Ransomware: che fare?

Ransomware. Ciò che sappiamo

Nell'ultimo anno abbiamo assistito ad una crescita esponenziale degli attacchi di tipo ransomware che hanno provocato, tra gli altri, un aumento di circa tre volte dei riscatti pagati per ottenere le chiavi di cifratura ed un altrettanto pesante aumento dei costi per cyber insurance. Si stima che uno solo dei gruppi criminali attivi nel settore abbia incassato nell'ultimo anno riscatti per circa 90 milioni di dollari. Il rischio generato dal ransomware è talmente elevato che alcune compagnie di assicurazione hanno abbandonato il settore della cyber security.

La situazione in realtà potrebbe essere ancora più pesante di quanto sappiamo, perchè spesso le vittime non condividono informazioni sull'attacco che hanno subito. Oltre ad evitare danni di immagine, questo oscuramento sugli attacchi subiti vuole spesso evitare accuse di collaborazione con il crimine organizzato. La possibilità di accusare di questo crimine chi paga un riscatto è stata evidenziata da recenti prese di posizioni e dichiarazioni del governo USA.

Un altro problema fortemente correlato agli attacchi di tipo ransomware è il furto dei dati. Spesso gli attaccanti non si limitano a criptare le informazioni ma le esfiltrano sui propri sistemi e usano la minaccia di renderle pubbliche per accelerare le trattative sul riscatto o per un ulteriore riscatto se e quando il sistema target è tornato al normale funzionamento. Ciò fa sorgere interessanti correlazioni tra attacco ransomware, rispetto del GDPR ed obblighi di notifica ai proprietari dei dati esfiltrati. In generale, comunque, la necessità di poter riutilizzare il proprio sistema è un motivo più che sufficiente perchè il proprietario del sistema attaccato paghi velocemente il riscatto. Ad esempio gli

ospedali che sono state tra le recenti vittime del ransomware non hanno molte alternative al pagamento se vogliono salvaguardare i loro pazienti. Una delle innovazioni più significative degli attacchi ransomware rispetto a quelli tradizionali è che non servono IOC o simili per scoprire un attacco, il mancato funzionamento del sistema è di per se uno IOC più che sufficiente.

Vale anche la pena di notare che per ora non vi sono evidenze di una qualche attacco di tipo ransomware che abbia avuto successo contro impianti di controllo industriale. Anche l'attacco che viene indicato come attacco all'oleodotto Colonial in realtà è stato un attacco al sistema informatico di Colonial che poi ha fermato il proprio oleodotto per paura di non essere in grado di fatturare quanto veniva distribuito ai vari clienti.

Ultima caratteristica recentemente emersa sugli attacchi ransomware è il piccolo numero di gruppi criminali che sono dietro a questi attacchi. Questa deduzione è stata possibile grazie all'analisi dei flussi di pagamenti mediante criptovalute, il metodo di pagamento tipico per i riscatti. L'analisi dei flussi di pagamento memorizzati sulle blockchain ha evidenziato come il numero dei destinatari finali sia molto basso. Questi effetti sono evidenti anche se il numero dei flussi di valuta legati al ransomware è una minima parte dei fussi di criptovalute. La esistenza di pochi gruppi è anche provata da una analisi degli strain di malware usati contemporaneamente. Il numero di strain di malware diversi risulta sempre basso e spesso all'aumentare della frequenza di un certo strain di malware corrisponde la contemporanea diminuzione della frequenza di un altro strain.

Ransomware: che fare?

Uno degli aspetti che ritengo più interessanti della recente impennata degli attacchi ransomware sono le strategie di difesa che si propone di usare. In particolare, pochissimi

propongono di migliorare la robustezza e la resilienza, r&r, dei sistemi informativi e quasi tutti puntano su strategie basate su “deterrence and disruption”, d&d.

Tipiche strategie r&r sono basate su defence in depth, hardening dei sistemi, autenticazione a più fattori, patching mirato dei sistemi in base al rischio associato. Le strategie di tipo deterrence prevedono invece di aumentare la collaborazione ed i trattati internazionali per impedire il riciclaggio dei riscatti, perseguire i gruppi criminali che lanciano gli attacchi e scoraggiare alcuni stati a favorire questi gruppi in modo da poterli usare anche come APT quando utile. La deterrence comprende anche l’introduzione di nuove leggi per le criptovalute per tener conto del fatto che, come qualcuno dice, il ransomware non è altro che un problema generato da bitcoin e levato bitcoin sparisce anche il problema. Infine, un vantaggio della deterrence è che si può usare anche contro i propri utenti per evitare che, nonostante gli avvisi e la formazione ricevuta, continuino a cliccare su link in email di phishing o a rivelare le password al telefono.

Le strategie di tipo disruption prevedono invece ritorsioni informatiche contro le infrastrutture di command and control da cui provengono gli attacchi. Ciò avrebbe l’indubbio risultato di rallentare l’attività di questi gruppi ma come dice la pubblicità di Hydra, un darkweb marketplace, tagliata una testa all’idra ne ricrescono almeno altre due. Il rischio del sorgere di altre teste è dovuto ai modelli di business basati sostanzialmente su ransomware as a service. In questo modello, pochi gruppi producono il malware che implementa l’attacco e poi lo rivendono a molti gruppi che implementano l’attacco in cambio di parte dei profitti. Ciò diminuisce l’efficacia di attacchi contro i gruppi che eseguono gli attacchi mentre sarebbe opportuno concentrarsi sulle origini della supply chain ovvero quei, pochi, gruppi che forniscono il malware che gli attaccanti utilizzano.

I veri punti critici delle strategie d&d sono i tempi che richiedono e la volontà internazionale di arrivare a trattati che permettano di perseguire questi reati informatici anche in altri stati. E' lecito dubitare della disponibilità di alcuni stati in particolare a fornire quelle informazioni che possono facilitare l'attribuzione degli attacchi. Sappiamo che la condivisione di alcune delle informazioni utili fornisce anche indicazioni sulle capacità informatiche di chi condivide le informazioni e sulla sua presenza e persistenza in reti avversarie. Una volta ammesso che i tempi per le strategie di d&d sono non banali, sparisce anche quello che molti invocano come il loro principale vantaggio rispetto a strategie r&r ovvero i tempi ridotti di applicazione.

La deduzione più importante permessa dal fatto che si punti unicamente su strategie d&d è che l'unica difesa contro il ransomware è quella che impedisce l'esecuzione di attacchi di questo tipo vista l'incapacità di prevederli e sconfiggerli se e quando vengono eseguiti. In pratica, invocare strategie di d&d o equiparare il ransomware al terrorismo equivale all'ammissione di un pesante fallimento nel modo in cui la tecnologia ICT è stata progettata, sviluppata ed utilizzata. E' interessante che per molti il focus siano le strategie migliori di d&d e non il fallimento nell'uso della tecnologia esse ammettono.

Ransomware: cosa stiamo facendo?

L'ammissione del fallimento della tecnologia ICT è l'ultimo frutto di un modello di adozione delle tecnologie ICT utilizzato fino ad ora ed, in particolare, della strategia di difesa utilizzata. Questa strategia di difesa è sostanzialmente passiva perchè è basata non sulla prevenzione dell'attacco aumentando la resilienza del sistema ma sulla scoperta e gestione a posteriori degli attacchi informatici. Vi sono molte conferme della popolarità della strategia passiva. Si consideri ad esempio l'adozione di tecnologie di

IA per la scoperta di anomalie nel comportamento degli utenti o dei componenti in seguito ad un attacco. Soluzioni di questo tipo sono molto più popolari di altre che l'IA permetterebbe ad esempio l'automazione della scoperta di vulnerabilità o di percorsi di attacco in un sistema. Ed è quasi commovente, ma molto rivelatore, vedere l'entusiasmo di molti per avere finalmente un modo di scoprire se sono stati attaccati. Purtroppo, questo modo di utilizzare l'IA non li aiuta a capire cosa fare dopo la scoperta dell'attacco per evitare la fatica di Sisifo di scacciare un attaccante per essere attaccati da un altro, o dallo stesso se è persistente.

L'amore per la strategia passiva è difficile da capire perchè, fortunatamente, sono state definite molte soluzioni r&r di tipo proattivo che vanno dall'applicazione rigorosa del privilegio minimo, la segmentazione delle reti in modo da applicare la defence -in-depth. A fianco di queste soluzioni, ben note da anni, ne sono state sviluppate altre fondate, ad esempio, sulla adversary emulation per capire le strategie ed i comportamenti degli attaccanti e per valutare e migliorare la robustezza dei sistemi tenendo conto di questi comportamenti. La possibilità di integrare queste tecniche con informazioni di threat intelligence permette di anticipare in modo accurato i comportamenti degli attaccanti e di riconoscere e predisporre le difese opportune.

La disponibilità di strategie r&r ha portato ad alcuni importanti ripensamenti. Ad esempio, l'esecutivo USA ha annunciato la creazione di un Cyber Safety Review Board (CSRB) nel Department of Homeland Security per investigare gli incidenti ed anche le vulnerabilità che li hanno permessi, i controlli che si possono applicare e simili. Il board dovrà soprattutto investigare gli incidenti per fornire raccomandazioni su come difendersi ed impedirli. Lo scopo finale dovrebbe essere quello di analizzare i sistemi per rimediare alle loro vulnerabilità e debolezze. Ottima notizia ma, come evidenziato da S.Bellovin e A.Shostak, l'importante è

eseguire una analisi approfondita degli incidenti usando ad esempio la metodologia dei “5 perchè” in sequenza in modo da scoprire la root cause dei problemi incontrati. L’analisi deve ovviamente evitare facili risposte, estremamente generiche e quindi utilizzabili per un qualsiasi evento di sicurezza, quali “Tutto dipende dalla stupidità degli utenti” oppure “Tutto dipende dalla incredibile abilità degli attaccanti”. Se è vero che molto spesso i comportamenti degli utenti offrono un contributo fondamentale del successo degli attaccanti, altrettanto vero è che un sistema messo in crisi dai comportamenti degli utenti è strutturalmente debole perchè non è stato progettato per compensare questi comportamenti degli utenti, noti da tempo. Quasi tutte le strategie r&r citate in precedenza possono essere usate per compensare, ad esempio, i comportamenti degli utenti. La soluzione che viene cosi costruita è molto più robusta di quella permessa della semplice educazione degli utenti. Soluzione nota ma poco efficace se già circa 20 anni M.Ranum ci aveva avvertito che educare gli utenti non è una idea intelligente. Ci aveva anche detto che basare la sicurezza su una strategia “patch all” non aveva mai funzionato e non funzionerà mai. Oggi dopo un po di anni possiamo verificare quanto le profezie fossero accurate. Per quanto riguarda la risposta “Tutto dipende dalla incredibile abilità degli attaccanti” basterà ricordare la password solarwind1234, oppure il componente vpn che nessuno sapeva fosse attivo ed utilizzato per l’attacco a Colonial ed anche la scelta di JBS, il fornitore di carne bloccato per due settimane, che non riteneva la sicurezza informatica una priorità aziendale.

Nel pensare una strategia contro gli attacchi ransomware è bene evitare gli errori generati da un approccio passivo e basato su *penetrate and patch* e non inventare strategie per il ranking delle vulnerabilità indipendenti dal sistema ed metodi qualitativi per la gestione del rischio. Le strategie per il ranking indipendenti dal sistema si sono già rivelate non efficaci o poco economiche. Forse molto dipende dal fatto che

molti dei metodi qualitativi per l'analisi del rischio su cui si basano sono inconsistenti. E' anche opportuno non limitarci a delle best practices per i sistemi più critici perchè le vicende di Solarwinds ci hanno fatto toccare con mano come mettere in sicurezza un sistema critico sia difficile se i fornitori dei componenti del sistema non ci offrono qualche garanzia sullo sviluppo dei loro componenti. Infine, decidiamo una volta per tutte che "meglio fare qualcosa che nulla" non è vero. Ci sono delle strategie che dovrebbero aumentare la sicurezza ma che invece danneggiano i sistemi riducendone la già scarsa sicurezza: Ad esempio, non sempre l'acquisto di un nuovo componente aiuta ad aumentare la sicurezza. L'unica cosa che il nuovo componente aumenta sicuramente è la superficie d'attacco. Di contro, l'hardening di un sistema garantisce comunque di non aumentare tale superficie.

Risolvere tutti i vari problemi descritti è indubbiamente complicato e challenging ma la buona notizia è che molte delle tecnologie r&r descritte hanno ottime prestazioni e possono essere applicate. Di conseguenza, è fondamentale smettere di pensare che la soluzione ottima sia quella di mettersi in un framework d&d ed attaccare coloro che sfruttano le nostre debolezze invece che rimediare alle debolezze setesse. Indubbiamente, molti non saranno convinti di quanto ho detto e preferiranno continuare a sperare che le forze di polizia riescano, come è appena accaduto, a recuperare alcuni dei riscatti pagati. Focalizzarsi unicamente sul riscatto, le modalità di pagamento et simili trascura che il problema di interesse non è ridurre gli esborsi economici ma di come una tecnologia è stata e viene utilizzata. Invito chi non è ancora convinto della inutilità di d&d e di approcci post hoc a rileggere il già citato contributo di M.Ranum che evidenzia quanta poca strada sia stata fatta da quando è stato scritto e quanto tempo abbiamo perso, e stiamo perdendo, applicando strategie come *Hacking is cool, Action is better than inaction* o *Penetrate and patch*. Queste strategie non sono mai state efficaci e continueranno a non esserlo.

Riferimenti

1. ChainAnalysis, The 2021 Crypto Crime Report, February 2021
2. Bellovin, A.Shostack, *Finally! A Cybersecurity Safety Review Board*, Lawfare, June 2021, https://www.lawfareblog.com/finally-cybersecurity-safety-review-board
3. Dempsey, *Regulatory Alchemy: Turning Cybersecurity Guidelines Into Rules,* Lawfare, June 2021, https://www.lawfareblog.com/regulatory-alchemy-turning-cybersecurity-guidelines-rules
4. Crowdstrike blog, *Under Attack: Protecting Against Conti, DarkSide, REvil and Other Ransomware,* https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/
5. Jenkins, M.Olney, *Intelligence-driven disruption of ransomware campaigns,* https://blog.talosintelligence.com/2021/06/intelligence-driven-disruption.html
6. Ranum, The Six Dumbiest Ideas in Computer Security, http://www.ranum.com/security/computer_security/editorials/dumb/, 2005

Articolo a cura di **Fabrizio Baiardi**

Laureato in Scienze dell'Informazione all'Università di Pisa.

E' attualmente è professore ordinario di Informatica presso l'Università di Pisa dove coordina il gruppo di ricerca sy ICT risk assessment and management. La sua attività di ricerca è focalizzata su strumenti e metodi formali l'automazione dell'analisi e la gestione del rischio.

Ha partecipato a numerosi assessment di sistemi ICT con particolare interesse per quelli con componenti SCADA.

Attualmente è responsabile scientifico del progetto Haruspex

che ha prodotto una suite integrata di strumenti per analisi e gestione del rischio.

Una lista aggiornata delle pubblicazioni scientifiche sul progetto Haruspex e dei premi ricevuti si può trovare alla pagina
http://www.di.unipi.it/~tonelli/securityteam/publications.php

F. Baiardi è stato presidente della laurea in Informatica Applicata e della laurea magistrale in Sicurezza Informatica dell'Università di Pisa.

E' stato coinvolto in vari progetti nazionali ed europei sulla valutazione della qualità dei corsi di studio e di formazione superiore. Inoltre è valutatore di progetti di innovazione tecnologica per enti pubblici e fondazioni private nazionali ed europei.

https://www.ictsecuritymagazine.com/articoli/ransomware-che-fare/