RANSOMWARE

Evoluzione e misure di protezione

maggio 2021

INDICE

1. Introduzione

La presente pubblicazione è volta a descrivere l'evoluzione della minaccia relativa ai ransomware, descrivendone le fasi dell'attacco e le relative Tattiche Tecniche e Procedure (TTP). Vengono infine proposti un elenco di misure utili a ridurre il rischio e i possibili impatti provenienti da un attacco ransomware.

2. Dal ransomware ai Leak Site

In origine l'obiettivo degli attori malevoli, per lo più singoli individui o piccoli gruppi, era limitato alla cifratura dei dati e alla successiva richiesta di pagamento per la decrittazione. La metodologia principale di diffusione è stata affidata, per un lungo periodo, quasi esclusivamente all'invio, in allegati malevoli, di cosiddetti dropper o downloader, ovvero programmi in grado di contenere ed eseguire o effettuare il download del malware che avrebbe poi cifrato le informazioni.
Nel corso del tempo, le crescenti prospettive di guadagno illecito hanno portato a una graduale "industrializzazione" delle attività di sviluppo dei ransomware, attraverso la nascita di gruppi organizzati, altamente motivati e dotati di elevate competenze tecniche, i cui obiettivi primari sono diventati le aziende, anche di grandi dimensioni.
A partire dalla fine del 2019, le organizzazioni criminali specializzate nella diffusione di ransomware all'interno di reti aziendali hanno iniziato ad adottare una nuova strategia per indurre le vittime a pagare il riscatto, esfiltrando i dati presenti sui sistemi colpiti e minacciandone la divulgazione pubblica in caso di mancato pagamento.
L'efficacia persuasiva di tale pratica, introdotta per la prima volta dal gruppo denominato Maze, è risultata evidente, tanto da renderla in breve tempo una costante tra le tattiche utilizzate anche da gruppi criminali emergenti i più noti tra i quali sono AVADDON, BABUK LOCKER, CLOP, CONTI, EGREGOR, NEFILIM, NETWALKER, DARKSIDE e RYUK.
Questa tipologia di attacco, che prevede l'utilizzo di una doppia modalità di estorsione nota come "double extortion attack", viene supportata dai cosiddetti "leak site", spazi web solitamente ospitati sul "dark web", con l'obiettivo di elencare i target colpiti e di pubblicare, all'occorrenza, le informazioni illecitamente raccolte. La

presenza di un'azienda all'interno della lista delle vittime può generare ripercussioni negative sull'immagine del marchio oltre agli impatti conseguenti alla perdita o alla diffusione di informazioni anche confidenziali.

3. Ransomware as a service

Come spesso accade, i modelli di business efficaci per attività lecite sono riproposti anche in ambito illecito. Per quanto concerne l'evoluzione della minaccia in esame, si è infatti assistito alla nascita dei servizi "ransomware as a service" (RaaS), tramite i quali gli sviluppatori della componente malware cercano di massimizzare i propri profitti fornendo infrastrutture pre-configurate e pronte all'uso a fronte del pagamento di una sottoscrizione da parte degli utilizzatori. Il servizio si basa quindi sulla vendita o noleggio di varianti ransomware e, in taluni casi, delle relative infrastrutture di comando e controllo, tramite i canali del dark web. Gli acquirenti del servizio saranno quindi messi in grado di individuare e attaccare le vittime senza bisogno di particolari abilità o competenze.
Infatti la complessità relativa alle conoscenze tecniche necessarie alla conduzione delle campagne, allo sfruttamento di vulnerabilità e all'utilizzo di strumenti e/o framework offensivi viene demandata all'infrastruttura RaaS (con differenti livelli qualitativi), in analogia a quanto legittimamente accade con altri modelli di servizio come ad esempio IaaS, PaaS e SaaS, ampliando in questo modo la platea di attori malevoli interessati a guadagnare tramite attività illecite e massimizzando di conseguenza i profitti del gruppo criminale responsabile dell'erogazione del servizio.

4. Ransomware e Big Hunting Game

Oltre alla diffusione del modello RaaS, la minaccia legata all'utilizzo dei ransomware ha subìto un ulteriore cambiamento legato alla selezione dei target. Come detto infatti, in questo ambito si assiste al passaggio da un approccio basato su una diffusione casuale, per lo più demandata all'invio massivo di allegati malevoli nei confronti di un'estesa e variegata platea di possibili vittime, a una più precisa individuazione delle stesse. Questo scenario, che ha visto le organizzazioni criminali orientare i propri sforzi in direzione di specifiche organizzazioni selezionate in base alla loro redditività e, di conseguenza, alla loro potenziale capacità di pagare importi di riscatto elevati al fine di limitare le perdite, prende il nome di "big game hunting"

(BGH)[1]. Gli attori malevoli, prima di dare il via alle attività tecniche di preparazione dell'attacco procedono, pertanto, con la profilazione delle possibili aziende target e la definizione, in base al fatturato e ad altri indicatori finanziari, di un possibile valore del riscatto in modo che sia da un lato commisurato alle disponibilità economiche della vittima e dall'altro sia invitante rispetto alle potenziali perdite e/o ai costi derivanti dalle attività di protezione e ripristino.
È bene sottolineare che anche la richiesta di una cifra modica rispetto alle potenziali perdite si configura tra le tattiche impiegate in quanto, in caso di pagamento, è estremamente probabile che la vittima venga fatta oggetto di successivi attacchi. Non vi è inoltre nessuna garanzia che gli attori malevoli forniscano le chiavi di sblocco dei file cifrati e/o non procedano, comunque, alla vendita o alla pubblicazione dei dati esfiltrati.

5. Tecnologie bersaglio degli attacchi ransomware

Il sistema operativo Microsoft Windows risulta tra quelli maggiormente interessati dagli attacchi ransomware[2], anche in ragione della sua ampia e capillare diffusione, in particolare in ambito aziendale. Non mancano tuttavia esempi nei quali gli attori, specialmente nel contesto del BGH, si rivolgono a sistemi Linux, fino ad arrivare a prodotti software specialistici più o meno diffusi. Ad esempio, recenti eventi rilevati a partire dalla seconda metà del 2020 hanno visto gruppi come SPRITE SPIDER e CARBON SPIDER orientare la propria attenzione verso l'hypervisor ESXi, prodotto di VMware per la virtualizzazione nel contesto Enterprise, spesso utilizzato dalle organizzazioni per ospitare i server aziendali. Grazie alla distribuzione di ransomware sugli host ESXi, gli avversari sono in grado di aumentare rapidamente la portata dell'impatto: la compromissione di un solo server infligge infatti un danno proporzionale al numero di Virtual Machine su di esso ospitate.
Gli attacchi verso infrastrutture ESXi, considerata la potenziale redditività, rappresentano un esempio di come le operazioni BGH sollecitino la nascita di gruppi specializzati nella compromissione di tecnologie ad alto impatto sistemico.
Infatti, il panorama criminale presenta diversi gruppi specializzati nello sfruttamento di gravi vulnerabilità di prodotti, quali ad esempio Oracle WebLogic, QNAP,

[1] Un esempio di tale attività è rappresentato dall'attacco ransomware occorso all'azienda Colonial Pipeline che ha comportato l'interruzione dell'operatività della stessa con impatti elevati su diversi settori produttivi.
[2] https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomware/

dispositivi di accesso remoto o servizi VPN, tali da consentire l'esecuzione di codice arbitrario favorendo la diffusione e compromissione dei sistemi all'interno delle reti target.

6. Caso di studio: Egregor

Un esempio di quanto descritto in precedenza è rappresentato dalla famiglia di ransomware conosciuta come Egregor.
Tale minaccia, identificata per la prima volta nel settembre 2020, consiste in una famiglia di malware largamente utilizzata in modalità "RaaS" da differenti attori, verosimilmente non coincidenti con lo sviluppatore del malware. Si tratta di una delle famiglie di ransomware più utilizzate dai cyber criminali e l'Europa è tra le regioni più colpite.

Nome	Numero di vittime
Conti	291
Maze	266
Egregor	206

Tabella 1 - Prime 3 famiglie di ransomware per numero di vittime

(dato aggiornato al 23 marzo 2021 in riferimento ai rispettivi leak site)

L'utilizzo di Egregor è stato osservato in più attacchi, anche di tipo BGH, a danno di importanti aziende italiane, in particolare nei settori manifatturiero e industriale.
Da un punto di vista tecnico, il malware presenta una sovrapposizione di codice e funzionalità con Sekhmet e con Maze. Inoltre, sono state osservate analogie tra i packer di Egregor e Maze. Queste somiglianze suggeriscono che Egregor possa essere stato sviluppato dai medesimi autori di Sekhmet o da soggetti terzi che hanno avuto accesso al codice sorgente di quest'ultimo.
Le similitudini osservate interessano principalmente le tecniche anti-analisi implementate, di offuscamento del codice e di crittografia dei file. Egregor utilizza un loader personalizzato per decifrare ed eseguire il ransomware tramite un cifrario di flusso denominato RABBIT e richiede una password che deve essere specificata in fase di esecuzione mediante linea di comando. Le possibilità di analizzare il ransomware senza conoscere la password corretta di ogni sample, sono molto limitate.
Il ransomware solitamente esegue alcuni controlli attraverso le seguenti funzionalità:

- controllo dello spazio libero sugli hard disk;
- rilevamento dell'esecuzione in macchine virtuali;
- esecuzione di loop evasivi attraverso funzioni di sleep;
- enumerazione del file system;
- accesso all'elenco di tutti i processi in esecuzione;
- rilevamento dell'esecuzione in sandbox o ambienti di virtualizzazione;
- enumerazione e chiusura di alcuni specifici processi in esecuzione.

Gli autori hanno inoltre predisposto alcuni controlli sull'hardware, sul sistema operativo e sulla lingua del sistema, elemento che consente al ransomware di non eseguire la cifratura delle macchine che adottano una delle seguenti lingue:

- ru-RU (russa)
- uk-UA (ucraina)
- ro-MD (romena-moldava)
- hy-AM (armena)
- az-Latn-AZ (azera)
- ky-KG (Kyrgyz)
- tk-TM (turkmena)
- uz-Latn-UZ (uzbeca)
- kk-KZ (kazaca)
- be-BY (bielorussa)
- az-Cyrl-AZ (azera-cirillica)
- ru-MD (russa-moldava)
- tt-RU (tartara)

Al termine di tutti i controlli, se le condizioni sono soddisfatte, il ransomware cifra i file presenti sulla macchina target tramite una combinazione degli algoritmi ChaCha e RSA-2048 e li rinomina aggiungendo a essi l'estensione dichiarata dal parametro "-append", specificato tramite riga di comando, che può corrispondere al nome dell'azienda colpita o a un suo diretto riferimento.
In ogni directory a cui Egregor accede viene creato un file denominato RECOVER-FILES.txt contenente la specifica nota di riscatto tramite la quale la vittima viene invitata a comunicare, per mezzo di una chat online, con gli autori dell'attacco. Tali

comunicazioni possono essere trasmesse anche in forma cartacea, sfruttando le funzionalità di stampa dei sistemi compromessi.
Normalmente viene richiesta una somma di denaro per la restituzione dei file sottratti e/o la decrittazione di quelli resi illeggibili. Nel caso in cui la vittima si rifiuti di pagare, i dati vengono rilasciati, anche in fasi incrementali e in momenti differenti, su un sito pubblicamente accessibile.

Tattiche, tecniche e procedure.

Gli attacchi che utilizzano infrastrutture "Ransomware as a services" hanno, per loro natura, modalità e caratteristiche tecniche che tendono a variare a seconda dell'attore. In questo senso gli eventi associati a Egregor non fanno eccezione e, considerata l'esistenza di diversi attori normalmente coinvolti nella sua distribuzione, ne consegue che le tattiche, tecniche e procedure (TTP) utilizzate nelle fasi dell'attacco sono estremamente mutevoli, con rilevanti ripercussioni sugli sforzi necessari per la difesa e mitigazione della minaccia.
Gli attori malevoli che diffondono il ransomware Egregor tendono inoltre a utilizzare diversi approcci per compromettere le reti aziendali.
Dopo la fase preparatoria, che consiste nell'acquisizione passiva e/o attiva di informazioni sulla rete dell'obiettivo, l'attacco si concentra su uno o più servizi informatici vulnerabili e, all'occorrenza, viene supportato dall'invio di allegati di posta malevoli, per lo più riferibili alle famiglie Qakbot, Ursnif o IcedID, utilizzando tecniche di phishing.
In genere, per ottenere un primo accesso alla rete dell'obiettivo, gli attaccanti sono soliti:

- colpire le installazioni RDP (Remote Desktop Protocol) o altri sistemi di accesso alle reti private virtuali;
- utilizzare email di phishing con allegati/link malevoli;
- sfruttare vulnerabilità conosciute e non corrette nei prodotti/apparati esposti su Internet.
- considerata l'estensione della superficie potenzialmente accessibile, il vettore iniziale dell'attacco spesso rimane l'elemento più difficile da rilevare con certezza negli incidenti. Le fasi che tendono invece a essere meglio definite sono quelle successive, vale a dire:
- l'escalation dei privilegi;
- l'attivazione di meccanismi di persistenza;

- l’esfiltrazione dei dati.

Questi stadi, che possono variare a seconda della grandezza e complessità della rete, si realizzano con tempistiche differenti, culminano nella distribuzione massiva del ransomware sui sistemi centrali dell’infrastruttura di riferimento e possono interessare all’occorrenza sistemi secondari, anche geograficamente distanti.
Gli utilizzatori di Egregor, ad esempio, sono soliti avviare la distribuzione del ransomware solo dopo essersi garantiti un profondo livello di compromissione dell’infrastruttura oggetto dell’attacco, in modo da assicurare il buon esito dell’esfiltrazione di informazioni ad alto valore e la cifratura dei dati, ovvero gli elementi sostanziali del ricatto (double extortion).
La strategia più comune adottata dagli attori ostili prevede:

- l’ottenimento di un punto di accesso;
- l’impianto di meccanismi di persistenza nella rete;
- la ricognizione interna;
- i movimenti laterali;
- la compromissione di sistemi aggiuntivi;
- l’esfiltrazione dei dati della vittima;
- l’esecuzione massiva del payload del ransomware.

Una volta avuto accesso alla rete, gli attaccanti tendono a effettuare movimenti laterali sfruttando il protocollo RDP o utilizzando strumenti specifici, come ad esempio Advanced IP Scanner o Net Scanner, al fine di visualizzare i dispositivi di rete, scansionare porte, individuare e consentire l'accesso alle cartelle condivise.
Un ulteriore elemento molto diffuso nelle attività di lateral movement è rappresentato dallo strumento opensource Mimikatz, utilizzato per la raccolta delle credenziali. Le credenziali ottenute possono essere in seguito utilizzate per eseguire movimenti laterali e accedere a informazioni riservate.
Un’ulteriore tecnica utilizzata per massimizzare gli impatti dell’attacco prevede, sulla base delle informazioni architetturali raccolte, l’elevazione dei privilegi acquisiti in fase di prima compromissione al fine di eseguire codice arbitrario sui sistemi di destinazione. Tale attività è genericamente effettuata tramite lo sfruttamento di eventuali vulnerabilità rilevate sui sistemi compromessi attraverso l’utilizzo di PoC pubbliche che consentono di ottenere privilegi associati all’account NT AUTHORITY\SYSTEM.

Recenti attacchi hanno ad esempio interessato la vulnerabilità associata alla CVE-2020-0787, corretta nell'aggiornamento di sicurezza rilasciato da Microsoft a marzo 2020, che consiste in una falla di tipo "Arbitrary File Move" nella componente Windows BITS (Background Intelligent Transfer Service). Altre segnalazioni, limitate e non confermate, hanno comunicato l'utilizzo della CVE-2020-0688 (vulnerabilità che consente l'esecuzione di codice remoto in Microsoft Exchange), mentre altri eventi ancora sembrano contemplare il possibile sfruttamento della CVE-2018-8174 (VBScript Engine) e delle CVE-2018-4878 e CVE-2018-15982 di Adobe Flash Player.
I movimenti laterali rilevati vengono spesso associati all'utilizzo di beacon SMB tramite lo strumento Cobalt Strike o ad accessi con privilegi di amministratore dove o quando non previsto.
In taluni casi gli attaccanti, ottenute credenziali di amministratore valide, prediligono l'uso dello strumento PsTools. Un ulteriore strumento da riga di comando per l'esecuzione di query in Active Directory (AD) che può essere usato per l'identificazione degli oggetti/utenti di AD e relative configurazioni è AdFind, come evidenziato in una recente pubblicazione.
Alcuni attori si limitano a elencare i processi attualmente in esecuzione nel computer locale o in un computer remoto utilizzando strumenti nativi come il comando Tasklist, eseguito tramite Windows Management Instrumentation Command line (WMIC). In altri casi fanno uso di strumenti, spesso gratuiti, per verificare cosa è in esecuzione sul sistema prima di effettuare operazioni che potrebbero essere rilevate o interrotte dai software di sicurezza. Ad esempio, possono essere scaricati ed eseguiti, almeno su una minoranza dei server, strumenti come PowerTool, nella maggior parte dei casi rinominati all'occorrenza, necessari per scansionare e analizzare file a livello di kernel e consentire l'identificazione e manomissione delle soluzioni di sicurezza presenti.
Nella fase di esfiltrazione, il trasferimento di file può avvenire tramite protocollo FTP verso indirizzi IP predisposti dall'attaccante e l'attività può essere facilitata dall'uso di strumenti comuni come Rclone, a volte rinominato in svchost, programma versatile con funzionalità di trasferimento, in combinazione con il noto 7zip per la creazione e gestione di archivi file compressi.
L'attacco è solitamente supportato dalla predisposizione di un canale di comunicazione cifrato che può essere instaurato, verso un server esterno, attraverso l'utilizzo del modulo Beacon di Cobalt Strike – potente framework commerciale di penetration testing che fornisce un agente di post-exploitation caricabile in memoria

noto come Beacon e una componente server definita Team Server. L'agente consente di interagire con la macchina infetta, di gestire la distribuzione di moduli aggiuntivi e di eseguire attività. Il beacon di CobaltStrike utilizza vari strumenti ed exploit di terze parti per compromettere la macchina target, tali moduli vengono eseguiti in memoria per ridurre al minimo la possibilità che le tracce vengano individuate.
Questo framework solitamente rappresenta anche il metodo di distribuzione principale per Egregor. Infatti, una volta che il payload del beacon di Cobalt Strike è attivo e persistente, può essere utilizzato per diffondere e lanciare i payload del malware.
Nella propagazione massiva di Egregor, quindi in genere nella fase finale dell'attacco, gli autori possono limitarsi a utilizzare strumenti come PsExec che consente di eseguire processi e comandi interattivi su sistemi remoti senza ulteriori installazioni manuali. Grazie a questa tecnica, il payload del ransomware, supportato dall'esecuzione automatizzata di script, può essere facilmente propagato su tutte le macchine di un dominio Active Directory.
Negli attacchi osservati è risultato piuttosto frequente l'uso di alcuni degli strumenti inclusi nella Windows SysInternal Suite di Microsoft, software che offre il vantaggio di rimanere sotto la soglia di rilevamento in quanto non viene necessariamente identificato dai prodotti antimalware come pericoloso, anzi è spesso consentito, in termini di white list, in ragione dell'utilizzo amministrativo che ricopre nelle attività di gestione e manutenzione delle infrastrutture Microsoft.
Nella fase intermedia della catena di attacco, viene generalmente individuato un sistema in grado di fungere da punto di snodo (pivot point), con la finalità di agevolare il trasferimento locale di file verosimilmente malevoli.
Recenti attacchi hanno visto l'uso di C2 identificati da domini, contattati tramite HTTPS da host compromessi (CobaltStrike C2). Tali domini possono essere associati a una tecnica nota come Fast Flux, che permette di variare il proprio indirizzo IP per sfuggire a eventuali attività di monitoraggio e analisi, oltre che di ostacolare eventuali azioni di contrasto.
La tecnica permette di nascondere i DNS usati per la risoluzione dei domini malevoli dietro una rete di macchine compromesse che agisce da proxy, cambiando in continuazione.
Tipicamente, attraverso reti Fast Flux vengono allestiti servizi web illeciti che possono ospitare, ad esempio, siti di phishing o market illegali. Un singolo dominio può essere

associato a migliaia di "agent Flux" sparsi per il mondo e attestati su differenti provider, di conseguenza la mappatura e il take-down dei servizi malevoli è di difficile attuazione.
Relativamente alle connessioni di beaconing effettuate verso gli indirizzi IP, è possibile notare che gli attaccanti tentano di aggirare le protezioni di sicurezza adottate dai firewall di nuova generazione che identificano la tipologia di traffico di rete. Il traffico viene infatti fatto risultare come riferibile a servizi noti genericamente consentiti, tra cui Google o Amazon, tramite l'utilizzo di CobaltStrike e l'impostazione di un valore fuorviante nel campo host dell'header HTTP.
Di seguito vengono elencate le TTP identificate secondo il framework MITRE ATT&CK correlate, ove esistenti, dalle relative mitigazioni:

Vettore di infezione iniziale:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1078	Valid Accounts	M1026	Privileged Account Management
		M1027	Password Policies
		M1013	Application Developer Guidance
T1566	Phishing	M1031	Network Intrusion Prevention
		M1021	Restrict Web-Based Content
		M1017	User Training
T1190	Exploit Public-Facing Application	M1051	Update Software
		M1048	Application Isolation and Sandboxing
		M1026	Privileged Account Management
		M1030	Network Segmentation
		M1050	Exploit Protection
		M1016	Vulnerability Scanning

T1133	External Remote Services	M1035	Limit Access to Resource Over Network
		M1030	Network Segmentation
		M1042	Disable or Remove Feature or Program
		M1032	Multi-factor Authentication

Esecuzione:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1569	System Services	M1022	Restrict File and Directory Permissions
		M1026	Privileged Account Management
T1053	Scheduled Task/Job	M1026	Privileged Account Management
		M1028	Operating System Configuration
		M1047	Audit
		M1018	User Account Management
T1047	Windows Management Instrumentation	M1018	User Account Management

Persistenza:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1543	Create or Modify System Process	M1047	Audit
		M1033	Limit Software Installation
		M1022	Restrict File and Directory Permissions

T1098	Account Manipulation	M1030	Network Segmentation
		M1032	Multi-factor Authentication
		M1028	Operating System Configuration

Elevazione dei privilegi:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1548	Abuse Elevation Control Mechanism	M1047	Audit
		M1022	Restrict File and Directory Permissions
		M1038	Execution Prevention
		M1026	Privileged Account Management
		M1028	Operating System Configuration

Elusione delle difese:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1562	Impair Defenses	M1018	User Account Management
		M1024	Restrict Registry Permissions
T1222	File and Directory Permissions Modification	M1022	Restrict File and Directory Permissions
T1001	Data Obfuscation	M1031	Network Intrusion Prevention
T1027	Obfuscated Files or Information		

Accesso alle credenziali:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1110	Brute Force	M1027	Password Policies
		M1032	Multi-factor Authentication
		M1036	Account Use Policies
		M1018	User Account Management
T1552	Unsecured Credentials	M1015	Active Directory Configuration
		M1022	Restrict File and Directory Permissions
		M1017	User Training
		M1037	Filter Network Traffic
		M1026	Privileged Account Management
		M1027	Password Policies
		M1028	Operating System Configuration
		M1041	Encrypt Sensitive Information
		M1051	Update Software
T1003	OS Credential Dumping	M1026	Privileged Account Management
		M1027	Password Policies
		M1043	Credential Access Protection
		M1017	User Training
		M1015	Active Directory Configuration
		M1025	Privileged Process Integrity
		M1028	Operating System Configuration
		M1041	Encrypt Sensitive Information

Movimento laterale:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1087	Account Discovery	M1028	Operating System Configuration
T1482	Domain Trust Discovery	M1030	Network Segmentation
		M1047	Audit
T1069	Permission Groups Discovery		
T1082	System Information Discovery		
T1057	Process Discovery		
T1021	Remote Services	M1018	User Account Management

Comando e controllo:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1071	Application Layer Protocol		

Esfiltrazione:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1567	Exfiltration Over Web Service		

Impatto:

ID	TECNICA	ID MITIGAZIONE	NOME MITIGAZIONE
T1486	Data Encrypted for Impact	M1053	Data Backup
T1222	File and Directory Permissions Modification	M1022	Restrict File and Directory Permissions
T1490	Inhibit System Recovery	M1028	Operating System Configuration
		M1053	Data Backup

Raccomandazioni

Benché sia difficile contrastare l'acquisizione di informazioni potenzialmente utili a perpetrare attacchi informatici (reconnaissance) e la preparazione di artefatti malevoli (weaponization) da parte degli innumerevoli threat-group esistenti, è opportuno minimizzare le informazioni pubbliche da cui l'avversario possa trarre vantaggio. È stato verificato che le tecniche per ottenere il cosiddetto foothold all'interno delle infrastrutture target contemplano l'invio di malspam (delivery) o l'impiego di exploit per lo sfruttamento di vulnerabilità (exploitation) sui servizi Internet esposti, come VPN, sistemi di accesso remoto, load-balancer o applicazioni web. È dunque necessario un addestramento specifico del personale preposto alla ricezione, apertura e lettura di mail oltre a un'ordinaria valutazione delle vulnerabilità dell'infrastruttura utilizzata. Sarebbe utile adottare una politica più stringente circa la ricezione di determinate tipologie di file ed evitare sempre e comunque l'apertura di link direttamente ricevuti nelle mail. In ogni caso, è consigliato impiegare un sistema di monitoraggio e di rilevamento di eventuali eventi di sicurezza che possano indicare il tentativo o l'avvenuta compromissione delle reti e dei sistemi in uso. Ai fini dell'analisi di eventuali incidenti, inoltre, è auspicabile l'impiego di un sistema di logging dei citati eventi di sicurezza, sia a livello host che network.
Di seguito vengono riportate le misure di protezione organizzative/procedurali e tecniche suddivise per tipologia ed elencate in ordine crescente di efficacia.

Misure organizzative/procedurali:
Non aprire senza opportune verifiche allegati o collegamenti in e-mail
Prevedere per il personale periodiche sessioni di formazione finalizzate a riconoscere il phishing e le minacce associate alla posta elettronica anche attraverso esercitazioni pratiche;
Valutare la capacità di rilevare e bloccare l'uso di Cobalt Strike sulla rete;
Impedire l'esecuzione di macro nei prodotti MS Office, consentendone l'esecuzione solo agli utenti che ne hanno comprovata necessità e, ove possibile, esclusivamente per le macro firmate digitalmente;

Analizzare in dettaglio le TTP e le relative mitigazioni MITRE ATT&CK, riportate nella sezione precedente, per valutare ulteriori e personalizzate strategie finalizzate alla mitigazione e al rilevamento
Limitare quanto possibile il numero e l'uso di account privilegiati, adottando il principio del privilegio minimo per tutti i task di amministrazione (just-in-time/just-enough)
Analizzare e ridurre quanto possibile la superficie di attacco di Active Directory secondo le best practices di riferimento di Microsoft
Organizzare la rete operativa in zone autoconsistenti ed isolate tra loro in modo da limitare l'impatto di una compromissione
Implementare un piano di risposta agli attacchi informatici
Misure tecniche
Impiegare su tutti i sistemi soluzioni di Endpoint Detection & Response (EDR) che contengano almeno la componente antimalware avendo cura di mantenerlo aggiornato
Abilitare un firewall sui sistemi garantendo esclusivamente il traffico verso i servizi e sistemi necessari
Bloccare il traffico in ingresso a tutti gli indirizzi ip facenti parte la rete Tor o altri servizi di anonimizzazione conosciuti
Mantenere aggiornati i software e i sistemi, in particolare quelli impiegati per i servizi di accesso remoto ed in generale tutti i sistemi esposti su Internet
Disattivare i servizi non necessari, sia nelle postazioni utente che sui server
Verificare le comunicazioni tramite email security gateway, implementando filtri stringenti al fine di evitare che le email di spam/phishing raggiungano gli utenti
Implementare regole di base per il controllo degli script
Introdurre restrizioni sull'impiego di tool di amministrazione come BitsAdmin, WMIC, Psexec e PowerShell sulla rete
Rilevare l'impiego improprio di tool di amministrazione come BitsAdmin, WMIC, Psexec e PowerShell sulla rete
Segmentare la rete in particolare separando la rete operativa dalla rete business
Monitorare gli eventi di Active Directory per rilevare eventuali indicatori di intrusione e compromissione e rilevare eventuali movimenti laterali non previsti
Verificare la presenza di vulnerabilità che impattano prodotti e applicazioni di accesso remoto rivolti al pubblico, con particolare riferimento alle recenti vulnerabilità del protocollo RDP (CVE-2020-0609, CVE-2020-0610, CVE-2020-16896, CVE-2019-1489, CVE-2019-1225, CVE-2019-1224, CVE-2019-1108)

Configurare in modo sicuro i servizi di connessione remota come quelli basati su RDP impostando limiti di accesso e password complesse e ove possibile, sistemi di autenticazione multifattoriale
Utilizzare l'autenticazione multi fattoriale per gli accessi in VPN ed, in particolare, per l'accesso ai servizi esposti su Internet;
Impiegare soluzioni di Data Loss/Leak Prevention (DLP)
Crittografare i documenti sensibili sulla rete per impedirne la possibile divulgazione
Mantenere, se necessario, hardware di backup compatibile con i sistemi in esercizio
Effettuare regolari backup dei dati critici (dati, sistemi operativi, applicativi, codice sorgente, eseguibili), conservandoli su supporti non connessi in modo permanente alla rete o ai sistemi, verificandone periodicamente l'integrità

Lo sfruttamento di vulnerabilità o di configurazioni di sicurezza non ottimali che interessano le tecnologie e servizi esposti sulla rete perimetrale è tra i punti di accesso privilegiati nelle incursioni ransomware. Le attività di difesa devono pertanto prevedere cicli di verifica, ad esempio tramite vulnerability assessment (VA), al fine di garantire la tempestiva risoluzione delle stesse.
Un'ulteriore superficie di attacco, sfruttata in recenti compromissioni, è rappresentata da domini, accessi e sistemi di interoperabilità con partner e società terze: è quindi necessario porre particolare attenzione ad attività non previste e/o che si discostino dal normale utilizzo.

Riferimenti

- https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
- https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
- https://www.ic3.gov/Media/News/2021/210108.pdf
- https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf
- https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/
- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-007.pdf
- https://www.group-ib.com/media/ransomware-empire-2021/
- https://us-cert.cisa.gov/ncas/alerts/aa21-131a