3 novembre 2022 | Centro nazionale per la cibersicurezza NCSC

Rapporto semestrale 2022/I (gennaio – giugno)

Sicurezza delle informazioni

La situazione in Svizzera e a livello internazionale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

1 Panoramica / Contenuto

Management Summary

L'informatica nei conflitti armati

I conflitti armati si combattono sempre più anche a colpi di attacchi informatici. Gli autori di questi attacchi possono essere attori statali ma anche non statali come organizzazioni di hacktivisti e gruppi criminali. In particolare il conflitto in Ucraina mostra in quali ambiti il settore ciber può rappresentare una risorsa. Questo complesso argomento è al centro del rapporto e viene esaminato sotto diversi aspetti.

Sensibile aumento delle e-mail minatorie

Nel primo semestre del 2022 l'NCSC ha registrato un massiccio aumento delle segnalazioni da parte della popolazione. A fine giugno aveva ricevuto in totale 17'186 segnalazioni. Rispetto al semestre precedente (10'234 segnalazioni), vi è stata quindi una crescita pari a circa il 70 per cento. Il sensibile aumento è da ricondurre principalmente ai casi di e-mail di falsa estorsione (cosiddette «fake extortion») inviate a nome della polizia.

Le truffe sempre in cima alla classifica nazionale

Nel periodo in esame la maggior parte delle segnalazioni all'NCSC (10'447) ha riguardato vari tipi di truffa e circa la metà (5'872) concerneva e-mail di falsa estorsione. Sono diffuse anche la truffa dell'anticipo (1'834), la fake sextortion (615) e le truffe relative ad annunci (419). Il numero di segnalazioni riguardanti casi di phishing e malware è rimasto stabile rispetto al semestre precedente.

Ingenti i danni provocati da truffa dell'investimento e BEC

Oltre ai ransomware, il fenomeno che rischia di provocare maggiori danni alle aziende è la truffa BEC («business e-mail compromise»). Nel primo semestre del 2022 l'NCSC ha ricevuto 47 segnalazioni di questo tipo con perdite complessive pari a 2,3 milioni di franchi svizzeri. La truffa dell'investimento, in particolare presso i privati, è il reato che provoca i danni più ingenti. I casi segnalati nella prima metà del 2022 hanno causato complessivamente perdite per oltre tre milioni di franchi.

Leggera diminuzione dei casi di ransomware

Rispetto al semestre precedente, le segnalazioni di ransomware sono leggermente diminuite, passando da 91 a 83 incidenti. Ciononostante, questo tipo di attacco continua a essere la minaccia informatica più presente a cui sono esposte le organizzazioni in Svizzera. Dall'inizio dell'anno, nel nostro Paese diverse organizzazioni attive in vari settori sono state vittima di attacchi ransomware.

Lo spoofing ha il vento in poppa

L'NCSC ha anche registrato un forte aumento di segnalazioni di numeri di telefono falsificati («spoofing»). In questi casi call center sospetti falsificano il numero di telefono visualizzato, utilizzando i numeri di telefono di privati, affinché le vittime siano più propense a rispondere alla chiamata. Nel primo semestre del 2022 l'NCSC ha ricevuto 319 segnalazioni di questo tipo, mentre nello stesso periodo dell'anno precedente le segnalazioni sono state solo 17.

Editoriale

Negli ultimi sei mesi, parlando di cibersicurezza non si è potuto evitare di menzionare la situazione in Ucraina. Il conflitto non ha avuto quasi nessun impatto diretto sul ciberspazio svizzero, tranne una leggera diminuzione della minaccia di attacchi ransomware. Ciò è dovuto principalmente a due motivi: da un lato, nei gruppi composti da membri russi e ucraini ci sono stati dei contrasti, e, dall'altro, vari gruppi si sono impegnati nel conflitto facendone una priorità.

La situazione in Ucraina mostra anche in quali ambiti il settore ciber può essere una risorsa e dove sono i limiti. Nel conflitto, le attività consistono principalmente in operazioni informative o attacchi tattici, soprattutto ai mezzi di comunicazione utili sul piano militare. Le aggressioni informatiche su larga scala alle infrastrutture hanno scarse ripercussioni nel conflitto. Le bombe sono spesso un mezzo più efficace ed economico. Inoltre, i danni collaterali dei ciberattacchi sono difficilmente gestibili e c'è il rischio di cosiddetti effetti «spillover», che potrebbero portare a un'escalation fuori controllo.

La situazione era diversa nel periodo che ha preceduto l'inizio degli scontri, quando i ciberattacchi avevano lo scopo di paralizzare le infrastrutture ucraine di importanza strategica. Tuttavia, avuto scarso successo, poiché il sistema di difesa informatica era ben predisposto. In questi frangenti le autorità civili e le imprese svolgono un ruolo decisivo. Il conflitto lo mostra bene: l'esercito deve combattere anche nel ciberspazio, ma è occupato nelle operazioni belliche. Prima e anche durante il conflitto, è quindi fondamentale che le infrastrutture digitali possano essere messe in sicurezza con mezzi civili e che in caso di crisi la cooperazione tra autorità civili e militari sia garantita. Proprio come nella realtà materiale, dove in caso di bombardamenti devono intervenire anche i vigili del fuoco perché l'esercito è impegnato nei combattimenti. Nel suo contributo, il nostro ospite Stéphane Duguin del CyberPeace Institute, si sofferma sulla problematica dei ciberattacchi alle infrastrutture civili e sull'impatto delle operazioni informatiche in Ucraina sia nella regione che a livello globale.

In Svizzera continuano a dominare le segnalazioni di truffe online, che nel primo semestre sono aumentate del 70 per cento. Fra i tipi di truffa più comuni ritroviamo la fake extortion, la truffa dell'anticipo, la fake sextortion e le truffe relative agli annunci. Nel presente rapporto ci soffermiamo sui trucchi utilizzati e sulle ripercussioni.

Nella panoramica della situazione ci siamo concentrati sulle modalità di accesso iniziale ai sistemi. Naturalmente il rapporto contiene anche raccomandazioni per rendere più difficili gli attacchi, perché purtroppo molte misure di igiene informatica di base, come mantenere i sistemi aggiornati, spesso non vengono adottate e questo facilita le cose per gli aggressori. Come di consueto, sono presenti anche una parte sulle principali famiglie di malware e una parte dedicata ai ransomware. Il rapporto si conclude con alcuni casi concreti.

Spero che la lettura sia di vostro gradimento. Come in passato, chiediamo a voi, cari lettori, di darci il vostro feedback. Solo così potremo adattare costantemente i contenuti alle vostre esigenze.

Florian Schütz, delegato federale alla cibersicurezza

2 Contributo ospite del CyberPeace Institute

Stéphane Duguin è il direttore del CyberPeace Institute, un'organizzazione non governativa (ONG) neutrale e indipendente impegnata a favore della pace informatica. L'istituto segue e analizza i ciberattacchi contro bersagli civili attraverso la sua piattaforma Cyber Attacks in Times of Conflict Platform #Ukraine.

Come un conflitto armato può destabilizzare il ciberspazio per ognuno di noi

Stéphane Duguin,
CEO del CyberPeace Institute

Oltre che per terra, per mare e nello spazio aereo, oggi i conflitti armati si combattono sempre più spesso anche nello spazio, nel settore delle informazioni e nel ciberspazio. Dal momento, però, che in questi «luoghi» i confini non esistono, un conflitto armato tra Stati può avere ripercussioni anche al di là degli obiettivi militari delle parti in guerra. L'invasione militare dell'Ucraina del febbraio 2022 è stata preceduta da una serie di attacchi informatici a istituzioni e organizzazioni pubbliche ucraine, ponendo così le basi di una guerra che oggi è combattuta sia online che sul campo. Le operazioni e gli attacchi nel ciberspazio collegati alla guerra tra la Federazione Russa e l'Ucraina hanno destabilizzato Internet e stanno minando la fiducia e la sicurezza con cui le persone utilizzano la tecnologia.

Quando a essere prese di mira sono le infrastrutture critiche

Le infrastrutture critiche sono spesso nel mirino dei criminali informatici – che si tratti di oleodotti (Stati Uniti, 2021), stazioni di pompaggio dell'acqua (Israele, 2020) o servizi sanitari (Regno Unito, 2017) – e il conflitto armato in Ucraina lo ha dimostrato chiaramente. Prima dello scoppio delle ostilità e nei primi giorni di guerra sono state impiegati sei diversi tipi di malware per la cancellazione dei dati contro organizzazioni ucraine operanti in settori critici. I malware possono causare ingenti danni se portano all'interruzione di servizi importanti per la popolazione civile. L'attacco alla rete satellitare KA-SAT di Viasat che, secondo quanto riportato, avrebbe avuto come obiettivo alcuni sistemi di controllo delle operazioni militari ucraine, ha portato a una parziale interruzione delle comunicazioni tramite Internet in tutta Europa e causato notevoli disagi a un'azienda tedesca operante nel settore energetico, che ha perso l'accesso al sistema di monitoraggio da remoto di oltre 5800 pale eoliche. Questo attacco e la diffusione di altri malware utilizzati durante il conflitto per cancellare dati sono stati attribuiti ad attori statali estremamente evoluti.

Attori insoliti che disturbano il ciberspazio

In questo conflitto armato, oltre ai protagonisti tradizionali, hanno svolto un ruolo molto importante anche altri attori, ma il confine tra tutti questi soggetti è sempre meno definito. L'esercito cibernetico creato dal governo ucraino, conosciuto come «IT Army of Ukraine», è un'organizzazione poco convenzionale i cui attacchi DDoS («distributed denial of service») provocano pesanti danni alle risorse online russe. I cosiddetti «collettivi di hacktivisti» hanno sommerso le reti di enti governativi, imprese statali e altre organizzazioni con una valanga di attacchi DDoS. Questi attori hanno svolto un ruolo attivo nelle operazioni volte a compromettere le infrastrutture online dei loro obiettivi accessibili alla collettività rendendo inaccessibili siti web

e portali utilizzati dalla popolazione anche per attività quotidiane, come prenotare un biglietto per i mezzi di trasporto o presentare dichiarazioni fiscali.

Diversi Stati membri della NATO, anche se non direttamente coinvolti nel conflitto, negli ultimi mesi hanno subito molti ciberattacchi a opera di collettivi di hacktivisti, probabilmente in risposta alle loro posizioni in merito a questioni di natura geopolitica, ideologica o economica.

La pubblicazione di grandi quantità di dati sensibili nel corso del conflitto è ormai diventata una componente fissa delle minacce informatiche. I collettivi contrari alla guerra si sono resi responsabili di numerosi attacchi informatici e di fughe di dati che hanno portato alla pubblicazione di dati sensibili di clienti e imprese nonché di dati personali. Tali attacchi sollevano questioni importanti in merito alla tutela delle persone, alla protezione dei dati e ai potenziali effetti di un utilizzo di questi dati in futuro da parte di malintenzionati.

Altrettante problematiche sorgono poi in relazione a questi attori meno tradizionali che stanno partecipando al conflitto, soprattutto quando si tratta di cercare di individuare i responsabili di questi attacchi, ovvero di stabilire chi ha ideato, lanciato o autorizzato un determinato ciberattacco.

La tutela del «nostro» ciberspazio

Le operazioni e gli attacchi informatici condotti durante una guerra o in tempi di pace da attori statali e non hanno reso ancora più instabile il ciberspazio e, di conseguenza, la società, fortemente dipendente dalla tecnologia. Questa destabilizzazione avrà però effetti che si protrarranno a lungo nel tempo, molti dei quali non sono stati ancora indagati. Se vogliamo assicurarci un ambiente digitale aperto, libero, stabile e sicuro è assolutamente necessario che tutte le persone coinvolte si comportino in modo responsabile e dimostrino il loro impegno:

- sia in tempi di guerra che di pace i ciberattacchi devono rispettare il diritto e le normative internazionali e non possono avere come bersaglio delle infrastrutture critiche essenziali per la sopravvivenza della popolazione civile;
- prima di agire è necessario tenere conto dei danni potenziali, delle ripercussioni sulla popolazione e delle conseguenze di tipo umanitario che determinati ciberattacchi potrebbero avere;
- gli Stati devono garantire l'applicazione di pene contro gli autori di attacchi informatici che violano le leggi e le norme internazionali;
- le istituzioni pubbliche, come il Computer Emergency Response Team (CERT), sono indispensabili per procedere alla tutela dei sistemi e all'analisi degli attacchi attraverso una collaborazione effettiva e lo scambio di informazioni;
- le imprese private possono avere un ruolo attraverso lo sviluppo e la distribuzione di prodotti e servizi sicuri per i soggetti più vulnerabili della società e proteggere in modo proattivo i governi e i loro cittadini;
- infine, le organizzazioni della società civile possono fornire il loro contributo anche documentando e analizzando i ciberattacchi e le loro ripercussioni, in modo da facilitare le indagini e sostenere il dibattito politico.

3 Tema principale: l'informatica nei conflitti armati

In questo capitolo vengono esaminati i principali fatti avvenuti nel ciberspazio durante l'attuale guerra tra Russia e Ucraina. In buona parte si è trattato di attività di condizionamento, il cui obiettivo era influenzare idee, opinioni o motivazioni di determinati gruppi e interferire nei processi decisionali. Non ci soffermeremo però su queste attività di condizionamento, bensì sugli eventi accaduti nel ciberspazio che hanno avuto conseguenze dirette sulla confidenzialità, sull'integrità e sulla disponibilità di dati o anche ripercussioni sul piano materiale.[1]

3.1 Ciberattività prima dell'invasione

Il cibersabottaggio è un problema con cui l'Ucraina è confrontata da diversi anni. Di seguito tre tra gli esempi più significativi:

- nel 2015 a causa del malware BlackEnergy3, attribuito al gruppo di hacker russi Sandworm, diverse migliaia di utenti rimasero senza energia elettrica fino a sei ore;[2]
- nel 2016 Sandworm tornò a colpire, questa volta attraverso Industroyer, un malware appositamente sviluppato per attaccare i sistemi di controllo industriali della rete elettrica e che in alcune zone di Kiev provocò un blackout di circa un'ora;[3]
- a differenza degli attacchi mirati alla rete elettrica del 2015 e del 2016, nel 2017 vi fu una diffusione su larga scala del malware NotPetya. Dopo aver infettato il sistema, il software criptava i dati al suo interno e poi mostrava un messaggio in cui veniva richiesto il pagamento di un modico riscatto. L'infezione tramite NotPetya partì da un aggiornamento manipolato di un software di contabilità ucraino, che successivamente si diffuse in numerosi sistemi in tutta l'Ucraina. Il malware, però, superò i confini ucraini e colpì sistemi in oltre 65 Paesi. Il funzionamento del software, il fatto che era stata presa di mira l'Ucraina e la mancanza di un sistema di decodifica, inusuale per un ransomware, fece pensare che non si trattasse di un caso di estorsione, ma di sabotaggio.[4]

I servizi segreti ucraini (SBU), hanno dichiarato che nel solo 2021 è riuscito a respingere oltre 2000 ciberattacchi diretti contro sistemi governativi e infrastrutture critiche del Paese e che una parte di queste aggressioni è stata ricollegata ai servizi segreti russi.[5] All'inizio del 2022 in Ucraina sono stati registrati diversi incidenti informatici eclatanti. Il 15 gennaio 2022 Microsoft ha annunciato di aver scoperto un malware battezzato «WhisperGate» che dal 13 gennaio 2022 in Ucraina aveva già colpito i sistemi di istituzioni governative, aziende IT e organizzazioni di pubblica utilità.[6] WhisperGate sembrava un ransomware, ma, data l'assenza di un meccanismo di ripristino dei dati, si è dedotto che in realtà si trattasse di un wiper, ovvero un malware in grado di sovrascrivere i dati presenti nel sistema infettato cancellandoli

---

1 Per esempi di attività di condizionamento svolte nell'ambito della guerra in Ucraina consultare il capitolo 4 del rapporto pubblicato da Microsoft il 22 giugno 2022 sulla guerra in Ucraina (microsoft.com) (in inglese) nonché la pagina EU vs DISINFO (euvsdisinfo.eu).

2 V. rapporto semestrale 2015/2 (ncsc.admin.ch), n. 5.3.1.

3 V. rapporto semestrale 2016/2 (ncsc.admin.ch), n. 5.3.1 e 2017/1 (ncsc.admin.ch), n. 5.3.1.

4 V. rapporto semestrale 2017/1 (ncsc.admin.ch), n. 3.

5 SSU neutralizes over 2,000 cyber attacks on government resources in 2021 (ssu.gov.ua)

6 Destructive malware targeting Ukrainian organizations (microsoft.com)

definitivamente. Dopo aver analizzato il malware, il governo ucraino ha dichiarato che si era trattato di un'operazione russa condotta sotto falsa bandiera al fine di attribuire la responsabilità di WhisperGate a cibercriminali ucraini.[7] Nello stesso periodo in cui si è diffuso WhisperGate, molti siti governativi ucraini sono stati vittima di «defacing».[8] A metà febbraio si sono verificati numerosi attacchi DDoS che hanno compromesso la disponibilità di un numero elevato di pagine Internet e servizi online in Ucraina. Tra le vittime vi sono stati anche istituti finanziari e autorità statali.[9]

3.2 I principali ciberincidenti durante l'attuale conflitto in Ucraina

3.2.1 Interruzione delle connessioni satellitari

Il 24 febbraio 2022, circa un'ora prima dell'inizio dell'offensiva russa contro l'Ucraina, in Europa le connessioni con i satelliti KA-SAT dell'azienda statunitense ViaSat sono saltate a più riprese. Numerose aziende, autorità e utenti privati europei utilizzano questi satelliti per accedere a Internet, soprattutto nelle regioni più isolate. Questo incidente non ha provocato interruzioni soltanto in Ucraina, ma anche in altri Paesi. In Germania, ad esempio, non era più possibile accedere ai sistemi di monitoraggio e controllo da remoto di molte pale eoliche. Il 30 marzo 2022 ViaSat ha pubblicato un'analisi dell'incidente dalla quale è emerso che si era trattato di un attacco mirato che avrebbe dovuto riguardare soltanto la parte della rete satellitare preposta alla copertura dell'Ucraina,[10] ma i cui effetti in realtà si erano fatti sentire anche oltre i confini del Paese. Gli hacker, sfruttando un errore di configurazione di una connessione VPN, erano riusciti ad accedere all'interfaccia amministratore e da qui avevano distribuito su numerosi dispositivi client un aggiornamento del firmware manipolato. I sistemi colpiti, quindi, non riuscivano più a stabilire una connessione con i satelliti e dovevano essere ripristinati sul posto. All'inizio di maggio l'Unione Europea e i suoi Stati membri, così come gli Stati Uniti, il Regno Unito e altri Paesi, hanno condannato l'attacco attribuendone ufficialmente la responsabilità alla Russia.[11]

Commento

Gli attacchi a infrastrutture utilizzate per scopi militari e civili ma anche a livello internazionale sollevano vari interrogativi sulle norme di condotta degli Stati nel ciberspazio. Nei prossimi anni sarà dunque necessario avviare un'ampia discussione, ad esempio, sui danni collaterali e sulla proporzionalità, ma anche sugli obblighi di rispetto delle norme degli hacker statali.

7 Information on the possible provocation (cip.gov.ua)Information on the possible provocation (cip.gov.ua)
8 Ukraine hit by 'massive' cyber-attack on government websites (theguardian.com)
9 Ukraine Ministry of Defense confirms DDoS attack; state banks lose connectivity (zdnet.com); DDoS attacks hit Ukrainian government websites (therecord.media).
10 KA-SAT Network cyber attack overview (viasat.com)
11 Operazioni informatiche russe contro l'Ucraina: dichiarazione […] dell'Unione europea (europa.eu); Attribution of Russia's Malicious Cyber Activity Against Ukraine (state.gov); Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion (www.gov.uk)

3.2.2 Industroyer2 e il tentato sabotaggio della rete elettrica

Il 12 aprile 2022 il Computer Emergency Response Team ucraino (CERT-UA), Microsoft e all'azienda slovacca specializzata in sicurezza informatica ESET, hanno comunicato di aver scoperto ed eliminato Industroyer2, il primo malware in questa guerra di attacchi informatici volto a danneggiare sistemi di controllo industriali.[12] Probabilmente si trattava di una nuova versione di Industroyer, il malware che nel 2016 aveva provocato una serie di blackout nella città di Kiev (v. n. 3.1), in quanto si ritiene che anche la nuova versione sia stata sviluppata dal gruppo Sandworm.[13] Era stata presa di mira un'azienda di approvvigionamento elettrico ucraina, la cui rete informatica aveva già subito un attacco nel mese di febbraio. Gli hacker sono riusciti a infiltrarsi nella rete di controllo e di gestione delle tecnologie operative attraverso la rete IT e a installare il malware Industroyer2. L'attacco avrebbe dovuto svelare i suoi effetti distruttivi l'8 aprile 2022, quando alcune sottostazioni elettriche avrebbero dovuto essere disconnesse dalla rete e parti dell'infrastruttura aziendale sarebbero state paralizzate. Nello stesso periodo di attività di Industroyer2 si suppone fosse attivo anche il wiper CaddyWiper, probabilmente con lo scopo di ostacolare il ripristino dei sistemi ed eliminare le tracce dell'attacco. Alcuni giorni dopo il messaggio del CERT-UA il governo ucraino aveva reso noto che dall'inizio della guerra erano già stati sventati oltre 50 attacchi simili. Queste dichiarazioni sono però smentite da un rapporto riservato trapelato, dal quale emerge che, poco prima della diffusione del comunicato di cui sopra, nove sottostazioni erano rimaste paralizzate in seguito a un attacco.[14]

Commento

Industroyer2 è il primo malware scoperto dall'inizio dell'invasione dell'Ucraina attraverso il quale, date le sue funzionalità, gli hacker non soltanto hanno compromesso i sistemi IT, ma intendevano anche danneggiare alcuni processi fisici approfittando dell'interazione diretta con sistemi di controllo industriali.

3.2.3 Wiper

Dall'inizio della guerra in Ucraina sono apparsi numerosi wiper di vario tipo.[15] Questi malware vengono utilizzati per distruggere dati o renderli illeggibili crittografandoli o sovrascrivendoli per poi cancellarli definitivamente. Sono state prese di mira organizzazioni attive in diversi ambiti come l'amministrazione pubblica, il settore energetico e quello finanziario. Tuttavia le fonti ufficiali non hanno rilasciato informazioni sulla reale entità e il successo di questi attacchi. Stando alle analisi, il malware sarebbe programmato in modo tale da evitare una diffusione incontrollata, come era invece avvenuto nel 2017 con NotPetya. Ciononostante, il

12 Heavy cyberattack on Ukraine's energy sector prevented (cip.gov.ua); Industroyer2: Industroyer reloaded (welivesecurity.com).
13 Ukraine Power Grid Cyberattacks (securityboulevard.com); INDUSTROYER.V2: Old Malware Learns New Tricks (mandiant.com).
14 Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine (wired.com); Russian hackers tried to bring down Ukraine's power grid to help the invasion (technologyreview.com).
15 An Overview of the Increasing Wiper Malware Threat (fortinet.com)

23 febbraio 2022 presso alcune aziende lituane e lettoni che forniscono servizi anche al governo ucraino è stata riscontrata la presenza di HermeticWiper.[16]

Commento

Gli attori statali russi sembrano molto scrupolosi e fanno in modo che i loro sabotaggi informatici abbiano effetti soltanto sull'Ucraina. Non vogliono certo dare a un altro Stato, tanto meno alla NATO, un pretesto per intervenire attivamente nel conflitto.

3.3 Hacker non statali da entrambe le parti

Dopo l'offensiva sferrata il 24 febbraio 2022 dalla Russia, numerosi attori non statali (organizzazioni di hacktivisti e gruppi criminali) si sono fatti avanti dichiarando di voler prendere parte alla guerra nel ciberspazio. Lanciano attacchi o minacciano rappresaglie contro chi attacca la «loro» parte. In totale è stata accertata la presenza di oltre 80 gruppi non statali di questo genere.

Uno dei principali gruppi filorussi è Killnet. In reazione al supporto fornito all'Ucraina e alle sanzioni contro la Russia, il gruppo si è reso responsabile di numerosi attacchi DDoS. I danni che ne derivano variano molto a seconda di quanto la vittima dipenda dalla sua presenza online e da quanto sia preparata a questo tipo di aggressioni. Nella maggior parte dei casi gli attacchi DDoS possono essere respinti o neutralizzati in tempi relativamente brevi. Tra le principali vittime vi sono state le pagine Internet di aeroporti, enti statali e istituti finanziari di numerosi Paesi europei.

Per quanto riguarda i gruppi schierati a fianco dell'Ucraina, invece, il collettivo Anonymous ha rivendicato numerosi attacchi ai danni, non solo di organizzazioni russe, ma anche di aziende occidentali operanti in Russia. Il 20 marzo 2022, ad esempio, Anonymous ha dichiarato che le aziende occidentali che non avessero abbandonato il mercato russo entro 48 ore avrebbero rischiato di diventare un potenziale bersaglio di attacchi hacker. Da quel momento Anonymous ha firmato svariate operazioni di «hack and leak» conclusesi con il furto e la pubblicazione di dati aziendali e governativi riservati provenienti principalmente dalla Russia.

Il 26 febbraio 2022 l'Ucraina ha annunciato la creazione di una «IT Army of Ukraine», invitando volontari da tutto il mondo ad unirsi a questo ciberesercito per lanciare attacchi a favore dell'Ucraina. Uno dei principali pilastri di questo gruppo è il suo canale Telegram, attraverso il quale comunica gli obiettivi degli attacchi DDoS.

Nonostante l'elevata frequenza di attacchi a opera di gruppi non statali, finora tali operazioni hanno avuto effetti solo marginali sull'andamento della guerra.

16 Russia unleashed data-wiper malware on Ukraine (theguardian.com)

Commento

Durante ogni manifestazione di piazza motivata da questioni politiche vengono compiuti reati, ad esempio danni materiali a cose. Anche online vengono compiute azioni virtuali simili (defacing, DDoS). Tuttavia, quando gli hacktivisti si inseriscono in un conflitto armato tra Stati, in determinate circostanze possono essere considerati a tutti gli effetti combattenti e subire rappresaglie. A questo riguardo sorgono domande anche in merito alla responsabilità degli Stati dai quali partono gli attacchi.

3.4 Ulteriori aspetti del conflitto nel ciberspazio

3.4.1 Supporto da parte di Stati e imprese

All'inizio del 2022 sono state annunciate diverse misure a supporto dell'Ucraina nell'ambito della cibersicurezza. Il 14 gennaio 2022 il Segretario generale della NATO aveva prospettato la firma di un accordo con l'Ucraina per un maggiore supporto nell'ambito della ciberdifesa. Nella dichiarazione rilasciata si affermava che da anni la NATO collabora con l'Ucraina per migliorare le capacità di ciberdifesa del Paese fornendo anche supporto in loco. Il 22 febbraio 2022 l'Unione Europea ha da parte sua annunciato la costituzione di un gruppo di dieci esperti, in rappresentanza di diversi Paesi europei, incaricato di aiutare l'Ucraina a fronteggiare le sempre maggiori minacce informatiche sia sul posto che a distanza.

Il 10 maggio 2022 sono stati resi noti i dati effettivi sull'aiuto fornito all'Ucraina da altri Stati. In una dichiarazione congiunta, l'Unione Europea e i suoi Stati membri, gli Stati Uniti, il Regno Unito e altri Stati hanno condannato gli attacchi a ViaSat (v. n. 3.2.1) e annunciato che avrebbero continuato ad aiutare l'Ucraina per rafforzare la sua resilienza ai ciberattacchi. Contemporaneamente gli Stati Uniti hanno fornito maggiori dettagli sulle azioni intraprese a sostegno dell'Ucraina per garantire l'accesso a Internet e assicurare la cibersicurezza.[17]

Il 1° giugno 2022 il comandante dell'US Cyber Command ha comunicato che gli Stati Uniti avrebbero avviato una serie di operazioni offensive e difensive e misure d'informazione nel ciberspazio a favore dell'Ucraina.[18] Dal momento però che la maggior parte di queste operazioni non è stata condotta pubblicamente, è difficile valutarne la portata. L'analisi pubblicata nel mese di aprile su un malware progettato per attaccare sistemi di controllo industriali (v. n. 5.4.1), ma che fino a quel momento non era stato ancora impiegato, potrebbe essere in relazione con le suddette misure dell'US Cyber Command. Il malware avrebbe potuto essere utilizzato per futuri attacchi contro l'Ucraina, ma anche contro altri Stati. Un'altra operazione che ha fornito un potenziale aiuto all'Ucraina ed è stata annunciata pubblicamente, è stato il parziale smantellamento dell'infrastruttura botnet del malware Cyclops Blink, utilizzata dal gruppo Sandworm (v. n. 5.2.4).

17 U.S. Support for Connectivity and Cybersecurity in Ukraine (state.gov)
18 US military hackers conducting offensive operations in support of Ukraine (sky.com)

Numerose società di sicurezza informatica attribuiscono alla guerra in Ucraina un significato particolare e per questo hanno dedicato al tema analisi e rapporti. ESET e Microsoft, ad esempio, insieme al CERT ucraino hanno annunciato pubblicamente la scoperta di Industroyer2. Il 22 giugno 2022 Microsoft ha pubblicato un rapporto sulle osservazioni riguardo le minacce informatiche connesse alla guerra in Ucraina.[19] Nella relazione si spiega anche che per dieci settimane Microsoft e altre aziende tecnologiche hanno aiutato l'Ucraina a trasferire la maggior parte dei dati e delle attività digitali del governo su cloud situati fuori dai confini ucraini. Questo ha permesso all'Ucraina di portare avanti le proprie attività digitali quando i centri di calcolo ucraini sono stati distrutti da attacchi missilistici all'inizio dell'offensiva russa. Inoltre, il rapporto parla della stretta collaborazione delle aziende IT con il governo di Kiev. Microsoft ha dichiarato di aver aiutato fornendo prestazioni gratuite per un valore totale stimato in 239 milioni di dollari americani. L'aiuto di aziende private è senza dubbio fondamentale, perché sono in grado di assicurare la protezione dei sistemi anche in condizioni normali e, al contrario delle autorità, solitamente hanno una panoramica decisamente più ampia su sistemi e processi.

3.4.2 Utilizzo di ciberstrumenti nell'ambito di un conflitto armato

Le notizie diffuse sui ciberattacchi verificatisi in Ucraina dal 24 febbraio 2022 non permettono di ricostruire un quadro completo né di giungere a conclusioni definitive su come il ciberspazio potrebbe essere utilizzato nel corso di un conflitto armato.

Dal momento che le ostilità sono ancora in corso, infatti, numerosi incidenti e la loro portata non sono stati resi noti. I protagonisti rivendicano di aver messo a segno o sventato una serie di attacchi, senza che i fatti possano essere verificati da un organismo indipendente. Spesso queste notizie vengono diffuse per scatenare o smorzare l'entusiasmo dell'opinione pubblica e della popolazione. Ad esempio, non sono state rese note ciberaggressioni contro sistemi militari, come era stata ipotizzato invece in Siria nel 2007, quando le forze armate israeliane avrebbero sfruttato le proprie competenze informatiche per mettere fuori gioco i sistemi di difesa contraerea e scagliare un attacco aereo contro obiettivi in Siria.[20]

Dopo l'annessione della Crimea nel 2014, il conflitto tra Ucraina e Russia per le repubbliche separatiste nella zona orientale del Paese ha attraversato fasi alterne. In questi anni sono state svolte anche operazioni di tipo informatico (v. n. 3.1), che il presunto autore è riuscito in modo più o meno credibile a negare. Dall'inizio dell'offensiva russa, però, l'impiego di mezzi militari convenzionali è riuscito a mettere in secondo piano l'utilizzo degli strumenti informatici. Effettivamente molti obiettivi militari possono essere raggiunti in modo più veloce, preciso, semplice e duraturo con i tradizionali mezzi militari piuttosto che attraverso ciberattacchi.

Sono state formulate varie ipotesi sul perché non circolino notizie sui ciberattacchi distruttivi (ossia che provocano la distruzione di beni materiali) condotti dalla Russia contro l'Ucraina:

1. la Russia lancia con successo ciberattacchi distruttivi contro l'Ucraina, ma non sono resi pubblici principalmente perché il conflitto è ancora in corso;
2. la Russia conduce ciberattacchi distruttivi contro l'Ucraina, ma quest'ultima riesce a difendersi, anche grazie all'appoggio di altri Stati e partner privati;

---

19 Defending Ukraine:Early Lessons from the Cyber War (microsoft.com)

20 Operation Orchard/Outside the Box (2007) - International cyber law: interactive toolkit (ccdcoe.org)

3. la Russia non conduce ciberattacchi distruttivi contro l'Ucraina, in particolare perché ritiene che i mezzi militari tradizionali siano più adatti per raggiungere determinati obiettivi.

Infine, l'apparente assenza di questi attacchi è verosimilmente dovuta a una combinazione di queste ipotesi ed è probabile che nel ciberspazio si siano verificati più incidenti di quanto sia stato reso noto.

4 Segnalazioni da parte della popolazione

4.1 Segnalazioni di ciberincidenti ricevute

Nel primo semestre 2022 l'NCSC ha ricevuto in totale 17'186 segnalazioni. Rispetto al semestre precedente (10'234 segnalazioni), vi è stata quindi una crescita pari a circa il 70 per cento. Il sensibile incremento è da ricondurre principalmente ai casi di e-mail di falsa estorsione («fake extortion»), che attualmente rappresentano circa un terzo di tutte le segnalazioni e la metà delle truffe annunciate. Le segnalazioni di truffe sono anche quelle nettamente più frequenti (10'447). Oltre ai casi di fake extortion, sono diffuse anche truffe dell'anticipo (1'834), casi di fake sextortion (615) e truffe relative ad annunci (419). Il numero di segnalazioni riguardanti casi di phishing e malware è paragonabile a quello del semestre precedente.

Segnalazioni settimanali all'NCSC nel primo semestre del 2022

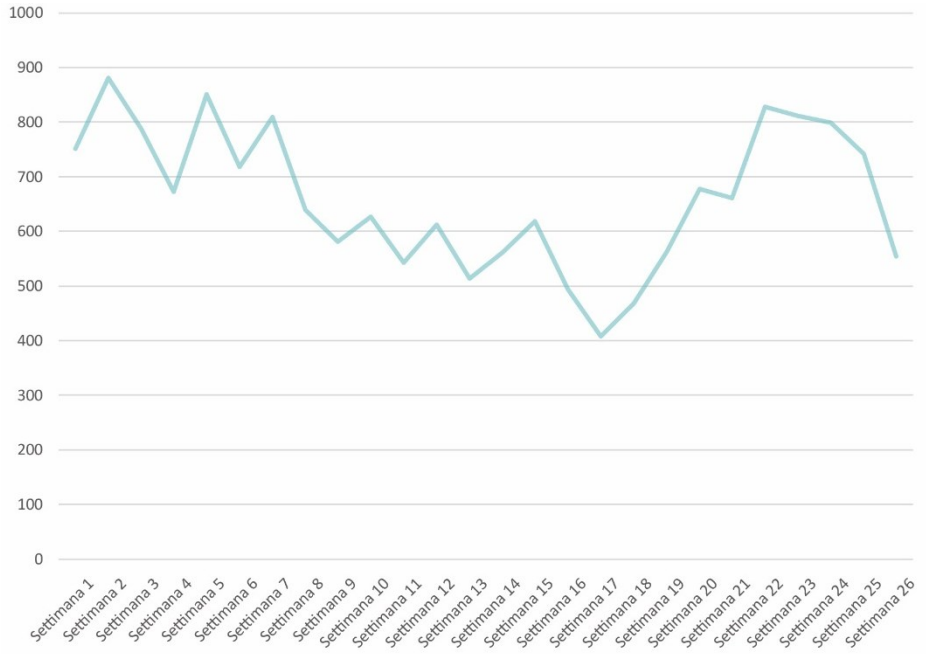


Fig. 1: Segnalazioni settimanali all'NCSC tra gennaio e giugno 2022 (v. anche Numeri attuali (ncsc.admin.ch)).

Segnalazioni all'NCSC nel primo semestre del 2022 per categorie

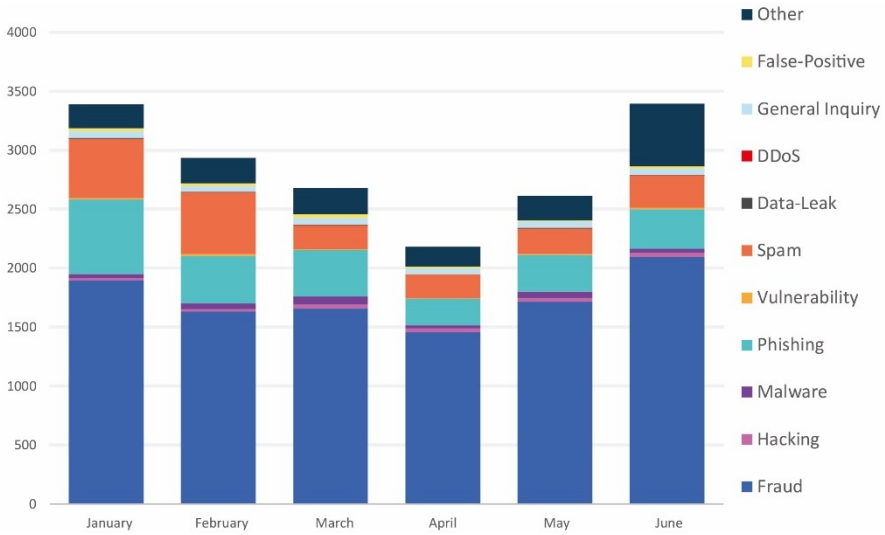
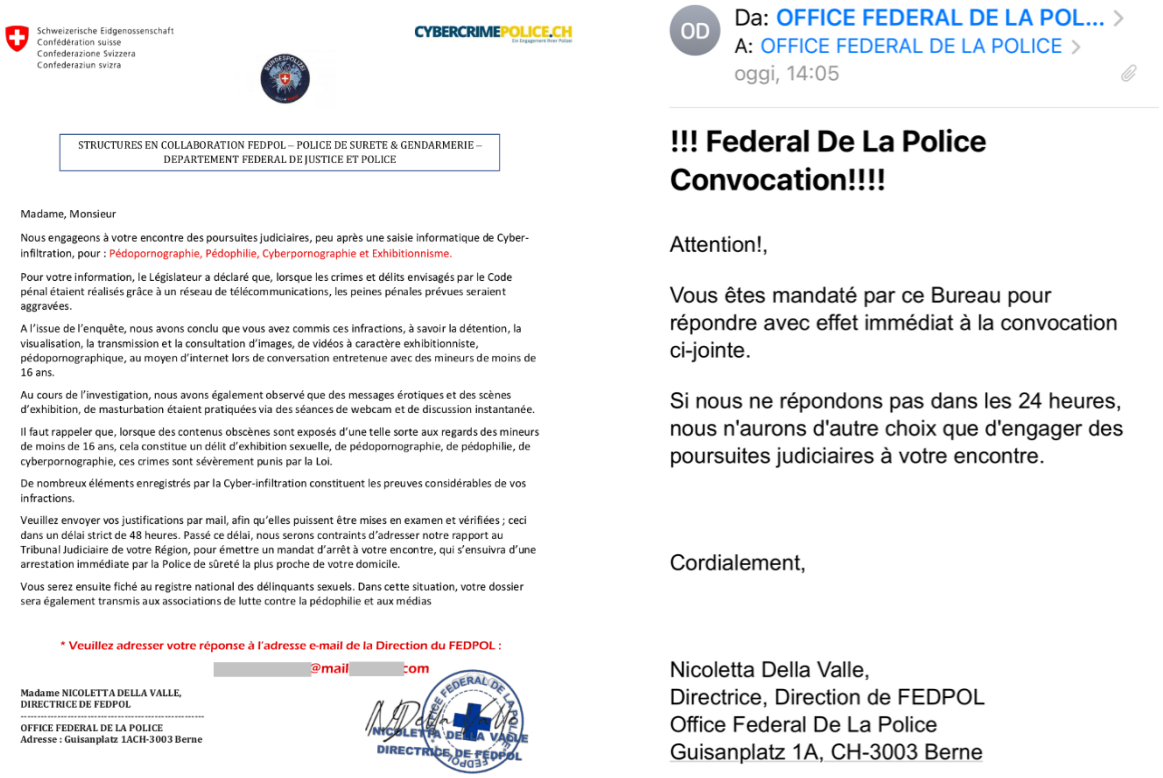


Fig. 2: Segnalazioni all'NCSC nel primo semestre del 2022 per categorie (v. anche Numeri attuali (ncsc.admin.ch)).

4.2 Il tipo di incidente più segnalato: la truffa

4.2.1 Prosegue la tendenza all'aumento dei casi di fake extortion

La tendenza all'aumento dei casi di e-mail minatorie inviate per conto della polizia, già registrati alla fine dello scorso anno, si è confermata nel primo semestre del 2022. Attualmente questo tipo di e-mail rappresenta circa un terzo (5'872) di tutte le segnalazioni pervenute e circa la metà delle truffe. Nelle e-mail di fake extortion si comunica alla vittima che è ritenuta colpevole di un grave reato (solitamente connesso alla pedopornografia) e che l'unico modo per evitare un'azione penale è versare una somma di denaro. In Francia questo tipo di truffa è presente già da diversi anni e ora è arrivato anche in Svizzera. All'inizio le e-mail erano soltanto in francese, successivamente però sono state segnalate anche e-mail in tedesco e, a metà maggio, l'NCSC ha ricevuto le prime segnalazioni di e-mail di questo tipo in italiano. Nella variante più diffusa, le e-mail sembrano provenire dall'Ufficio federale di polizia o addirittura dalla sua direttrice, Nicoletta della Valle.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYBERCRIMEPOLICE.CH

STRUCTURES EN COLLABORATION FEDPOL – POLICE DE SURETE & GENDARMERIE – DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Madame, Monsieur

Nous engageons à votre encontre des poursuites judiciaires, peu après une saisie informatique de Cyber-infiltration, pour : Pédopornographie, Pédophilie, Cyberpornographie et Exhibitionnisme.

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal étaient réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

A l'issue de l'enquête, nous avons conclu que vous avez commis ces infractions, à savoir la détention, la visualisation, la transmission et la consultation d'images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d'internet lors de conversation entretenue avec des mineurs de moins de 16 ans.

Au cours de l'investigation, nous avons également observé que des messages érotiques et des scènes d'exhibition, de masturbation étaient pratiquées via des séances de webcam et de discussion instantanée.

Il faut rappeler que, lorsque des contenus obscènes sont exposés d'une telle sorte aux regards des mineurs de moins de 16 ans, cela constitue un délit d'exhibition sexuelle, de pédopornographie, de pédophilie, de cyberpornographie, ces crimes sont sévèrement punis par la Loi.

De nombreux éléments enregistrés par la Cyber-infiltration constituent les preuves considérables de vos infractions.

Veuillez envoyer vos justifications par mail, afin qu'elles puissent être mises en examen et vérifiées ; ceci dans un délai strict de 48 heures. Passé ce délai, nous serons contraints d'adresser notre rapport au Tribunal Judiciaire de votre Région, pour émettre un mandat d'arrêt à votre encontre, qui s'ensuivra d'une arrestation immédiate par la Police de sûreté la plus proche de votre domicile.

Vous serez ensuite fiché au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias

* Veuillez adresser votre réponse à l'adresse e-mail de la Direction du FEDPOL :

[redacted]@mail[redacted]com

Madame NICOLETTA DELLA VALLE,
DIRECTRICE DE FEDPOL

OFFICE FEDERAL DE LA POLICE
Adresse : Guisanplatz 1ACH-3003 Berne

NICOLETTA DELLA VALLE
DIRECTRICE DE FEDPOL

OD

Da: OFFICE FEDERAL DE LA POL...
A: OFFICE FEDERAL DE LA POLICE
oggi, 14:05

!!! Federal De La Police Convocation!!!!

Attention!,

Vous êtes mandaté par ce Bureau pour répondre avec effet immédiat à la convocation ci-jointe.

Si nous ne répondons pas dans les 24 heures, nous n'aurons d'autre choix que d'engager des poursuites judiciaires à votre encontre.

Cordialement,

Nicoletta Della Valle,
Directrice, Direction de FEDPOL
Office Federal De La Police
Guisanplatz 1A, CH-3003 Berne

Fig. 3: tipiche e-mail minatorie a nome della direttrice della fedpol Nicoletta della Valle.

Gli indirizzi delle presunte autorità da cui partono queste e-mail minatorie, però, cambiano spesso e si susseguono senza una logica. Inoltre, sono state segnalate anche altre e-mail simili inviate a nome di vari organi di polizia cantonali o dal portale Cybercrimepolice. Gli hacker utilizzano in modo illecito anche il nome dell'NCSC per dare una parvenza di ufficialità a queste comunicazioni fraudolente. Per comunicare con le vittime gli autori spesso utilizzano account di posta elettronica hackerati di studenti di varie università in Europa e in Brasile. L'NCSC ha già segnalato ai relativi provider centinaia di account di posta elettronica falsificati o hackerati, in modo tale che possano prendere provvedimenti per evitarne un utilizzo illecito.

4.2.2 Elevati i danni provocati dalle truffe dell'investimento e BEC

Le truffe dell'investimento continuano a essere tra i reati che provocano i danni maggiori. I casi segnalati all'NCSC nel primo semestre del 2022 hanno portato complessivamente a perdite superiori a tre milioni di franchi svizzeri. Per questo tipo di truffe le perdite con importi a sei cifre non sono una rarità. Essendo in un periodo caratterizzato da un crescente rincaro e tassi d'interesse bassi, queste offerte di investimento appaiono molto allettanti. Abbagliati dagli elevati rendimenti (sospetti) promessi, le vittime non prestano attenzione a tutta una serie di segnali ed elementi che potrebbero invece far pensare a una truffa. Nella maggior parte dei casi, ad esempio, i siti di investimenti sospetti sono stati creati solo un paio di mesi prima.

Stando alle informazioni raccolte dall'NCSC, oltre ai ransomware, i fenomeni che rischiano di provocare le perdite più ingenti per le aziende sono le truffe BEC («business e-mail compromise»). Nel periodo in esame l'NCSC ha ricevuto 47 segnalazioni di questo tipo. In questi casi i truffatori si ricollegano a uno scambio di e-mail avvenuto in precedenza che contiene un ordine di pagamento o una fattura, ma modificano l'IBAN del conto sul quale deve essere

effettuato il versamento. Per accedere allo scambio di e-mail, gli hacker devono entrare nell'account di posta elettronica del mittente o del destinatario. Tra le vittime vi sono principalmente i fornitori. Innanzitutto perché le fatture spesso hanno importi consistenti e, in secondo luogo, perché vengono inviate contemporaneamente più fatture, aumentando così le possibilità di successo per i truffatori. Le perdite causate da questo tipo di truffa segnalate all'NCSC ammontano in totale a 2,3 milioni di franchi svizzeri.

4.2.3 Lo spoofing ha il vento in poppa

Le segnalazioni di numeri di telefono falsificati («spoofing») sono letteralmente esplose. Rispetto al semestre precedente si è passati da 17 a 319 segnalazioni, questo perché di solito le chiamate ricevute da call center sospetti sono effettuate da un numero falsificato, che in realtà appartiene a un privato. Per le truffe telefoniche o le chiamate da call center sospetti, è piuttosto frequente che i malviventi utilizzino un numero falsificato, perché vedendo un normale numero svizzero le vittime sono più propense a rispondere. Se vengono utilizzati sempre gli stessi numeri, i reali detentori del numero utilizzato vengono sommersi di telefonate da parte di chi prova a richiamare dopo aver trovato una chiamata senza risposta. Alcuni hanno riferito di aver ricevuto fino a 50 chiamate al giorno. In genere i call center cambiano regolarmente il numero falsificato, proprio per evitare questo problema. Tuttavia, in alcuni casi lo stesso numero è stato utilizzato per settimane o addirittura mesi. Per il detentore del numero è molto fastidioso , anche perché purtroppo non c'è molto da fare.[21]

4.3 Segnalazioni di Phishing

Il fenomeno del phishing è rimasto praticamente stabile rispetto al semestre precedente. Attraverso l'apposito modulo sono infatti giunte 2'308 segnalazioni, ovvero 100 in meno rispetto alla seconda metà del 2021. Sul portale dedicato antiphishing.ch sono state però elaborate direttamente 4'535 pagine. Anche nel periodo in esame, si è trattato perlopiù di e-mail fraudolente in cui sedicenti corrieri annunciavano l'arrivo di un pacco. 464 segnalazioni hanno riguardato casi di questo tipo. Tra le strategie di phishing più diffuse continuano però a esserci anche i presunti pagamenti doppi delle fatture di provider di servizi Internet, come Swisscom o Sunrise. In questi casi alle vittime viene chiesto di fornire il numero di carta di credito per effettuare il rimborso.

Con 145 segnalazioni totali nel primo semestre del 2022, sono aumentati i casi di phishing legati agli annunci. Nelle truffe di questo tipo gli autori fingono interesse per un prodotto. Una volta trovato l'accordo sul prezzo, il compratore si offre di organizzare il trasporto e si impegna a versare l'importo concordato insieme alle spese di spedizione, che in seguito il venditore dovrà versare al servizio di consegna. A questo punto il venditore viene contattato da un presunto corriere che chiede alla vittima di accedere al suo sito web e di inserire i dati della carta di credito per effettuare il pagamento. Queste pagine web in alcuni punti sono molto personalizzate, tanto che oltre all'indirizzo e al nome del venditore spesso è inserita anche l'immagine dell'oggetto acquistato, che il truffatore ha copiato dal portale di annunci. Gli hacker investono quindi parecchie risorse, ma evidentemente ne vale la pena.

---

[21] V. messaggio concernente la revisione della legge sulle telecomunicazioni (admin.ch) (FF **2017** 5599: pag. 5620 e 5635).

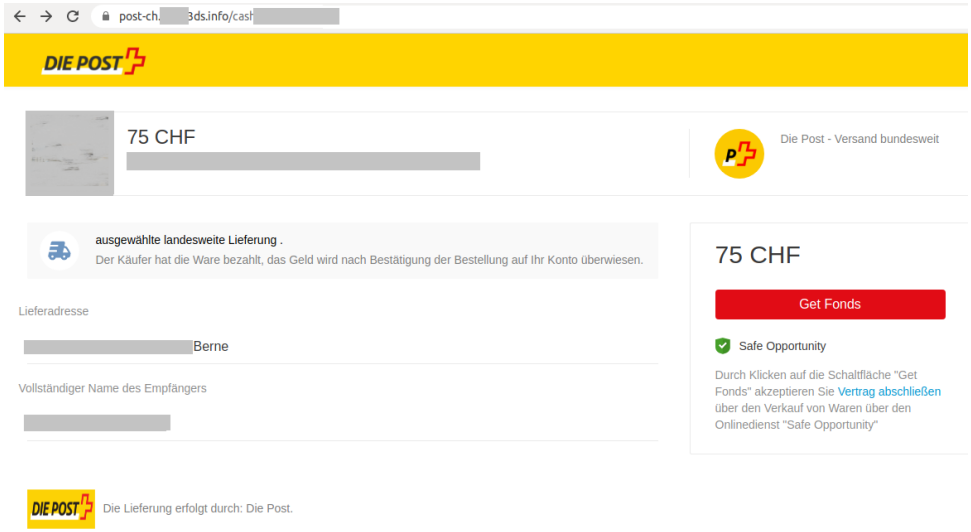


Fig. 4: Pagina web personalizzata con l'indirizzo del venditore e un'immagine del prodotto.

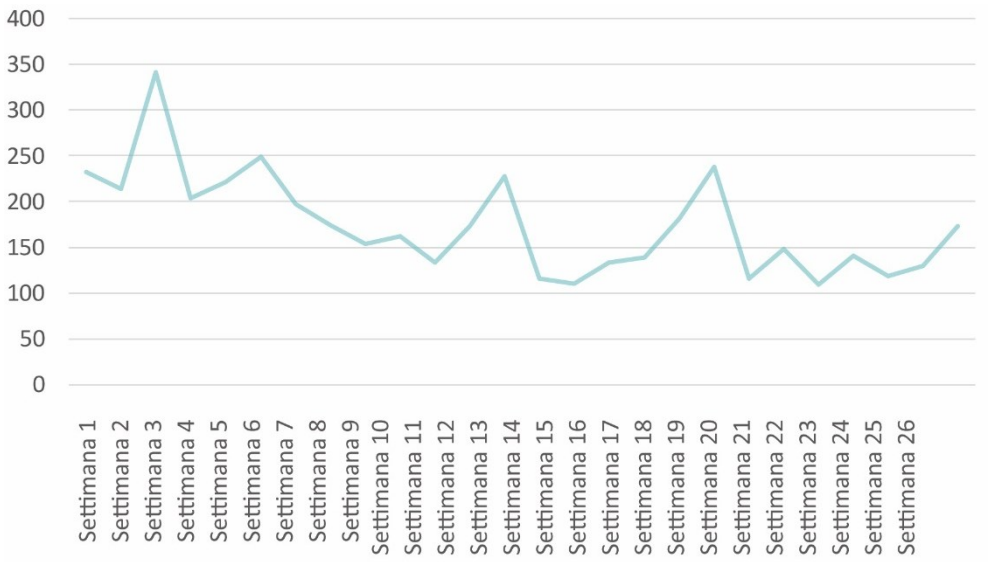


Fig. 5: URL di phishing verificati e confermati dall'NCSC ogni settimana nel primo semestre del 2022. Per i dati aggiornati consultare la pagina: https://www.govcert.admin.ch/statistics/phishing.

4.4 Segnalazioni di malware e hacking

Nel primo semestre del 2022 in totale sono state registrate 255 segnalazioni di malware, con un calo del 20 per cento rispetto al periodo precedente. Non vi sono quindi state grandi ondate. Degne di nota sono due piccole ondate legate a FluBot osservate a marzo e a maggio che hanno fatto registrare complessivamente 56 segnalazioni. In questi casi le vittime hanno ricevuto un SMS che annunciava il presunto arrivo di un pacco. I messaggi in circolazione non erano tutti identici. Il link in fondo al testo rimandava a una pagina web dove la vittima veniva invitata a scaricare e installare sul proprio smartphone Android un software del corriere. Nel

mese di giugno gli inquirenti internazionali sono riusciti a bloccare la rete che si nascondeva dietro al trojan FluBot (v. n. 5.2.3).

Un'altra ondata di 30 segnalazioni ha riguardato il malware QakBot (noto anche come «QuakBot» o «Qbot»), diffuso tramite e-mail. In questi casi i cibercriminali spesso utilizzano scambi di e-mail tra l'azienda e i propri fornitori o clienti, ad esempio, a cui gli hacker hanno avuto accesso tramite precedenti attacchi, in modo da indurre il destinatario del messaggio ad aprire un allegato malevolo. Viene quindi scaricato sul sistema della vittima il malware che serve da varco per accedere alle reti aziendali (cfr. n. 5.1.2) e installare trojan di crittografia (o «ransomware»).

Rispetto al semestre precedente le segnalazioni di ransomware sono leggermente diminuite, passando da 91 a 83. Le famiglie di ransomware più diffuse sembrano essere state QLocker e Deadbolt, per i dispositivi NAS, oltre a LockBit 2.0, Sodinokibi e Conti. Sono invece aumentati i casi di hacking (da 139 a 184 segnalazioni); la maggior parte delle segnalazioni ha riguardato account di social media (ben 91 su Facebook, Instagram e Twitter).

5 Eventi / situazione

5.1 Accesso iniziale

Ottenere l'accesso ai sistemi informatici da remoto o agli account degli utenti solitamente è la prima tappa per la maggior parte dei ciberattacchi. Soltanto in questo modo, infatti, gli hacker possono arrivare al loro vero obiettivo, sia esso l'utilizzo illecito del sistema o dell'account per frodi, l'acquisizione illecita di dati o l'installazione di ransomware. L'accesso iniziale può essere ottenuto in vari modi.

5.1.1 Nome utente / password

Quando l'accesso a un account o un sistema è protetto soltanto dal nome utente (che spesso corrisponde all'indirizzo e-mail) e dalla password per gli hacker è molto semplice infiltrarsi. In questi casi basta infatti un semplice phishing all'indirizzo e-mail per carpire la password e accedere all'account o al sistema. L'hacker ottiene così un accesso completo e può utilizzare tutte le funzionalità a disposizione del legittimo utente dell'account o del sistema, anche se quest'ultimo non è online.

Inoltre, se l'accesso è protetto soltanto da nome utente e password e le stesse credenziali vengono utilizzate per più account, c'è il rischio che vengano hackerati tutti questi account. I cibercriminali, infatti, spesso utilizzano anche il «credential stuffing», ovvero provano a utilizzare le credenziali rubate per tutti i servizi più diffusi (fornitori di posta elettronica, Twitter, Facebook, Instagram, Amazon, ecc.). Una volta verificate, le credenziali sono rivendute.

Conclusione / raccomandazione

Utilizzando un'autentificazione a due o più fattori è possibile proteggersi da questa minaccia.

L'incaricato federale della protezione dei dati e della trasparenza (IFPDT) ha partecipato alla redazione di un rapporto[22] e delle linee guida[23] della Conferenza internazionale degli incaricati della protezione dei dati («Global Privacy Assembly», GPA) sul credential stuffing.

5.1.2 Malware (trojan)

Un'altra strategia utilizzata per ottenere un accesso non autorizzato consiste nell'utilizzo di un software dannoso che apre un varco nel sistema. Come il cavallo di Troia del mito greco, una volta introdotto furtivamente nel sistema, il malware apre una breccia che consente agli hacker di installare altri software dannosi. Per indurre gli utenti a cliccare su un link o ad aprire il file che contiene il trojan, i truffatori ricorrono a varie strategie di ingegneria sociale. Fra i sentimenti su cui solitamente si fa leva in questi tentativi di manipolazione vi sono la curiosità, il timore di essersi persi qualcosa o ancora lo stress dato dall'urgenza.

Oggi la maggior parte dei trojan è in grado di caricare e installare altri malware (ad es. Emotet[24], Qakbot[25] e Formbook/XLoader[26]). Esistono però ancora trojan che fanno soprattutto degli screenshot o registrano i dati immessi dalla tastiera (i cosiddetti «keylogger»). In seguito inviano regolarmente le credenziali (ma anche i dati della carta di credito e altre informazioni) all'hacker, oppure le salva online nelle cosiddette «drop zone», da dove poi i criminali possono recuperarli. Nel periodo in oggetto un trojan di questo tipo molto attivo è stato Snake Keylogger.[27]

Conclusione / raccomandazione

Il vettore più utilizzato per diffondere trojan continua a essere la posta elettronica. Spesso le e-mail riguardano argomenti quotidiani come offerte, consegne o fatture. A volte invece per stuzzicare la curiosità degli utenti facendo leva su informazioni esclusive concernenti temi di attualità come la pandemia, la guerra in Ucraina, catastrofi naturali o eventi sportivi. In molti casi, poi, per spingere chi riceve l'e-mail a compiere determinate azioni senza riflettere troppo, si fa credere che sia necessario agire in fretta.

Non cliccate mai su link inviati con e-mail sospette e non aprite mai gli allegati.

22 22-06-27-Credential-Stuffing-General-Public-Awareness.pdf (globalprivacyassembly.org)
23 22-06-27-Credential-stuffing-guidelines.pdf (globalprivacyassembly.org)
24 Emotet (fraunhofer.de)Emotet (fraunhofer.de); Emotet Botnet C&Cs (abuse.ch); URLhaus | emotet (abuse.ch).
25 QakBot (fraunhofer.de); Qakbot Botnet C&Cs (abuse.ch); URLhaus | Qakbot (abuse.ch);
v. anche rapporto semestrale 2021/2 (ncsc.admin.ch), n. 4.2.3.
26 Formbook (fraunhofer.de); Xloader (fraunhofer.de); URLhaus | Formbook (abuse.ch).
27 404 Keylogger (fraunhofer.de); URLhaus | SnakeKeylogger (abuse.ch) .

5.1.3 Sfruttamento delle vulnerabilità

Le vulnerabilità di un software e una configurazione errata creano delle falle che possono essere sfruttate come accesso diretto o indiretto. I sistemi direttamente raggiungibili da Internet sono maggiormente esposti a questo rischio, perché in ogni caso non sono o possono essere protetti da un ulteriore livello di sicurezza.

Un software che fa regolarmente parlare di sé dall'inizio del 2021 per le sue vulnerabilità è Microsoft Exchange.[28] Dopo il grande clamore suscitato nel marzo 2021, sono state rese note altre vulnerabilità. Questo software per server di messaggistica è utilizzato da molte aziende, pertanto offre agli hacker un bacino di potenziali vittime molto ampio, dato che non tutti i responsabili di sistemi installano subito gli aggiornamenti disponibili. Altre porte che i cibercriminali sfruttano di frequente per infiltrarsi nelle reti sono i software per l'accesso remoto e i firewall non aggiornati.[29]

Le piattaforme gestite su cloud sono a rischio e in presenza di misure di protezione inadeguate, configurazioni errate o vulnerabilità del software possono subire attacchi. Lo stesso può accadere con le interfacce utente («web interface») di sistemi controllati o gestiti da remoto.

Conclusione / raccomandazione

Non appena viene resa nota una vulnerabilità di un prodotto, diversi attori iniziano a perlustrare la rete alla ricerca dei sistemi esposti e dopo poche ore o qualche giorno iniziano a sfruttare la falla.

Privati e aziende dovrebbero quindi mantenere sempre aggiornati i software su tutti i loro dispositivi, possibilmente attraverso la funzione di aggiornamento automatico.

L'NCSC informa regolarmente le organizzazioni esposte ad attacchi a causa di sistemi non aggiornati.[30] Questi suggerimenti vengono forniti da specialisti nel campo della cibersicurezza che setacciano Internet alla ricerca dei sistemi a rischio. Allo stesso modo anche i criminali possono individuare e attaccare i sistemi vulnerabili. I gestori dei sistemi non dovrebbero quindi aspettare di ricevere un avviso da parte dell'NCSC. Raccomandiamo caldamente di dotarsi di un proprio sistema efficiente di gestione dei software, con un inventario e procedure per gli aggiornamenti.[31] Occorre intervenire al più tardi quando l'organizzazione riceve una lettera raccomandata dall'NCSC.

---

28 V. rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.1.1.
29 V. rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.1.2.
30 È giunta l'ora di correggere le vulnerabilità di Microsoft Exchange Server (ncsc.admin.ch); Microsoft Exchange presenta ancora lacune (ncsc.admin.ch).
31 V. rapporto semestrale 2021/1 (ncsc.admin.ch), n. 3.2.

5.2 Software dannosi / malware

5.2.1 Situazione generale

Il grafico seguente mostra le famiglie di malware che l'NCSC ha analizzato e identificato lo scorso semestre. Individuati grazie a varie fonti come sensori, segnalazioni da parte di responsabili della sicurezza di infrastrutture critiche, cittadini e PMI, i file e i codici vengono analizzati e attribuiti a una famiglia di malware. In seguito, l'NCSC trasmette gli indicatori di compromissione («indicators of compromise», IOC) trovati ai gestori delle infrastrutture critiche, in modo che possano adottare misure adeguate.

Analisi delle famiglie di malware

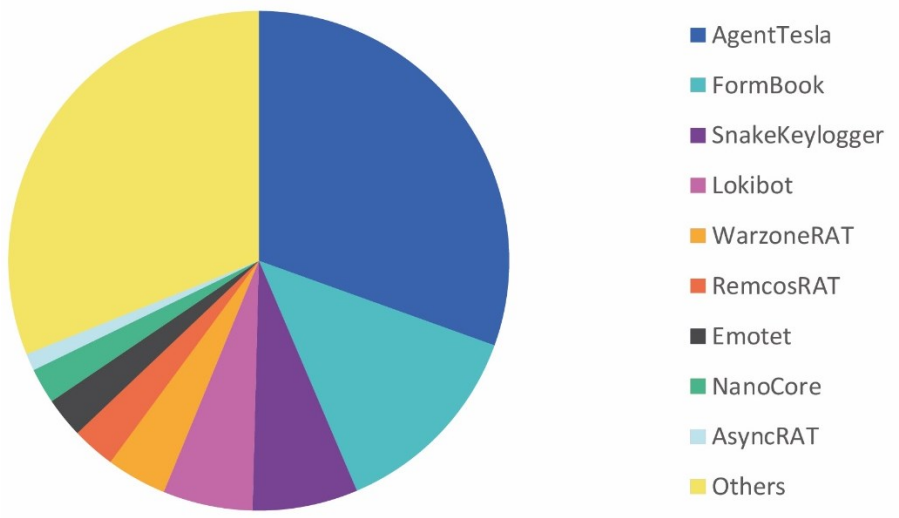


Fig. 6: Famiglie di malware in Svizzera analizzate dall'NCSC nel primo semestre del 2022.

Il grafico seguente mostra le famiglie di malware identificate in Svizzera nel periodo in esame attraverso analisi di dati provenienti da server DNS sinkhole. Questi ultimi permettono di difendersi perché impediscono ai malware di accedere ai domini presi di mira 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.

Infezioni da malware

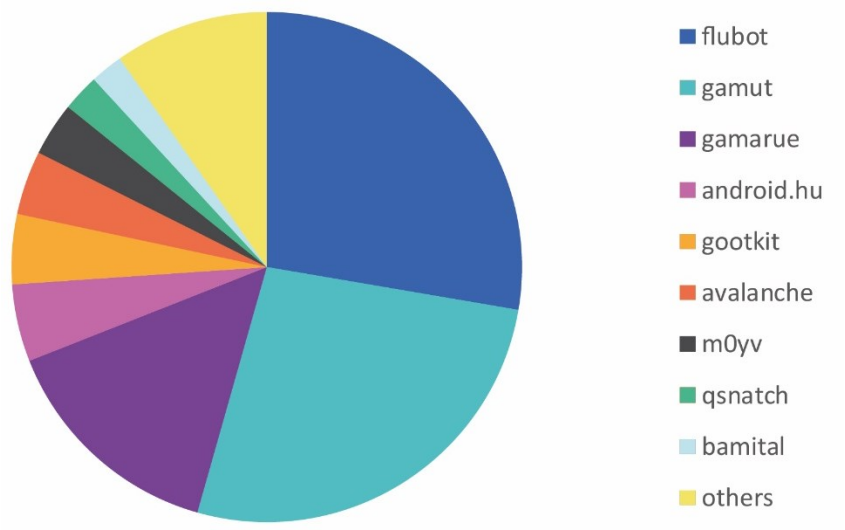


Fig. 7: Ripartizione delle infezioni da malware in Svizzera rilevate dall'NCSC nel primo semestre del 2022.

5.2.2 Ransomware

Anche quest'anno i cibercriminali hanno condotto campagne di ransomware. Attualmente in tutto il mondo nessun settore è al riparo da attacchi di questo tipo[32] e i ransomware[33] continuano a essere la minaccia informatica più temuta a cui sono esposte le organizzazioni in Svizzera.

5.2.2.1 Incidenti in Svizzera

Dall'inizio dell'anno, diverse organizzazioni attive in vari settori sono state vittima di attacchi in Svizzera.[34]

In ambito sanitario spesso i malviventi fanno ricorso al sistema della doppia estorsione («double extortion») utilizzando il ransomware LockBit 2.0,[35] che permette di copiare i dati sensibili della vittima e poi di crittografarli sul sistema preso di mira. Diverse organizzazioni del settore sanitario svizzero, quindi, oltre a trovarsi i propri server crittografati, hanno anche dovuto affrontare i problemi connessi alla fuga di dati. Spesso le informazioni sono finite sul dark web. A essere colpiti da questi attacchi, quindi, non sono soltanto le istituzioni, ma indirettamente anche i pazienti, perché i dati sottratti, oltre ai dati personali, spesso comprendono anche informazioni sensibili come le cartelle cliniche.[36]

---

32 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)

33 Ransomware (ncsc.admin.ch); What Is Ransomware? (trellix.com)

34 Hackerangriff auf Schweizer Spitalverband (inside-it.ch); Hackerangriff auf Swissport sorgt für Verspätungen im Flugbetrieb (computerworld.ch); Cyberangriff auf Luzerner ÖV bleibt ohne grössere Folgen (inside-it.ch); Cyberattaque contre Emil Frey: des données publiées sur le darkweb (ictjournal.ch); Ransomware-Attacke: «BlackByte» hackt Schweizer Logistikkonzern (watson.ch); Le pire est survenu: les données volées à l'Université de Neuchâtel ont été publiées (letemps.ch)

35 Hacker veröffentlichen erneut sensible Schweizer Gesundheitsdaten (inside-it.ch)

36 Des hackers diffusent les données médicales de Neuchâtelois (watson.ch)

In settori come il trasporto e la logistica, dal cui funzionamento dipendono molti altri settori, i malviventi cercano di perturbare il più possibile le attività operative per mettere la vittima sotto pressione e spingerla a pagare il riscatto chiesto.[37] Nel caso di Swissport, la gestione della continuità operativa e i backup hanno consentito di limitare le ripercussioni per altre aziende.[38]

Nel settore della formazione, a febbraio 2022 l'Università di Neuchâtel è stata vittima di un attacco ransomware. Questo evento ha quanto meno portato ad accelerare l'implementazione delle misure di sicurezza che il Cantone aveva già pianificato dopo i ciberattacchi ai danni dei comuni vodesi di Rolle e Montreux.[39] Tali misure comprendono principalmente test di sicurezza («penetration test») ripetuti e un miglior sistema di riconoscimento precoce degli attacchi.[40]

Gli esempi menzionati sono solo una parte degli attacchi ransomware registrati in Svizzera dall'inizio dell'anno. Per un elenco completo a livello nazionale e internazionale è possibile consultare vari media.[41]

5.2.2.2 Incidenti all'estero

Attacchi a governi e autorità

Da aprile 2022 in America Latina varie autorità governative hanno subito attacchi ransomware a cui si presume abbiano partecipato anche attori russofoni.[42] Costa Rica, Perù, Messico, Ecuador, Brasile e Argentina sono tra i Paesi che hanno condannato l'invasione dell'Ucraina da parte della Russia in occasione dell'Assemblea generale delle Nazioni Unite. Dopo un attacco, in Costa Rica è addirittura stato necessario dichiarare lo stato di emergenza. Tra gli autori degli attacchi ai danni dei governi sudamericani figuravano tra gli altri gruppi ransomware come Conti, ALPHV/BlackCat, LockBit e BlackByte. Il 24 maggio i sistemi informatici dello stato austriaco della Carinzia sono stati colpiti da un attacco ransomware a opera del gruppo BlackCat che ha provocato alcune interruzioni dei servizi statali.[43]

Attacchi a infrastrutture energetiche

In Europa dalla fine di gennaio 2022 diversi terminal petroliferi nei Paesi Bassi e in Belgio (Amsterdam, Rotterdam e Anversa), ma anche in Germania (Oiltanking GmbH) hanno avuto problemi di tipo informatico a causa di vari attacchi ransomware.[44] Gli esperti di sicurezza informatica di questi Paesi hanno spiegato che non hanno motivo di ritenere che questi attacchi siano collegati tra loro.[45] Gli incidenti hanno riguardato circa dieci terminal petroliferi in totale in tutto il mondo che hanno subito interruzioni dei servizi.[46] Si ritiene che in questi incidenti siano coinvolti i gruppi ransomware russi BlackCat e Conti.[47]

---

37 The future of cyber security: Ransomware groups aim for maximum disruption (darktrace.com)
38 BlackCat ransomware gang claims responsibility for Swissport attack (computerweekly.com)
39 Neuchâtel a amélioré sa cybersécurité (rtn.ch)
40 Cyberattaque: le canton a pris des mesures (swissinfo.ch)
41 The terrifying list of cyber attacks worldwide (konbriefing.com);
Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste (watson.ch).
42 Latin American Governments Targeted By Ransomware (recordedfuture.com)
43 Hackerangriff auf Land Kärnten: "Black Cat" will fünf Millionen Dollar in Bitcoin (derstandard.at)
44 Des cyberattaques signalées contre des sites portuaires en Allemagne, en Belgique et aux Pays-Bas (lemonde.fr)
45 String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say (therecord.media)
46 Oil terminals in Europe's biggest ports hit by a cyberattack (securityaffairs.co)
47 BlackCat ransomware implicated in attack on German oil companies (zdnet.com)

5.2.2.3 Panoramica degli attori più attivi

Conti e i suoi successori

Nel maggio 2022 il famigerato gruppo russo Conti[48] ha interrotto le proprie attività.[49] Dopo aver assicurato il suo appoggio alla Russia all'inizio dell'invasione dell'Ucraina, in primavera il gruppo ha fatto molto parlare di sé[50] quando un insider ha fatto trapelare le chat interne dei suoi membri, che hanno permesso di svelare come opera il gruppo.[51] L'evento, oggi conosciuto come «Conti leaks»,[52] e una serie di prese di posizioni politiche hanno spinto il gruppo a sciogliersi. Vari membri si sono riorganizzati in gruppi più piccoli specializzati in determinate fasi degli attacchi ransomware, come l'accesso alle reti o il furto di dati.[53] Ad esempio, tra le tattiche, tecniche e procedure («tactics, techniques, and procedures», TTPs) di Conti e dei nuovi gruppi come BlackBasta[54] e BlackByte[55] vi sono varie similitudini. BlackBasta si è fatto notare già ad aprile, quando nel giro di poche settimane è riuscito a infettare con un malware decine di aziende in tutto il mondo.[56] Le analogie tra questo gruppo e Conti riguardano i blog per la pubblicazione dei dati rubati, le pagine di pagamento, i portali di recovery, la comunicazione con le vittime e i metodi di negoziazione.[57] Nel caso di BlackByte, invece, i ransomware hanno funzioni e caratteristiche molto simili a quelle di Conti.[58]

Il nuovo gruppo BlackCat

Comparso per la prima volta nel novembre 2021, BlackCat, conosciuto anche come ALPHV, è operato dall'omonimo gruppo, composto da ex membri della famigerata organizzazione BlackMatter/DarkSide[59]. Questo ransomware ha elevate capacità di adattamento e offre vari metodi e opzioni di crittografia, pertanto può essere utilizzato per attaccare molti tipi diversi di aziende (in particolare di grandi dimensioni).[60] Una delle particolarità del modello di servizio applicato è data dal fatto che il nome della vittima non viene reso immediatamente pubblico nelle prime fasi dell'estorsione, sul data leak site viene soltanto fornita una descrizione dell'organizzazione colpita. In alternativa viene creato un sito nascosto, il cui indirizzo viene inviato soltanto alla vittima per verificare la veridicità di quanto affermato. In questo modo i malviventi danno ai loro bersagli la possibilità di trattare in modo riservato sul riscatto, ma mantengono la pressione minacciando di pubblicare i dati tenuti «in ostaggio».[61] Se il gruppo decide di

---

48 The Conti Enterprise: ransomware gang that published data belonging to 850 companies (group-ib.com); The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs (securelist.com).
49 Conti ransomware finally shuts down data leak, negotiation sites (bleepingcomputer.com); Ransomware-Gang Conti schließt Leak- und Verhandlungsplattform (heise.de).
50 Conti ransomware gang backs Russia, threatens US (techtarget.com)
51 Inside Conti leaks: The Panama Papers of ransomware (therecord.media)
52 Conti-nuation: methods and techniques observed in operations post the leaks (nccgroup.com)
53 Conti ransomware shuts down operation, rebrands into smaller units (bleepingcomputer.com); Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com).
54 Shining the Light on Black Basta (nccgroup.com)
55 Threat Spotlight: The BlackByte ransomware group is striking users all over the globe (talosintelligence.com)
56 New Black Basta ransomware springs into action with a dozen breaches (bleepingcomputer.com)
57 New Black Basta Ransomware Possibly Linked to Conti Group (securityweek.com)
58 Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
59 Aggressive BlackCat Ransomware on the Rise (darkreading.com)
60 Threat Assessment: BlackCat Ransomware (paloaltonetworks.com)
61 Ransomware gangs now give victims time to save their reputation (bleepingcomputer.com)

rendere pubblici i dati, utilizza un normale sito web e non una pagina del dark web. In questo modo può raggiungere un pubblico più ampio. Inoltre, anche le persone che hanno subito danni dalla fuga di dati messa in atto ai danni della vittima, ma non particolarmente esperti a livello tecnologico (come dipendenti e clienti), possono verificare se i propri dati sono stati compromessi e scaricare tutti i dati e i documenti rubati all'azienda.[62]

Il ritorno di REvil e Cl0p

L'inizio del 2022 è stato caratterizzato dalla comparsa di nuovi gruppi ransomware, ma anche dal ritorno di vecchie conoscenze.

La famigerata organizzazione ransomware REvil è tornata in attività alla fine di aprile con una nuova infrastruttura e un ransomware di nuova concezione.[63] La banda aveva interrotto le proprie attività nell'ottobre 2021 e nel gennaio successivo un'azione di polizia coordinata tra Stati Uniti e Russia aveva portato all'arresto dei suoi membri in Russia.[64] Stando a quanto dichiarato da fonti russe, la comunicazione tra i due Paesi si sarebbe interrotta dopo l'attacco militare della Russia all'Ucraina e in più il governo americano non avrebbe inoltrato sufficienti informazioni per poter incriminare i responsabili.[65]

Anche il gruppo Cl0p, dopo alcuni mesi di presunta inattività, è tornato in azione nel mese di aprile. I ricercatori se ne sono accorti dopo che il gruppo ransomware in un solo mese aveva aggiunto 21 nuove vittime sul proprio data leak site.[66]

LockBit

Il gruppo responsabile del ransomware-as-a-service (RaaS)[67] LockBit quest'anno ha già provocato numerosi incidenti.[68] Sul suo data leak site vengono sempre menzionate le presunte vittime e un conto alla rovescia indica quando saranno pubblicati i dati sottratti. Più volte, però, si è scoperto che gli annunci fatti da LockBit non erano troppo attendibili. Ad esempio, l'attacco che sostenevano di aver organizzato ai danni del ministero della giustizia francese, in realtà, aveva preso di mira uno studio legale di Caen.[69] Allo stesso modo, la presunta fuga di dati ai danni della società americana di sicurezza informatica Mandiant non è mai avvenuta.[70] A volte sembra che il gruppo voglia principalmente attirare l'attenzione. Non bisogna però sottovalutare la forza distruttiva di questo gruppo, poiché soltanto in Europa in un semestre vi sono state un centinaio di vittime al mese.[71]

---

62 Ransomware gang publishes stolen victim data on the public Internet (helpnetsecurity.com)
63 REvil ransomware returns: New malware sample confirms gang is back (bleepingcomputer.com)
64 Russia takes down REvil hacking group at U.S. request - FSB (reuters.com)
65 REvil prosecutions reach a 'dead end,' Russian media reports (cyberscoop.com)
66 Clop ransomware gang is back, hits 21 victims in a single month (bleepingcomputer.com)
67 Il «ransomware as a service» (RaaS) è un modello di business che coinvolge gestori di ransomware e loro partner e nel quale quest'ultimi pagano per poter lanciare attacchi con i ransomware sviluppati dai gestori. Tale strategia può quindi essere considerata una variante del modello di servizio «software as a service» (SaaS); Ransomware as a Service (RaaS) Explained (crowdstrike.com)
68 LockBit overtakes Conti as most active ransomware group so far in 2022 (scmagazine.com)
69 Ministère de la Justice : Le groupe Lockbit publie des données, mais pas les bonnes (zdnet.fr)
70 Mandiant: "No evidence" we were hacked by LockBit ransomware (bleepingcomputer.com)
71 Ransomware LockBit : une centaine de victimes par mois au premier semestre (lemagit.fr)

Il ransomware utilizzato viene aggiornato regolarmente, come un normale software. La versione 2.0 è comparsa nel giugno del 2022[72] e nel frattempo è già in circolazione la versione 3.0.[73]

Conclusioni, previsioni e raccomandazioni

Il numero di attacchi ransomware quest'anno è destinato ad aumentare ulteriormente e a colpire sempre di più anche infrastrutture critiche. La Cybersecurity and Infrastructure Security Agency (CISA) statunitense nel 2021 aveva già registrato un aumento di casi ben architettati organizzati ai danni di infrastrutture critiche e con conseguenze importanti.[74] Nel 2021 infatti le tecnologie e le strategie dei ransomware si erano evolute e questo aveva portato non soltanto a un avanzamento della tecnologia, ma anche a un aumento della minaccia rappresentata dai ransomware per le organizzazioni di ogni settore in tutto il mondo.[75]

Nonostante lo scoppio della guerra in Ucraina abbia indotto delle riorganizzazioni nel mondo della cibercriminalità, gli attori ransomware hanno dimostrato tutta la loro resilienza. Alcuni gruppi si sono sciolti, altri si sono formati dal nulla, altri ancora si sono dati un nuovo nome o, quando necessario, hanno sostituito alcuni capi (ad es. se la pressione esercitata dalle autorità di perseguimento penale era troppo elevata o se le divergenze di opinioni in merito alla guerra in Ucraina disturbavano la collaborazione all'interno di un gruppo).

Oltre alle misure di cibersicurezza, che proteggono i sistemi dalle infezioni tramite malware e, in generale, anche ransomware, esistono anche misure che possono essere adottate a un livello più profondo rispetto alla prima linea difensiva. Analizzando alcuni ransomware, i ricercatori hanno individuato delle «falle» che possono essere sfruttate per evitare almeno la crittografia finale dei dati.[76]

I ransomware possono causare ingenti danni, soprattutto quando interessano anche i sistemi di protezione dei dati (backup). Sul sito web dell'NCSC sono riassunti alcuni suggerimenti per la gestione di questi incidenti: Sono vittima di un attacco ransomware. E adesso? (ncsc.admin.ch).

Inoltre, l'autorità statunitense per la cibersicurezza (CISA) ha pubblicato dei suggerimenti per aiutare le imprese a evitare e rispondere agli attacchi ransomware.[77]

5.2.3 Mobile malware

Dopo l'ultima grande ondata registrata nell'autunno del 2021, dal 18 marzo 2022 in Svizzera è tornato a circolare il malware FluBot. Attraverso degli SMS, i cibercriminali cercavano di convincere la vittima a installare il software dannoso sullo smartphone. La campagna ha preso di mira i dispositivi Android in tutto il mondo.[78] In Svizzera sono circolati soprattutto SMS frau-

72 LockBit 2.0: How This RaaS Operates and How to Protect Against It (paloaltonetworks.com)
73 LockBit 3.0: Significantly Improved Ransomware Helps the Gang Stay on Top (darkreading.com)
74 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)
75 Ransomware: Over half of attacks are targeting these three industries (zdnet.com)
76 Conti, REvil, LockBit ransomware bugs exploited to block encryption (bleepingcomputer.com)
77 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)
78 New FluBot and TeaBot campaigns target Android devices worldwide (bleepingcomputer.com)

dolenti che annunciavano l'arrivo di un pacco, mentre a livello internazionale sono stati osservati anche SMS con il testo «Sei tu nel video?» e falsi inviti ad aggiornare il browser o il sistema operativo. L'NCSC ha trattato questo argomento nella retrospettiva della settimana 12.[79]

FluBot si è inoltre specializzato nel furto di SMS dai cellulari allo scopo di scovare le «one-time password» (OTP o «password usa e getta»). Dopo che il dispositivo è stato infettato, l'intero elenco dei contatti viene inviato al server di controllo degli aggressori. Il cellulare riceve poi una serie di numeri di telefono presi da altri dispositivi hackerati a cui inviare l'SMS dannoso. Nel primo semestre del 2022 l'NCSC ha ricevuto in totale 56 segnalazioni relative a FluBot.

All'inizio di maggio la polizia olandese è riuscita a smantellare l'infrastruttura di FluBot e il ceppo del malware è stato disattivato. L'azione però è stata possibile soltanto grazie al complesso lavoro di indagine a cui hanno preso parte le autorità di perseguimento penale di Australia, Belgio, Finlandia, Ungheria, Irlanda, Spagna, Svezia, Svizzera, Paesi Bassi e Stati Uniti. Le attività internazionali sono state coordinate dal Centro Europeo contro il Cybercrimine (EC3) dell'Europol.[80] Da allora in Svizzera non sono state più rilevate altre attività legate a FluBot.

Raccomandazioni

- Non installate mai sul vostro smartphone app offerte da piattaforme diverse dagli store ufficiali.
- In particolare, raccomandiamo di non installare app suggerite attraverso un link ricevuto per SMS o con un altro servizio di messaggistica (WhatsApp, Telegram, ecc.).

79 Settimana 12: Il malware FluBot è di nuovo attivo in Svizzera (ncsc.admin.ch)
80 Takedown of SMS-based FluBot spyware infecting Android phones (europol.europa.eu)

5.2.4 Botnet CyclopsBlink: intralciato il successore di VPNFilter

A maggio 2018 la società di sicurezza informatica Cisco Talos ha pubblicato le ultime scoperte sul malware VPNFilter,[81] che infettava soprattutto i router del settore SOHO («Small Office Home Office») e i dispositivi NAS («Network Attached Storage»). Dopo il sequestro di gran parte dell'infrastruttura di VPNFilter da parte del Dipartimento di giustizia americano[82], le attività attribuite al gruppo Sandworm[83] sono nettamente diminuite.

La sera prima dell'attacco russo all'Ucraina, le autorità di sicurezza britanniche[84] e americane hanno pubblicato alcuni dettagli sul presunto successore della botnet CyclopsBlink, che infettava principalmente dispositivi Watchguard e router Asus[85].

I gestori dei dispositivi colpiti, alcuni dei quali anche in Svizzera, sono stati informati dai rispettivi fornitori di servizi Internet o dal CERT nazionale.[86] Nel caso di alcuni dispositivi di comando della botnet i cui gestori non avevano adottato le misure necessarie, il Dipartimento di giustizia americano si è attivato e ha eliminato il malware sulla base di una decisione giudiziaria in questo senso.[87]

In questo modo la comunità occidentale di esperti di cibersicurezza ha potuto indebolire efficacemente la struttura alla base degli attacchi di Sandworm ed evitare, o quanto meno ostacolare, potenziali ulteriori attacchi, come descritto nelle parti dedicate al tema principale (n. 3.1 e 3.2) e ai sistemi di controllo industriali (n. 5.4.1).

Raccomandazioni

Sul sito web dell'NCSC sono pubblicate alcune raccomandazioni destinate a utenti finali e gestori di dispositivi dell'Internet delle cose (IoT) per l'utilizzo sicuro dei dispositivi.

5.3 Attacchi a siti e servizi web

I problemi di disponibilità dei siti web provocati da attacchi DDoS restano un fenomeno costante tanto in Svizzera quanto all'estero. Nel primo semestre del 2022 l'NCSC ha ricevuto dieci segnalazioni di incidenti di questo tipo da varie PMI svizzere attive in settori diversi. Questi attacchi possono essere scagliati con l'intento di estorcere denaro, per danneggiare imprese concorrenti, ma anche per motivi politici.

Stando a quanto riportato dalle società specializzate in sicurezza informatica operative a livello mondiale, nonostante si registrino attacchi sempre più potenti (fino a 1,4 Tbit/s) e complessi (grazie alla combinazione di varie strategie),[88] la stragrande maggioranza degli attacchi DDoS

---

81 New VPNFilter malware targets at least 500K networking devices worldwide (thalosintelligence.com)
82 Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (justice.gov)
83 Sandworm (Threat Actor) (fraunhofer.de)Sandworm (Threat Actor) (fraunhofer.de); v. anche n. 3.1 e 3.2.2.
84 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)
85 Cyclops Blink Sets Sights on Asus Routers (trendmicro.com)
86 Shadowserver Special Reports – Cyclops Blink (shadowserver.org)
87 Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (justice.gov)
88 DDoS attacks becoming larger and more complex, finance most targeted sector (helpnetsecurity.com)

continua a essere di modesta intensità (inferiori ai 10 Gbit/s).[89] Oltre alla velocità di trasferimento dei dati è importante prendere in considerazione anche altri fattori, come i pacchetti al secondo (pps) e le richieste al secondo (rps). Cloudflare, ad esempio, ha registrato un attacco con 26 milioni di richieste al secondo proveniente da una botnet piccola ma con elevate capacità in questo senso con appena 5067 dispositivi.[90]

Nella guerra di aggressione all'Ucraina, un gruppo di hacktivisti filorussi e anti-NATO che si fa chiamare Killnet da aprile 2022 ha lanciato una serie di attacchi DDoS contro i Paesi che sostenevano l'Ucraina attraverso la fornitura di armi, denaro e sanzioni. Le vittime di questi attacchi sono state, solo per fare qualche esempio, i siti dell'ONU, dell'OSCE, della NATO ma anche di organizzazioni con sede in Ucraina, Repubblica Ceca, Estonia, Lettonia, Lituania, Germania, Norvegia, Polonia, Romania, Gran Bretagna, Italia e Stati Uniti. Nel mirino degli hacker sono finiti molti aeroporti,[91] diverse autorità, banche, società ferroviarie, gruppi energetici e fornitori di servizi Internet (v. anche n. 3.3).

Conclusione / raccomandazioni

L'NCSC consiglia di sottoscrivere un abbonamento a un servizio di protezione contro gli attacchi DDoS («DDoS mitigation service»). Molti fornitori di servizi Internet offrono questo tipo di servizi.

Sul sito web dell'NCSC sono riportate varie misure che possono essere adottate per prevenire e proteggersi dagli attacchi DDoS: Attacchi alla disponibilità (DDoS) (ncsc.admin.ch)

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

Nel quadro di conflitti geopolitici, di tanto in tanto si osservano anche sabotaggi informatici distruttivi.[92] Per fare in modo che questi abbiano anche ripercussioni concrete sui processi, quasi sempre è necessaria anche una manipolazione della tecnologia operativa o dei relativi sistemi di comando. Questi attacchi richiedono molto tempo e risorse, ma solitamente portano più facilmente a dei risultati se si inseriscono nell'ambito di un conflitto già arrivato allo scontro armato con l'impiego di mezzi cinetici (v. tema principale al n. 3.2.2 su Industroyer2).

5.4.1 Pipedream / Incontroller: strumenti d'attacco OT

Il giorno dopo la diffusione delle informazioni sull'attacco tramite Industroyer2 (v. n. 3.2.2), diverse autorità statunitensi hanno diramato un avviso congiunto con i dettagli su un'altra serie di strumenti d'attacco modulari[93] che avrebbero potuto essere impiegati per sabotaggi informatici contro società energetiche e organizzazioni attive in settori simili. La comunicazione è stata effettuata a scopo preventivo, prima dell'utilizzo concreto di una delle varianti di malware descritte.

89 DDoS threats growing in sophistication, size, and frequency (helpnetsecurity.com)
90 Cloudflare mitigates 26 million request per second DDoS attack (cloudflare.com)
91 Russia-Ukraine: malicious cyber activity targeting aviation entities (ospreyflightsolutions.com)
92 In merito a Stuxnet v. in particolare rapporto semestrale 2010/2 (ncsc.admin.ch), n. 4.1 e 5.1, e riguardo a Triton/Trisis v. rapporto semestrale 2017/2 (ncsc.admin.ch), n. 5.3.2.
93 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)

Il governo statunitense ha preparato la pubblicazione degli strumenti di cibersabotaggio scoperti in collaborazione con due società americane di sicurezza informatica specializzate in sistemi industriali, che avevano denominato questa raccolta di malware Pipedream[94] e Incontroller[95]. Il rapporto preventivo ha fatto seguito a una serie di precedenti rivelazioni concernenti infrastrutture d'attacco principalmente russe. Oltre a limitare il potenziale di impiego degli strumenti di attacco scoperti, l'amministrazione Biden rende note le capacità offensive dei potenziali attacchi contro i gestori di infrastrutture critiche nazionali anche per sottolineare l'urgenza di adottare in tempi brevi le misure di protezione raccomandate con lo slogan «Shields Up»[96].

5.4.2 ICEFALL: 56 vulnerabilità OT

L'appello a far ricorso a dispositivi di difesa multilivello non è dettato soltanto dalle nuove conoscenze riguardo le capacità degli hacker[97] che attaccano i sistemi di controllo industriali, ma anche dalla preparazione in parte non sufficientemente sicura della tecnologia impiegata. La società di sicurezza informatica Forescout, ad esempio, ha pubblicato la raccolta «ICEFALL»[98] con 56 vulnerabilità rilevate in noti prodotti OT. L'ICS-CERT della CISA pubblica costantemente nuove raccomandazioni di sicurezza[99] di diversi produttori. Per rimanere aggiornati su questi temi può essere utile fare ricorso al Common Security Advisory Framework (CSAF), sviluppato dal Cyber Defence Campus (CYD) di armasuisse in collaborazione con gli esperti dell'autorità tedesca per la sicurezza nell'ambito della tecnologia dell'informazione («Bundesamt für Sicherheit in der Informationstechnik», BSI).[100]

Conclusione / raccomandazioni

Gli strumenti di attacco e le vulnerabilità scoperti di recente mostrano che è necessario investire per garantire la sicurezza degli accessi ai sistemi di controllo industriali e monitorare l'esercizio e le manipolazioni. In questo modo, se si sospetta siano state apportate modifiche indebite, si può intervenire tempestivamente.

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

94 CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) (dragos.com)
95 INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple ICS (mandiant.com)
96 Shields Up (cisa.gov)
97 Three new ICS threat groups discovered, one primed to disrupt energy targets (scmagazine.com)
98 OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT (forescout.com)
99 ICS-CERT Advisories (cisa.gov)
100 Proficua collaborazione tra il Cyber Defence Campus e la BSI (admin.ch)

5.5 Vulnerabilità

5.5.1 Log4Shell

La vulnerabilità Log4Shell, già citata nel rapporto dell'NCSC relativo al secondo semestre del 2021, continua a essere attuale. Nel primo semestre del 2022 è stata sfruttata soprattutto per attaccare e compromettere i server VMware su cui non erano installate le patch.[101]

Questa vulnerabilità per sua natura può essere nascosta in un'applicazione o in un sistema che non è sotto la diretta responsabilità del team di sicurezza di un'organizzazione. Pertanto è difficile individuarla ed eliminarla.

Recentemente, il Cyber Safety Review Board del Dipartimento della sicurezza interna statunitense in un rapporto ha affermato che «l'evento Log4j non può considerarsi risolto. La commissione ritiene che si tratti di una "vulnerabilità endemica" e che nei sistemi potrebbero rimanere istanze vulnerabili di Log4j ancora per molti anni, probabilmente per un decennio o anche di più. Il rischio quindi continua a essere elevato.»[102]

Conclusione / raccomandazioni

Dal momento che questo tipo di vulnerabilità può penetrare nell'infrastruttura di un'organizzazione attraverso software messi a disposizione da fornitori terzi, all'interno di un'organizzazione si raccomanda di sviluppare le capacità per tenere un inventario preciso degli asset e delle applicazioni IT, eseguire in via prioritaria gli aggiornamenti dei software e investire nelle risorse necessarie per individuare eventuali sistemi vulnerabili. Il rapporto del Cyber Safety Review Board contiene anche raccomandazioni dettagliate su Log4Shell.

5.5.2 Follina

Il 31 maggio 2022 Microsoft ha segnalato una vulnerabilità denominata «Follina», identificata dal numero CVE-2022-30190. Questa falla permette, anche se la macro è disattivata, di eseguire un codice da remoto tramite MSDT (uno strumento di diagnostica di Microsoft) quando un documento viene aperto nelle applicazioni della suite Office o viene visualizzato in anteprima. Microsoft era stata informata di questa lacuna nel marzo del 2021. Il numero CVE però è stato assegnato soltanto quando la vulnerabilità era già stata sfruttata.

Ricercatori specializzati in sicurezza informatica hanno pubblicato online varie tecniche di difesa e identificazione degli attacchi, ma la vulnerabilità è stata risolta soltanto in occasione del «Patch Tuesday» dello scorso mese di giugno.

Una cronologia dettagliata degli eventi, dall'individuazione fino all'attuazione delle misure di difesa, documenta come la vulnerabilità sia stata sfruttata prima che venisse resa nota.[103]

---

101 Log4Shell Vulnerability Targeted in VMware Servers to Exfiltrate Data (threatpost.com)
102 CSRB Report on Log4j - Public Report - July 11 2022_508 Compliant (cisa.gov)
103 Follina — a Microsoft Office code execution vulnerability (doublepulsar.com)

Conclusione / raccomandazioni

Nel caso di Follina, i dettagli necessari per un exploit sono stati resi noti prima che fosse disponibile una patch ufficiale e quando la vulnerabilità era già stata sfruttata da diversi attori. In una situazione come questa, per le imprese e le organizzazioni è importante mantenersi sempre informati, analizzare le raccomandazioni più recenti e, se necessario, adottare misure volte a limitare i rischi fino a quando non viene resa disponibile e può essere installata una patch ufficiale.

Come sempre, raccomandiamo di adottare procedure consolidate per quanto riguarda la sicurezza informatica. I collaboratori che hanno ricevuto un'adeguata formazione sono in grado di riconoscere le e-mail pericolose e sanno che non devono scaricare o eseguire eventuali allegati possono contribuire a sventare questo tipo di attacchi.[104]

5.5.3 Confluence

Il 2 giugno 2022 Atlassian ha pubblicato un bollettino di sicurezza su una vulnerabilità critica del suo software Wiki Confluence a cui è stato attribuito il numero CVE-2022-26134.[105] Un exploit riuscito permetteva di eseguire da remoto qualsiasi codice sui server di Confluence. Al momento della pubblicazione del bollettino non era ancora disponibile una patch, sebbene i dettagli che consentivano un exploit fossero noti e la vulnerabilità venisse sfruttata attivamente. Nel bollettino si raccomandava pertanto di limitare quanto prima l'accesso alle istanze di Confluence da Internet o di disattivarle fino a quando la vulnerabilità non fosse stata eliminata.

La patch è stata pubblicata il giorno successivo. La vulnerabilità è stata sfruttata in almeno un caso di ransomware in Svizzera.

Conclusione / raccomandazioni

Come già accaduto nel caso di Follina, la vulnerabilità CVE-2022-26134 è stata sfruttata in modo attivo prima che fosse disponibile una patch ufficiale. È importante quindi reagire rapidamente e seguire le raccomandazioni, che possono comportare anche la disattivazione del sistema, fino a quando non è disponibile una patch ufficiale.

Una strategia chiara per l'accesso diretto via Internet alle interfacce di gestione e alle applicazioni interne può ridurre la superficie esposta agli attacchi di un'organizzazione. Se vi sono applicazioni sensibili che devono essere raggiungibili da Internet, l'accesso deve essere protetto in modo particolare (tramite VPN con autenticazione a due fattori, un elenco degli IP autorizzati alla manutenzione, ecc.). Se per una vulnerabilità sfruttata attivamente non esiste ancora una patch, una buona gestione degli accessi dall'esterno permette di guadagnare tempo per adottare le misure di difesa. Questo però non esonera dall'installazione delle patch non appena sono disponibili.

---

104 Gestione sicura della posta elettronica (admin.ch)

105 Confluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 (atlassian.com)

5.6 Fughe di dati

5.6.1 Per proteggere i dati bisogna garantirne la sicurezza

Le fughe di dati mettono in una situazione spiacevole tutti coloro che sono coinvolti. Nessuno vuole che le proprie informazioni personali o riservate vengano rese pubbliche, o dover dire a qualcuno che i suoi dati sono stati rivelati. Ciononostante, le fughe di dati sono sempre più frequenti, a causa di una scarsa protezione o manutenzione dei sistemi, di errori umani o di attacchi con finalità criminali. Quando si verificano attacchi ransomware vi è anche la possibilità che gli autori, per avere un ulteriore motivo di ricatto, sottraggano dati da un sistema. In questi casi, in un secondo tempo le persone interessate possono anche subire minacce dirette da parte dei criminali. Questa strategia è detta «triplice ricatto»: quando l'azienda che ha subito l'attacco non vuole pagare né per la decodifica né per evitare la pubblicazione dei dati, a volte gli estorsori si rivolgono direttamente alle persone interessate minacciandole di pubblicare determinati dati o attraverso attacchi personali di ingegneria sociale molto mirati. Questo rappresenta un rischio soprattutto nel caso di dati personali sensibili, come i dati clinici di un paziente. Sul sito dell'NCSC sono disponibili delle misure per le imprese in caso di fuga di dati.

Commento

In Svizzera non vi è ancora l'obbligo legale di notificare le violazioni della sicurezza dei dati o le fughe di dati. Tuttavia, in futuro i gestori di infrastrutture critiche dovranno informare le autorità in caso di ciberattacchi e anche la nuova legge federale sulla protezione dei dati prevede un obbligo di notifica o d'informazione.

5.6.2 Lapsus$

Il gruppo di cibercriminali Lapsus$ ha fatto molto parlare di sé alla fine del 2021 per i numerosi attacchi in Sud America e Portogallo. Durante uno di questi attacchi il gruppo ha sottratto oltre 50 TB di dati al Ministero della salute brasiliano prima di cancellarli dai server.[106] In un altro attacco è stata presa di mira Impresa, il principale gruppo mediatico portoghese. I criminali, dopo aver deturpato il sito ufficiale hanno chiesto un riscatto e durante le trattative è emerso che il gruppo criminale era riuscito anche ad accedere al cloud dell'azienda.[107] In entrambi i casi Lapsus$ ha chiesto denaro per restituire i dati o non pubblicarli. Nei primi mesi del 2022 il gruppo ha guadagnato ancora più popolarità dopo gli attacchi andati a segno ai danni di grandi società tecnologiche internazionali come NVIDIA,[108] Samsung,[109] Vodafone,[110] Ubisoft,[111] Microsoft[112] e Okta[113]. A seguito di questi attacchi una serie di dati sensibili delle società interessate è stata

106 Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes (zdnet.com)
107 Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel (therecord.media)
108 NVIDIA confirms data was stolen in recent cyberattack (bleepingcomputer.com)
109 Hackers leak 190GB of alleged Samsung data, source code (bleepingcomputer.com)
110 Vodafone Investigating Source Code Theft Claims (securityweek.com)
111 Ubisoft Cyber Security Incident Update (ubisoft.com)
112 DEV-0537 criminal actor targeting organizations for data exfiltration and destruction (microsoft.com)
113 Updated Okta Statement on LAPSUS$ (okta.com)

resa nota. Successivamente, però, Lapsus$ avrebbe subito un contrattacco da parte di NVIDIA e si sarebbe lamentato affermando che i dati del gruppo erano stati crittografati.[114] Alla fine di marzo in Gran Bretagna sette persone di età compresa tra i 16 e i 21 anni sono state arrestate in quanto ritenute potenziali membri del gruppo. Le accuse per due di loro sono state formalizzate all'inizio di aprile. Le attività del gruppo sono quindi diminuite e fino alla fine del primo semestre non sono pervenute altre segnalazioni. All'inizio della sua attività, Lapsus$ era considerato un gruppo che operava con ransomware, ma si limitava a sottrarre dati, a volte li cancellava anche, e in seguito ricattava le vittime minacciando di pubblicarli. Per ottenere l'accesso ai sistemi, Lapsus$ ha spesso utilizzato tecniche di ingegneria sociale per ottenere le credenziali[115]. Alcuni attacchi potrebbero anche essere stati facilitati da dipendenti delle aziende prese di mira (insider, minaccia dall'interno). Il gruppo aveva pubblicato un annuncio sul suo canale Telegram in cui offriva una grossa somma ai dipendenti delle aziende nei settori di suo interesse in cambio dell'accesso remoto alle VPN.[116] Questo canale Telegram è stato anche l'unica piattaforma pubblica del gruppo, utilizzata in alcuni casi dai membri per comunicare in tempo reale sulle loro attività, ed era seguito da oltre 60 000 follower. Riassumendo, quindi, nonostante la breve attività Lapsus$ è riuscito a mandare a segno numerosi attacchi ai danni di rinomate aziende e a sottrarre dati con mezzi modesti e tecniche poco sofisticate.

114 vx-underground on Twitter (twitter.com)
115 LAPSUS$: Recent techniques, tactics and procedures (nccgroup.com)
116 Lapsus$ Ransomware Group Announced Recruitment of Insiders (securityaffairs.co)