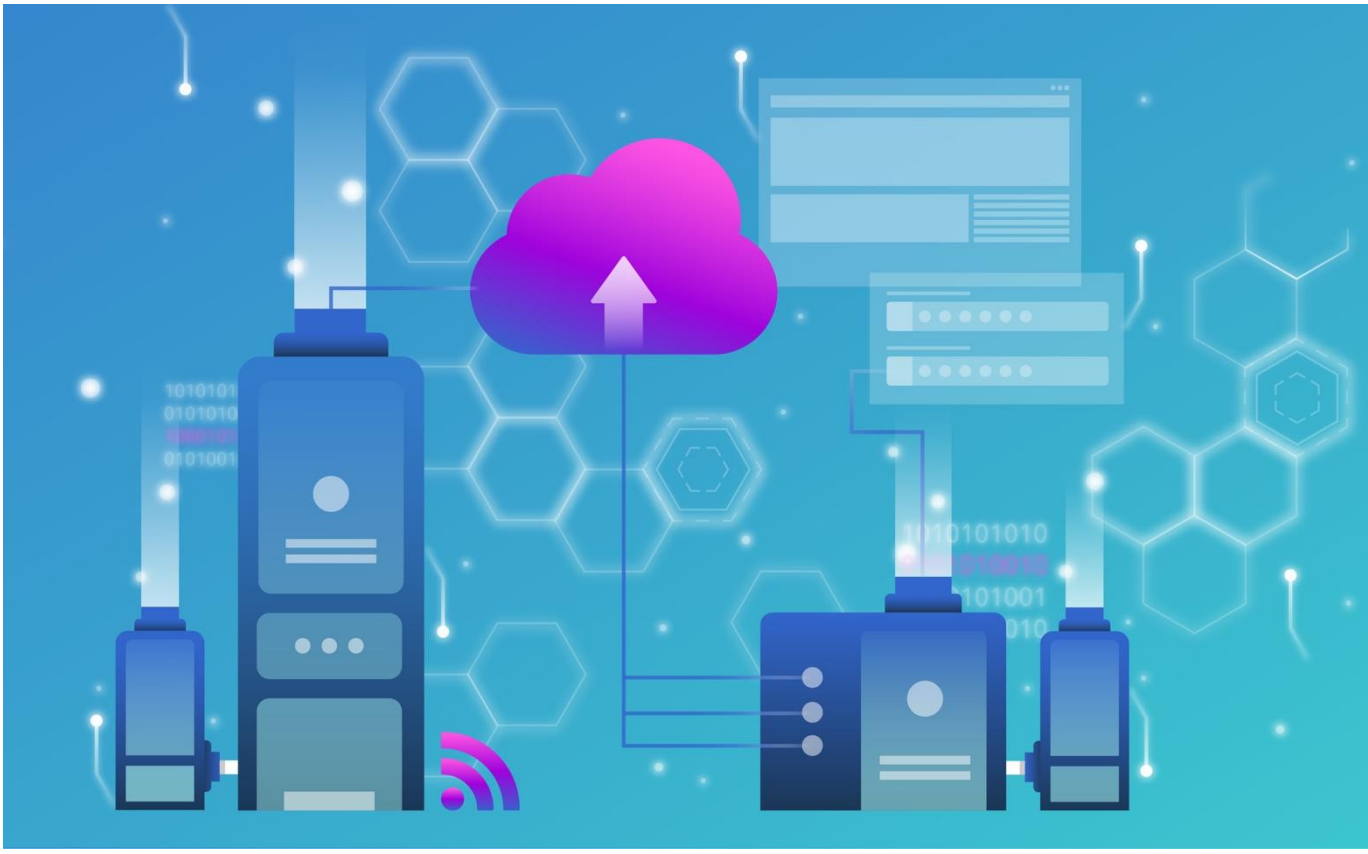
5 maggio 2022 | Centro nazionale per la cibersicurezza NCSC



Rapporto semestrale 2021/II (luglio – dicembre)

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

1 Panoramica / Contenuto

1 Panoramica / Contenuto 2

Management Summary 4

2 Editoriale 5

3 Tema principale: attacchi alla catena di approvvigionamento 7

3.1 Che cos'è un attacco alla catena di approvvigionamento? 7

3.2 Attacchi ransomware alla catena di approvvigionamento del software VSA di Kaseya 8

3.3 Incidenti in Svizzera 8

3.4 Proposte e misure 9

3.5 Vulnerabilità nei componenti software 10

4 Eventi / situazione 10

4.1 Riepilogo dei ciberincidenti segnalati 10

4.1.1 Il tipo di incidente più segnalato: la truffa 11

4.1.2 Segnalazioni di phishing 12

4.1.3 Segnalazioni di software dannosi (malware) 13

4.1.4 Segnalazioni di vulnerabilità 13

4.2 Software dannosi (malware) 13

4.2.1 Situazione generale 13

4.2.2 Ransomware 17

4.2.3 Qakbot 19

4.3 Attacchi a siti e servizi web 21

4.3.1 DDoS 21

4.3.2 Attacchi a sistemi VoIP 22

4.4 Sistemi di controllo industriali (ICS) e technologia operativa (OT) 22

4.4.1 In Iran un ciberattacco ha limitato l'approvvigionamento di carburante 22

4.4.2 Gestori esclusi dai sistemi di controllo degli impianti automatizzati degli edifici 23

4.4.3 Tentativi di ricognizione e danni collaterali minacciano la tecnologia operativa (OT) 24

4.5 Vulnerabilità 26

4.5.1 Atlassian Confluence – CVE-2021-26084 – remote code execution 26

4.5.2 Azure – OMIGOD – privilege escalation, remote code execution 26

4.5.3 Log4j – CVE-2021-44228 – Log4Shell 27

4.5.4 Blacksmith – CVE-2021-42114 28

4.6 Fughe di dati 28

4.6.1 Credenziali della VPN di Fortinet 28
4.6.2 EasyGov 29
4.7 Spionaggio 30
4.7.1 Pegasus 30
4.7.2 Furto di dati tramite l'API di Slack 30
4.7.3 Nobelium 31
4.7.4 Nickel / K3chang 31
4.8 Ingegneria sociale e phishing 31
4.8.1 Panoramica sul phishing 31
4.8.2 Smishing 34
4.8.3 SIM swapping 34
4.8.4 Finte chiamate di assistenza per i servizi di e-banking tramite gli annunci su Google 35
5 Fenomeni di ingegneria sociale combinati 36
5.1 Aumentano gli attacchi mirati, scendono quelli di massa 36
5.2 Quando gli annunci si trasformano in tentativi di phishing 37
5.3 Perché comprare casa se ci attende un'eredità 37
5.4 Gli investimenti soppiantano i prestiti 37

Management Summary

Questo rapporto semestrale dell'NCSC prende in esame i ciberincidenti più importanti che si sono verificati in Svizzera e all'estero nella seconda metà del 2021, ponendo in particolare l'accento sugli attacchi alle catene di approvvigionamento dei prodotti IT.

Oggigiorno nella produzione di beni e servizi sono coinvolti diversi fornitori e offerenti terzi. Gli attacchi ai singoli fornitori o offerenti possono avere pesanti ripercussioni su tutta la catena di approvvigionamento (ad es. blocco della produzione), come il noto caso dell'azienda produttrice di software Kaseya, avvenuto a metà del 2021. Anche in Svizzera un attacco DDoS ai danni di un provider di hosting ha provocato disservizi temporanei sui vari siti web della città e del Cantone di San Gallo.

Casi di truffa sempre più frequenti

Nel semestre in esame l'NCSC ha ricevuto in totale 11 480 segnalazioni di ciberincidenti, molte delle quali riguardanti diversi tipi di truffa. Nella maggior parte dei casi si è trattato di e-mail inviate a nome di autorità di perseguimento penale. Sono state riportate anche truffe dell'anticipo, truffe dell'investimento, truffe del CEO e truffe relative ad annunci. Gli hacker agiscono in modo sempre più mirato e complesso. Prima di passare all'azione dedicano diverso tempo alla vittima al fine di guadagnarne la fiducia.

Ransomware e fuga di dati

Anche nel secondo semestre del 2021 vi sono stati numerosi attacchi ransomware, con cui gli aggressori criptano i dati e in seguito chiedono un riscatto. Sempre più spesso gli hacker ricorrono alla doppia estorsione e copiano i dati prima di criptarli, in modo da avere un margine di manovra maggiore ed esercitare più pressione. Se la vittima non è disposta a pagare il riscatto, minacciano di diffondere pubblicamente i dati.

Vulnerabilità nei componenti software

Spesso i software sono sviluppati utilizzando componenti già esistenti come librerie o codici open source. In questi componenti possono però essere presenti delle vulnerabilità che, quando vengono individuate, devono essere corrette in tutti i prodotti che contengono il componente in questione. Questo problema è emerso a dicembre 2021 con la vulnerabilità critica nella popolare libreria Java Log4j.

Il phishing resta di tendenza

Dall'inizio della pandemia l'NCSC ha ricevuto numerose segnalazioni di attacchi di phishing lanciati tramite messaggi (e-mail o sms) che comunicavano l'imminente arrivo di un pacco o problemi di consegna. Sono stati registrati anche tentativi di phishing ai danni di webmail e Microsoft 365 (già Office 365). I dati di accesso ottenuti in questo modo vengono spesso utilizzati per falsificare fatture. Tra gli stratagemmi più diffusi vi sono anche le e-mail in cui sedicenti provider di servizi Internet tentano di raggirare la vittima facendole credere che una fattura è stata pagata due volte.

2 Editoriale

Nessun uomo è un’isola

Nella sua opera «Devotions Upon Emergent Occasions» pubblicata nel 1624, lo scrittore inglese John Donne ha coniato la frase «Nessun uomo è un’isola», con la quale intendeva che ognuno di noi è parte di un tutto e condivide il proprio destino con gli altri.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid SA

Il contesto economico attuale è caratterizzato da una continua specializzazione, dalla conseguente riduzione dell’integrazione verticale, volta a incrementare l’efficienza e a ridurre i costi, e dunque da un allontanamento dal modello di economia di scala. Di conseguenza, la catena di creazione del valore delle imprese dipende sempre di più da fornitori di beni e servizi e partner, anche se la pandemia da coronavirus ci ha mostrato chiaramente i limiti e i rischi di una tale ripartizione globale del lavoro.

Soprattutto quando si tratta di attacchi informatici alle imprese, tutte le parti coinvolte nella catena di approvvigionamento condividono lo stesso destino: un attacco informatico a un fornitore può avere ripercussioni sul suo acquirente e di riflesso sul destinatario della prestazione. Lo scorso febbraio, ad esempio, Toyota ha dovuto chiudere temporaneamente le sue fabbriche in Giappone a causa di un attacco informatico di cui è stato vittima un fornitore. La metafora «Nessun uomo è un’isola» si può applicare anche alle organizzazioni.

Ad acuire ulteriormente il problema è il fatto che gli aggressori hanno iniziato a prendere di mira direttamente le catene di approvvigionamento. Quando ad esempio forniscono prodotti di offerenti di dispositivi di rete tramite delle backdoor per attaccare in seguito i clienti con questi sistemi di accesso secondari (come è successo recentemente all’impresa texana SolarWinds), ottengono un effetto domino.

Non proteggere se stessi, teoricamente, significa mettere in pericolo anche gli altri.
Ai miei interlocutori faccio sempre notare che molte imprese si occupano solo in minima parte della gestione dei rischi della catena di approvvigionamento.

Se consideriamo il grado di interconnessione e interdipendenza, ci rendiamo conto che stiamo correndo uno dei maggiori ciber-rischi sistemici possibili nella nostra società moderna!

Occorre dunque chiedersi perché questa tematica non goda di molta attenzione. Una spiegazione plausibile potrebbe essere che esternalizzando le prestazioni i dirigenti delle imprese provino anche a cedere le relative responsabilità. Ma questo ci porta ad un punto cieco, poiché, se posso delegare la responsabilità della fornitura delle prestazioni («responsibility»), l'obbligo di rendiconto («accountability») nei confronti dei miei gruppi interessati spetta comunque a me. E come posso ottemperare a quest'obbligo nei confronti dei miei stakeholder se, esternalizzando le prestazioni, non controllo i rischi legati alla mia catena di approvvigionamento?

A mio parere, la gestione dei rischi della catena di approvvigionamento deve essere parte integrante della gestione operativa di ogni impresa.

Una gestione sistematica dei rischi della catena di approvvigionamento si basa sull'identificazione e sulla comprensione degli stessi. In questo caso, un'analisi dei processi centrali può contribuire a identificare delle dipendenze critiche da terzi. Anche le metodologie di «threat modeling» come STRIDE possono aiutare a individuare le minacce e le vulnerabilità nelle transizioni tra sistemi.

Deve essere data grande importanza anche alla realizzazione di un'organizzazione resiliente. Se riesco a mantenere i miei processi centrali con mezzi alternativi ad esempio in caso di evento critico (gestione della continuità operativa o «business continuity management»), o prendo provvedimenti per limitare le ripercussioni di un attacco e ripristinare velocemente gli strumenti TIC e OT dopo un incidente («incident response» e «disaster recovery»), allora fornisco anche un contributo diretto al rafforzamento della resilienza dell'intera catena di approvvigionamento, nella quale la mia impresa gioca un ruolo.

Nelle imprese tali provvedimenti devono essere regolarmente sottoposti a verifica e testati con il personale per assicurare la loro efficacia in caso di emergenza.

Anche la definizione di standard e certificazioni da applicare a prodotti e prestazioni a livello settoriale può contribuire. Perché funzioni, le imprese di un determinato settore devono unirsi per imporre il rispetto di standard e norme anche ai loro fornitori.

Per contrastare efficacemente l'azione di questi attori sempre più organizzati, ogni impresa deve proteggersi in modo adeguato dai ciber-rischi presenti nella propria catena di approvvigionamento.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid SA

3 Tema principale: attacchi alla catena di approvvigionamento

3.1 Che cos'è un attacco alla catena di approvvigionamento?

Molte aziende collaborano con diversi partner (fornitori, prestatori terzi) che procurano loro prodotti di vario tipo, come materie prime, prestazioni di servizi o tecnologie, che le aziende utilizzano per realizzare i propri prodotti finali oppure inseriscono nella propria offerta o nei propri servizi. L'attività di molte imprese dipende quindi da prestazioni esterne. Questa catena di fornitura o di approvvigionamento, detta anche «supply chain», in un contesto più ampio comprende l'intera produzione di valore aggiunto. Ogni anello di questa catena è integrato nel processo generale e può essere potenzialmente sfruttato dagli hacker come vettore per penetrare i sistemi dell'azienda (attacco *tramite* la catena di approvvigionamento). Questa catena, però, può essere interrotta anche da elementi di disturbo specifici (attacco *alla* catena di approvvigionamento). Per mettersi al riparo dai ciberattacchi, tutta la catena, e con essa anche i fornitori di servizi coinvolti, deve essere adeguatamente protetta, funzionare in modo affidabile e, se possibile, ne deve essere garantita la continuità attraverso ridondanze.

Un attacco tramite la catena di approvvigionamento è il risultato di due aggressioni: la prima è rivolta a un singolo fornitore allo scopo di accedere ai suoi sistemi e al suo rapporto privilegiato con la clientela per sferrare l'attacco all'obiettivo vero e proprio. Nei casi più semplici gli hacker raggiungono il loro obiettivo sfruttando sistemi di accesso da remoto o collegamenti di rete non adeguatamente protetti, ma anche connessioni consolidate per il trasferimento dati. Nei casi più complessi, invece, gli hacker attaccano le aziende già durante la fase di sviluppo del software inserendo al suo interno un codice che in seguito raggiunge i dispositivi dei clienti attraverso i regolari aggiornamenti.[1] Sono plausibili anche casi in cui software o hardware vengono attaccati già durante il processo di produzione. In questi casi il prodotto viene venduto già con una vulnerabilità, una backdoor o un software dannoso preinstallato. Gli attacchi tramite la catena di approvvigionamento possono avere un obiettivo importante ben preciso[2], essere diretti contro un numero ristretto di destinatari[3], o essere pensati per colpire su larga scala e in un secondo tempo permettere agli autori di scegliere obiettivi specifici.[4] Tramite la catena di approvvigionamento, inoltre, possono essere sferrati anche attacchi contro un numero presumibilmente alto di potenziali vittime, ad esempio sfruttando un attacco riuscito a un fornitore di servizi IT per diffondere ransomware.[5]

Quando si verificano attacchi *alla* catena di approvvigionamento volti a compromettere l'attività di determinati clienti finali, spesso non è facile risalire all'autore. Nel 2016 gli attacchi DDoS ai

---

1 V. Rapporto semestrale 2020/2 (ncsc.admin.ch), n. 4.7.2 su Solarwinds.

2 V. Rapporto semestrale 2010/2 (ncsc.admin.ch), n. 4.1 su Stuxnet, il verme informatico con il quale è stato sabotato in modo mirato l'arricchimento dell'uranio in Iran.

3 V. Rapporto semestrale 2017/1 (ncsc.admin.ch), n. 3 su NotPetya, il malware diffuso attraverso il software per le dichiarazioni fiscali in Ucraina.

4 V. Rapporto semestrale 2020/2 (ncsc.admin.ch), n. 4.7.2 sull'attacco a Solarwinds e Rapporto semestrale 2017/1 (ncsc.admin.ch), n. 5.1.1 sull'operazione «CloudHopper».

5 V. n. 3.3 e n. 4.2.2.

danni di Dyn, un servizio di DNS («domain name system»), hanno impedito a un elevato numero di persone di accedere a varie piattaforme (tra cui Twitter, Spotify e Soundcloud) che utilizzavano i suoi servizi.[6] Solitamente le imprese che fanno parte di una catena di approvvigionamento stipulano con i loro clienti dei contratti per la fornitura di beni e servizi. Recentemente numerosi attacchi ransomware sono stati diretti proprio contro queste aziende, che si sono trovate nella scomoda situazione di dover trovare un modo per riprendere a fornire i propri servizi o a produrre i propri beni al più presto per rispettare gli obblighi contrattuali verso i loro clienti. Gli hacker adottano questa strategia sperando che date le condizioni le vittime siano più facilmente disposte a pagare un riscatto.

3.2 Attacchi ransomware alla catena di approvvigionamento del software VSA di Kaseya

Kaseya Limited è un produttore di software specializzato in strumenti per il controllo e la gestione di sistemi da remoto. La sua offerta comprende il software VSA («virtual system/server administrator»), che può essere scaricato e utilizzato sul server cloud di proprietà dell'azienda. I fornitori di servizi gestiti («managed service provider», MSP) possono utilizzare VSA localmente oppure sui server cloud dedicati di Kaseya che in seguito offrono a loro volta i propri servizi IT ad altri clienti. Quando viene rilasciato un aggiornamento del software, Kaseya può inviare gli update da remoto a tutti i server VSA.
A metà 2021 alcuni hacker hanno sfruttato una vulnerabilità zero-day presente nei sistemi di Kaseya (CVE-2021-30116)[7], per eseguire da remoto codici malevoli sulle applicazioni VSA dei clienti di Kaseya. Il 2 luglio 2021 i clienti di Kaseya hanno ricevuto un aggiornamento per il software VSA contenente un codice malevolo che installava un ransomware sui dispositivi dei clienti gestiti da VSA.[8]
A seguito di quanto accaduto le autorità americane hanno diffuso delle direttive per gli MSP e i loro clienti colpiti da attacchi ransomware contro la catena di approvvigionamento del software VSA di Kaseya.[9]

3.3 Incidenti in Svizzera

All'inizio di settembre 2021 diverse PMI sono state colpite dal ransomware BlackMatter con il quale gli hacker sono riusciti a compromettere un provider di servizi IT austriaco e ad attaccare i suoi clienti.[10] Un attacco DDoS ai danni di un fornitore di hosting, che ospitava anche il sito web del Cantone di San Gallo[11], ha provocato disservizi temporanei su vari siti web. (cfr. n. 4.3.1).

---

6 V. Rapporto semestrale 2016/2 (ncsc.admin.ch), n. 3.2, 4.4.1 e 4.6.
7 CVE - CVE-2021-30116 (mitre.org)
8 REvil ransomware hits 1,000+ companies in MSP supply-chain attack (bleepingcomputer.com); v. n. 4.2.2.
9 CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack (cisa.gov)
10 Hackerangriff auf 34 Firmen (orf.at)
11 Website des Kantons wieder online (sg.ch)

3.4 Proposte e misure

Sul piano politico, alla fine del 2021 nel rapporto[12] del Consiglio federale in adempimento dei postulati Dobler 19.3135[13] e 19.3136[14] è stato affrontato il tema della gestione dei rischi nelle catene di approvvigionamento («supply chain risk management», SCRM) e sono stati presentati i regolamenti nazionali e gli standard internazionali applicabili. Inoltre sono state esaminate le basi legali per l'applicazione di standard per le infrastrutture critiche.

Il rapporto prende in esame anche le richieste formulate nel documento interlocutorio «Supply Chain Security»[15] di un gruppo di lavoro della Commissione per la cibersicurezza di ICTSwitzerland, al quale partecipa anche l'istituzione di centri di controllo per i componenti hardware e software in Svizzera. La Confederazione sostiene iniziative private con competenze specifiche in questo ambito.[16]

Conclusione / raccomandazioni:

Di fronte alla progressiva digitalizzazione di tutti i settori aziendali, prevedere una verifica periodica dell'evoluzione del profilo di rischio nei contratti con i propri fornitori di servizi è una delle sfide più urgenti per gli organi dirigenti delle aziende.

Per le piccole organizzazioni che non dispongono di personale interno specializzato, l'unico modo per proteggersi da questi rischi è stipulare contratti con associazioni o consulenti esterni specializzati, riservandosi anche il diritto di sottoporre il fornitore stesso del servizio a verifiche indipendenti. Tutto questo, però, comporta inevitabilmente un aumento dei costi, che vale la pena sostenere soltanto in presenza di un rischio maggiore per l'organizzazione.

L'NCSC del Regno Unito (NCSC-UK) sul proprio sito web ha pubblicato una guida[17] e un questionario[18] che possono essere utili durante il processo di definizione delle priorità e selezione dei fornitori.

Anche l'autorità americana per la cibersicurezza (CISA) fornisce molte informazioni[19] sui rischi connessi alla catena di approvvigionamento.

Inoltre, sul sito dell'NCSC sono disponibili alcune raccomandazioni per la collaborazione con i fornitori di servizi informatici (ncsc.admin.ch).

12 Sicurezza dei prodotti e supply chain risk management nei settori della cibersicurezza e della ciberdifesa (parlament.ch)
13 Abbiamo sotto controllo la cibersicurezza nel settore degli acquisti dell'esercito? (parlament.ch)
14 Infrastrutture critiche. Abbiamo il controllo sui componenti hardware e software? (parlament.ch)
15 White_Paper_Supply_Chain_Security_2019_09_25_DE.pdf (digitalswitzerland.com)
16 V. Rapporto semestrale 2020/2 (ncsc.admin.ch), n. 4.5.2.
17 Supply chain security guidance (ncsc.gov.uk)
18 Supplier assurance questions (ncsc.gov.uk)
19 Supply Chain (cisa.gov)

3.5 Vulnerabilità nei componenti software

La maggior parte dei software non è scritta partendo da zero, ma spesso viene sviluppata integrando librerie di codice già esistenti o codici open source. Può però capitare che insieme a questi componenti vengano inavvertitamente integrate e diffuse anche vulnerabilità già presenti, che quando poi vengono individuate devono essere corrette in tutti i prodotti che contengono la componente in questione. Questo problema è venuto alla luce nel 2014, quando in tutto il mondo si scoprì la falla Heartbleed.[20]

A dicembre 2021 nella popolare libreria Java Log4j è stata rilevata una vulnerabilità[21] classificata mondialmente come critica. Log4j è un framework di programmazione utilizzato per il logging e oggi rappresenta un componente essenziale per lo sviluppo dei software, per questo si trova all'interno di molti software commerciali e open source.[22] La falla di sicurezza permette di eseguire da remoto qualsiasi codice («remote code execution», RCE) e al momento della sua scoperta era già stato ampiamente sfruttato dai cibercriminali di tutto il mondo. Per maggiori informazioni al riguardo si veda il numero 4.5.3.

4 Eventi / situazione

4.1 Riepilogo dei ciberincidenti segnalati

Nel 2021 l'NCSC ha ricevuto quasi il doppio delle segnalazioni rispetto all'anno precedente (10 833), arrivando a ben 21 714 notifiche. Tra i motivi di questa forte crescita potrebbero esserci l'introduzione, alla fine del 2020, della versione rinnovata e semplificata del modulo di segnalazione e il suo posizionamento in primo piano sulla pagina iniziale del sito. A questo aumento, però, ha contribuito anche una notevole crescita di singoli fenomeni.

Molte segnalazioni hanno riguardato tentativi di attacco sventati e attacchi falliti. A queste cifre sono poi da aggiungere un numero non trascurabile di tentativi di attacco, perlopiù non riusciti, che non sono stati segnalati all'NCSC perché in Svizzera non esiste un obbligo generale di segnalazione.

---

20 V. Rapporto semestrale 2014/1 (ncsc.admin.ch), n. 4.1.

21 Log4j – Apache Log4j Security Vulnerabilities (apache.org)

22 New zero-day exploit for Log4j Java library is an enterprise nightmare (bleepingcomputer.com)

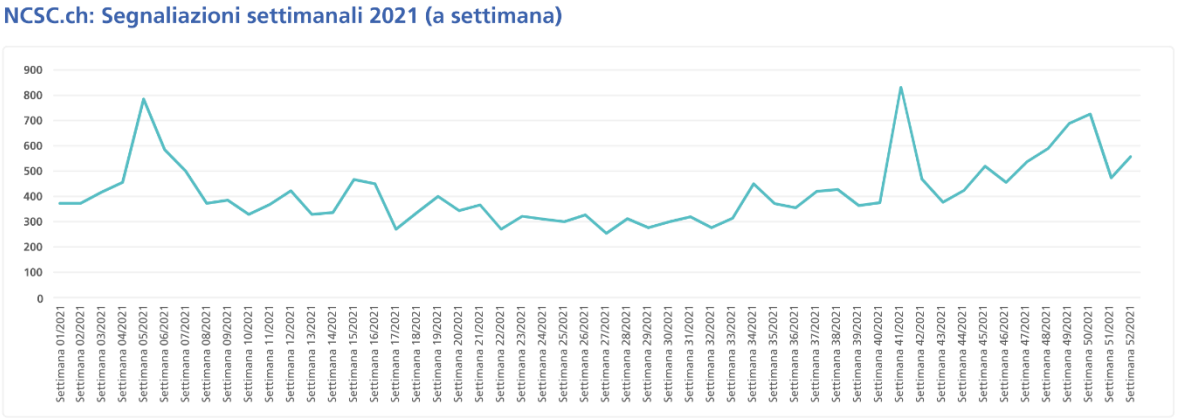


Fig. 1: Segnalazioni settimanali all'NCSC tra gennaio e dicembre 2021, vedasi anche Numeri attuali (ncsc.admin.ch).

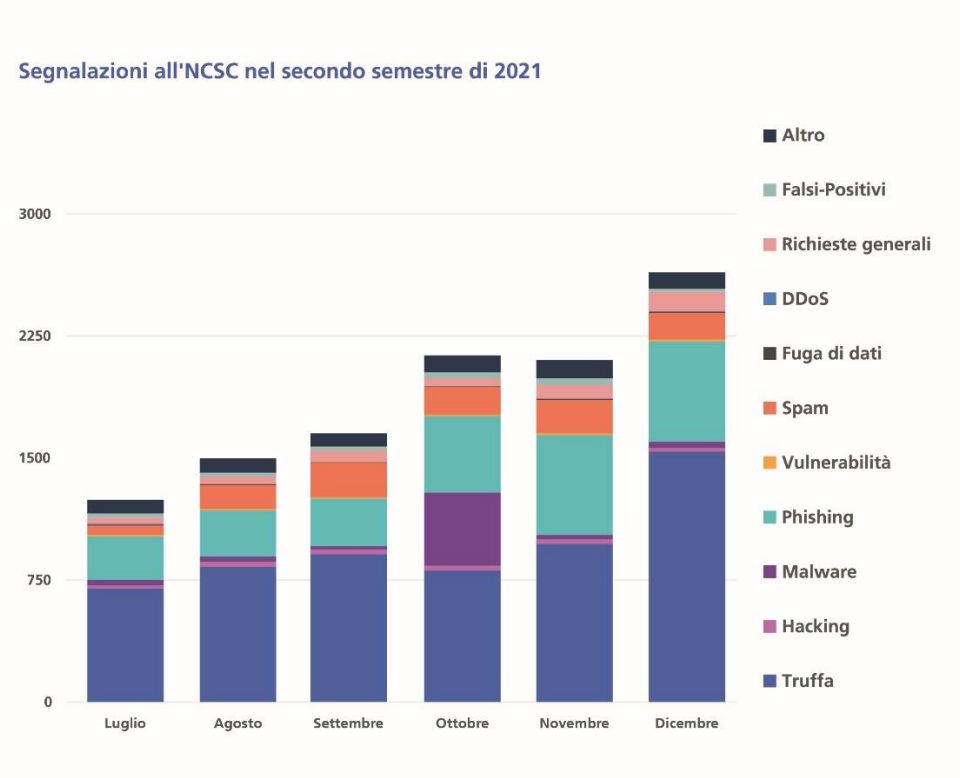


Fig. 2: Segnalazioni all'NCSC nel secondo semestre del 2021 per categorie, vedasi anche Numeri attuali (ncsc.admin.ch).

4.1.1 Il tipo di incidente più segnalato: la truffa

Così come l'anno precedente, anche nel 2021 la maggior parte delle segnalazioni inviate all'NCSC ha riguardato tentativi di truffa (oltre 11 300). Mentre nel primo semestre si è registrata una predominanza di casi di fake sextortion[23] e ne sono state registrate numerose ondate, nel secondo semestre le segnalazioni relative a questo fenomeno sono sostanzialmente diminuite. Da ottobre sono invece aumentate le segnalazioni di e-mail minatorie, nelle quali gli

[23] Fake sextortion (ncsc.admin.ch)

autori si fingono autorità di perseguimento penale e chiedono alla vittima di pagare una multa o una cauzione.[24] Tra novembre e dicembre 2021 questo fenomeno, già diffuso da tempo in Francia e connesso a quello della fake sextortion, è stato oggetto della maggior parte delle segnalazioni e ha portato a un notevole aumento delle notifiche totali. Altri tipi di truffe segnalate di frequente nel 2021 sono stati la truffa dell'anticipo (2704), la truffa dell'investimento (397), la truffa del CEO (394) e le truffe relative ad annunci (820). Per quanto riguarda queste ultime, stando alle segnalazioni, nella maggior parte dei casi al venditore veniva richiesto di anticipare delle somme per un presunto trasporto.[25]

Per quanto riguarda le truffe dell'investimento, oltre alle varianti classiche[26] sono state segnalate anche le cosiddette «campagne give-away». I malintenzionati chiedono di versare un importo a un determinato indirizzo wallet di una criptovaluta promettendo il raddoppio della somma in un secondo tempo. Una volta giunta sul sito web, inoltre, la vittima viene messa sotto pressione attraverso un timer che indica il tempo mancante allo scadere dell'offerta e la somma di denaro ancora disponibile.

4.1.2 Segnalazioni di phishing

Anche nel 2021 sono state registrate numerose segnalazioni di phishing. Nella maggior parte dei casi si è trattato di e-mail fraudolente in cui sedicenti corrieri annunciavano l'arrivo di un pacco o inviate a nome dell'Amministrazione federale delle dogane per chiedere il pagamento di somme di denaro. Sono circolate diverse versioni di queste e-mail. In alcuni casi alle vittime veniva chiesto di acquistare una PaySafeCard e di inviarne il codice ai malviventi, in altri nell'e-mail era presente un link verso una pagina con un abbonamento trappola. Nella maggior parte dei casi però le e-mail portavano le vittime su un sito di phishing, dove veniva chiesto loro di fornire i dati della propria carta di credito.

Tra le strategie di phishing più diffuse vi sono i presunti pagamenti doppi delle fatture dei provider di servizi Internet. In questi casi, però, i malviventi non sempre prestano attenzione ai dati che inseriscono nelle loro comunicazioni. In alcuni casi la data indicata come termine ultimo per una risposta, che quindi avrebbe dovuto mettere la vittima sotto pressione, era di quasi sei mesi precedente alla data di ricezione.

Sono stati registrati anche tentativi di phishing ai danni di webmail e Microsoft 365 (già Office 365). Queste credenziali spesso vengono utilizzate per le cosiddette «truffe BEC» («business email compromise»). In questi casi i truffatori fanno riferimento a uno scambio di e-mail esistente che contiene un ordine di pagamento o una fattura, ma modificano l'IBAN del conto sul quale deve essere effettuato il versamento. Dal momento che i malviventi hanno accesso all'account di posta del mittente o di uno dei destinatari, hanno accesso anche alle comunicazioni aziendali interne e quelle con i clienti, nelle quali possono trovare anche informazioni riservate da utilizzare per truffare e ricattare la vittima in altri modi.

---

[24] La settimana 37 in retrospettiva (ncsc.admin.ch)

[25] V. anche n. 5.2.

[26] V. Truffa dell'investimento (ncsc.admin.ch) e Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 4.8.

4.1.3 Segnalazioni di software dannosi (malware)

Quasi la metà delle segnalazioni relative a software dannosi ha riguardato il malware FluBot.[27] Questo a causa di un'ondata nelle settimane 41 e 42 durante la quale alle vittime veniva inviato un SMS che le invitava a installare sul proprio smartphone un'app Android malevola che conteneva FluBot. Nella settimana 41 questa ondata ha fatto registrare il maggior numero di segnalazioni su base settimanale.

Anche le segnalazioni relative ai ransomware sono sensibilmente aumentate. Rispetto all'anno precedente, nel quale le segnalazioni di questo tipo erano 67, nel 2021 le segnalazioni sono state 161. All'inizio dell'anno, ad esempio, all'NCSC sono stati segnalati 44 casi riguardantiil ransomware Qlocker[28] ai danni dei sistemi di archiviazione di rete (NAS), utilizzati soprattutto da privati.

Circolano ancora e continuano a essere segnalati anche tentativi di attacco con il malware Retefe. Le e-mail sono spesso accompagnate da una telefonata da SwissExpress Service (o da un'altra azienda con un nome simile) che chiede alla vittima di convalidare i documenti di spedizione. Nel corso della telefonata l'operatore comunica che i documenti sono stati inviati via e-mail. La vittima controlla la posta e nel messaggio o nel documento PDF allegato trova un link che porta a un software dannoso, solitamente un trojan bancario.

4.1.4 Segnalazioni di vulnerabilità

Per quanto riguarda le vulnerabilità, oltre a Log4j[29] lo scorso anno sono state segnalate lacune relative soprattutto ai server Exchange.[30] Queste falle vengono sfruttate ad esempio per diffondere malware. I malintenzionati fanno circolare vecchi scambi di e-mail sottratti in precedenza al destinatario e a cui hanno aggiunto un link verso un malware. In questo modo la potenziale vittima, riconoscendo l'e-mail, viene indotta ad aprire il documento allegato. I documenti Office, però, contengono una macro malevola con le istruzioni per modificare le impostazioni e farla eseguire sul computer. Il modo migliore per proteggersi da questi attacchi è non eseguire le macro anche quando richiesto esplicitamente e si è messi sotto pressione.

4.2 Software dannosi (malware)

4.2.1 Situazione generale

Nel secondo semestre del 2021 i media hanno dimostrato un particolare interesse verso i ransomware, nonostante questi rappresentino solo una piccola parte degli attacchi malware. L'interesse è stato dettato dal fatto che molti di questi attacchi in Svizzera e all'estero hanno avuto conseguenze gravi per le vittime (v. n. 4.2.2). Per poter fare ricorso ai ransomware gli hacker

---

27 Cfr. Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 4.2.1 e n. 4.2.1.
28 Cfr. Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 4.1.3.
29 V. n. 4.5.3.
30 V. Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.1.1.

hanno bisogno innanzitutto di un accesso al sistema target, che ottengono principalmente attraverso altri malware progettati per diffondersi e annidarsi nei sistemi. Uno di questi malware è Qakbot (v. n. 4.2.3). Il malware Emotet, prima molto diffuso, all'inizio 2021 ha subito un duro colpo quando un'operazione di polizia internazionale ne ha smantellato l'infrastruttura.[31] Ciononostante, alla fine del 2021 Emotet è ricomparso.[32] La rinascita è stata possibile grazie a TrickBot, un malware già individuato in passato insieme a Emotet. Se in precedenza Emotet installava TrickBot, adesso Emotet utilizza TrickBot per ricostruire la sua infrastruttura. Queste interazioni sono riconducibili principalmente allo sviluppo del modello «Malware-as-a-Service»[33], con il quale gli sviluppatori di malware o gli operatori di botnet noleggiano la propria infrastruttura ad altri criminali. Così facendo ogni attore può specializzarsi in determinate prestazioni parziali e offrirle sul mercato nero.

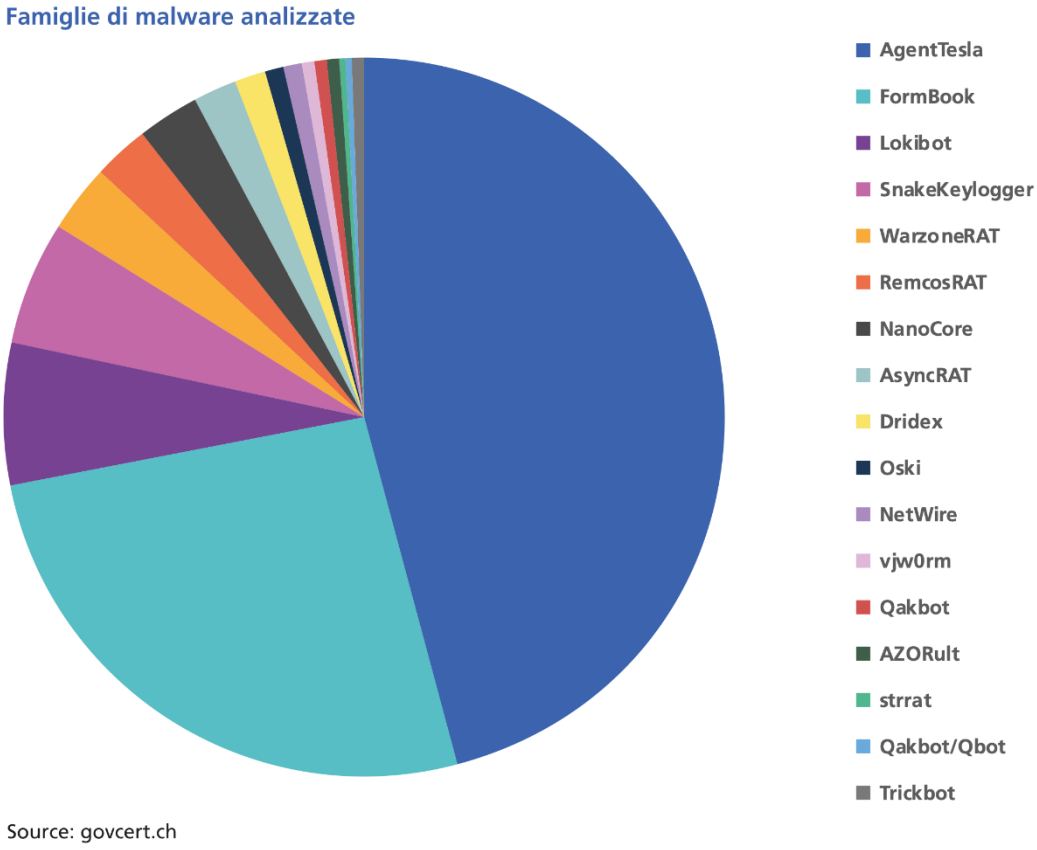


Fig. 3: Analisi dell'NCSC sulle famiglie di malware in Svizzera nel secondo semestre del 2021.

31 World's most dangerous malware EMOTET disrupted through global action (europa.eu); Rapporto semestrale 2020/2 (ncsc.admin.ch), n. 4.3.2.

32 Emotet malware is back and rebuilding its botnet via TrickBot (bleepingcomputer.com)

33 Malware-as-a-service is the growing threat every security team must confront today (securitymagazine.com); Malware-as-a-service (MaaS) (kaspersky.com); Malware Has Evolved: Defining Malware-as-a-Service (zerofox.com)

Il grafico seguente mostra le famiglie di malware identificate in Svizzera nella seconda metà del 2021 attraverso analisi di dati provenienti da server DNS sinkhole. Questi ultimi permettono di difendersi dai software dannosi perché impediscono l'accesso dei malware ai domini target e reindirizzano questi domini verso un'organizzazione di sicurezza. In questo modo è anche possibile identificare i dispositivi infettati, perché questi non si collegheranno più ai server dei gestori dei malware ma a quelli dell'organizzazione di sicurezza. L'NCSC riceve da diversi partner internazionali dati di questo tipo per tutti gli indirizzi IP svizzeri e informa i proprietari dei dispositivi infetti attraverso i loro provider.

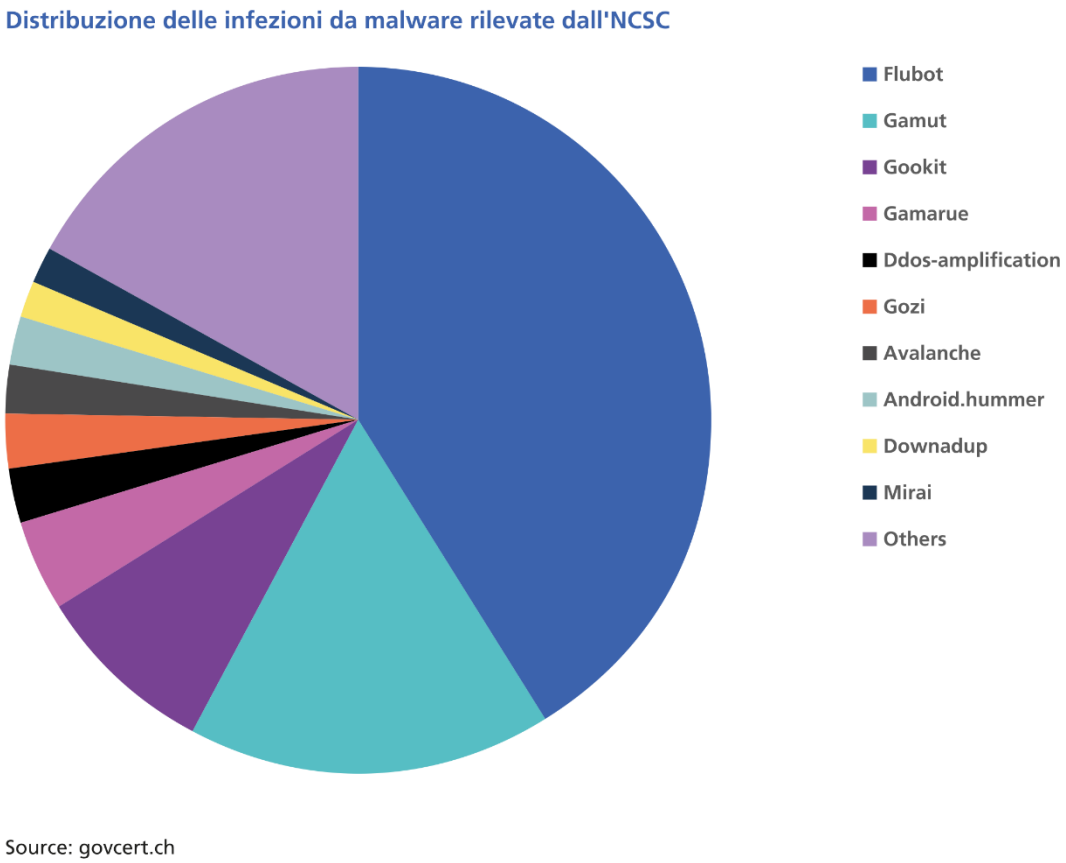


Fig. 4: Ripartizione delle infezioni da malware in Svizzera rilevate dall'NCSC nel secondo semestre del 2021.

Nel secondo semestre del 2021, così come nella prima metà dell'anno, la famiglia di malware più diffusa è stata FluBot. Per diffondere questo malware i criminali inviano un SMS sui dispositivi Android con un link a un presunto messaggio vocale. Il link porta a una pagina dove all'utente viene chiesto di scaricare un'app che sarebbe necessaria per ascoltare il messaggio vocale.

In realtà la vittima installa sul proprio dispositivo FluBot. Il malware permette quindi agli hacker di rubare i dati presenti sul dispositivo e di accedere ad applicazioni protette da un'autenticazione a due fattori, se il secondo fattore viene inviato per SMS. FluBot consente inoltre di spiare le attività sui siti di e-banking della vittima.[34]

Conclusione / raccomandazioni:

- Installate sullo smartphone solo applicazioni presenti sugli store ufficiali.
- Evitate in particolare le app a cui si accede tramite un link ricevuto via SMS o via un altro servizio di messaggistica (WhatsApp, Telegram, ecc.).
- Nel caso in cui abbiate installato un'app di questo tipo, non effettuate operazioni bancarie o acquisti online e non inserite password sul dispositivo finché il dispositivo non è stato controllato da un esperto.
- L'unico modo per eliminare definitivamente il malware dal dispositivo infettato è ripristinare le impostazioni di fabbrica.

Al secondo posto si trova lo spambot Gamut. I dispositivi infettati con Gamut vengono inseriti in una botnet e utilizzati per inviare mail di spam, che di solito riguardano incontri intimi, prodotti farmaceutici o opportunità di lavoro.[35]

Al terzo posto si posiziona invece l'infostealer Gootkit, un malware progettato per rubare dati bancari. Per raggiungere le vittime, oltre a campagne di spam, vengono utilizzate pagine Internet compromesse che inducono i visitatori a scaricare il malware.[36]

34 FluBot (Malware Family) (fraunhofer.de); La settimana 41 in retrospettiva (ncsc.admin.ch)

35 ENISA Threat Landscape 2020 - Spam (enisa.europa.eu)

36 GootKit (Malware Family) (fraunhofer.de); «Gootloader» expands its payload delivery options (sophos.com); Gootkit: the cautious Trojan (securelist.com)

4.2.2 Ransomware

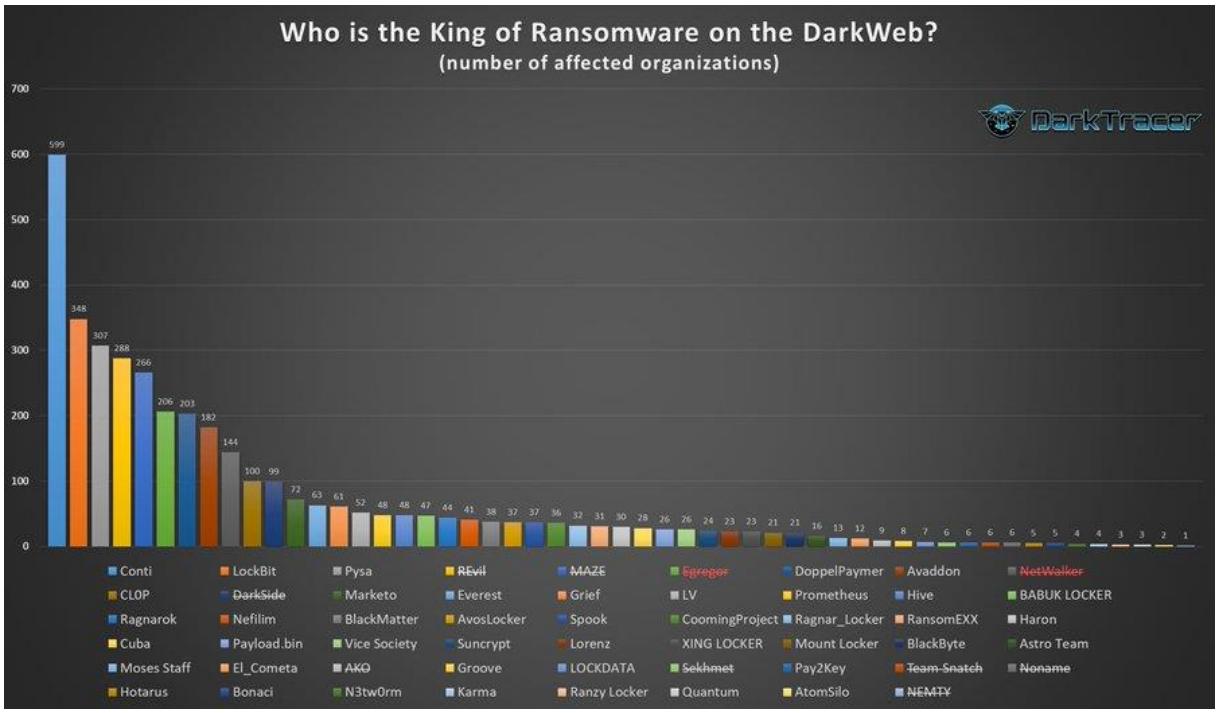


Fig. 5 : Numero di vittime dei vari ransomware in tutto il mondo secondo Data Leak Sites. I gruppi barrati non erano più attivi al momento dell'elaborazinoe del grafico. (fonte: darktracer.com).

Anche nella seconda metà del 2021 le infezioni da ransomware sono state tra gli incidenti con gli effetti potenzialmente più gravi per le imprese svizzere.

Durante il periodo in esame l'NCSC ha raccolto segnalazioni su oltre 20 diversi tipi di ransomware attivi in Svizzera. Tra i più attivi vi sono stati i già noti REvil (alias Sodinokibi), LockBit 2.0, Conti e ech0raix, mentre tra i nuovi arrivi si sono fatti notare Blackmatter e Grief, il successore di Doppelpaymer.

Nonostante le segnalazioni di attacchi ransomware pervenute all'NCSC siano leggermente diminuite rispetto al semestre precedente (91 vs. 70), in Svizzera anche nella seconda metà del 2021 gli attacchi a privati e PMI attive in diversi settori economici sono stati molto numerosi. Inoltre sono state colpite anche varie infrastrutture critiche, tra cui diversi Comuni[37], ma anche una banca[38] e una clinica privata.[39] Altri incidenti che sono stati oggetto di grande attenzione in tutta la Svizzera hanno coinvolto la cineteca nazionale[40], la società MCH Fiera Svizzera[41], il noto portale svizzero di confronto tra le offerte Comparis.ch[42] e Matisa, l'azienda leader nella

37 Montreux a été victime d'une cyber-attaque (watson.ch)
38 Hacker-Angriff hält Aquila in Bann (finews.ch)
39 20210823_MM_Pallas_Kliniken_Cyberattacke.pdf (pallas-kliniken.ch)
40 Cinémathèque suisse: Cyberattaque à la Cinémathèque suisse (cinematheque.ch)
41 Cyber-Angriff: Informationen und Empfehlungen an unsere Kunden und Partner (mch-group.com)
42 Ransomware attackers demand $400,000 from Swiss website (swissinfo.ch)

produzione di macchinari per la manutenzione delle tratte ferroviarie.[43] Anche le filiali in Svizzera di alcune imprese con sede all'estero hanno subito danni a seguito di attacchi ransomware. Tutte le società nazionali di MediaMarktSaturn, ad esempio, sono state colpite dall'attacco ransomware Hive scagliato contro la casa madre Ceconomy.[44]

Come illustrato anche in rapporti semestrali precedenti, diversi autori di attacchi ransomware hanno iniziato ad adottare una tattica di estorsione multipla.[45] Una volta ottenuto l'accesso ai sistemi della vittima, i criminali copiano il maggior numero possibile di dati prima di criptarli. Quindi, se la vittima rifiuta di pagare il riscatto, gli hacker minacciano di rendere pubblici i dati. Anche nel semestre in esame nel dark web sono state vendute o pubblicate informazioni sensibili rubate a imprese e cittadini svizzeri nel corso di attacchi ransomware, fra cui dati fiscali sottratti ad alcune fiduciarie con il ransomware Lockbit 2.0[46], i dati degli abitanti del comune di Rolle trafugati dal gruppo Vice Society[47], o ancora i passaporti di alcuni viaggiatori svizzeri rubati all'agenzia di viaggi tedesca FTI attraverso il ransomware Conti.[48]

I fornitori di servizi IT sono bersagli particolarmente interessanti per i cibercriminali che dispongono di buone competenze tecniche, perché intrufolandosi nella loro rete possono poi spostarsi all'interno dei sistemi dei loro clienti. Gli attacchi sferrati tramite REvil contro la società Kaseya e quelli con BlackMatter contro un provider di servizi IT austriaco già menzionato ai numeri 3.2 e 3.3 lo mostrano bene.

A seguito dell'attacco al sistema di oleodotti Colonial Pipeline[49] le autorità di tutto il mondo hanno intensificato la pressione sui gestori di ransomware e, di conseguenza, anche le azioni penali. In autunno le autorità di perseguimento penale europee e americane sono riuscite attraverso diverse azioni ad arrestare alcuni responsabili di attacchi di ransomware.[50]

Conclusione / raccomandazioni:

I ransomware possono causare ingenti danni, soprattutto se colpiscono anche i sistemi di backup. Sul sito web dell'NCSC vengono descritti gli aspetti principali da non dimenticare in caso di attacco: Sono vittima di un attacco ransomware. E adesso? (ncsc.admin.ch).

43 Matisa: les hackers Grief ayant piraté Comparis volent le géant du rail (watson.ch)
44 Cyberangriff auf Media-Markt-Mutter Ceconomy (inside-it.ch)
45 V. Rapporto semestrale 2020/2 (ncsc.admin.ch), n. 4.3.1; Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 4.3.2.
46 48 heures pour payer la rançon de 200'000 francs en bitcoins (24heures.ch)
47 Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance (ictjourna.ch)
48 Hacker stehlen Daten eines Touristikriesen, darunter Reisepässe von Schweizern (inside-it.ch)
49 V. Rapporto semestrale 2021/1 (ncsc.admin.ch), n. 4.2.3.
50 Five affiliates to Sodinokibi/REvil unplugged (europol.europa.eu); Ransomware gang arrested in Ukraine with Europol's support (europol.europa.eu); Arrest in Romania of a ransomware affiliate scavenging for sensitive data (europol.europa.eu); Joint global ransomware operation sees arrests and criminal network dismantled (interpol.int); Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (justice.gov)

In generale l'NCSC raccomanda di non pagare mai il riscatto. Cedere significa confermare l'efficacia del modello di business dei criminali, sostenerli finanziariamente e incoraggiarli a continuare e a sviluppare le loro attività. Inoltre, nella peggiore delle ipotesi, si perdono sia i dati che il denaro. L'NCSC consiglia di sporgere denuncia presso le autorità di polizia competenti.

Al numero 4.2.3 dell'ultima edizione del rapporto semestrale vengono fatte alcune considerazione sulla possibilità di stipulare assicurazioni contro i ciberincidenti.

La CISA, inoltre, ha pubblicato un documento destinato alle aziende nel quale fornisce consigli su come evitare, ed eventualmente reagire, in caso di fughe di dati provocate da attacchi ransomware.[51] Un altro importante contributo a livello internazionale è stato fornito dal CERT neozelandese, che ha elaborato un diagramma in cui illustra il ciclo di vita di un ransomware e i controlli da attuare per bloccare l'attacco.[52]

4.2.3 Qakbot

Scoperto nel 2007, Qakbot (noto anche come Pinkslipbot, Quakbot o Qbot) era un trojan che serviva principalmente a rubare dati bancari e altre informazioni finanziarie delle vittime. Da allora il malware è stato ulteriormente sviluppato ed integrato con svariati moduli aggiuntivi. Oggi può diffondersi nelle reti dei sistemi infettati, raccogliere ed estrapolare dati (in particolare contenuti di e-mail da utilizzare in campagne successive) o installare sul dispositivo infettato altri componenti malware (i cosiddetti «payload»). Queste funzioni rendono Qakbot un software dannoso molto pericoloso che l'NCSC ha individuato svariate volte in Svizzera come vettore per attacchi ransomware.[53]

Un'analisi ha permesso di scomporre la catena di attacchi di Qakbot in singoli moduli, che possono essere combinati in modi diversi a seconda dell'obiettivo. I criminali possono creare catene di attacchi diverse rendendo quindi più difficile il riconoscimento di una campagna Qakbot in una rete infettata. Le infezioni tramite Qakbot, però, avvengono quasi sempre attraverso un'e-mail. Oltre ai già noti allegati e link, ultimamente vengono utilizzate anche immagini sulle quali è presente un URL che la vittima deve inserire manualmente nel browser. Per installare Qakbot sul computer viene però ancora utilizzato un documento Office contenente delle macro.[54]

Nel periodo in esame, l'NCSC ha notato che spesso le e-mail inviate riprendono degli scambi preesistenti («thread hijacking»).[55] Visto che l'e-mail è familiare, la vittima è più propensa ad aprire il documento e seguirne le istruzioni. Generalmente nelle istruzioni si dice che per aprire

---

51 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)

52 How ransomware happens and how to stop it (cert.gov.nz)

53 QAKBOT - Threat Encyclopedia (trendmicro.com); QakBot (Malware Family) (fraunhofer.de); QakBot, Software S0650 (mitre.org)

54 A closer look at Qakbot's latest building blocks (and how to knock them down) (microsoft.com)

55 La settimana 44 in retrospettiva (ncsc.admin.ch); La settimana 50 in retrospettiva (ncsc.admin.ch)

il contenuto è necessario attivare le macro e in seguito vengono spiegati i passaggi da eseguire per abilitarle.[56]

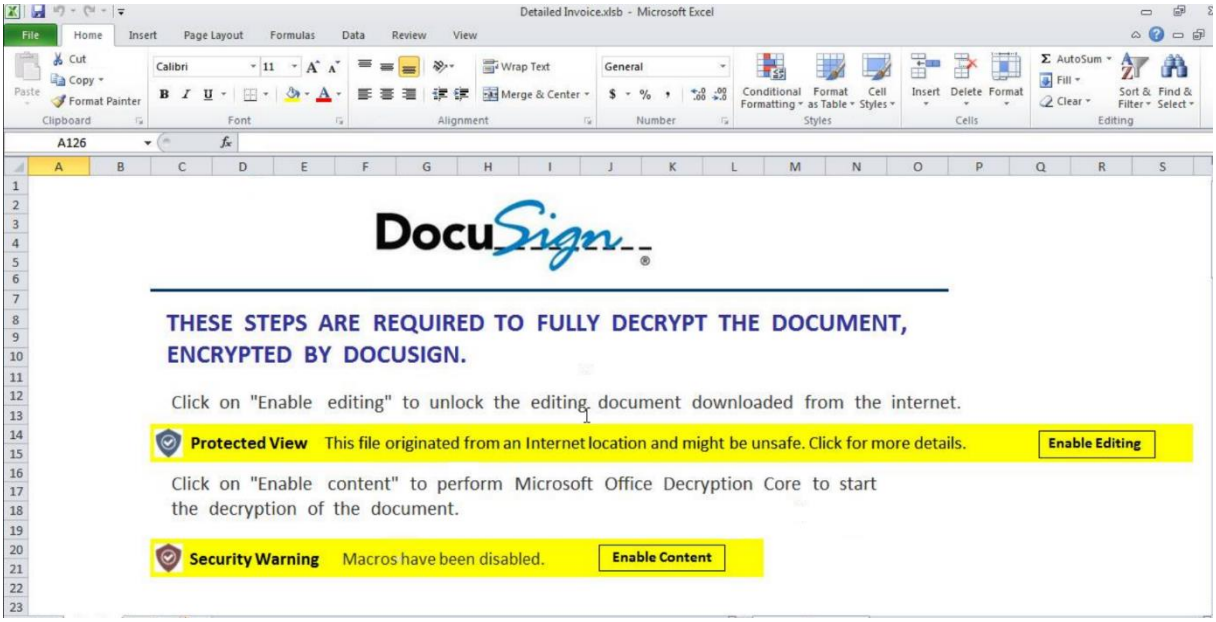


Fig. 6: File Excel con macro nocive.

Da ottobre 2021 è noto che Squirrelwaffle, un altro malware loader diffuso tramite documenti di MS Office con macro nocive, installa anche Qakbot. Inoltre, nel secondo semestre le attività di Qakbot sono state caratterizzate dall'utilizzo di server Exchange compromessi.[57]

Conclusione / raccomandazioni:

- Le e-mail fraudolente possono arrivare anche da mittenti in apparenza conosciuti. Siate prudenti quando all'improvviso un vecchio scambio di messaggi viene ripreso senza seguire un filo logico.
- Spesso i malware sono diffusi tramite documenti Office e nella maggior parte dei casi viene sfruttata la funzione macro, perciò non autorizzatene mai l'attivazione.
- L'NCSC raccomanda ai gestori di server Microsoft Exchange di installare immediatamente tutte le patch disponibili e di mantenere i server aggiornati.
- I server Exchange non devono essere direttamente accessibili da Internet. Attivate un WAF («web application firewall») o un proxy SMTP che filtri il traffico dati prima del server Exchange.
- I siti web utilizzati per la distribuzione di Qakbot dovrebbero essere bloccati sul perimetro della rete. URLhaus (abuse.ch) mette a disposizione gratuitamente un elenco di questi siti web.

56 La settimana 20 in retrospettiva (ncsc.admin.ch)
57 Cfr. n. 4.1.4.

4.3 Attacchi a siti e servizi web

4.3.1 DDoS

Gli attacchi DDoS («Distributed Denial of Service») che influiscono sulla disponibilità dei siti web continuano a essere un fenomeno diffuso sia in Svizzera che all'estero. Nel secondo semestre del 2021 l'NCSC ha ricevuto 17 segnalazioni relative ad aggressioni di questo tipo.

Il settore finanziario continua a essere uno dei principali obiettivi delle ondate di attacchi DDoS a scopo di estorsione. Nella seconda metà del 2021, però, sono stati presi di mira anche fornitori di servizi IT, autorità e istituti di formazione. Estorsori membri del gruppo Fancy Lazarus hanno cercato di ricattare diverse aziende svizzere e autorità cantonali. Tuttavia le minacce di attacchi di maggiore portata dopo aggressioni dimostrative non sono mai state concretizzate. A luglio e a ottobre il provider di hosting della città e del Cantone di San Gallo è stato vittima di attacchi DDoS che hanno reso temporaneamente inaccessibili i rispettivi siti web.[58]

Diversi fornitori di servizi VoIP («Voice over IP»), come Telnyx, Bandwidth e Twilio, hanno segnalato disservizi temporanei provocati da attacchi DDoS.[59] Nel mese di settembre i servizi online di alcune banche in Nuova Zelanda hanno subito delle interruzioni[60] e nel mese di dicembre la filiale polacca di T-Mobile ha dovuto affrontare un'importante ondata di attacchi DDoS.[61]

Stando ai comunicati stampa diffusi, durante il periodo delle elezioni parlamentari in Germania si sono registrati diversi attacchi DDoS di natura politica.[62]
Attacchi DDoS possono venir combinati con altri tipi di attacchi, come le famiglie di ransomware HelloKitty e Yanluowang che operano con DDoS per mettere ancor più sotto pressione le vittime.[63]

Conclusione / raccomandazioni:

L'attacco DDoS a scopo di estorsione è un'operazione di massa. I truffatori scelgono in modo relativamente arbitrario con il maggior numero possibile di imprese. Se non riescono nel loro intento, provano con altri bersagli. Ma se l'attacco DDoS (dimostrativo) riesce a perturbare i sistemi di un'impresa, questa viene presa di mira e gli attacchi intensificati per cercare di ottenere il riscatto. È quindi consigliabile essere preparati a eventuali attacchi DDoS.

In caso di sistemi critici, l'NCSC raccomanda di stipulare un abbonamento di protezione commerciale DDoS («DDoS mitigation service»). Molti fornitori di servizi Internet («Internet service provider», ISP) offrono servizi di questo tipo.

58 Homepages der St.Galler Behörden durch Hackerangriff lahmgelegt (tagblatt.ch)
59 DDoS attack takes yet another VoIP provider offline (techradar.com)
60 Government still gauging impact of Wednesday's denial-of-service attacks (stuff.co.nz)
61 Polish T-Mobile unit faces cyber attack, systems not compromised (reuters.com)
62 Bundestagswahl 2021: Hackerangriff auf Website des Bundeswahlleiters (businessinsider.de)
63 Kaspersky Q4 2021 DDoS attack report (securelist.com)

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

Inoltre, nell'ultimo semestre l'Inter-University Computation Center (IUCC) ha pubblicato una guida esaustiva riguardo le buone prassi per le strategie di mitigazione degli attacchi DDoS: Best Practices for DDoS Mitigation Strategies (geant.org)

4.3.2 Attacchi a sistemi VoIP

Attualmente i sistemi telefonici sono quasi esclusivamente digitali e la maggior parte delle comunicazioni vocali avviene tramite Internet («Voice-over-IP», VoIP). Di conseguenza, se non sono adeguatamente protetti, i sistemi VoIP delle aziende sono un potenziale bersaglio degli attacchi DDoS (cfr. n. 4.3.1) ma possono anche essere sfruttati per fini illeciti. I sistemi VoIP di un'organizzazione svizzera che erano protetti soltanto da una password standard sono stati sfruttati per effettuare chiamate a pagamento in Tunisia e l'organizzazione si è vista recapitare una fattura di centinaia di migliaia di franchi.

4.4 Sistemi di controllo industriali (ICS) e technologia operativa (OT)

Gli attacchi diretti contro sistemi di controllo industriali volti a perturbare o influenzare processi fisici, sono rimasti un'eccezione anche nel semestre in esame. Nella maggior parte dei casi ad avere ripercussioni sull'attività aziendale sono stati i collegamenti tra le reti dei sistemi di controllo e sistemi IT amministrativi con i quali vengono gestite le attività amministrative dell'azienda, come i rapporti commerciali con i clienti e i fornitori.

4.4.1 In Iran un ciberattacco ha limitato l'approvvigionamento di carburante

Lo scorso ottobre in Iran molte stazioni di servizio hanno dovuto limitare l'erogazione di carburante. Il sistema che permette il pagamento del carburante unsando sussidi statali non funzionava[64] e, secondo le autorità iraniane, il problema è stato provocato da un ciberattacco sferrato da una potenza straniera.[65] Le pompe erano in grado di erogare benzina, ma il sistema di pagamento con i sussidi statali non funzionava. La maggior parte dei clienti locali è stata toccata, perché senza gli sconti garantiti dai sussidi la non può sostenere i costi del carburante.

Il guasto è avvenuto pochi giorni prima del secondo anniversario dell'ultima grande ondata di proteste in Iranprovocate dall'aumento del prezzo della benzina. Allo stesso tempo le persone in viaggio sulle autostrade hanno visto comparire sui tabelloni elettronici il messaggio «Khamenei, dov'è la nostra benzina?». Questo messaggio ha ricordato un ciberattacco simile sfer-

64 Störung der Benzinversorgung - Schlangen vor Irans Zapfsäulen: «Khamenei, wo ist unser Benzin?» (srf.ch)
65 Iran says Israel, U.S. likely behind cyberattack on gas stations (reuters.com)

rato nel luglio dell'anno precedente al sistema ferroviario iraniano e nel quale erano stati impiegati anche componenti «wiper».[66] Tuttavia, finora non è stato possibile confermare un legame tra i due attacchi.

4.4.2 Gestori esclusi dai sistemi di controllo degli impianti automatizzati degli edifici

Il servizio di sicurezza informatica di Limes Security è ha vissuto gli effetti di una manipolazione mirata dei sistemi di controllo industriali da parte di soggetti non autorizzati.[67] Dopo essere riusciti ad accedere ai componenti basati sullo standard KNX, i malviventi ne hanno manipolato la configurazione e assunto il controllo degli impianti.

Il responsabile doveva avere competenze specifiche sul funzionamento di KNX per riuscire a trasformare un edificio «smart» in un edificio controllabile soltanto in parte manualmente da locale o del tutto fuori controllo. Non è stato chiarito quale fosse esattamente lo scopo dell'attacco. Grazie alle indagini forensi condotte sulla memoria dei dispositivi è stato possibile evitare la sostituzione dei dispositivi integrati all'interno della struttura architettonica e in parte fissi, che avrebbe avuto un costo notevole.

Conclusione / raccomandazioni:

È necessario investire nella sicurezza degli accessi ai sistemi di controllo industriali e nel monitoraggio del funzionamento e delle manipolazioni, in modo tale che in caso di dubbio si possa intervenire tempestivamente.

Sul proprio sito web l'NCSC raccomanda alcune misure da adottare per proteggere i sistemi di controllo industriali: Misure di protezione dei sistemi di controllo industriali (ICS) (ncsc.admin.ch)

66 MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll (sentinelone.com)
67 KNXlock – an attack campaign against KNX-based building automation systems (limessecurity.com)

4.4.3 Tentativi di ricognizione e danni collaterali minacciano la tecnologia operativa (OT)

Gli attacchi come quello descritto nel paragrafo precedente, che compromettono il funzionamento dei sistemi di controllo industriali attraverso un abuso mirato delle sue funzioni, rappresentano eccezioni nel panorama dei ciberincidenti che hanno effetti negativi sui processi fisici. Sono molto più frequenti i casi in cui i sistemi IT utilizzati per far funzionare i sistemi di controllo vengono infettati da software dannosi diffusi su ampia scala[68] oppure quelli in cui i malintenzionati cercano di utilizzare dispositivi IoT per botnet che lanciano attacchi DDoS o di crypto mining.[69]

Questo tipo di infezioni spesso non hanno ripercussioni sui processi controllati, ma se successivamente sui sistemi vengono installati dei ransomware, la situazione cambia. Sei famiglie di ransomware conosciute (Cl0p, MegaCortex, Netfilim, LockerGoga, Maze e EKANS) nel corso dell'attacco cercano esplicitamente di arrestare i processi IT relativi ai sistemi OT. Nel quarto trimestre del 2021 Dragos, una società specializzata nella sicurezza degli ICS, ha scoperto che alcuni gruppi ransomware avevano pubblicato sul dark web 176 contenuti relativi a ICS.[70] Il settore più colpito da questa problematica è stata l'industria manifatturiera, seguita dai trasporti e dal settore alimentare.

68 https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/

69 Honeypot experiment reveals what hackers want from IoT devices (bleepingcomputer.com)

70 Dragos ICS/OT Ransomware Analysis: Q4 2021 (dragos.com)

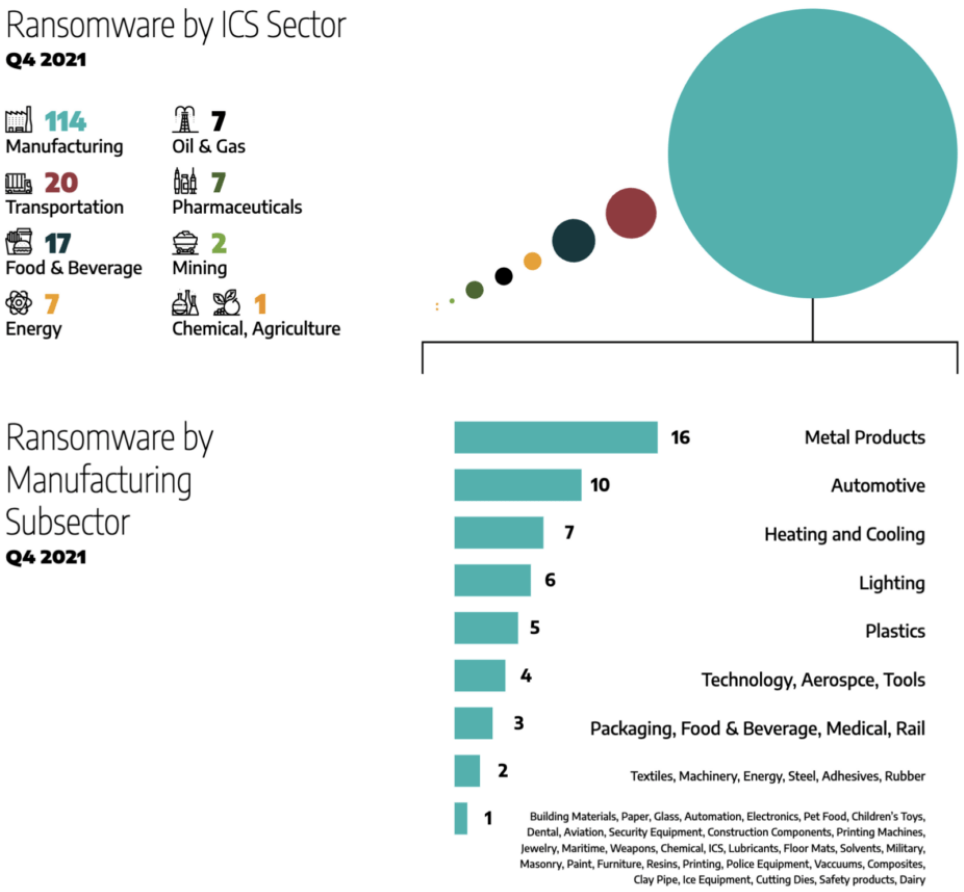


Fig. 7: Dati relativi agli ICS pubblicati da gruppi ransomware per settore (fonte: dragos.com)

Un'indagine[71] condotta da Claroty, un'altra società specializzata nella sicurezza dell'OT, ha confermato che i ransomware rappresentano una minaccia per i sistemi. Il 47 per cento dei 1100 gestori intervistati ha osservato che gli attacchi ransomware hanno avuto ripercussioni sui sistemi OT.

Secondo la società di sicurezza informatica Mandiant, in un caso su sette i dati trafugati durante attacchi ransomware e pubblicati contengono documenti con informazioni sui sistemi OT (architettura di rete, hardware e software utilizzati, ecc.) che potenzialmente potrebbero essere utilizzati anche per attacchi futuri.

I tentativi effettivi di sabotaggio dei sistemi di controllo industriali continuano a essere più probabili nell'ambito di conflitti in corso. L'Ucraina, ad esempio, con il supporto di esperti statunitensi e britannici, ha rafforzato il suo sistema di difesa dedicato[72] dopo il dispiegamento di truppe al confine con la Russia.

---

71 Ransomware Often Hits Industrial Systems, With Significant Impact: Survey (securityweek.com)

72 U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault (nytimes.com)

4.5 Vulnerabilità

4.5.1 Atlassian Confluence – CVE-2021-26084 – remote code execution

Il 25 agosto 2021 il provider di software Atlassian ha annunciato la pubblicazione di una patch per una vulnerabilità critica nel software Confluence[73], un tool collaborativo utilizzato per la gestione di lavoro e progetti utilizzato da numerose aziende in tutto il mondo che spesso contiene anche dati interni. La falla di sicurezza consente all'hacker di eseguire da remoto qualsiasi codice (RCE) e compromettere l'intero server su cui è in esecuzione Confluence. In svariati casi è stato installato un sistema di «crypto mining»[74], oppure i dati delle aziende sono stati criptatied è stato chiesto loro un riscatto.[75]

Secondo Atlassian il problema ha riguardato soltanto la versione installata («on-premises») e non quella cloud.

Conclusione / raccomandazioni:

Questa vulnerabilità è facile da sfruttare. Tenuto conto dei dettagli noti il rischio è stato classificato come molto elevato.

L'opinione pubblica è colpita indirettamente quando è cliente di un'azienda che subisce un attacco. Le aziende che utilizzano soluzioni «on-premises» devono prestare particolare attenzione. L'NCSC raccomanda alle aziende che effettuano autonomamente la manutenzione del proprio server Confluence di installare immediatamente le patch necessarie.[76]

4.5.2 Azure – OMIGOD – privilege escalation, remote code execution

L'8 settembre 2021 Microsoft ha annunciato la pubblicazione di una patch per diverse vulnerabilità critiche che minacciavano la sua piattaforma di servizi cloud Azure. Questo gruppo di vulnerabilità, chiamato OMIGD, riguarda OMI, uno strumento per la gestione dei sistemi Linux e UNIX utilizzato in vari servizi offerti su Azure. Le vulnerabilità consentono la «privilege escalation», cioè lo sfruttamento di una falla per ottenere maggiori privilegi per un utente (CVE-2021-38645, CVE-2021-38648, CVE-202138649) e l'RCE, ovvero l'esecuzione di un codice arbitrario da parte di un hacker non autentificato (CVE-2021-38647). La gravità di queste falle è stata stimata tra 7.0 e 9.8 su una scala da 1 a 10. Sei giorni dopo il rilascio delle patch l'azienda che ha scoperto le falle ha pubblicato un articolo in cui spiegava il loro funzionamento.[77]

---

73 Confluence Security Advisory - 2021-08-25 | Confluence Data Center and Server 7.16 (atlassian.com)
74 Cryptominer z0Miner Uses Newly Discovered Vulnerability CVE-2021-26084 to Its Advantage (trendmicro.com)
75 New Atom Silo ransomware targets vulnerable Confluence servers (bleepingcomputer.com)
76 [CONFSERVER-67940] Confluence Server Webwork OGNL injection - CVE-2021-26084 (atlassian.com)
77 OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers (wiz.io)

Il 14 settembre 2021 Microsoft ha rilasciato una patch che è stata messa automaticamente a disposizione soltanto per determinate offerte cloud. I clienti che gestiscono autonomamente la propria infrastruttura Azure devono installare autonomamente la patch. Microsoft ha messo a disposizione un elenco dei servizi interessati e descritto la procedura da seguire.[78]

Conclusione / raccomandazioni:

Questi tipi di vulnerabilità critiche rappresentano una minaccia indiretta per i privati, se le informazioni personali detenute dalle imprese di cui sono clienti possono essere divulgate. Per le aziende che gestiscono in autonomia la propria infrastruttura Azure il rischio è elevato. L'NCSC raccomanda di controllare e seguire le istruzioni fornite da Microsoft.

4.5.3 Log4j – CVE-2021-44228 – Log4Shell

Il 9 dicembre 2021 è stata segnalata la vulnerabilità critica CVE-2021-44228 presente in Log4j, la libreria open source di Apache, e sono stati resi pubblici anche alcuni dettagli necessari per il suo sfruttamento. Log4j è una libreria Java molto diffusa, che mette a disposizione un framework di logging per applicazioni di terzi. La falla è stata classificata come critica (grado di gravità 10 su 10) perché permette di eseguire RCE.

Numerosi prodotti e software open source utilizzano Log4j come framework di logging. Molte aziende utilizzando prodotti esterni in parti della loro infrastruttura e senza saperlo potrebbero essere esposte a questa vulnerabilità.

Dopo la scoperta di CVE-2021-44228 sono state corrette varie falle di sicurezza legate a Log4j. Nel blog GovCERT l'NCSC ha pubblicato una descrizione dettagliata degli eventi.[79]

Conclusione / raccomandazioni:

L'NCSC ha raccomandato di installare immediatamente le patch di sicurezza disponibili e chiesto alle aziende che nella loro infrastruttura utilizzano direttamente o indirettamente Log4j di seguire con attenzione l'evoluzione della situazione.

Dal momento che questa vulnerabilità può interessare anche componenti di un'infrastruttura sviluppata da terzi, l'NCSC raccomanda anche di stilare al più presto un inventario aggiornato di questi servizi e di aggiornare costantemente quelli interessati.

Dal momento che questa falla di sicurezza può essere sfruttata facilmente e che sono state pubblicate anche le istruzioni per farlo, i sistemi sui quali non sono state installate le patch continuano a essere esposti a un rischio estremamente elevato.

78 Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions (microsoft.com)
79 Zero-Day Exploit Targeting Popular Java Library Log4j (govcert.admin.ch)

Oltre alle ripercussioni indirette sulla collettività, se un'azienda subisce un attacco questa vulnerabilità ha effetti diretti anche sui soggetti privati. È stato inoltre rilevato che anche i dispositivi NAS («network attached storage») utilizzati sia da privati che da aziende possono essere soggetti a questo tipo di attacchi. QNAP, produttore di dispositivi NAS, ha pubblicato raccomandazioni e informazioni sui prodotti interessati da queste vulnerabilità[80] e ha segnalato diversi attacchi ransomware andati a segno.

4.5.4 Blacksmith – CVE-2021-42114

Il 15 novembre 2021 i ricercatori del Politecnico federale di Zurigo, di Qualcomm e dell'università di Amsterdam hanno pubblicato uno studio sulla vulnerabilità hardware Blacksmith[81], che interessa gli apparecchi dotati di un determinato chip RAM e mostra un nuovo metodo con cui è possibile aggirare in modo efficiente i sistemi di sicurezza implementati su chip DDR4.

Visto che a settembre 2021 è stato riconosciuto come servizio autorizzato ad assegnare numeri CVE, l'NCSC ha svolto il ruolo di mediatore tra il team di ricerca e i produttori di chip. In questa occasione ha anche assegnato il suo primo numero CVE alla vulnerabilità Blacksmith.

Conclusione / raccomandazioni:

La vulnerabilità interessa i chip di Samsung, SK Hynix e Micron, utilizzati da diverse imprese di tecnologia. Dato il loro impiego in tutto il mondo, questa vulnerabilità è stata classificata come critica. Tuttavia, il rischio di sfruttamento è molto ridotto perché richiede troppe risorse.

Dato che i produttori non hanno rilasciato patch i chip RAM DDR4 restano vulnerabili. Per le infrastrutture critiche l'NCSC raccomanda di utilizzare chip che possono essere protetti in modo più efficace contro gli attacchi Rowhammer (ovvero ECC o DDR5).

4.6 Fughe di dati

4.6.1 Credenziali della VPN di Fortinet

I gruppo di hacker Orange ha pubblicato mezzo milione di credenziali per gli account VPN di Fortinet sul suo nuovo forum underground.[82] I dati di accesso sarebbero stati rubati in estate sfruttando una vulnerabilità per la quale nel frattempo è stata rilasciata una patch.

L'NCSC ha analizzato le circa 400 voci dell'elenco legate alla Svizzera e informato le organizzazioni interessate.

---

80 Multiple Vulnerabilities in Apache Log4j Library - Security Advisory (qnap.com)
81 Blacksmith – Computer Security Group (ethz.ch)
82 Hackers leak passwords for 500,000 Fortinet VPN accounts (bleepingcomputer.com)

Conclusione / raccomandazioni:

Spesso per il lancio di ransomware vengono utilizzate soluzioni di accesso da remoto vulnerabili. Quando i criminali entrano in possesso di credenziali complete e valide per l'accesso da remoto, i sistemi sono esposti, anche se sono state installate le patch.

Gli accessi a dati, account, sistemi e reti dovrebbero essere protetti da un'autenticazione a due fattori e non soltanto da una combinazione di nome utente e password.

Le credenziali devono essere cambiate di frequente, soprattutto dopo la risoluzione di una vulnerabilità che comporta il rischio di una fuga di dati.

4.6.2 EasyGov

Attraverso una consultazione automatica di massa della piattaforma web www.easygov.swiss, gestita dalla Segreteria di Stato dell'economia (SECO), ad agosto 2021 alcuni hacker sarebbero riusciti ad ottenere fino a 130 000 nomi di aziende che nel 2020 hanno richiesto un credito COVID-19. Tuttavia, gli hacker non sarebbero riusciti a venire a conoscenza dell'ammontare del credito e di altri dati delle aziende interessate. La SECO è stata informata dell'accaduto il 19 ottobre e ha preso subito provvedimenti: l'interfaccia web colpita è stata chiusa nel giro di pochi minuti, i dati sono stati rimossi dal server e il processo utilizzato su EasyGov è stato completamente disattivato.[83] L'NCSC ha fornito supporto e consulenza alla SECO, che ha anche avviato un'indagine.

Conclusione / raccomandazioni:

La digitalizzazione permette di semplificare i processi amministrativi, da cui il nome «EasyGov» del. portale della SECO. Durante la pandemia vi era urgenza di fornire aiuti all'economia in modo semplice. Per questo le aziende, inserendo il proprio numero d'identificazione delle imprese (IDI), potevano compilare un modulo e richiedere un credito. Se il sistema rilevava che era già stato richiesto un (primo) credito collegato a un determinato IDI, il modulo non si apriva. Gli hacker hanno sfruttato questa funzione per confrontare i dati rilevati attraverso una consultazione automatica di massa e gli IDI consultabili sul registro di commercio per scoprire quali aziende avevano usufruito dei crediti.

Quando viene data la possibilità di consultare o di accedere a dei contenuti associati a un database, vi è sempre il rischio che questa funzionalità venga utilizzata in modo improprio. È necessario riflettere precedentemente su quali informazioni potrebbe ottenere un utente non autorizzato effettuando svariate richieste, ricordando che anche una risposta «negativa» può portare a delle conclusioni. In ogni caso è fondamentale impedire le ricerche di massa per evitare che persone non autorizzate possano accedere in breve tempo a grandi quantità di dati.

[83] Ciberattacco a EasyGov (seco.admin.ch)

4.7 Spionaggio

4.7.1 Pegasus

Nel secondo semestre del 2021 giornalisti, ricercatori, ONG e l'opinione pubblica hanno discusso dell'utilizzo del programma di spionaggio Pegasus, dopo che nel mese di luglio Amnesty International aveva pubblicato un rapporto sull'impiego di questo software in tutto il mondo contro gli attivisti per i diritti umani.[84] La piattaforma di ricerca canadese Citizien Lab aveva pubblicato già nel 2018 una ricerca sul suo utilizzo in 45 Paesi tra il 2016 e il 2018.[85] Sviluppato dalla NSO, un'azienda israeliana, Pegasus è un software che consente di sorvegliare le attività di un dispositivo mobile e, stando a quanto dichiarato dalla società, è stato progettato per la lotta al terrorismo e viene venduto ad autorità statali. Queste soluzioni vengono impiegate in tutto il mondo nell'ambito di indagini penali e misure di acquisizione di informazioni per chiarire la posizione di determinate persone. Le autorità di sicurezza scelgono queste modalità soprattutto perché i sospettati utilizzano sempre di più canali di comunicazione e applicazioni con crittografia end-to-end e quindi non è più possibile intercettare le comunicazioni. Negli ultimi anni si è quindi sviluppato un vero e proprio settore che offre alle autorità statali prodotti per il monitoraggio degli endpoint. Il problema è che questi strumenti devono sempre essere impiegati nel rispetto del quadro normativo del Paese dell'acquirente. A settembre 2021 Apple ha risolto una vulnerabilità del servizio di messaggistica iMessage che veniva sfruttata da Pegasus.[86]

4.7.2 Furto di dati tramite l'API di Slack

Il gruppo di hacker MuddyWater, che si presume sia supportato dallo stato iraniano[87], sta utilizzando la backdoor appena scoperta Aclip che sfrutta l'interfaccia (API) di Slack, il servizio di messaggistica istantanea basato sul web per comunicare in segreto. Aclip viene eseguita attraverso lo script batch di Windows aclip.bat, da cui prende il nome. La backdoor rimane sul dispositivo infettato aggiungendo una chiave del registro di sistema e si avvia automaticamente all'accensione del sistema. Aclip riceve i comandi PowerShell dal server C2 tramite le funzioni dell'API di Slack e può essere utilizzata per eseguire altri comandi, inviare screenshot del desktop di Windows attivo e trafugare file. Stando a un rapporto di IBM i responsabili hanno utilizzato questa strategia per attaccare delle compagnie aeree.[88]

---

84 Pegasus Projekt: Spionage-Software späht Medien, Zivilgesellschaft und Oppositionelle aus (amnesty.ch)
85 HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (citizenlab.ca)
86 Analyzing Pegasus Spyware's Zero-Click iPhone Exploit ForcedEntry (trendmicro.com)
87 MuddyWater (Threat Actor) (fraunhofer.de)
88 Nation State Threat Group Targets Airline with Aclip Backdoor (securityintelligence.com)

4.7.3 Nobelium

Il gruppo responsabile dell'attacco alla catena di fornitura di SolarWinds è stato denominato Nobelium. Vari organismi ritengono che Nobelium faccia parte del collettivo APT29 o del servizio russo per le attività informative all'estero SVR.[89] Nel secondo semestre del 2021 Nobelium ha portato avanti la sua attività e, secondo Microsoft, ha preso di mira fornitori di servizi IT, servizi gestiti e cloud negli Stati Uniti e in Europa per accedere ai dati dei loro clienti. Microsoft ha constatato che gli attacchi si sono concentrati principalmente sugli account con maggiori privilegi, per permettere una diffusione larga negli ambienti cloud e sfruttare le relazioni con i clienti.[90] La campagna dimostra l'importanza dei rapporti di fiducia e con i clienti, soprattutto quando sono coinvolti fornitori di servizi IT.

4.7.4 Nickel / K3chang

Per il ciberspionaggio continuano a essere sfruttate spesso soluzioni per l'accesso da remoto su cui non sono state installate le necessarie patch: questo è il caso di una campagna lanciata dal gruppo Nickel.[91] Nickel sembra operare dalla Cina e si ritiene faccia parte del collettivo K3chang.[92] La campagna riportata da Microsoft era diretta contro vari obiettivi, tra cui organizzazioni governative, rappresentanze diplomatiche e organizzazioni non governative di vari Paesi, tra cui anche la Svizzera.

4.8 Ingegneria sociale e phishing

4.8.1 Panoramica sul phishing

Nel periodo in esame sono stati verificati 90 046 URL a seguito delle segnalazioni fatte sul portale antiphishing.ch gestito dall'NCSC, o al Servizio nazionale di contatto attraverso l'apposito modulo. 3991 URL sono risultati essere effettivamente siti web di phishing. L'NCSC ha inoltrato queste informazioni ai rispettivi provider di servizi di hosting, a diversi produttori di browser e a gruppi di lavoro antiphishing. Rispetto alla prima metà del 2021 (4682 siti di phishing rilevati), il fenomeno si è lievemente ridotto.

89 APT29, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, Group G0016 (mitre.org)
90 NOBELIUM targeting delegated administrative privileges to facilitate broader attacks (microsoft.com)
91 NICKEL targeting government organizations across Latin America and Europe (microsoft.com)
92 Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, Group G0004 (mitre.org)

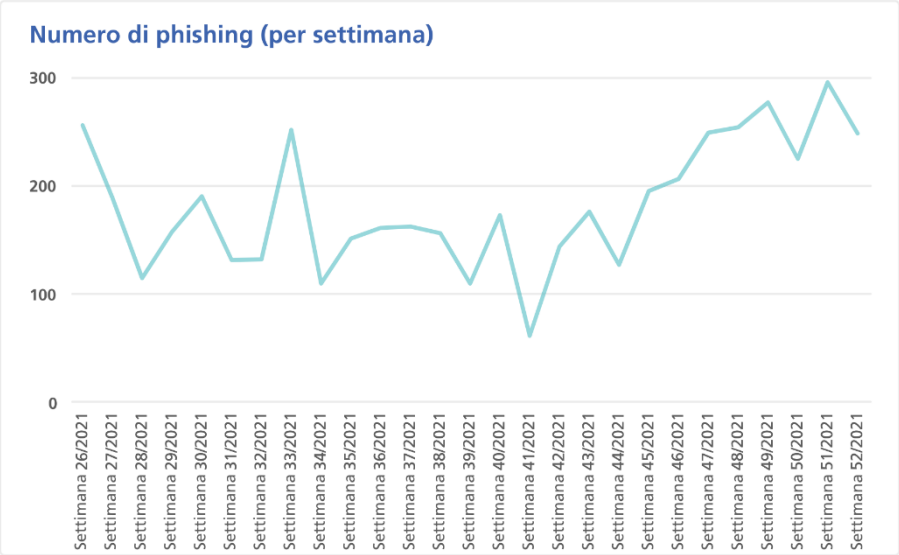


Fig. 8: URL di phishing verificati e confermati dall'NCSC ogni settimana nel secondo semestre 2021.
Per i dati aggiornati consultare la pagina: https://www.govcert.admin.ch/statistics/phishing/

L'NCSC ha osservato che, mentre in passato i tentativi di phishing sfruttavano principalmente i nomi di grandi marchi internazionali, ora si concentrano su imprese locali in parte attive solo sul mercato svizzero. Tra gli obiettivi rimangono i dati di accesso ai servizi finanziari e ai servizi Internet. Per accedere ai dati delle carte di credito invece i criminali solitamente utilizzano i marchi di svariate imprese e usano vari pretesti.[93]

Il phishing è nato come un fenomeno di massa. Nel frattempo però i malintenzionati attaccano anche obiettivi molto specifici. Nel semestre in esame, ad esempio, è stato osservato un tentativo di phishing mirato contro le aziende clienti della Banca Migros. Accedendo alla pagina web di phishing e cliccando sulla sezione dedicata ai privati, l'utente veniva reindirizzato alla vera pagina web della Banca Migros. L'obiettivo degli hacker era ottenere le credenziali tramite i software di contabilità delle aziende.

[93] V. n. 4.1.2 e n. 5.2.

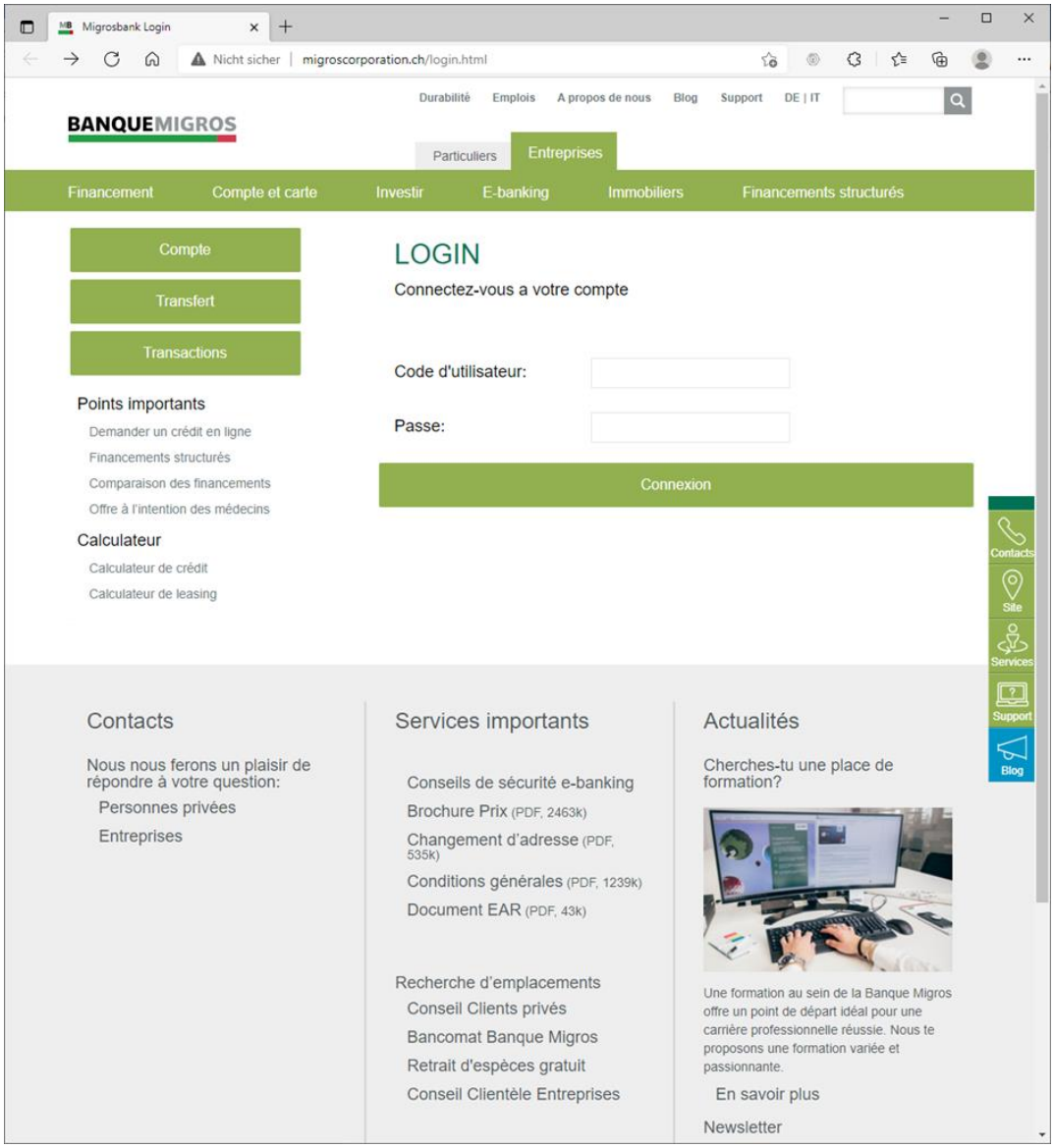


Fig. 9: Pagina web di phishing per i clienti aziendali della Banca Migros.

Inoltre, nel secondo semestre sono stati nuovamente osservati attacchi di phishing in tempo reale ai danni di clienti di istituti finanziari svizzeri, anche se il loro numero è decisamente inferiore rispetto al totale degli attacchi di phishing. Questa strategia aggira l'autenticazione a due fattori ma richiede un intervento più attivo del malvivente, il quale deve effettuare l'accesso al sistema di e-banking nello stesso momento in cui lo effettua la vittima. Al riguardo si veda anche il rapporto relativo al primo semestrale del 2019.[94]

[94] Rapporto semestrale 2019/1 (ncsc.admin.ch), n. 4.4.2.

Anche i social network possono essere utilizzati per attacchi di phishing. A metà dello scorso mese di novembre, ad esempio, la funzione di Facebook che consente di visualizzare le pagine in cui si è stati taggati è stata sfruttata per lanciare attacchi di phishing mirati.[95]

4.8.2 Smishing

Per il phishing vengono utilizzati sempre più spesso gli SMS e altri servizi di messaggistica breve: in questo caso si tratta di «smishing». Solitamente questi messaggi sembrano provenire da mittenti affidabili, come rivenditori conosciuti o aziende di logistica. A volte vengono anche spacciati per concorsi. Il link presente nel messaggio reindirizza l'utente verso un sito web creato appositamente dai criminali, dove alla vittima viene chiesto di inserire i suoi dati personali o della carta di credito.

Nel periodo in esame, ad esempio Coop ha avvisato tramite i social network che su WhatsApp circolava un messaggio di phishing nel quale si comunicava al destinatario che era il vincitore di un concorso organizzato da Coop.

Fig. 10: Avviso di Coop relativo ad attività fraudolente organizzate a suo nome.[96]

4.8.3 SIM swapping

Lo swap (scambio) di carte SIM è una tecnica che permette di deviare il traffico di rete un abbonato mobile senza avere accesso al dispositivo.[97] Attraverso il cosiddetto «SIM swapping» (o «SIM hijacking»), l'hacker induce un gestore telefonico a emettere una nuova SIM e ad associarla a un numero di telefono e a un account esistenti. In questo modo il criminale che si è fatto emettere questa nuova SIM riceverà ad esempio i messaggi SMS con i codici per

95 La settimana 45 in retrospettiva (ncsc.admin.ch)
96 coop_ch auf Twitter: "#Washington-Nachricht auf WhatsApp." (twitter.com)
97 Network Effects, Tactic TA0038 - Mobile (mitre.org)

l'autenticazione a due fattori per accedere a determinati servizi o potrà reimpostare la password di un account, dal momento che spesso per effettuare questa operazione è necessario inserire un codice che viene inviato tramite SMS.[98]

Per richiedere l'emissione di una nuova carta SIM i criminali possono fare ricorso a tecniche di ingegneria sociale con i dipendenti dei gestori telefonici. Le informazioni utili per portare a termine queste operazioni possono provenire da fughe di dati ai danni di queste stesse aziende. La filiale americana di Deutsche Telekom, T-Mobile US Inc., ha denunciato diverse fughe di dati negli ultimi anni. La più recente è avvenuta nel dicembre 2021 e T-Mobile l'ha resa pubblica dopo aver ricevuto numerose segnalazioni di utenti che erano stati vittime di SIM swapping.[99]

In alternativa i criminali possono indurre i dipendenti delle società di telecomunicazioni a installare un software per l'accesso da remoto o a fornire le informazioni necessarie per accedere da remoto a un servizio in esecuzione. In questo modo i responsabili hanno accesso al computer dall'esterno e possono emettere la nuova SIM e inviarla a un indirizzo di loro scelta.[100]

4.8.4 Finte chiamate di assistenza per i servizi di e-banking tramite gli annunci su Google

Il fenomeno dei finti operatori del servizio di assistenza[101] che chiamano per comunicare che il computer ha subito un attacco è ormai noto. I criminali solitamente si fingono dipendenti di una società informatica e cercano di infettare il sistema della vittima o di vendere un servizio per ottenere i dati della carta di credito. Nella versione osservata dall'NCSC[102] e dalle autorità di polizia cantonali[103] tra fine agosto e fine settembre , i malviventi hanno pubblicato degli annunci su Google nelle ricerche di piattaforme di e-banking di determinate banche svizzere che comparivano tra i primi risultati. Un clic sul link dell'annuncio, però, reindirizzava l'utente verso una pagina di phishing. Dopo aver inserito nome utente e password compariva un messaggio di errore che invitava la vittima a chiamare un numero di telefono svizzero. All'altro capo rispondeva un presunto membro del personale della banca. La vittima veniva quindi convinta a scaricare un software per l'accesso da remoto in modo da permettere all'operatore di accedere al computer e risolvere il «problema». Il sedicente operatore prendeva quindi il controllo del PC, effettuava un presunto pagamento di prova e poi scompariva.

98 SIM Card Swap, Technique T1451 - Mobile (mitre.org)
99 T-Mobile says new data breach caused by SIM swap attacks (bleepingcomputer.com)
100 Hackers Are Breaking Directly Into AT&T, T-Mobile, Sprint to Take Over Customer Phone Numbers (vice.com)
101 Fake-Support (ncsc.admin.ch)
102 La settimana 32 in retrospettiva (ncsc.admin.ch); La settimana 34 in retrospettiva (ncsc.admin.ch)
103 Raiffeisen Meldung "Aufgrund verdächtiger Aktivitäten wurde Ihr Konto gesperrt" ist Betrug (cybercrimepolice.ch)

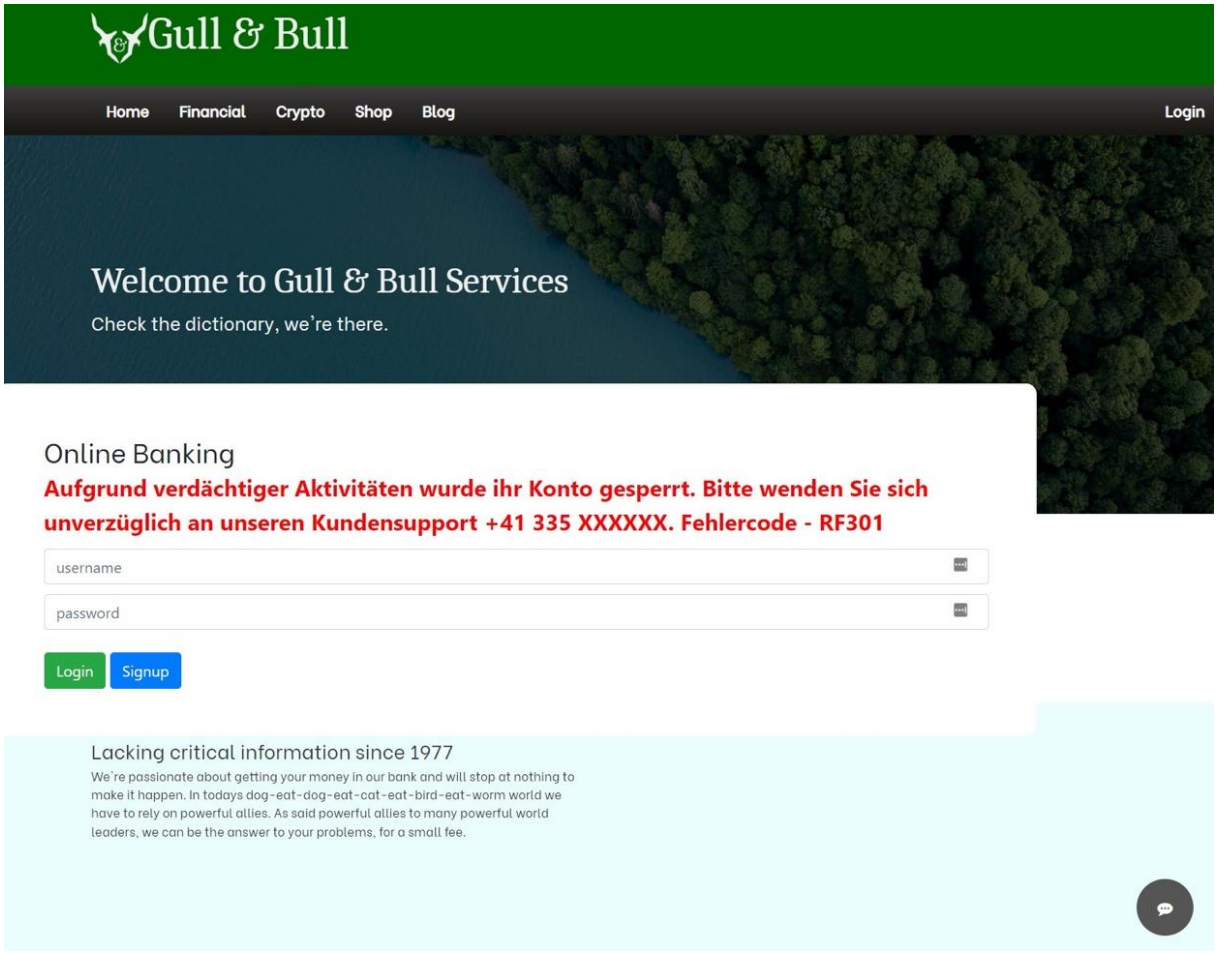


Fig. 11: Fenomeni di ingegneria sociale combinati

5 Fenomeni di ingegneria sociale combinati

5.1 Aumentano gli attacchi mirati, scendono quelli di massa

Truffa dell'anticipo, fake sextortion o fake support sono solo una piccola parte dei fenomeni osservati dall'NCSC nell'ultimo anno. Sulla pagina «Ciberminacce»[104] dell'NCSC è pubblicato l'elenco dei 45 fenomeni attualmente attivi. Diventa però sempre più difficile inserire i fenomeni osservati in una categoria specifica. I malviventi combinano tra loro varie tecniche perché sta diventando sempre più difficile ingannare le vittime con delle «semplici» e-mail fraudolente e quindi devono fare uno sforzo in più per raggiungere il loro obiettivo.

Negli anni scorsi i tentativi di truffa solitamente erano effettuati con campagne di massa: i malviventi inviavano in automatico centinaia di migliaia di e-mail nella speranza che un certo numero di destinatari cadesse nella trappola. Il lavoro dei malviventi quindi era minimo, ma

104 Ciberminacce (ncsc.admin.ch)

anche il tasso di successo. Tuttavia, questo modello di business sembra continuare a funzionare, visto che l'NCSC continua ad osservare numerosi casi di questo tipo.

Chi utilizza Internet ha imparato a riconoscere truffe e i tentativi di attacco mal progettati vengono spesso scoperti. I truffatori escogitano dunque nuovi metodi per convincere le potenziali vittime a compiere azioni insolite. Il primo passo è instaurare un rapporto di fiducia per un determinato periodo di tempo. Il contatto può avvenire ad esempio tramite piattaforme che il destinatario conosce e sulle quali ha già fatto delle esperienze positive.

5.2 Quando gli annunci si trasformano in tentativi di phishing

Le piattaforme di annunci sono molto frequentate da impostori. Non a caso la truffa degli annunci è quella più segnalata. Oltre alle versioni classiche nella quali viene venduta merce inesistente o che non viene spedita, l'NCSC osserva sempre più spesso casi creativi per rubare i dati della carta di credito. I malviventi per esempio creano pagine web che assomigliano a quelle ufficiali dei corrieri e che però non sono pagine generiche. Oppure creano pagine web personalizzate per ogni venditore che oltre al nome del destinatario contengono anche una descrizione e un'immagine dell'articolo in vendita.

5.3 Perché comprare casa se ci attende un'eredità

Le e-mail vettrici della truffa dell'anticipo sono un classico tra le e-mail di frode inviate in massa. La possibilità di ricevere un'eredità o di aver vinto una lotteria può suscitare la curiosità del destinatario e spingerlo a reagire al messaggio ricevuto. Dato che la truffa è ormai conosciuta, i truffatori stanno testando nuove varianti. In una di queste rispondono a un annuncio immobiliare fingendo di essere un soldato che era di stanza in Afghanistan e che ora desidera stabilirsi in Svizzera ed è alla ricerca di un immobile. Dopo un intenso scambio di e-mail volto a costruire un rapporto di fiducia, il presunto soldato sposta la discussione su un patrimonio che dice di possedere e di voler investire in Svizzera. Al proprietario dell'immobile viene promessa un'ingente somma di denaro in cambio di un aiuto con l'investimento. A un certo punto viene poichiesto di pagare delle commissioni.

5.4 Gli investimenti soppiantano i prestiti

La versione digitale della «truffa con promessa di matrimonio», detta anche «romance scam», «love scam» o «truffa dell'amore» è pure molto conosciuta: prevede la creazione di profili fittizi su social media e siti di incontro per avviare relazioni amorose fasulle con le vittime ed estorcere loro prestazioni finanziarie. Dato che è sempre più difficile convincere le vittime a versare dei soldi per una presunta madre malata o per un debito che il partner fittizio deve pagare urgentemente per non finire in mezzo a una strada, anche qui gli hacker provano nuove tecniche. Per esempio cercano di convincere le vittime a investire denaro raccontando che un partner o conoscente lavora in un determinato settore oppure di aver già guadagnato molto denaro su una determinata piattaforma. In questi casi il criminale invece di chiedere denaro per sé condivide le sue «conoscenze» e promette un grosso guadagno. Così facendo la vittima è confusa e non nota che il gestore della presunta piattaforma di investimento e la persona che l'ha contattata stanno tramando insieme.

Conclusione / raccomandazioni:

I malviventi stanno passando almeno in parte dagli attacchi di massa ai tentativi di truffa mirati. Qualsiasi sia la strategia il criminale per prima cosa cerca sempre di stabilire un contatto per ottenere la fiducia della vittima. È importante rimanere cauti anche quando si ha l'impressione di conoscere la persona con cui si sta parlando. Internet è e rimane un luogo in cui chiunque può fingere di essere un'altra persona. Questo vale anche per i profili creati su piattaforme conosciute. Anche se da tempo si conosce virtualmente una persona, non significa che ci si possa fidare.