Il panorama degli zeroday e la ricerca svolta in TIM

Massimiliano Brolli, Elenia Cianfarani, Andrea Carlo Maria Dattola

Per vulnerabilità zeroday si intendono i bug di sicurezza di un prodotto non ancora conosciuti dal vendor, per i quali non è disponibile una patch correttiva. Oggi rappresentano uno dei rischi maggiori per la sicurezza informatica delle aziende e degli stati. Gli zeroday sono considerati dai cybercriminali e dalle entità governative delle risorse preziose, che consentono attraverso il loro sfruttamento di rubare dati, praticare attività di sorveglianza o spionaggio, oppure distruggere infrastrutture critiche. In questo articolo andremo ad analizzare queste "armi cibernetiche" andando ad esplorare cosa sono, i mercati che alimentano, il processo di divulgazione responsabile e le attività di ricerca che vengono svolte in TIM.

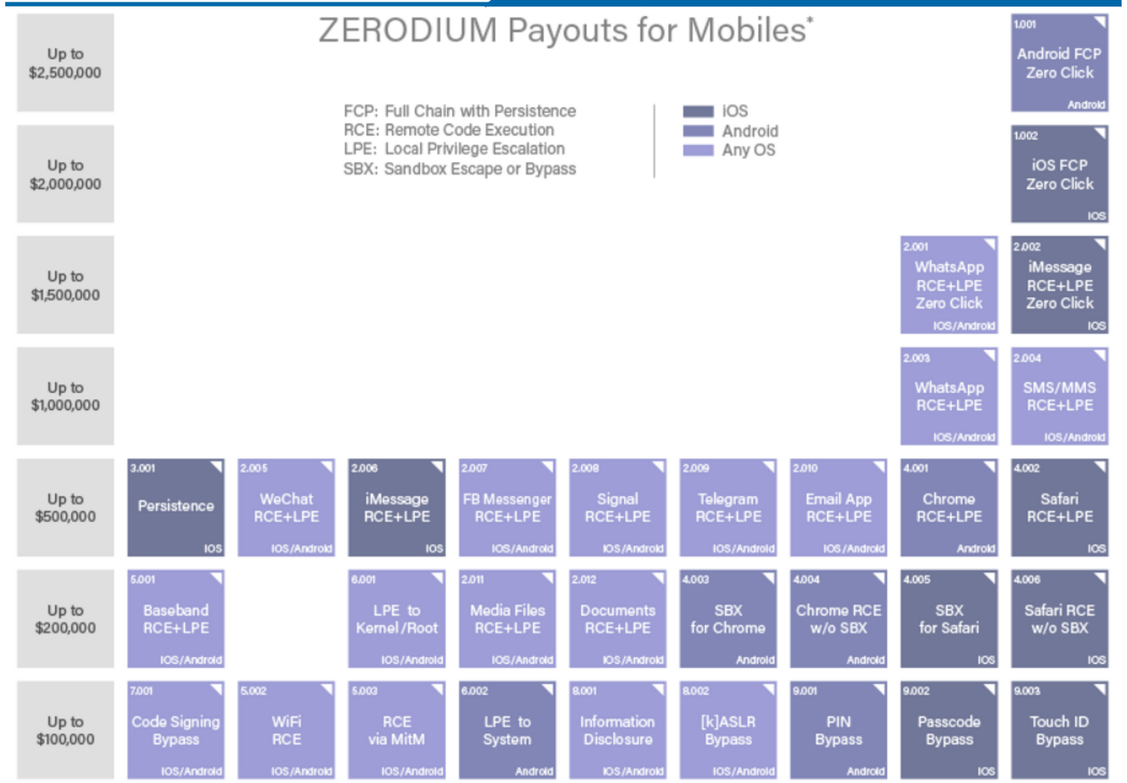
Cosa sono gli zeroday

Ogni prodotto hardware e software contiene del codice che a sua volta può contenere degli "errori" (o "falle di sicurezza" o semplicemente bug) che possono essere sfruttati da un malintenzionato per poter effettuare accessi illeciti ad una qualsiasi infrastruttura.
Tali "errori", sconosciuti al produttore del software ma conosciuti da un limitato numero di persone, vengono chiamati 0day.
Il nome deriva dal fatto che il fornitore ha 0 giorni per correre al riparo e quindi produrre una patch che consenta di rendere quell'errore non più sfruttabile da un ipotetico attaccante.

Zeroday tra etica e cybercrime

Come accennato nell'introduzione, le vulnerabilità zeroday sono molto pregiate. Una falla che consenta una totale compromissione di un dispositivo iPhone oggi può raggiungere il valore di circa tre milioni di euro.
Queste vulnerabilità possono essere sfruttate per accedere e compromettere completamente un dispositivo di un utente, come ad esempio avere il pieno accesso da remoto alla fotocamera e alle chat di uno smartphone. In sintesi, l'accesso a tutte le informazioni e le abitudini di una persona.
Va da sé che tali strumenti possono essere utilizzati per monitorare e sorvegliare le attività di un individuo, ma possono anche es-

Figura 1: Tabella dei pagamenti per exploit zeroday su dispositivi mobile disponibile sulla pagina web di Zerodium



sere utilizzati per interrompere un servizio come una filiera di produzione cartacea o addirittura un servizio idrico di una grande città.

Ricercatori di sicurezza

I bug 0day possono essere individuati dai "ricercatori di sicurezza", professionisti specializzati che esaminano attentamente il software per identificare vulnerabilità di sicurezza ancora sconosciute. Questi esperti, noti anche come "bug hunter", possono differire notevolmente l'uno dall'altro in base all'approccio etico che adottano nel loro lavoro.

I broker zeroday

I broker zeroday sono individui o aziende che si pongono come intermediari nell'acquisto e rivendita di vulnerabilità zeroday. Si è osservato negli ultimi anni che quello degli zeroday è un mercato in espansione e il prezzo di alcuni di essi, trattandosi di vulnerabilità difficili da reperire, può raggiungere anche milioni di dollari. Uno dei broker zeroday più noto è Zerodium, sito disponibile nel surface web che consente ad un bug hunter di vendere al broker gli exploit zeroday, ossia il codice (payload) di sfruttamento del bug (Fig.1).

Nel mercato degli intermediari zeroday sta emergendo anche un altro antagonista, Operation Zero, società russa che ha recentemente aumentato i pagamenti di alcuni exploit su dispositivi mobile, raggiungendo anche i 20 milioni di dollari, un valore decisamente più elevato rispetto a quello offerto da Zerodium.

Cybercrime da profitto

I bug hunter che decidono di non seguire la strada etica (in Fig.2 Gray Hat e Black Hat) possono rivolgersi a intermediari (zeroday broker) oppure mettere direttamente in vendita zeroday ed exploit zeroday su forum nel dark web. I loro clienti non sono solo criminali alla ricerca di guadagni illeciti; spesso gli exploit sono acquistati dagli stessi governi e dalle agenzie di intelligence per attività di spionaggio e sorveglianza. Per citare alcuni casi conosciuti in letteratura citiamo, Stuxnet ed Eternal Blue (si veda box approfondimento).

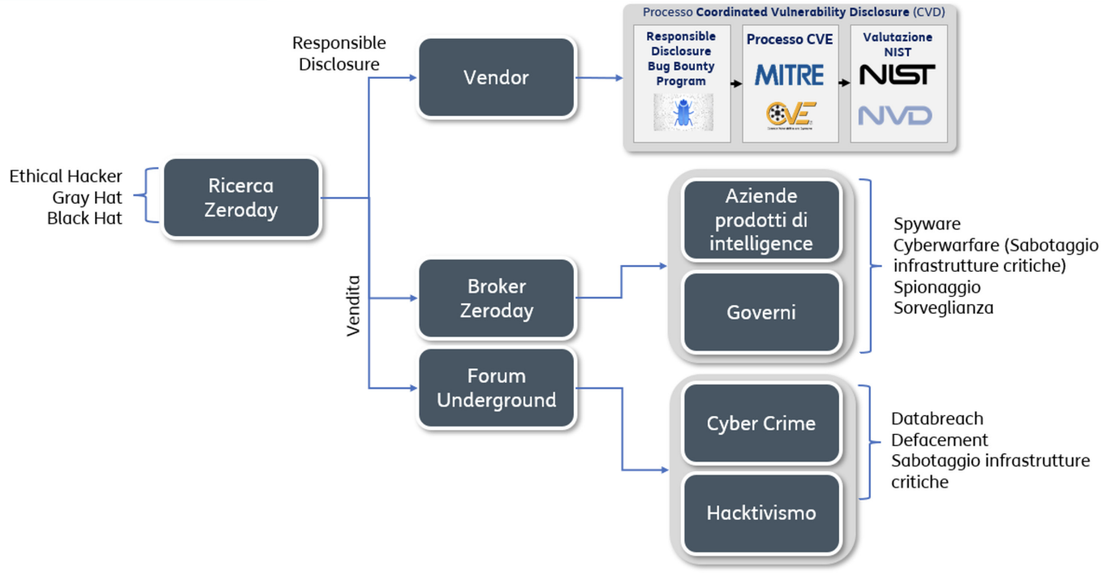
Inoltre, ci sono le aziende che producono sistemi di intelligence e che sono particolarmente interessate agli exploit zeroday no-click, ossia quelle preziose vulnerabilità che non richiedono l'azione degli utenti per entrare in azione.

Nello specifico tali bug consentono di installare spyware sui dispositivi senza alcuna interazione da parte degli utenti che li utilizzano sfruttando ad esempio una chiamata vocale WhatsApp non risposta (come nel caso di Pegasus, un potente spyware creato dall'azienda israeliana NSO Group). Queste aziende sfruttano il mercato degli 0day no-click per migliorare i loro prodotti e rivenderli ad agenzie di intelligence per eseguire operazioni mirate verso persone o paesi ostili.

Come abbiamo visto in precedenza, NSO Group è una azienda israeliana nota per aver sviluppato diversi spyware, come ad esempio Pegasus e Karma, utilizzati per la sorveglianza dei dispositivi mobile di giornalisti, dissidenti e attivisti in diversi paesi del mondo e nello spionaggio di stato. Oggi, è stato classificato come arma dallo stato d'Israele, pertanto, qualsiasi esportazione e utilizzo in paesi esteri deve essere approvata dal governo.

In conclusione, i vantaggi che si possono trarre dallo sfruttamento degli zeroday possono essere notevoli, sia dal punto di vista economico che dal punto di vista strategico, dipende dal vantaggio che vuole trarne l'attore che li utilizza. È da tenere in considerazione anche il rischio che si assume chi compra uno zeroday: potrebbe essere emessa una patch correttiva per quella vulnerabilità addirittura a distanza di poche ore dall'acquisto. Per questo generalmente vengono sfruttati dagli attaccanti verso target mirati, al fine di ridurre al minimo la possibilità che tali preziosi exploit possano essere intercettati.

Figura 2: Flusso di gestione di uno zeroday, dalla divulgazione responsabile alla vendita



La Coordinated Vulnerability Disclosure (CVD)

Esistono diversi modi per divulgare vulnerabilità zeroday: Coordinate Vulnerability Disclosure, divulgazione pubblica, divulgazione a terze parti o a programmi di bug bounty privati.

La Coordinated Vulnerability Disclosure è probabilmente la più etica, che prevede la comunicazione delle vulnerabilità zeroday da parte del bug hunter direttamente al vendor, in via confidenziale, consentendo al vendor stesso di emettere una patch di sicurezza prima della diffusione pubblica. La divulgazione etica rappresenta un vantaggio per l'intera comunità a discapito del cyber crime.

Nella CVD, i ricercatori che individuano una potenziale vulnerabilità zeroday, contattano il vendor del prodotto vulnerabile per segnalare il bug. Il quale, dopo un'analisi interna, può riconoscere o meno la vulnerabilità come zeroday e nel caso positivo avvia lo sviluppo di una patch correttiva; contestualmente, se il vendor non è una CNA (CVE Numbering Authorities), i ricercatori richiedono un identificativo univoco chiamato Common Vulnerabilities and Exposures (CVE) ad un ente no-profit degli Stati Uniti d'Ameri-

ca chiamato MITRE. Si tratta di un codice univoco che viene assegnato a ciascuna vulnerabilità. Nel momento in cui la patch di sicurezza viene rilasciata al pubblico, i ricercatori, in accordo con il vendor, procedono a richiedere al MITRE la divulgazione dello 0-day. Questo sarà disponibile pubblicamente nel National Vulnerability Database (NVD) statunitense con associata una Severity, ovvero una valutazione in scala 1 a 10 della criticità del bug di sicurezza rilevato.

Un cenno sui bug bounty program

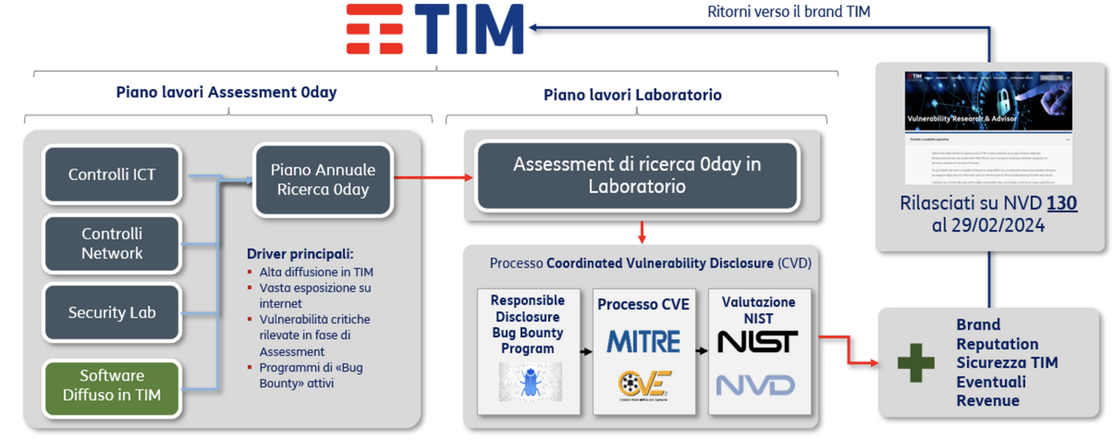
Alcune aziende hanno avviato dei programmi di bug bounty che gli hanno consentito di beneficiare delle competenze della comunità degli hacker etici. Nello specifico un programma di bug bounty è un programma promosso da un'azienda attraverso il quale fornisce una ricompensa, in denaro o altre forme di premi, a coloro che identificano e segnalano un bug di sicurezza non documentato sui prodotti dell'azienda. Le ricompense rilasciate sono molto inferiori ai guadagni che un hacker non etico potrebbe ottenere vendendoli in autonomia o attraverso un intermediario di vulnerabilità come visto in precedenza.

Il lavoro di ricerca in TIM

La storia e i numeri

A partire dalla fine del 2019, la funzione coordinata da Massimiliano Brolli all'interno della Security di TIM ha avviato il processo di Coordinated Vulnerability Disclosure (CVD) nell'ambito delle attività di ethical hacking (Red Team).
Il processo aderisce alla Coordinated Vulnerability Disclosure descritta sopra e prevede la divulgazione pubblica, previo consenso del vendor, quando sarà emessa la patch di sicurezza. Il processo adottato in TIM prevede che prima della pubblicazione, qualora il vendor non sia una CNA (e quindi capace di assegnare autonomamente le CVE) venga svolta una verifica in campo per valutare che la patch rilasciata dal vendor, ed installata sull'infrastruttura di TIM, sia stata efficace nella risoluzione del problema di sicurezza segnalato (Fig.3).
Fino a febbraio 2024 sono state inoltrate ai vendor 230 segnalazioni di bug zeroday, di cui 130 riconosciuti, risolti e pubblicati. In TIM cerchiamo sempre di promuovere con questi l'importanza della divulgazione responsabile delle vulnerabilità (Fig.4).

Figura 3: Processo di alimentazione della ricerca degli zeroday in TIM e Coordinated Vulnerability Disclosure



Infatti, questo processo adottato, oltre ad aiutare i vendor nell'identificazione di nuove vulnerabilità, comporta una serie di altri vantaggi:

- gli amministratori di sistema sono più solerti nell'installare una patch di sicurezza una volta che i dettagli dell'exploit sono stati resi pubblici;
- i fornitori di strumenti di protezione perimetrale potranno aggiornare le policy e far sì che il loro software intercetti e blocchi il "payload" ormai pubblico;
- i fornitori di soluzioni per l'esecuzione di Vulnerability Assessment potranno aggiornare il loro software al fine di rilevare le nuove vulnerabilità;
- altri vendor potranno prendere spunto e verificare se hanno replicato lo stesso problema di sicurezza su prodotti analoghi.

Cenni sulle vulnerabilità più critiche rilevate

Nel corso dell'attività di ricerca del Red Team di TIM si vogliono citare alcuni degli impatti più critici rilevati:

- un malintenzionato privo di credenziali, ma attestato nella rete TIM avrebbe potuto disabilitare le dorsali in fibra ottica di tutta TIM;
- un malintenzionato, con accesso alla rete aziendale, avrebbe potuto aprire qualsiasi varco all'interno degli edifici di TIM (compresi i data center);
- un malintenzionato avrebbe potuto manomettere la temperatura dei re-

Figura 4: Sintesi del lavoro di ricerca in TIM

frigeratori necessari alla corretta conservazione dei medicinali compromettendone l'utilizzo (vulnerabilità rilevata durante la pandemia per Covid-19 per cui è stato emesso uno speciale bollettino di sicurezza da CISA - Cybersecurity & Infrastructure Security Agency degli Stati Uniti d'America).

Principali tecniche per identificare gli zeroday

I ricercatori di sicurezza giocano un ruolo fondamentale nell'individuare vulnerabilità zeroday utilizzando una serie di strumenti e tecniche manuali sofisticate.
Generalmente il primo passo per scoprire una vulnerabilità zeroday è avere una comprensione approfondita del funzionamento interno del software e delle tecnologie che si intendono esaminare. Questo richiede una buona conoscenza dei linguaggi di programmazione, dei protocolli di comunicazione e delle architetture di sistema.
Esaminiamo adesso quali sono i metodi, le tecniche e le pratiche più comuni per trovare vulnerabilità zeroday per un bug hunter.

Analisi statica e dinamica

Le tecniche di analisi statica e dinamica sono fondamentali per individuare vulnerabilità nei codici sorgente e nei programmi in esecuzione. Gli strumenti di analisi statica esaminano il codice senza eseguirlo, cercando pattern ed errori comuni, come buffer overflow o problemi di gestione della memoria.
D'altra parte, l'analisi dinamica coinvolge l'esecuzione del software in un ambiente controllato, monitorando il suo comportamento per rilevare eventuali anomalie o vulnerabilità.
Tool comunemente usati:

- **analisi statica**: SonarQube, Fortify Static Code Analyzer, Checkmarx, Bandit (Python);
- **analisi dinamica**: Burp Suite, OWASP ZAP, Acunetix.

Reverse engineering

È una pratica comune tra i ricercatori di sicurezza per comprendere il funzionamento interno del software e identificare potenziali vulnerabilità. Questo processo coinvolge l'analisi dei file binari per comprendere la logica del programma, individuare funzionalità nascoste o vulnerabilità di sicurezza.
Tool comunemente usati:

- IDA Pro, Ghidra, Radare2, gdb, Cutter.

Fuzzing

Si tratta di una tecnica automatizzata utilizzata per scoprire vulnerabilità attraverso l'iniezione di dati casuali o semi-casuali nel software al fine di provocare errori o crash. Gli strumenti di fuzzing possono essere configurati per testare diversi input e scenari, esplorando il software in modo esaustivo alla ricerca di vulnerabilità.
Tool comunemente usati:

- AFL++(American Fuzzy Lop), Wfuzz, Hongfuzz, libFuzzer, Jazzer, OSSFuzz, Synopsys.

Penetration testing

È un'attività in cui un ricercatore di sicurezza simula un attacco informatico contro un sistema o una rete per identificare e sfruttare vulnerabilità. Anche attraverso questa metodologia, i Penetration Tester hanno la possibilità scoprire vulnerabilità zeroday.
Tool comunemente usati:

- Metasploit, Nmap, Nessus, BurpSuite, Sqlmap.

Conclusioni

La vendita delle vulnerabilità zeroday è considerata una pratica altamente controversa che fa molto discutere poiché considerata poco etica. Il commercio di tali vulnerabilità contribuisce alla ricchezza di pochi danneggiando molti. Per questo motivo in TIM ci battiamo per la divulgazione etica. Dal 2019 contribuiamo attivamente alla divulgazione etica e responsabile delle vulnerabilità zeroday, supportando i vendor nella risoluzione dei bug e diffondendo l'importanza della divulgazione etica delle vulnerabilità. Abbiamo supportato alcuni vendor, con cui collaboriamo, nell'adesione al programma CNA (CVE Numbering Authorities), sponsorizzandolo come un percorso di crescita e arricchimento sia per l'azienda stessa e soprattutto per i suoi clienti.■

Casi famosi nella storia

Stuxnet la prima arma cibernetica

Stuxnet è il nome di un worm che nel 2010 ha seriamente danneggiato la centrale nucleare iraniana di Natanz (Fig.A).
Spesso viene definita come la prima arma cibernetica della storia e ha segnato sicuramente un cambiamento epocale nel contesto geopolitico e nelle modalità di conduzione di una guerra.
Gli Stati Uniti erano preoccupati già da alcuni anni del programma nucleare che stava portando avanti l'Iran, dall'altra parte anche la vicina Israele stava chiedendo supporto per un bombardamento di tipo convenzionale verso i bunker iraniani. L'amministrazione Bush respinse questa richiesta, ma diede il via alla pianificazione di un cyber attacco.
L'operazione, nome in codice "Giochi Olimpici", vide coinvolti gli Stati Uniti in collaborazione con tecnici informatici israeliani e i servizi segreti olandesi. L'attacco ha sfruttato quattro zeroday Windows che hanno colpito i PLC Siemens che gestivano le centrifughe di arricchimento dell'uranio facendole andare fuori controllo e compromettendone il funzionamento.
Trattandosi di un programma nucleare segreto non sono noti i danni effettivi, ma la stima è che l'attacco abbia rallentato di diversi anni il programma nucleare iraniano.

Figura A: Centrifughe della centrale nucleare di Natanz in Iran

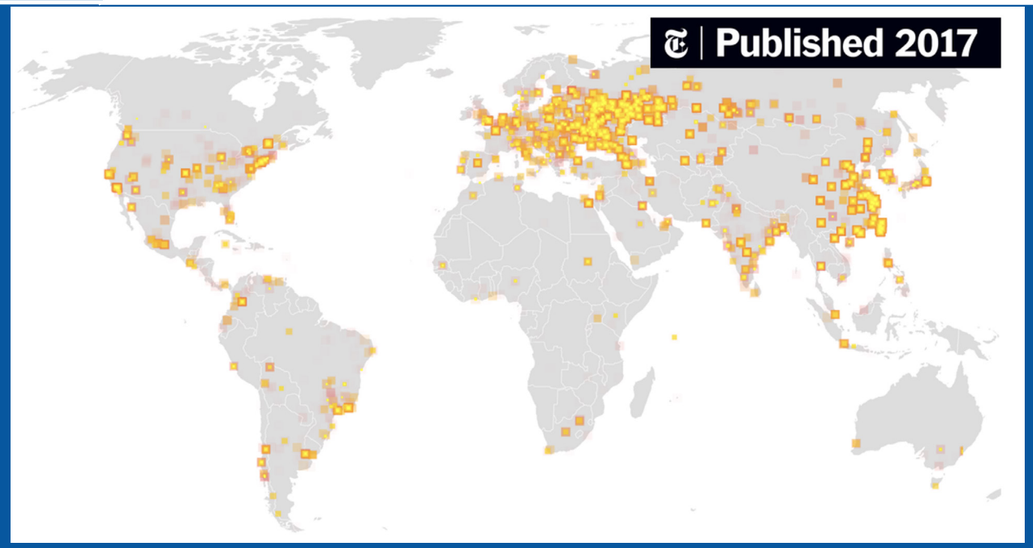
Lo zeroday nascosto dalla NSA

Nel maggio 2017 si diffuse a macchia d'olio nel mondo il malware WannaCry.
Tale malware utilizzava un potente 0day che era stato precedentemente rubato a una nota agenzia di intelligence statunitense: la National Security Agency (NSA).
WannaCray per diffondersi, utilizzava uno 0day chiamato EternalBlue che consentiva al malware di rendersi "wormable", ovvero espandersi da un computer windows ad un altro, avendo pieno accesso alle risorse del computer. Ma perché avvenne tutto questo?
Perché Microsoft, non conoscendo questo bug (e relativo exploit), non aveva aggiornato il servizio (nello specifico SAMBA) che risultava vulnerabile ad un attacco 0day. In sintesi, in quei giorni tutti i computer Windows del mondo erano vulnerabili a WannaCry (Fig.B).

Log4Shell – Lo zeroday che ha fatto tremare il mondo

Il 10 dicembre del 2021 è stata resa pubblica la vulnerabilità cosiddetta Log4Shell che consentiva, ad un attaccante remoto senza alcuna autenticazione, l'esecuzione di codice arbitrario su un server prendendone totale controllo.
La vulnerabilità era stata segnalata privatamente alla fine di novembre ad Apache, che l'aveva resa pubblica solo dopo aver emesso una patch che inizialmente era compatibile solo con un sottoinsieme di sistemi.
Il motivo per cui questa vulnerabilità ha sconvolto il mondo intero, oltre che per il livello di criticità massima ottenuta (10 su 10), era la sua scalabilità senza precedenti.
Il prodotto vulnerabile era ed è ampiamente diffuso a livello globale, e fino al momento della risoluzione della vulnerabilità qualsiasi sistema esposto su Internet che implementava il prodotto era un potenziale bersaglio.

Figura B: Mappa della propagazione di WannaCry nel mondo pubblicata da The New York Times (https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html)



Sitografia

- https://www.redhotcyber.com/post/full-disclosure-delle-vulnerabilita-l-arma-definitiva-a-prova-di-zona-grigia/
- https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-zero-day-cosa-sono-e-come-funziona-il-mercato-nero-degli-exploit/
- https://www.cve.org/
- https://zerodium.com/
- https://it.wikipedia.org/wiki/NSO_Group
- https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Acronimi

CISA	Cybersecurity and Infrastructure Security Agency
CNA	CVE Numbering Authorities
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
NSA	National Security Agency
NVD	National Vulnerability Database
PLC	Programmable Logic Controller

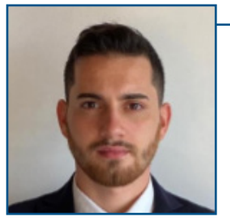
Autori

Massimiliano Brolli *massimiliano.brolli@telecomitalia.it*

Responsabile della funzione di Security Threat Management di TIM, è in azienda dal 2001, dopo aver maturato diversi anni di esperienza nell'ambito dello sviluppo software e aver avviato alcune startup innovative. In TIM ha ricoperto svariati incarichi entrando a far parte della struttura di Security nel 2008.
Attualmente coordina i gruppi di Cyber Threat Intelligence, Security Lab e il Red Team, dove ha sviluppato attività innovative di ricerca nell'ambito 4G/5G, protocolli di segnalazione e ha introdotto la ricerca di vulnerabilità zeroday in TIM. ■

Elenia Cianfarani *elenia.cianfarani@telecomitalia.it*

Cyber Security Specialist, entra a far parte del gruppo TIM nel 2019 ricoprendo il ruolo di Security Service Manager in Telsy, gestendo attività di ethical hacking principalmente in ambito Golden Power. Dal 2008 al 2019 ha lavorato per diverse multinazionali di consulenza, dove ha maturato esperienze in svariati ambiti della Cyber Security. Dal 2023 passa nella funzione Security Threat Management di TIM, dove attualmente dirige il processo di Coordinated Vulnerability Disclosure e le attività di Zeroday Research Assessment. ■



Andrea Carlo Maria Dattola *andreacarlomaria.dattola@telecomitalia.it*

Dal 2020 è un Penetration Tester/Ethical Hacker presso il Red Team di Telecom Italia (TIM), incluso nella funzione di Security Threat Management di TIM coordinata da Massimiliano Brolli. Ha conseguito la Laurea Magistrale in Ingegneria Informatica e dei Sistemi per le Telecomunicazioni. Attualmente si occupa di garantire la Sicurezza dei sistemi TIM attraverso attività di penetration testing sui prodotti aziendali e in Golden Power, ricerca sulle falle di sicurezza nei protocolli di segnalazione nell'ambito 4G/5G e ricerca di vulnerabilità 0day: ad oggi 17 CVE. ■