after FBI-led takedown \(theregister.com\)](#)

<sup>116</sup> [Breach Forums Return to Clearnet and Dark Web Despite FBI Seizure \(hackread.com\)](#)



## Conclusione / raccomandazioni

I dati sono preziosi. Vi è dunque anche un interesse criminale a impadronirsene e venderli con mezzi disonesti o a ricattare le vittime con la minaccia di pubblicare dati sensibili. È importante che ognuno abbia chiaro in mente che le informazioni in rete sono – volontariamente o involontariamente – a disposizione di tutti. I malintenzionati possono sfruttarle, utilizzandole per finalità di social engineering. Di conseguenza la discussione sul tema della sicurezza dei dati dovrebbe iniziare col chiedersi se una fuga di dati possa innanzitutto verificarsi e concludersi col domandarsi quando questo accada e come gli stessi dati, nel caso estremo di una fuga, siano resi inutilizzabili per l'aggressore.

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. Definite processi chiari e fattibili per la gestione 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 compaiono in un data leak, ad esempio sul sito [Have I Been Pwned \(haveibeenpwned.com\)](https://haveibeenpwned.com) o [Identity Leak Checker des Hasso Plattner Instituts \(hpi.de\)](https://www.hpi.de/identity-leak-checker).

Il commercio dei dati, tuttavia, non avviene soltanto nell'ambiente criminale, ma anche nella legalità. Data broker<sup>117</sup> e fornitori di servizi di dati, come ad esempio Snowflake, consentono alle aziende di comprare o ricevere gratuitamente dati con semplicità. Il problema delle piattaforme legali, tuttavia, è che su di esse possono finire anche set di dati raccolti illecitamente, che i gestori devono togliere dalla circolazione.<sup>118</sup> In linea di principio il trattamento dei dati personali da parte delle aziende è illecito sotto il profilo della protezione dei dati se questi ultimi vengono raccolti e trattati per finalità di analisi, per le quali non sussiste un interesse pubblico o privato preponderante, senza l'esplicito consenso delle persone interessate.<sup>119</sup> Per le aziende, inoltre, è relativamente semplice raccogliere i dati degli utenti con il loro consenso. Lo si fa in massa, in particolare, se tale attività rientra nel core business della società, come ad esempio nel caso del settore pubblicitario. Mediante ID pubblicitari unici contenenti un identificativo dei terminali mobili univoco, le aziende possono rilevare, accorpare e analizzare il comportamento degli utenti sotto forma di dati e realizzare per gli utilizzatori finali una pubblicità personalizzata. Essendo utilizzabili in modo persistente e su più terminali (interoperabili), gli ID pubblicitari rappresentano dunque una fonte preziosa di informazioni per le aziende.<sup>120</sup> In tale contesto, anche i cookie sono parte integrante dell'analisi del comportamento degli utenti. A differenza degli ID pubblicitari, però, i cookie sono user ID anonimizzati che vengono rilevati soltanto per singolo terminale e che non consentono la creazione di un profilo utente

---

<sup>117</sup> I data broker sono aziende che raccolgono sistematicamente le informazioni in set di dati, le arricchiscono di ulteriori informazioni e le rivendono a terzi.

<sup>118</sup> Cfr. [Databroker: Belgian data marketplace publishes passport data of thousands of people \(netzpolitik.org\)](https://www.netzpolitik.org/en/databroker-belgian-data-marketplace-publishes-passport-data-of-thousands-of-people/), [European data broker: Sensitive passport data of Germans published online \(netzpolitik.org\)](https://www.netzpolitik.org/en/european-data-broker-sensitive-passport-data-of-germans-published-online/)

<sup>119</sup> Cfr. in merito artt. 30 e 31 cpv. 1 della legge sulla protezione dei dati (LPD; RS 235.1); Sandra Husi/Stämpfli/Anne-Sophie Morand/Ursula Sury, Datenschutzrecht, Zurigo 2023, pag. 150 segg., N 277 segg.

<sup>120</sup> [Werbewelt ohne Cookies: Mit neuen ID-Technologien in die Zukunft \(traffactive.com\)](https://www.traffactive.com/de/werbewelt-ohne-cookies-mit-neuen-id-technologien-in-die-zukunft)

completo. Protocollano anche lo stile di navigazione e memorizzano preferenze e caratteristiche dell'utente.<sup>121</sup> A parte i cookie, anche metodi come il fingerprinting consentono la raccolta e il riconoscimento di utenti con l'ausilio dei metadati.<sup>122</sup> Ma anche prestando il consenso alle autorizzazioni delle varie app di telefonia mobile si possono trasmettere a terzi dati personali, come le informazioni di geolocalizzazione. È quanto mostra a titolo illustrativo un'analisi di giugno 2024 a cura della SRF.<sup>123</sup> Nel corso delle ricerche SRF ha ottenuto gratuitamente un set di dati di geolocalizzazione relativi a una settimana del 2024 di 1,3 milioni di dispositivi in Svizzera, che secondo il fornitore dovevano essere anonimizzati. Probabilmente queste informazioni erano state raccolte a scopi pubblicitari attraverso gli app tracker e i site tracker di varie aziende. Diversamente da quanto promesso dal fornitore, invece, dopo breve tempo la SRF è riuscita ad abbinare i dati a persone specifiche, compromettendo per sempre la loro privacy.



### Raccomandazioni

Nell'utilizzo quotidiano del vostro dispositivo mobile badate a cliccare soltanto sulle **autorizzazioni** che volete realmente dare nelle app da voi utilizzate. Nei banner dei **cookie** di siti e applicazioni non accettate automaticamente tutti i cookie. Con qualche ulteriore clic potete **rifiutare** i cookie che vanno oltre la normale funzionalità, evitando così che i vostri dati vengano memorizzati e rivenduti contro la vostra volontà. La [guida della SRF](#)<sup>124</sup> vi spiega come implementare questi punti e altri passaggi.

## 8 Ciberspionaggio e sabotaggio

Oltre che da attori non statali, il panorama delle cyberminacce è popolato anche da criminali statali. In genere sono definiti «Advanced Persistent Threat» (APT)<sup>125</sup>, dal momento che, considerate le loro risorse tecniche, finanziarie, di tempo e di personale, possono rappresentare una minaccia persistente e avanzata. Un APT si contraddistingue per il fatto che sviluppa le sue tecniche indipendentemente dai costi, al fine di mettere a segno attacchi concepiti su misura in funzione delle sue vittime. Non appena scovati ed eliminati da una rete, gli APTs cercano nuovamente di rientrarvi. Nonostante gli APTs agiscono soprattutto in ambito governativo, per raggiungere i loro obiettivi, interagiscono anche con attori non statali. Gli interessi sono tra i più disparati. Mentre alcuni hanno un movente finanziario, la maggior parte si è specializzata in ciberspionaggio, sabotaggio o in entrambi. Il capitolo tratta alcuni temi e sviluppi rilevanti in ambito internazionale, indispensabili per comprendere meglio la posizione della Svizzera nello spazio digitale.

---

<sup>121</sup> [DSGVO vs. ePrivacy: Datenschutz, einfach erklärt \(traffactive.com\)](#)

<sup>122</sup> [Browser fingerprinting explained \(+7 top techniques\) \(fingerprint.com\)](#)

<sup>123</sup> [Tracking mit Ortungsdiensten – Der Spion in unseren Handys \(srf.ch\)](#)

<sup>124</sup> [Anleitung gegen Tracking – So schützen Sie Ihr Handy vor Tracking \(srf.ch\)](#)

<sup>125</sup> [APT \(csrc.nist.gov\)](#)

## 8.1 Ciberspionaggio

### 8.1.1 Istituzioni politiche sotto pressione

A inizio anno il WEF ha definito il 2024 l'anno record delle elezioni, essendovene oltre 50 in programma in altrettanti Paesi del mondo.<sup>126</sup> L'esperienza dimostra che questi eventi politici cruciali offrono molteplici opportunità per minacce di diversa natura. Mentre i criminali hanno come movente l'arricchimento personale, gli hacktivisti vedono una possibilità di attirare attenzione verso la loro causa. Diverso è l'intento degli attori statali, che strumentalizzano le elezioni per raccogliere informazioni o per operazioni di lobby.<sup>127</sup> In linea con queste aspettative, le elezioni che si sono svolte nel periodo in esame sono state caratterizzate da un numero di ciberattacchi superiore alla norma. Sotto stretta osservazione sono state in particolare le elezioni europee. Dietro i casi più eclatanti di cui hanno riferito i media vi era spesso la mano degli hacktivisti, che hanno colpito sia con minacce che con veri e propri attacchi. Durante le prime fasi delle elezioni europee, ad esempio, si è parlato di attacchi DDoS ai danni di siti di partiti olandesi, rivendicati dal gruppo filorusso «Hacknet».<sup>128</sup> L'effettivo impatto diretto di queste attività pare essere contenuto, visto che con gli attacchi DDoS si riescono a causare solo restrizioni temporanee (cfr. cap. 6). Ciò nonostante il gruppo di hacktivisti ha raggiunto il suo obiettivo principale di attirare l'attenzione e ottenere visibilità.

Il contesto delle elezioni e dei parlamenti è esposto anche al ciberspionaggio. In vista di questo anno record per le elezioni e della grande rilevanza di un processo elettorale indipendente, a marzo l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) aveva provveduto ad aggiornare il suo compendio sulla sicurezza delle elezioni.<sup>129</sup> Ciò nonostante, una settimana prima delle elezioni europee il partito tedesco della CDU è stato vittima di un ciberattacco. Pur essendo stato confermato dal Ministero degli Interni tedesco, non sono stati pubblicati molti dettagli sull'incidente.<sup>130</sup> Ciò che si sa è che gli aggressori hanno avuto accesso ai sistemi informatici attraverso una vulnerabilità.<sup>131</sup> Si è inoltre lasciato intendere che l'attacco era stato ad opera di una mano molto abile.<sup>132</sup>

A differenza degli episodi di hacktivism durante le elezioni europee, i ciberattacchi – potenzialmente più gravi – sono maggiormente complessi da individuare e difficilmente hanno implicazioni geopolitiche. La Svizzera e le sue istituzioni politiche non fanno eccezione, come hanno evidenziato gli attacchi ai danni di 122 parlamentari svizzeri e di altri Paesi europei nel maggio del 2024.<sup>133</sup> Gli attacchi di spear phishing contro i parlamentari svizzeri facevano parte di una campagna più vasta rivolta contro vari membri dell'Alleanza Interparlamentare sulla

---

<sup>126</sup> [Why 2024 is a record year for elections around the world \(weforum.org\)](https://www.weforum.org)

<sup>127</sup> Cfr. per una panoramica generale: [Poll Vaulting: Cyber Threats to Global Elections \(cloud.google.com\)](https://cloud.google.com)

<sup>128</sup> [Dutch political websites hit by cyber attacks as EU voting starts \(cloudflare.com\)](https://cloudflare.com)

<sup>129</sup> [Safeguarding EU elections amidst cybersecurity challenges \(enisa.europa.eu\)](https://enisa.europa.eu)

<sup>130</sup> [CDU: Cyber-Angriff auf Parteizentrale – Verfassungsschutz eingeschaltet \(spiegel.de\)](https://spiegel.de)

<sup>131</sup> [Hackerangriff auf CDU: Software wird auch in Mitteldeutschland genutzt \(mdr.de\)](https://mdr.de)

<sup>132</sup> [Germany's Christian Democratic party hit by 'serious' cyberattack \(reuters.com\)](https://reuters.com)

<sup>133</sup> [Schweizer Parlamentarier von chinesischen Staatshackern attackiert \(watson.ch\)](https://watson.ch)

Cina (IPAC). Le autorità statunitensi e britanniche hanno pubblicamente puntato il dito contro il collettivo «APT31», controllato dallo stato cinese.<sup>134</sup>

## 8.1.2 Sviluppi internazionali nel ciberspionaggio

### ISoon – un dataleak molto istruttivo

Nel febbraio 2024 più di 500 documenti – molto probabilmente autentici – della società cinese ISoon sono stati resi pubblici sulla piattaforma di sviluppo collaborativo GitHub. Contenevano liste di bersagli d'attacco, descrizioni degli strumenti, ma anche conversazioni tra i dipendenti. I documenti, ritenuti legittimi da molti esperti, fanno luce sulle attività del fornitore di servizi, che opera nei settori della sorveglianza e dei ciberattacchi e pare che lavori anche per il Ministero della Pubblica Sicurezza, la Sicurezza di Stato e l'esercito cinese.<sup>135</sup>

Questi documenti evidenziano il ruolo cruciale dell'outsourcing nelle operazioni informatiche della Cina e il modo in cui funziona questo ecosistema. Il ricorso a fornitori di servizi esterni implica una serie di rischi per il mandatario, che può perdere il controllo su parti della catena di attacco (cfr. cap. 7.1). Il vantaggio di questa prassi, tuttavia, è che lo Stato può negare il suo coinvolgimento nel caso in cui un'operazione venga smascherata.

### Il boom delle reti ORB

A gennaio 2024 le autorità statunitensi hanno annunciato di aver messo fuori uso una rete d'attacco costituita da router compromessi.<sup>136</sup> Questa rete sarebbe stata utilizzata dal gruppo «Volt Typhoon»<sup>137</sup>, che le autorità statunitensi collegano allo Stato cinese. Gli USA accusano il collettivo di aver preso di mira varie infrastrutture critiche nazionali e di altri Paesi. Per paralizzare la rete, le autorità statunitensi necessitavano di un accesso remoto ai router compromessi, con cui distruggere il malware dall'interno e impedire ulteriori comunicazioni con l'infrastruttura d'attacco.

L'utilizzo delle reti con router o altri dispositivi di rete compromessi, nominata rete ORB (Operational Relay Boxes), è una tecnica nota. Ciò che è nuovo sono le dimensioni e la maggiore frequenza di utilizzo, soprattutto da parte di attori statali cinesi. Tuttavia, gli APTs cinesi, non sono gli unici ad utilizzare queste reti: anche l'«APT28» – noto altresì come «Sofacy», affiliato al servizio di intelligence militare russo (GRU) – ha fatto uso, di reti operate da criminali, per una serie di operazioni informatiche.<sup>138</sup> L'utilizzo di reti ORB offre molteplici vantaggi all'aggressore: ad esempio la possibilità di camuffare la propria identità complicando il rilevamento di un attacco. Se necessario, l'aggressore ha anche la possibilità di ripiegare velocemente su una nuova infrastruttura.

Questa evoluzione dimostra che la tendenza diffusa tra i cibercriminali di dividersi il lavoro sta influenzando anche le tecniche utilizzate dagli attori statali. Ad esempio, operatori di servizi

---

<sup>134</sup> [Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians \(justice.gov\)](#); [UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity \(gov.uk\)](#)

<sup>135</sup> [iSoon leak sheds light on China's use of extensive hacker-for-hire ecosystem \(huntandhackett.com\)](#)

<sup>136</sup> [U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure \(justice.gov\)](#)

<sup>137</sup> Cfr. [Rapporto semestrale 2023/02](#); cap. 3.5.

<sup>138</sup> [Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks \(trendmicro.com\)](#)



criminali, mettono a disposizione di attori statali reti per operazioni informatiche. Questo mostra quanto siano diventati sottili, i confini tra attori statali e privati nel ciberspazio.



### **Conclusione / raccomandazioni**

Al giorno d'oggi non sono solo i veri e propri dispositivi di rete, come i router, a essere connessi e costantemente online, ma anche altri apparecchi collegati ad internet presenti nelle nostre case come telecamere, televisori e dispositivi di archiviazione. Molto spesso questi dispositivi sono mal protetti o per niente protetti e rappresentano pertanto un bersaglio d'attacco. Possono essere utilizzati, all'insaputa del proprietario, per attività illecite, ad esempio nel contesto delle reti ORB. Anch'essi devono dunque essere protetti in maniera adeguata ed essere aggiornati nel momento in cui vengono rese note delle vulnerabilità. L'UFCS pubblica varie raccomandazioni al fine di garantire la sicurezza di questi dispositivi, cfr. [Ciberdritta: le precauzioni da prendere con l'Internet delle cose \(ncsc.admin.ch\)](#).

### **Dispositivi edge presi di mira dalla campagna Coathanger**

L'NCSC olandese nel mese di giugno 2024 ha riscontrato una tendenza di attacchi mirati a dispositivi edge come firewall, server VPN, router ed e-mail relay server. Trovandosi nella parte esposta della rete, spesso questi dispositivi sono collegati direttamente a Internet. I rischi associati a dispositivi edge come firewall o router sono emersi con particolare evidenza nell'ambito della campagna «Coathanger». Secondo l'NCSC olandese, un attore di spionaggio sponsorizzato dallo Stato cinese ha sfruttato sistematicamente una vulnerabilità presente in FortiGate firewall, ottenendo nel 2022 e nel 2023 l'accesso ad almeno 20 000 dispositivi in tutto il mondo. Prima che la vulnerabilità fosse pubblicata, l'attore l'ha sfruttata come zero-day<sup>139</sup> per due mesi. Oltre al Ministero della Difesa olandese, diversi altri governi occidentali e istituzioni diplomatiche sono finiti nel mirino della campagna. Se un obiettivo era ritenuto interessante, l'attore di spionaggio installava un malware per ottenere l'accesso permanente ai sistemi. Tale accesso ha persino continuato a essere possibile dopo che FortiGate ha scoperto la vulnerabilità ed effettuato un aggiornamento.<sup>140</sup>

### **Attività connesse ad APT29**

«APT29» è un gruppo di hacker con un ampio ventaglio di possibilità d'attacco, da tempo utilizzate per finalità di ciberspionaggio. Le autorità di vari Paesi ritengono che APT29 operi per conto del servizio segreto russo SVR.<sup>141</sup> Come è tipico degli APTs, il collettivo mette co-

---

<sup>139</sup> [0-day \(wikipedia.org\)](#)

<sup>140</sup> [Ongoing state-sponsored cyber espionage campaign via vulnerable edge devices \(ncsc.nl\)](#)

<sup>141</sup> Cfr. [Rapporto semestrale 2021/2](#); cap. 4.7.3.



stantemente a punto le sue tecniche d'attacco, come mostra un rapporto dei Paesi appartenenti all'alleanza Five Eyes<sup>142</sup>.<sup>143</sup> Anziché concentrarsi soprattutto sulle vulnerabilità del software nelle reti locali, ad esempio, APT29 ha colpito direttamente le infrastrutture cloud per ottenere l'accesso ai sistemi desiderati. Nell'ultimo semestre in esame il gruppo è stato particolarmente attivo, attaccando in particolare società operanti nel campo dell'informatica, come HPE<sup>144</sup>, Microsoft<sup>145</sup> e, ultimamente, Teamviewer<sup>146</sup>. APT29 si è distinto inoltre nell'ambito dello spionaggio politico, prendendo di mira organizzazioni diplomatiche e governi di tutto il mondo, nonché partiti politici. A giugno 2024 l'Agenzia Nazionale Francese per la Sicurezza dei Sistemi Informativi (ANSSI) ha annunciato<sup>147</sup> che, con la campagna «diplomatic orbiter», APT29 aveva compromesso vari account e-mail legittimi di organizzazioni diplomatiche utilizzando lo spear phishing. A inizio 2024, inoltre, hanno colpito anche alcuni partiti politici tedeschi.<sup>148</sup>

## 8.2 Minaccia a sistemi di controllo industriali e tecnologie operative

La digitalizzazione avanza non solo nel campo dei dati e delle informazioni; anche i processi fisici e il loro controllo vengono costantemente digitalizzati e spesso collegati in rete insieme ai rispettivi sistemi informatici. I lunghi cicli di vita di questi sistemi rendono spesso difficile un'integrazione sicura e duratura nel panorama delle tecnologie dell'informazione e della comunicazione (TIC). Basta una disattenzione nell'adattare i sistemi di controllo industriale per generare involontariamente nuovi rischi per la sicurezza. Poiché la manipolazione di un processo cyber-fisico può avere un impatto sugli impianti meccanici e persino rappresentare una minaccia per la vita e l'integrità delle persone, è necessaria particolare cautela.

Nella maggioranza dei casi, gli attacchi e i tentativi di sabotaggio con intento distruttivo o di disturbo si osservano unicamente nell'ambito di conflitti già in fase di escalation. A parte qualche strascico collaterale la Svizzera è stata pertanto risparmiata da questi attacchi, nonostante gli hacktivisti affermino il contrario. Questi ultimi sostengono regolarmente di aver manipolato sistemi di controllo industriale (ICS) esposti alla rete Internet.<sup>149</sup> Tra questi elenchi figuravano anche sistemi di organizzazioni svizzere, ma non se ne conoscono le conseguenze.

Nell'ambito dei conflitti in corso in Ucraina e a Gaza<sup>150</sup>, invece, sono stati sicuramente compiuti attacchi di natura sabotatoria. Oltre a quelli distruttivi ai danni di vari provider Internet in Ucraina<sup>151</sup>, a marzo mentre imperversavano gli attacchi missilistici, è stato impedito con mezzi

---

<sup>142</sup> Five Eyes è un'alleanza di sicurezza relativa all'attività di intelligence dei seguenti cinque Paesi: Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda. Per maggiori informazioni, cfr. [Five Eyes \(wikipedia.org\)](https://en.wikipedia.org/wiki/Five_Eyes) o [Five Eyes Intelligence Oversight and Review Council \(FIORC\) \(dni.gov\)](https://www.dni.gov/fiorc/).

<sup>143</sup> [SVR cyber actors adapt tactics for initial cloud access \(ncsc.gov.uk\)](https://www.ncsc.gov.uk/stories/svr-cyber-actors-adapt-tactics-for-initial-cloud-access)

<sup>144</sup> [Hewlett Packard Enterprise tells SEC it was breached by Russia's 'Cozy Bear' hackers \(therecord.media\)](https://www.therecord.media/news/hewlett-packard-enterprise-tells-sec-it-was-breached-by-russia-s-cozy-bear-hackers)

<sup>145</sup> [Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard \(msrc.microsoft.com\)](https://msrc.microsoft.com/update-details/2024/Microsoft-Actions-Following-Attack-by-Nation-State-Actor-Midnight-Blizzard)

<sup>146</sup> [Teamviewer \(teamviewer.com\)](https://www.teamviewer.com)

<sup>147</sup> [Malicious activities linked to the Nobelium intrusion set \(cert.ssi.gouv.fr\)](https://cert.ssi.gouv.fr/fr/actualites/activites-malicieuses-liees-a-l-intrusion-nobelium)

<sup>148</sup> [APT29 Uses WINELOADER to Target German Political Parties \(cloud.google.com\)](https://cloud.google.com/blog/topics/industry-trends/ap29-uses-wine-loader-to-target-german-political-parties)

<sup>149</sup> [Dark Web Profile: Hunt3r Kill3rs \(socradar.io\)](https://www.socradar.io/dark-web-profile-hunt3r-kill3rs)

<sup>150</sup> [Bad Karma, No Justice: Void Manticore Destructive Activities in Israel \(research.checkpoint.com\)](https://research.checkpoint.com/bad-karma-no-justice-void-manticore-destructive-activities-in-israel)

<sup>151</sup> [Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs \(cyberscoop.com\)](https://www.cyberscoop.com/russian-military-intelligence-wiper-ukrainian-isps/)

ciber anche a varie società di distribuzione energetica di fornire i loro servizi.<sup>152</sup> Per sferrare questi attacchi vengono costantemente sviluppati nuovi strumenti. Nel corso delle campagne di sabotaggio descritte, ad esempio, si è scoperto il nuovo malware wiper distruttivo «Acid-Pour»<sup>153</sup>. Una variante della backdoor «Kapeka»<sup>154</sup> ha consentito l'interruzione dell'approvvigionamento energetico ucraino. Le autorità ucraine hanno attribuito la paternità di questi sabotaggi all'APT «Sandworm»<sup>155</sup>, che si ritiene essere affiliato al servizio di intelligence militare russo GRU.

Anche la Russia è stata vittima di diversi atti di sabotaggio informatico. A Mosca, ad esempio, è stata attaccata la rete di sensori industriali Moscollector. Il gruppo «Blackjack» ha utilizzato il malware «Fuxnet»<sup>156</sup> per disabilitare i dispositivi d'accesso alla rete per i sensori legati a numeri d'emergenza, aeroporti o alla distribuzione di gas.

Rimane il rischio che le ripercussioni di queste azioni di sabotaggio – soprattutto da parte di presunti hacktivisti affiliati all'una o all'altra parte in conflitto – abbiano un impatto anche al di fuori delle operazioni di combattimento. Oltre ai danni collaterali, infatti, non è escluso che vengano prese di mira anche infrastrutture europee, se i cybercriminali considerano un Paese affiliato al nemico. Le autorità norvegesi<sup>157</sup> e ceche<sup>158</sup>, ad esempio, hanno già messo in guardia da un aumento del rischio di sabotaggi in Europa. Un altro indizio sono le allerte diramate dai produttori<sup>159</sup> di sistemi di controllo industriali per mettere in guardia dalle minacce soprattutto nei confronti dei dispositivi esposti alla rete Internet<sup>160</sup>. Effetti simili al sabotaggio sono generati anche da attacchi ransomware ai danni dei sistemi industriali, motivo per cui la protezione contro queste forme di attacco merita la massima attenzione



## Conclusione / 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.

Per respingere eventuali tentativi di attacco da parte di hacktivisti nel quadro dei conflitti in corso, vari partner internazionali hanno pubblicato una [scheda informativa](#) congiunta.

---

<sup>152</sup> [Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes \(therecord.media\)](#)

<sup>153</sup> [AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine \(sentinelone.com\)](#)

<sup>154</sup> [Kapeka: A novel backdoor spotted in Eastern Europe \(labs.withsecure.com\)](#)

<sup>155</sup> [APT44: Unearthing Ssandworm \(services.google.com\)](#)

<sup>156</sup> [Unpacking the Blackjack Group's Fuxnet Malware \(claroty.com\)](#)

<sup>157</sup> [Alarm over Russian-directed sabotage operations growing across Europe \(therecord.media\)](#)

<sup>158</sup> [Russia is trying to sabotage European railways, Czech minister said \(securityaffairs.com\)](#)

<sup>159</sup> [Security Advisory \(rockwellautomation.com\)](#)

<sup>160</sup> [It appears that the number of industrial devices accessible from the internet has risen by 30 thousand over the past three years \(isc.sans.edu\)](#)