15/11/2021

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 706
Utenti unici: 1.633

https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-e-tecniche-di-elusione-evoluzione-della-minaccia-e-soluzioni-preventive/

Ransomware e tecniche di elusione: evoluzione della minaccia e soluzioni preventive

Sono oltre 80 milioni i campioni di ransomware identificati negli ultimi anni, suddivisi in 130 differenti “famiglie”. Cifre che evidenziano quanto questo malware sia diffuso e quanto possa essere facile contrarlo non avendo adeguati sistemi di protezione. Analizziamone il comportamento per imparare a difenderci Negli ultimi anni la proliferazione dei malware di tipo ransomware è cresciuta in maniera esponenziale raggiungendo la ragguardevole cifra di oltre 80 milioni di campioni. Da una recente analisi condotta dal servizio VirusTotal di Google, nel periodo temporale compreso tra l’inizio del 2020 e la fine del primo semestre 2021 sono state attivate ben 130 famiglie di ransomware.Sono cifre che evidenziano quanto questo tipo di malware sia diffuso e quanto possa essere facile contrarlo non avendo adeguati sistemi di protezione.Guida al ransomware: cos’è, come si prende e come rimuoverloIndice degli argomenti Le due principali classi di ransomwareI Locker-ransomwareI Crypto-ransomwareLe modalità di distribuzione e acquisto dei ransomwareLa tendenza collaborativa tra i gruppi ransomwareIl fenomeno dei Ransomware-as-a-Service (RaaS)Ransomware progettati per sfruttare vulnerabilità noteLockFile: i ransomware con crittografia intermittenteCome opera un ransomware LockFileSoluzioni di mitigazione del rischio Le due principali classi di ransomware Per capire bene il fenomeno è importante fare una veloce panoramica sui ransomware, iniziando da una prima suddivisione in due classi: Locker-ransomware e Crypto-ransomware. WHITEPAPER Ransomware: tutto quello che c’è da sapere per una protezione avanzata Sicurezza Cybersecurity Scarica il Whitepaper I Locker-ransomware I Locker-ransomware sono la prima tipologia di ransomware che ha invaso la rete; questo tipo di malware blocca le funzioni del sistema ma non altera, non distrugge e non esfiltra dati. La richiesta di riscatto è avanzata per rilasciare un tool che sblocchi le funzionalità del sistema attaccato.Si presenta con una schermata di blocco con un messaggio che allude alla navigazione su siti particolari e indicante che il blocco è stato apposto dalle forze dell’ordine (FBI, Polizia Postale, Guardia di Finanza). I Crypto-ransomware I Crypto-ransomware sono malware che hanno lo scopo di criptare i dati, lasciando inalterate le funzionalità dei sistemi. Nelle nuove versioni questi malware esfiltrano i dati della vittima ed attuano un triplice ricatto: ricatto per rilasciare il tool di decriptazione; ricatto per non diffondere i dati; ricatto per non vendere i dati alla concorrenza. Le modalità di distribuzione e acquisto dei ransomware Le due classi appena menzionate, ma la seconda in modo particolare poiché è quella più diffusa ed anche la più pericolosa, sono suddivise in

tipologie diverse, differenziate tra loro per il modo in cui un ransomware può essere distribuito o può essere acquistato: Off-the-shelf (a scaffale): possono essere acquistati dai marketplace presenti nel darknet ed installati sui loro server. Le attività di hacking e di encryption dei dati sono gestite direttamente dal software installato su questi server. Alcuni esempi di Crypto-ransomware che ricadono in questa casistica sono Stampado e Cerber. As-a-Service: il più noto è sicuramente CBTLocker. I cybercriminali scaricano una sorta toolkit che consente di confezionare un eseguibile distribuibile che si appoggia agli stessi server messi a disposizione dai programmatori del ransomware che trattengono il 20% dei profitti. Affiliate program: possibilità di affiliazione, ovvero un programma di affiliazione mediante il pagamento di una fee che può essere criptovaluta o condivisione di informazioni che consentirebbero di attaccare uno specifico target. L'affiliazione consente di accedere al servizio messo a disposizione da coloro che hanno creato il malware ed indicare quali sono gli obiettivi da colpire senza utilizzare risorse proprie e delegando lo studio del target agli altri affiliati. In questo caso la fee è più alta: 30%. IoT Attackers: si infiltrano nei device IoT e li spengono fino a che non viene riconosciuto il pagamento del riscatto. Se i device IoT controllano sistemi critici la continuità del business di un'azienda è seriamente compromessa, se i device si interfacciano o controllano sistemi di erogazioni di forniture il problema è molto più grave. La tendenza collaborativa tra i gruppi ransomware Il sistema di affiliazione citato pocanzi ha favorito il sorgere di una nuova tendenza collaborativa tra i gruppi di cyber criminali, quella del cosiddetto "cartello".è stata rilevata, infatti, l'esistenza di rapporti tra i team che sviluppano e distribuiscono ransomware, i quali hanno creato relazioni tra loro per rafforzarsi reciprocamente ai danni degli utenti e contro legge. In figura un esempio di relazioni consolidate scoperte dal team di Analyst1. Questi gruppi condividono dati sulle potenziali vittime come privati, aziende, enti e cooperano sullo stesso target per raggiungere il loro obiettivo di profitto passandosi la vittima da un gruppo all'altro per cercare di ottenere quanto più profitto possibile.Oltre alla condivisione delle informazioni sono attenti alla gestione delle risorse, non è un caso che prediligano i RaaS (Ransomware-as-a-Service), e le stesse infrastrutture di Comando e Controllo (C&C).La cooperazione spinge i gruppi a rendere più efficienti e sofisticati gli attacchi, avendo rilevato che diversi di questi team ha aggiunto funzionalità automatizzate ai loro payload di riscatto, consentendogli di diffondere e infettare le vittime senza interazione umana. Altro fenomeno in aumento è quello rappresentato dal recruitment di giovani o aspiranti hacker per eseguire attacchi, ricompensando poi dai gruppi con Ransomware-as-a-Service e mettendo a loro disposizione malware, infrastrutture e servizi di negoziazione del riscatto.La forza derivante dall'essere parte di un gruppo rende i membri di questi gruppi piuttosto impavidi e sfrontati, a tal punto da intrattenere vere e proprie pubbliche relazioni, rilasciando interviste ai giornalisti, emanando comunicati stampa e sfruttando i social media per promuovere le loro attività e mostrarsi irraggiungibili e inattaccabili in modo da creare un alone di terrore verso le loro vittime e indurle a pagare i riscatti richiesti. Il fenomeno dei Ransomware-as-a-Service (RaaS) Riprendendo il focus sui ransomware, come già evidenziato, il

fenomeno dei RaaS (Ransomware-as-a-Service) è quello più diffuso perché risulta fruibile anche da coloro che non hanno competenze di sviluppo di codice malevolo e che si fanno abbindolare dalla chimera dei facili guadagni milionari.A guadagnare da questo fenomeno sono sempre e soltanto i gruppi organizzati o i grandi esperti del cyber crime che conseguono profitti dalla vendita dei "software" o progettando soluzioni su commissione per specifici target o noleggiando a terzi risorse informatiche da cui controllare i ransomware o su cui depositare i file esfiltrati alle malcapitate vittime. Ransomware progettati per sfruttare vulnerabilità note A far tremare più di qualche CISO o CSO nell'ultimo periodo ci hanno pensato i ransomware progettati e programmati per agire sulle vittime sfruttando vulnerabilità note, le CVE (Common Vulnerabilities and Exposures), non ancora sanate da parte dei sistemisti o degli esperti di sicurezza e che riescono ad eludere molti dei controlli di sicurezza operati dai sistemi antivirus meno avanzati. LockFile: i ransomware con crittografia intermittente A luglio 2021 è emersa una nuova famiglia di ransomware battezzata LockFile. Caratteristica principale di questo malware è l'introduzione della crittografia intermittente.Cosa ha di particolare questo tipo di crittografia rispetto ad altri algoritmi?Sostanzialmente nessuna differenza nell'algoritmo di cifratura ma una differenza sostanziale nell'applicazione dell'algoritmo, poiché la crittografica del file è parziale, quindi una parte del file resta ancora leggibile e i sistemi di rilevamento basati su algoritmi di analisi statistica come "chi quadrato" falliscono il rilevamento. Come opera un ransomware LockFile Quando lavora in modo automatico ricerca quei server Microsoft Exchange che non hanno applicato le patch sicurezza rilasciate da Microsoft a marzo 2021 relative alle CVE-2021-34523, CVE-2021-34473 e CVE-2021-31207.Queste vulnerabilità riguardano il Microsoft Client Access Service (CAS) eseguito sulla porta 443 in IIS che è comunemente esposto su rete pubblica per consentire l'accesso alla posta elettronica agli utenti di un'azienda.Sfruttando queste vulnerabilità il malware effettua un movimento laterale verso il server di dominio accedendovi attraverso un attacco PetitPotam che dirotta il Lan Manager di Windows NT (o NTLM) mediante il protocollo Microsoft Encryption File System Remote Protocol (MS-EFSRPC).Utilizzando il comando API EfsRpcOpenFileRaw forza il server ad avviare l'autenticazione NTLM su un altro computer (NTLM relay) e dirotta la sessione di autenticazione manipolando i risultati in modo tale che il server ritenga che l'attaccante abbia il diritto legittimo di accedervi.Quando rileva la presenza di un dominio Active Directory, utilizza la directory sysvoldomainscripts per depositare una serie di file (Autologin.bat, Autologin.exe, Autologin.dll, Autologin.sys, Autoupdate.exe), che saranno eseguiti dai client al loro accesso al dominio, avviando, di fatto, il ransomware sulla macchina appena autenticata. Una volta garantitosi l'accesso avvia il processo delle attività ed inizializza la libreria di crittografia.Prima di avviare il processo di crittografia vero e proprio, prepara il proprio campo di battaglia creando dapprima un mutex, ovvero un sistema di mutua esclusione che consente di bloccare altre esecuzioni dello stesso codice, evitando, così, che il ransomware venga eseguito due volte contemporaneamente, e poi termina una serie di processi che potrebbero consentire un rilevamento da parte di un sistema di

controllo (es. una sandbox in cui dirottare il malware) o processi business critical di database engine e di sistemi di virtualizzazione.Terminando i processi, i file gestiti da questi risulteranno non bloccati e per cui crittografabili, quindi la risposta alla domanda “un ransomware LockFile cripta database e macchine virtuali?” è “Sì”.Potrebbe sorgere un altro quesito a chi ha esperienza di analisi comportamentale dei malware: “Un antivirus non si accorgerebbe che un processo effettua tutte queste operazioni?”. In questo caso, purtroppo, la risposta è “No”, perché il malware sfruttando WMI (Windows Management Interface), attraverso il comando wmic.exe, è in grado terminare bruscamente i processi senza risultare il diretto responsabile, quindi un antivirus rileverebbe un’attività eseguita dal processo di Windows.Dopo aver terminato i processi, il malware procede ad invocare un comando di Windows con il quale recupera le lettere con cui sono mappate le unità logiche (C:, D:,..., X:, Y:, Z:), avendo in questo modo evidenza delle risorse di rete che sono condivise tramite protocollo Samba e su cui procederà alla scansione dei file da crittografare. Il ransomware avrà cura di avviare un thread specifico per ogni unità mappata, in modo da parallelizzare le operazioni di crittografia e poter essere estremamente veloce.Altra caratteristica che consente a questo ransomware di nascondersi ai sistemi di rilevamento è quella con la quale apre i file, mappandoli in memoria mediante Memory Mapped I/O, tecnica che permette al malware di accedere e crittografare velocemente i documenti “cached” e di delegare al processo Windows System la scrittura su disco dei byte modificati del file, rendendo più difficile la detection e anche l’analisi con tools di process monitoring. Tramite questo metodo, la scrittura su disco può avvenire in modo differito di secondi o minuti rispetto all’operazione di crittografia del ransomware.Un altro “trick” estremamente utile ad evadere la detection da parte di alcuni software di protezione da ransomware è il disinteresse per oltre 800 tipi di file, compresi file JPG, PNG, MP3 ed MP4, infatti questo malware non cripta questi file, riuscendo a concludere la fase di crittografia in tempi estremamente rapidi.Ultima peculiarità, il malware termina il proprio processo e si elimina autonomamente, lancia il comando cmd /c ping 127.0.0.1 -n 5 && del “C:...autoupdate.exe” && exit, per auto cancellarsi.È evidente che questo ransomware è stato studiato e progettato con molta cura e racchiude un livello di conoscenza dei sistemi e di ingegnerizzazione dei processi molto elevato. Soluzioni di mitigazione del rischio Come potersi difendere da un’arma simile?La prima risposta che mi verrebbe da dare è “spegnere e staccare tutto!”, ma questo non è possibile e neppure pensabile.Ci si deve difendere adottando delle soluzioni di rilevamento basate su AI e ML (Artificial Intelligence e Machine Learning) che consentono di monitorare i sistemi con tecniche innovative che studiano il comportamento anomalo dei processi e attivano una quarantena preventiva a protezione del sistema stesso.Queste soluzioni sono conosciute come EDR o XDR (Endpoint Detection and Response – eXtended Detection and Response) ovvero soluzioni software, spesso note come antivirus intelligenti, in grado di creare correlazioni tra diversi elementi e processi e attivare una serie di blocchi e di ripristini che permettono ai sistemi di continuare a funzionare o isolano il sistema per evitare danneggiamenti ad altri computer, server o dispositivi presenti in

rete.Altro consiglio è quello di aumentare la propria consapevolezza (awareness) in ambito cyber security. Come farlo? In azienda organizzando dei corsi di formazioni mirati e adottando soluzioni di cyber range per un addestramento più ampio basato sulla gamification, per i privati spendendo un'oretta del proprio tempo per seguire uno dei tanti corsi pubblicati sulle varie piattaforme come Udemy, dove ad esempio il team CyberSecurity di Exprivia ha pubblicato un corso di CyberSecurity Basics. WHITEPAPER Cybersecurity come sistema: una soluzione chiave per i MSP Sicurezza Trade Scarica il Whitepaper@RIPRODUZIONE RISERVATA