



Extortion Economics

Ransomware: un nuovo modello di business

Cyber Signals

Agosto 2022



● Ransomware attacks exploiting configuration errors

Oltre l'80 percento

degli attacchi ransomware puo essere ricondotto a banali errori di configurazione dei software e dei dispositivi.¹





Introduzione

L'attività dei criminali informatici e la ransomware underground economy

Sebbene il ransomware continui ad essere un tema in grado di catturare l'attenzione di molti, ultimamente stiamo assistendo alla nascita di un piccolo ecosistema che sta contribuendo ad alimentare il settore dell'industria criminale informatica. La specializzazione ed il consolidamento di tale settore ha portato alla diffusione del *Ransomware as a service* (RaaS) come modello di business dominante, permettendo a un range sempre più ampio di criminali di mettere in atto attacchi ransomware a prescindere dal loro grado di conoscenza tecnica.

We are all cybersecurity defenders.



Security Snapshot



Tra Luglio 2021 e Giugno 2022, la **Microsoft's Digital Crimes Unit (DCU)** ha diretto la rimozione di più di 531.000 phishing URL e 5.400 kit di phishing, che hanno portato all'identificazione e alla successiva chiusura di oltre 1.400 account email utilizzati per il furto di credenziali¹.



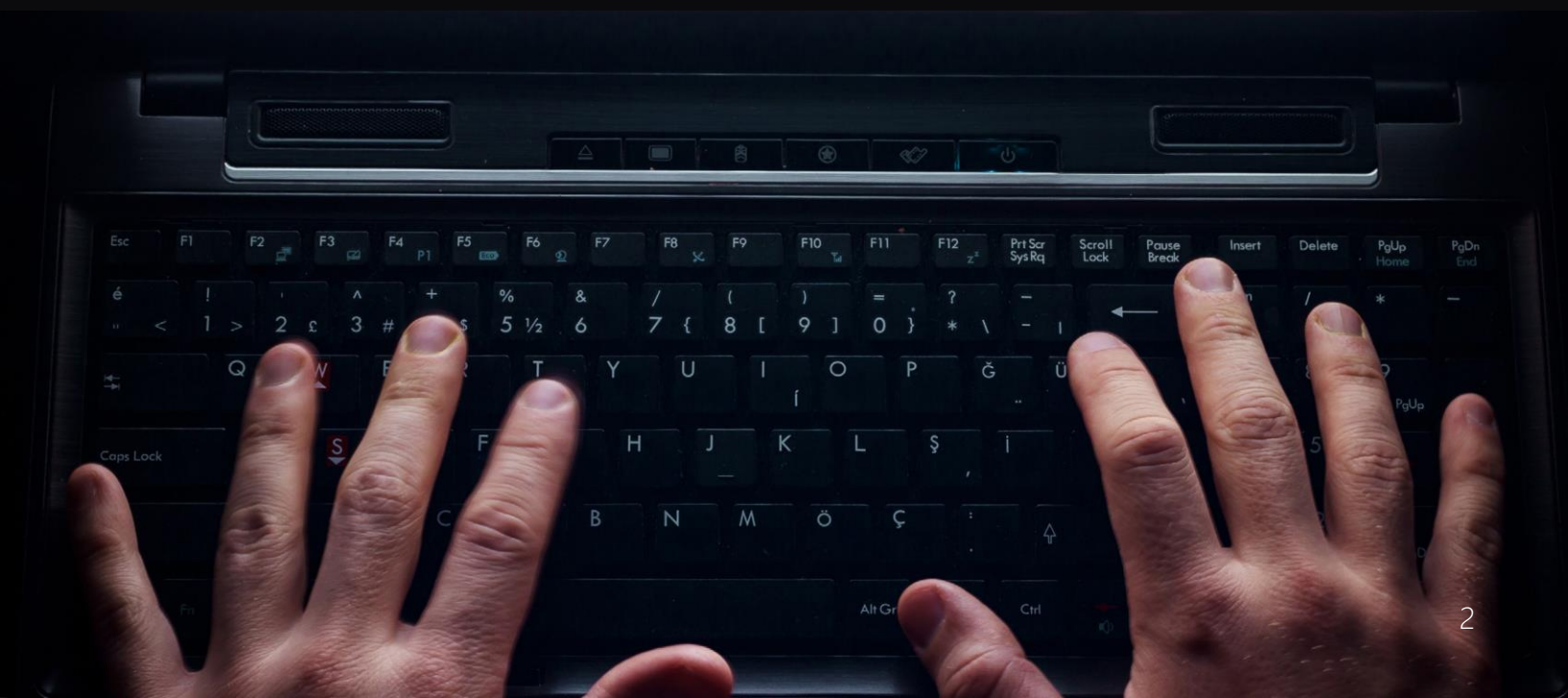
Email Threats

Se sei vittima di un email di phishing, il tempo medio necessario a chi perpetra tale attacco per accedere ai tuoi dati sensibili è pari a un'ora e 12 minuti¹.



Endpoint Threats

Se il tuo dispositivo è stato compromesso, il tempo medio necessario agli autori di tali minacce per dar via al così detto *lateral movement* (ovvero la fase più lunga dell'attacco, circa l'80% di questo) è pari a un'ora e 42 minuti¹.



Nuovi modelli di business

Oggi, i criminali informatici, mettono a disposizione gli strumenti e le tecniche necessarie alla diffusione del ransomware per trarre così profitti in maniera più intelligente. Si tratta della [Ransomware as a Service](#) (RaaS) economy, che permette ai criminali informatici, dietro pagamento, di distribuire il payload Ransomware e le perdite di dati senza avere necessariamente alcuna conoscenza tecnica preliminare.

Quando si parla di Ransomware "gangs" si tratta di varianti RaaS, come Conti o REvil, utilizzate dai criminali informatici che passano dai programmi RaaS ai payload. Alcuni di questi programmi contano persino 50 e più "affiliati". Il RaaS, offuscando l'identità degli aggressori, tiene in ostaggio i sistemi informatici ed i dati fino al pagamento di un riscatto.

Threat briefing

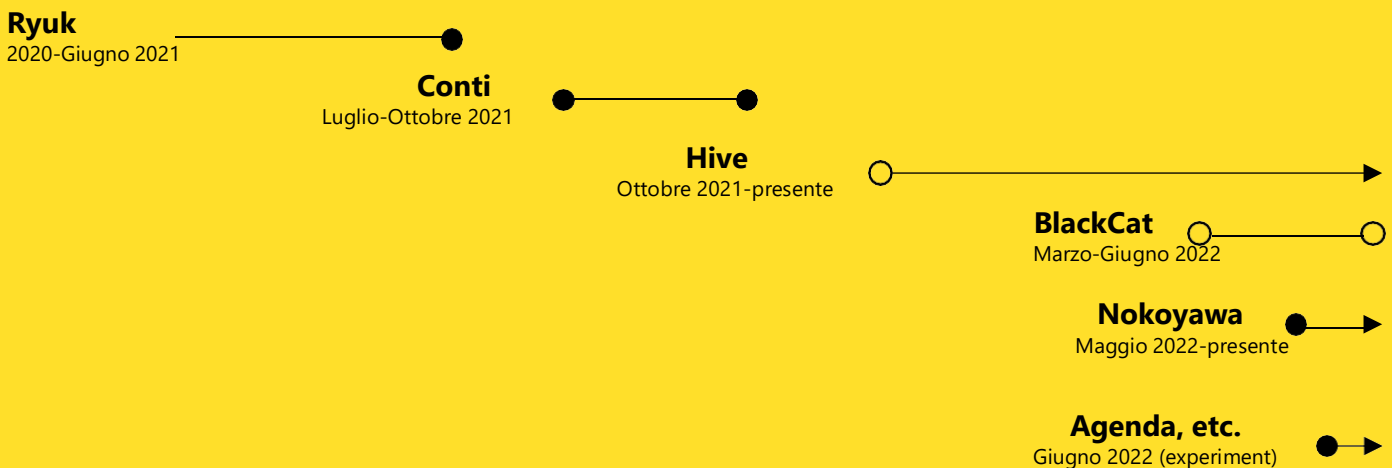
Dunque, potremmo concludere affermando che oggi, chiunque dotato di computer e di carta di credito, può facilmente accedere a questo modello di business.

L'industrializzazione del cybercrime, ha inoltre creato dei ruoli specializzati: un esempio è l'*access broker*, che vende ai criminali informatici gli accessi alle reti.

In questi casi spesso, una singola compromissione può coinvolgere diversi criminali informatici in diverse fasi di intrusione.

I kit RaaS sono facilmente reperibili sul dark web e pubblicizzati come prodotti ordinari che normalmente si trovano online. Inoltre, potrebbero includere servizi di supporto al cliente, abbonamenti, recensioni, forum e altre funzionalità.

DEV-0237 payload ransomware nel tempo




2021

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

2022

Jan Feb Mar Apr May Jun

Threat briefing



I criminali informatici, per un kit RaaS, pagano un prezzo che è solitamente stabilito, mentre i gruppi che vendono i “pacchetti” delle varianti RaaS secondo il modello “affiliato”, percepiscono una percentuale sui profitti.

La configurazione della rete è determinante nella scelta degli attacchi Ransomware, che risultano essere diversi per ciascuna vittima. Sebbene il Ransomware payload rimanga lo stesso, la scelta sulla configurazione di rete varia da vittima in vittima.

Solitamente il Ransomware culmina in un attacco che può includere esfiltrazione dei dati ed altri strumenti di attacco. Purtroppo, a causa della natura interconnessa dell'industria criminale informatica, tali tipologie di intrusioni spesso risultano essere non correlate tra loro, e quindi difficilmente identificabili.

In più con il passare del tempo, l'industrializzazione del settore ha consentito l'esecuzione di attacchi ransomware prolifici ed impattanti persino da parte di aggressori dotati di scarse competenze tecniche. Con la scomparsa della variante Conti, abbiamo assistito a una serie di cambiamenti nel panorama Ransomware.

Ad esempio, alcuni degli “affiliati” che si servivano della variante ransomware Conti sono passati a payload di ransomware come LockBit ed Hive, mentre altri ancora si servono di payload di ransomware appartenenti ai gruppi RaaS: è il caso di QuantumLocker e Black Basta, che colmano in qualche modo il vuoto lasciato dalla scomparsa della gang Conti.

Proprio perchè risulta difficile trovare una soluzione unica per ogni tipo di ransomware, la facilità con cui attacchi di questo tipo riescono a sfuggire al controllo dei governi e dei media, è elevata.

Raccomandazioni

Pulizia delle credenziali: Adotta strategie di segmentazione di rete che applichino il regime dei privilegi minimi agli accessi, limitando *il lateral movement*.

Esposizione delle credenziali: Mitigare il rischio di esposizione delle tue credenziali è fondamentale per prevenire gli attacchi ransomware. I team di sicurezza IT e SOCs operano per limitare l'accesso ai *privilegi di amministratore* monitorando i rischi ad alto impatto cui l'organizzazione è soggetta.

Riduzione della superficie di attacco: Abilita regole per la riduzione della superficie di attacco. Le organizzazioni dotate di policies definite, in questi casi, sono state in grado di mitigare gli attacchi già nelle loro fasi iniziali.



Gli attacchi a doppia estorsione dei criminali informatici

L'obiettivo del Ransomware è quello di estorcere pagamenti alle proprie vittime. La maggior parte dei programmi RaaS agisce perpetrando attacchi a *doppia estorsione*, minacciando cioè di divulgare i dati sensibili rubati. Due [extortion focused groups](#) sono DEV-0537(aka LAPSUS\$) e DEV-0390 (ex affiliato Conti). Le intrusioni DEV-0390, sebbene assumano la forma dei malware, si servono di strumenti legittimi per estorcere dati e pagamenti. Si servono di tools come Cobalt Strike, Brute Ratel C4,

Proteggiti dagli attacchi

ed *Atera remote management utility* per permettere alla vittima di continuare ad avere accesso ai propri device. DEV-0390 esegue il furto delle credenziali, individua i dati sensibili, e li invia ad un sito di condivisione di file cloud che si serve di una *utility* backup dei file. DEV-0537 si serve di una strategia totalmente differente. L'accesso iniziale è ottenuto tramite l'acquisto delle credenziali sul dark web o dai dipendenti delle organizzazioni presi di mira.

Problema

1 Furto delle password e protezione delle identità

I criminali informatici, per avere successo, oltre ai malware, hanno bisogno delle tue credenziali. In quasi tutti gli attacchi ransomware riusciti, gli autori delle minacce ottengono gli accessi privilegiati assicurandosi un ampio accesso alla rete.

2 Sistemi di sicurezza difettosi

In quasi tutti gli attacchi ransomware osservati, almeno uno dei sistemi coinvolti era stato configurato in modo errato e non rispettava i requisiti di privacy e sicurezza necessari.

3 Errata configurazione delle app

Persino le app che utilizzi possono rappresentare uno strumento di attacco per i criminali informatici. Troppo spesso configurazioni del tipo "legacy" permettono che l'app sia nel suo stato di default, permettendo a qualsiasi utente l'accesso alla rete aziendale. Non esitare a cambiare le impostazioni delle tue app.

4 Slow patching

Si tratta di un cliché, un pò come il famoso "Eat your vegetables!" – ma è la verità: Il miglior modo per proteggere il proprio software è quello di tenerlo aggiornato. Anche se alcune app basate sul cloud si aggiornano in automatico, le aziende devono comunque installare, sempre, le *patch dei fornitori*.

Soluzione

1 Autenticazione delle identità

Applica l'autenticazione a più fattori (MFA) a tutti gli account e dai maggiore priorità all'*administrator*. In caso di forza lavoro ibrida, è possibile richiedere l'MFA per tutti i dispositivi. Adotta il sistema di identificazione *passwordless* come FIDO keys o il Microsoft Authenticator per app in grado di supportarlo.

2 Elimina distorsioni e punti ciechi

I sistemi di sicurezza e la loro configurazione devono essere testati di frequente ed operare nel rispetto dei requisiti previsti.

Rinforza le risorse


3

Liberati delle app che non utilizzi: sarai maggiormente in grado di difenderti dalle minacce a cui sono esposte. Presta attenzione ad app da *remote helpdesk* come TeamViewer, spesso presa di mira dagli autori degli attacchi.

4 Tieni aggiornati i tuoi sistemi

Tieni sempre aggiornati i tuoi software e valuta, dove necessario, l'applicazione di *patch* ed il passaggio a servizi basati sul cloud.

Proteggiti dagli attacchi



Considerando la profonda interconnessione tra le identità e le relazioni di fiducia nei complessi ecosistemi tecnologici moderni, queste figure si specializzano in telecomunicazioni, tecnologia e servizi IT, contribuendo ad agevolare l'accesso di aziende a reti di partner o fornitori.

È essenziale che i difensori delle reti guardino oltre la semplice minaccia dei ransomware, percepita come "attacchi estorsivi", poiché è fondamentale monitorare con attenzione l'estrazione di dati e i *movimenti laterali*. Nel caso in cui un autore malevolo stia pianificando un'estorsione finanziaria, minacciando di divulgare i dati sensibili di un'organizzazione, il payload ransomware diventa una minaccia di gran lunga più grave.

In definitiva, è l'autore dell'attacco a scegliere il metodo da utilizzare, e non sempre il ransomware genera quel rendimento economico che spesso chi decide di intraprendere tali azioni ricerca.

Piuttosto che fare affidamento ai post nei forum o sui leaks delle chat, affidati ai nostri esperti sulla sicurezza, che analizzano le nuove tattiche ransomware e sviluppano strategie di difesa per contrastare le minacce.

La protezione integrata tra i vari dispositivi, app, e-mail, dati e cloud, ci aiuta ad identificare gli attacchi apparentemente perpetrati da più autori ma che in realtà provengono da un unico gruppo. La nostra Digital Crimes Unit, composta da esperti tecnici, legali e commerciali, continua a collaborare con le forze dell'ordine per contrastare il crimine informatico.

Raccomandazioni:

Rafforza il cloud: poiché gli aggressori si spostano verso le risorse cloud, è importante proteggere sia queste risorse sia le identità, nonché gli account on-premise.

Il team di sicurezza dovrebbero concentrarsi sulla protezione avanzata dell'infrastruttura delle identità di sicurezza, applicando l'autenticazione a più fattori (MFA) su tutti gli account, e trattando gli amministratori e i tenant del cloud con lo stesso livello di sicurezza e di igiene delle credenziali degli amministratori di dominio.

Previeni l'accesso iniziale: impedisci l'esecuzione di codice gestendo macro e script e abilitando le Attack Surface Reduction Rules.

Elimina i punti ciechi della sicurezza: le organizzazioni devono verificare che i loro strumenti di sicurezza funzionino in modo ottimale ed eseguire scansioni di rete regolari per garantire che un prodotto di sicurezza protegga tutti i sistemi.

Per maggiori informazioni visitare l'indirizzo <https://aka.ms/ransomware-as-a-service>.





Expert profile

Emily Hacker:

Threat intelligence analyst

Emily Hacker non si aspettava di diventare un'analista di threat intelligence in Microsoft dopo aver studiato giornalismo. Il suo primo lavoro nel campo della sicurezza informatica è stato come redattrice tecnica presso un'azienda petrolifera. "Redigevo rapporti di intelligence, e aiutavo con le metriche degli incidenti.

Nel corso di quel primo anno, sono rimasta assolutamente affascinata dal lavoro svolto dagli analisti dell'intelligence." Il lavoro di Emily in Microsoft è iniziato nel 2020 come analista per Microsoft Defender per Endpoint e per Office. Emily è direttamente coinvolta in molte delle indagini che hanno costruito la conoscenza base di Microsoft sull'economia RaaS e sulle relazioni tra broker di accesso/operatore/affiliato. "Seguire le tendenze e le tecniche utilizzate dagli operatori RaaS e dai loro affiliati nella fase pre-riscatto di un incidente è fondamentale per proteggere i clienti da queste minacce. Il mio compito è quello di individuare gli attori pre-ransomware il prima possibile. Se cerchi soltanto il payload del ransomware, sarà troppo tardi." Per rimanere al passo con il mutevole panorama RaaS, Emily e il suo team utilizzano una combinazione di sistemi automatizzati e analisi umana per eseguire l'escalation e agire sulle attività in tempo reale. Il team di Emily aiuta a prevenire e rispondere a diversi incidenti in prima linea

nelle reti dei clienti, contribuendo anche alla valutazione sempre crescente da parte di MSTIC delle strategie di ransomware. Gli operatori ransomware sono noti per prendere di mira reti di importanza critica relative all'istruzione, ai trasporti, all'assistenza sanitaria o ai sistemi di telecomunicazione. Quando queste reti sono colpite, i risultati possono essere catastrofici. "Il lavoro che svolgiamo in Microsoft per monitorare e prevenire gli incidenti ransomware è importante perché stiamo proteggendo non solo i nostri clienti, ma anche i loro clienti. Identificare il prima possibile gli strumenti e le tecniche associate agli incidenti pre-ransomware e ransomware è di critica importanza quando questi incidenti hanno potenziali conseguenze di vasta portata per le aziende, i loro dipendenti e i loro clienti."

"Il mio compito è quello di individuare gli attori pre-ransomware il prima possibile. Se cerchi soltanto il payload del ransomware, sarà troppo tardi."

**Threat intelligence analyst
Emily Hacker**



1. Methodology: For snapshot data, Microsoft platforms, including Defender and Azure Active Directory, and our Digital Crimes Unit provided anonymized data on threat activity, such as malicious email accounts, phishing emails, and attacker movement within networks. Additional insights are from the 43 trillion daily security signals gained across Microsoft, including the cloud, endpoints, the intelligent edge, and our Compromise Security Recovery Practice and Detection and Response teams. Cover art is representative of the affiliate business model. Percentages do not represent actual discounts. Cover stat is based on Microsoft engagements over the past year.

© 2022 Microsoft Corporation. All rights reserved. Cyber Signals is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document is provided "as is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.