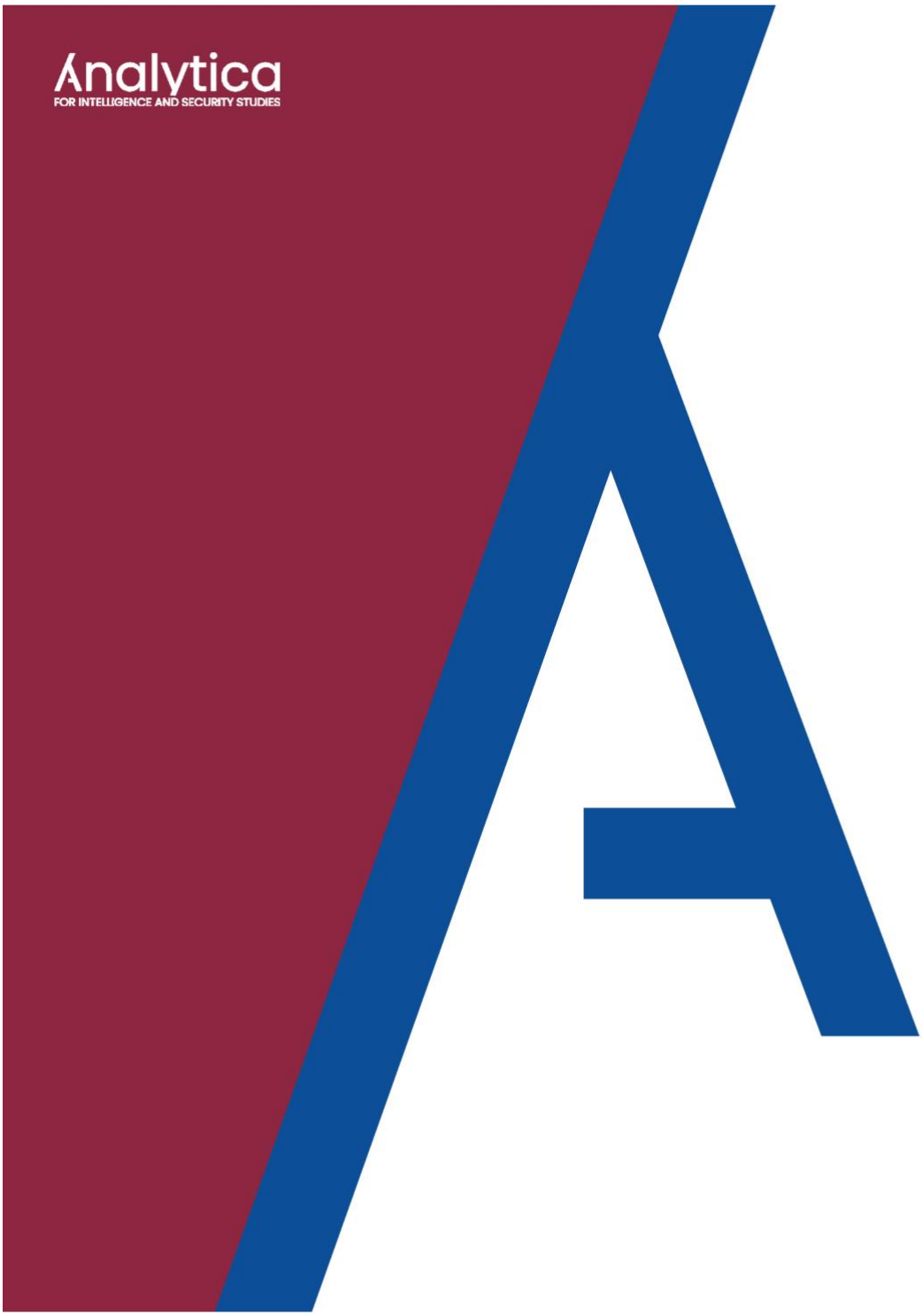

Resilienza del business: tra rischi tecnici e vulnerabilità unmane

Maniscalco Davide
Antonini Giulia – Molinari Giulia – Napoli Fabrizio – Parodi Irene

Analytica for intelligence and security studies

Paper Cyber-Security

Resilienza del business: tra rischi tecnici e vulnerabilità umane.

Maniscalco Davide
Antonini Giulia – Molinari Giulia – Napoli Fabrizio – Parodi Irene

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber - Security

Torino, giugno 2021

Sempre più numerosi sono gli attacchi di natura cyber ai danni di aziende: dalle PMI alle multinazionali, dal settore privato al pubblico, nessuno sembra esserne immune (o abbastanza preparato da non caderne vittima). I dati pubblicati nel Rapporto CLUSIT 2021, riportano un totale di 1871 cyber attacchi perpetrati ai danni di istituzioni, società bancarie e finanziarie, servizi cloud, infrastrutture critiche, ONG e altri. Nel 42% dei casi, i criminali hanno utilizzato dei malware per colpire il target; si tratta di un dato in costante aumento da alcuni anni. Di questi 783 episodi, il 67% vedeva l'impiego di ransomware. Negli ultimi anni, si è parlato spesso di aziende e istituzioni prese di mira dai cyber criminali con malware di questo tipo: per citarne alcuni, il recente attacco perpetrato dal gruppo Ragnarok ai danni dell'azienda di moda Boggi Milano, o i più famosi WannaCry e NotPetya.

Con il termine malware si intende un'ampia categoria di programmi e codici elaborati con lo scopo di mettere a rischio un sistema. I ransomware, invece, sono una tipologia di malware utilizzata per criptare sistemi e dati delle vittime per poi richiedere il pagamento di un riscatto in bitcoin per renderli nuovamente accessibili. Nell'ultimo anno, una nuova categoria di ransomware ha fatto il suo ingresso tra i metodi utilizzati per sferrare attacchi cyber: si tratta dei "double extortion ransomware", o ransomware a doppia estorsione. Si tratta di una modalità che unisce la richiesta di riscatto tipica dei ransomware, con il "data breach", ossia l'appropriazione di dati. I criminali, infatti, esfiltrano grandi quantità di file prima di criptarli, in modo da avanzare una duplice richiesta di riscatto: la prima per poter decrittare i documenti e la seconda per non diffonderli o venderli a terzi.

Recentemente, il team di Microsoft Security Intelligence ha dato la notizia della diffusione di un nuovo malware chiamato STRRAT. Si tratta di un particolare RAT (remote access trojan) che combina l'esfiltrazione dei dati di accesso ad account email e browser, il controllo da remoto e l'installazione di un keylogger con la (falsa) criptazione dei file e la richiesta di riscatto. È, dunque, un malware a tutti gli effetti che si camuffa da ransomware per poter operare indisturbato, spostando l'attenzione della vittima sui file criptati. I documenti, però, non sono realmente illeggibili: STRRAT, infatti, modifica l'estensione in .crimson come un normale ransomware ma senza criptare i file. Tuttavia, la vittima non si rende conto della truffa perché gli antivirus bloccano l'apertura dei file con tale estensione. Il rischio è che chi viene colpito da questi attacchi metta in atto le contromisure per rispondere ad un ransomware, come il ripristino dei file da backup cloud o fisico, senza rendersi conto che sarebbe bastato modificare l'estensione dei file per renderli di nuovo accessibili.

Inoltre, non si preoccupa di rimuovere il malware con dei software appositi poiché spesso non ne è a conoscenza.

Trattandosi di fenomeni in costante aumento ed evoluzione che lasciano dietro di sé conseguenze significative sia in termini economici che reputazionali, riteniamo sia importante analizzare nel dettaglio le minacce, i rischi e le contromisure necessarie per garantire la sicurezza dei sistemi e la continuità del servizio in caso di attacco. In questo paper verrà presentata una situazione di fantasia che però non si discosta molto da uno scenario realistico. Attraverso il seguente case study vogliamo portare alla luce le principali vulnerabilità che i cyber criminali sfruttano per perpetrare gli attacchi e le buone pratiche da seguire per aumentare il livello di sicurezza di un business.

Contesto

A gennaio 2021, la società estone di forniture militari MilitPRO ha comunicato di essere stata vittima di un ransomware.
Nel primo pomeriggio di mercoledì 13 gennaio, i dipendenti della divisione Amministrazione, Finanza e Controllo non riuscivano più ad accedere alla documentazione del dipartimento. Ad ogni tentativo di apertura dei file, compariva un pop-up nel quale la famosa organizzazione APT-HIKMA comunicava la criptazione dei documenti, chiedendo il pagamento di un riscatto in bitcoin per l'equivalente di 500.000 euro che sarebbe raddoppiato ogni 24 ore.
L'azienda, che fa parte della supply chain di forniture militari per il Ministero della Difesa estone, era dotata dei piani di Business Continuity, Disaster Recovery e Incident Handling, i quali hanno garantito il recovery dei processi primari di business e di backup per la continuità delle attività aziendali. Dopo aver messo in atto le contromisure necessarie per la mitigazione degli impatti, MilitPRO ha subito avviato un'indagine interna per risalire alla causa del ransomware, identificando la vulnerabilità nel capitale umano.

ANALISI DELL'ACCADUTO E DELLA MINACCIA

Il responsabile dell'ufficio di Amministrazione, Finanza e Controllo ha informato immediatamente il CISO dell'azienda riguardo l'accaduto. Una volta al corrente, il CISO si è prima occupato della mitigazione delle conseguenze per assicurare l'efficiente gestione dell'incidente e la business continuity dell'azienda, e, successivamente, di comprendere le cause dell'attacco.

1. Analisi dell'accaduto

Dato che l'attaccante è stato in grado di criptare i documenti, il CISO ha ipotizzato un'intrusione all'interno dell'account di uno dei dipendenti dell'ufficio. L'accesso può essere avvenuto sia in maniera fisica (attraverso il collegamento di un dispositivo all'interno di una parte del network dell'ufficio), sia attraverso il furto delle credenziali. Tenendo in considerazione questa seconda possibilità, la prima contromisura adottata è stata la modifica delle credenziali di accesso al sistema di tutti i dipendenti, in modo da evitare che l'hacker potesse rientrare nel network, qualora i dati fossero stati ottenuti in modo malevolo.

Allo stesso tempo, è molto importante che il CISO cominci subito un'analisi più approfondita per capire l'entità del danno. In particolare, si avvale dell'attività di code review che gli permette identificare la sequenza del ransomware. Inoltre, è anche di fondamentale importanza rilevare a quali livelli di privilegio hanno avuto accesso gli attaccanti. Al CISO è divenuto subito chiaro, analizzando i documenti criptati, che gli hacker hanno ottenuto le autorizzazioni da amministratore del sistema, poiché sono stati compromessi anche i file modificabili solo ed esclusivamente dagli amministratori. Questo ha reso il problema ancora più grave, perché implica la criptazione di file di massima importanza e riservatezza da parte degli attaccanti.

Proprio per questo motivo è stato essenziale individuare immediatamente quali documenti avrebbero potuto contenere informazioni personali e dati sensibili. Essendo l'azienda in questione il supplier di un'agenzia governativa, tale rischio era incredibilmente alto. In effetti, risultava che all'interno del materiale a cui gli hacker avevano avuto accesso, fossero presenti sia dati personali di subfornitori e privati, che documenti sensibili riguardanti il dipartimento della Difesa del governo estone. È stato compito del CISO e dei suoi collaboratori notificare immediatamente tutte le persone coinvolte.

Per assicurare un ritorno all'operatività (business continuity) il più celere possibile, dopo l'analisi dell'accaduto, le opzioni che si presentano sono quattro: la soluzione migliore è il ripristino dei file da un backup; in alternativa ci si può servire di un decryptor che però non si rivela sempre efficace; altrimenti si può decidere di non agire e di perdere i dati; oppure, in ultimissima ipotesi, si può accettare di pagare il riscatto. Il pagamento del riscatto, tuttavia, non garantisce in alcun modo l'effettiva decrittazione dei file, contribuendo invece al finanziamento di un'attività illegale. L'azienda in questione era ben organizzata e previdente, essendosi fornita di un ottimo sistema di back-up.

MilitPro, infatti, si era comportata virtuosamente poiché disponeva di due diversi tipi di archiviazione per lo storage backup dei dati: un backup schedulato su HD esterno e un cloud backup. Il primo è un supporto che resta sempre sconnesso e viene collegato al computer o alla rete solo per il tempo strettamente necessario alla creazione o all'aggiornamento del backup. Questo sistema è vantaggioso perché implica costi più bassi rispetto a un virtual server, ma, a differenza del secondo, comporta anche un tempo di ripristino delle attività più lungo. Per questo motivo, il CISO ha controllato per prime le versioni presenti sul cloud backup sperando che non fossero state infettate. Fortunatamente, i criminali non erano riusciti ad arrivare al cloud, anche grazie alla presenza di un sistema di accesso protetto ai dati di storage ed esclusivo solo all'Account Backup e all'utilizzo di un agent di connessione.

L'ultimo passaggio prima del ripristino dei dati, è stata l'eliminazione dei file infetti. Il CISO ha ripristinato i file attraverso lo storage backup e l'ufficio è stato poi in grado di proseguire con la normale attività lavorativa. Il procedimento ha richiesto diversi giorni ma la durata complessiva si è mantenuta coerente con il Recovery Time Object del BCP in uso.

2. Analisi della minaccia

Successivamente al ripristino dei dati criptati e all'aggiornamento delle credenziali per accedere alla VPN condivisa, l'azienda MilitPRO ha avviato due investigazioni parallele. La prima, un'analisi tecnica seguendo la procedura di code review per sincerarsi che il ransomware non fosse più presente e non fossero state lasciate back door durante l'attacco. La seconda ha riguardato, invece, tutto il personale dell'ufficio colpito.

Dall'analisi tecnica non sono emerse infiltrazioni o brecce potenzialmente in grado di eludere il sistema di sicurezza. Invece, durante le interviste fatte ai dipendenti, si è scoperto come un addetto alle relazioni con i subfornitori avesse ricevuto una mail sospetta qualche giorno prima dell'attacco.

Ulteriori controlli avvalorano l'ipotesi di un attacco phishing perpetrato attraverso la suddetta mail, inviata a nome del sub fornitore.

Il gruppo di hacker ha sfruttato l'utilizzo della VPN condivisa col subfornitore per accedere ad un più alto livello di privilegio, arrivando così ai dati sensibili riguardanti il Ministero della Difesa estone.
La mail in questione riportava l'impossibilità da parte del subfornitore ad accedere alla VPN. Cliccando sull'allegato (un PDF che, a quanto riportato nel testo della mail, mostrava lo screenshot della notifica di errore), il lavoratore ha dato all'attaccante l'accesso alle reti di processo e ai sistemi di controllo e monitoraggio delle attività svolte dall'ufficio.

Inoltre, la code review, iniziata subito dopo la riacquisizione dei file compromessi, ha rivelato che MilitPRO è stata attaccata da un malware STRRAT, non da un ransomware. Questo implica che il materiale interessato nell'attacco non è stato effettivamente reso illeggibile, il RAT ha modificato l'estensione in .crimson come un normale ransomware ma senza criptare i file. In più, è possibile che questi siano stati manipolati ed esfiltrati dagli attaccanti.
Vi è la possibilità che l'attacco sia stato perpetrato dal gruppo APT-HIKMA. Tale supposizione deriva dall'analisi dei codici del malware che riportano la stessa firma presente in un altro attacco risalente a 6 mesi prima, imputato appunto a questo gruppo di hacker attivo in Russia.
L'attacco ha imposto all'azienda MilitPRO di migliorare gli strumenti di filtering delle e-mail e di implementare un progetto di training per i dipendenti. Tutto questo sottolinea l'importanza di sviluppare, all'interno delle aziende, la consapevolezza dei pericoli cyber e la capacità di individuare le possibili minacce.

CONCLUSIONI

Il caso in questione evidenzia l'importanza del fattore umano nella difesa dagli attacchi informatici. Infatti, nonostante la compagnia MilitPro avesse preso tutte le precauzioni necessarie a prevenire un'eventualità del genere, l'impianto di sicurezza è stato compromesso tanto dall'apertura della e-mail infetta da parte di un dipendente, quanto dalla mancata notifica dell'hackeraggio subito dal subfornitore. Se quest'ultimo avesse informato tempestivamente la compagnia MilitPro, la soglia di attenzione del personale sarebbe stata più alta, rendendo improbabile il successo dell'attacco.

Inoltre, trattandosi di metodi in continua evoluzione, ci sono ancora poche informazioni riguardo lo STRRAT in questione e, pertanto, anche un basso livello di consapevolezza e di conoscenza di questo tipo di malware.

Secondo uno studio pubblicato da Kaspersky, effettuato su un campione di 5000 imprese provenienti da paesi diversi, il 52% degli intervistati individua nei propri dipendenti la maggior vulnerabilità dei sistemi di IT security. Uno staff negligente o privo di adeguata preparazione avrebbe contribuito al 46% degli attacchi informatici presi in esame, mentre nel 30% dei casi gli impiegati avrebbero agito consapevolmente contro i loro stessi colleghi. Nel 40% delle imprese, gli impiegati avrebbero nascosto l'attacco subìto.
Pertanto, si possono formulare tre ipotesi sul perché il subfornitore non abbia divulgato in tempo l'hackeraggio subito, compromettendo la sicurezza dell'azienda MilitPro:

1. Il subfornitore non era consapevole dell'hackeraggio. In tal caso, ciò dipenderebbe da un approccio poco virtuoso nei confronti della propria IT security, oppure, trattandosi di un'azienda di piccole dimensioni che lavora su commissione, dalle risorse disponibili per investire in IT security, senz'altro minori rispetto alla compagnia committente.
2. Gli impiegati dell'azienda subfornitore hanno consapevolmente nascosto l'hackeraggio ai propri superiori, forse temendo ripercussioni sul lavoro o semplicemente perché ne hanno sottostimato la portata.
3. Gli impiegati dell'azienda subfornitore hanno contribuito intenzionalmente all'attacco nei confronti della compagnia MilitPro. Trattandosi di aziende operanti nell'ambito delle forniture militari, è possibile che l'acquisizione da parte degli hacker di informazioni sensibili per il dipartimento della Difesa estone non sia stata accidentale, ma frutto di pianificazione. In tal caso, gli hacker avrebbero potuto servirsi di un complice nell'azienda subfornitore, ipotesi che diverrebbe plausibile qualora si dimostrasse il coinvolgimento di un governo straniero nell'operazione.

Comunque stiano le cose, una formazione adeguata e continua del personale può mitigare l'impatto del fattore umano sulla IT security, così come la condivisione di informazioni e tecnologie tra le aziende parte della stessa supply chain può fortificare il sistema nel suo complesso.

Le aziende che, operando in settori strategici quali le forniture energetiche o militari, lavorano a stretto contatto col governo del proprio paese, dovrebbero scegliere i propri subfornitori con attenzione e pretendere da loro gli stessi standard di sicurezza e i medesimi criteri di selezione del personale.

Eventuali attacchi subiti andrebbero notificati tempestivamente non solo alle aziende coinvolte, ma anche alle autorità competenti, permettendo la condivisione delle informazioni essenziali e velocizzando le operazioni di natura forense. La collaborazione tra pubblico e privato consente di sensibilizzare le aziende sulla cyber security, diffondendo degli standard e delle pratiche comuni in termini di sicurezza, fornendo le informazioni necessarie per prevenire un attacco informatico e reagire opportunamente, e facilitando l'analisi dei malware e l'individuazione degli hacker da parte delle autorità. L'importanza del partenariato pubblico-privato nel campo della cyber security è persino maggiore per le aziende di piccole e medie dimensioni, spesso meno informate sulle minacce cibernetiche e dotate di meno risorse economiche da investire nel settore.