La Comunicazione - Note, Recensioni e Notizie n. 67
Anno 2023

Ransomware: gang criminali, stati e possibili difese

Ransomware: criminal gangs, states, and possible defenses

Fabrizio Baiardi ♦

♦ Università di Pisa & Haruspex srl

Sommario

Questo lavoro analizza il fenomeno del ransomware sia in una prospettiva tecnologica che in uno scenario più ampio. La prima prospettiva considera le principali caratteristiche di una intrusione ransomware che la contraddistinguono da una normale intrusione, per poi adottare una prospettiva più vasta partendo da un 'analisi del fenomeno del ransomware-as-a-service e dei mercati sul dark web che offrono i vari servizi. Vengono poi illustrate le informazioni disponibili su alcune gang criminali che operano mediante ransomware ed i loro possibili rapporti con alcuni Stati. Infine vengono discusse alcune contromisure con i loro punti di forza e di debolezza. Il lavoro si chiude proponendo una strategia innovativa per contrastare il fenomeno.

Abstract

This paper reviews ransomware intrusion from a technological perspective and in a broader scenario. The former considers the distinguishing features of a ransomware intrusion with respect to a standard one. Then we analyze the broader contest of ransomware starting from ransomware-as-a-service and the dark web market offering this and further similar services. We also consider leaked information on criminal ransomware gangs and their relationship with some states. Lastly, we review possible countermeasures and outline some strengths and weaknesses of each one. The paper ends with a discussion of an innovative strategy to defeat these intrusions.

Keyword

Ransomware, dark web, exfiltration, initial access, double extortion, state-sponsored intrusion

1 - Introduzione

Il tema di questo lavoro è l'analisi delle evoluzioni che hanno permesso ad una forma di crimine, le intrusioni ransomware, che rendeva ad un gruppo criminale poche migliaia di euro al mese nel 2016, di rendere oggi milioni di euro al mese. Queste intrusioni hanno impatti non solo finanziari perché alcune intrusioni ad ospedali hanno sicuramente provocato delle morti rallentando o impedendo le cure di alcuni pazienti. Un'incursione ransomware in un ospedale universitario del nord est degli Stati Uniti ha bloccato la diagnostica per immagini per più di 40 giorni. Ad ulteriore conferma della pericolosità del fenomeno, molte riunioni del Cobra, il comitato del governo inglese per la gestione delle crisi, hanno avuto il ransomware come tema. Nonostante questa attenzione, a gennaio 2023 la Royal Mail è stata vittima di una intrusione della gang Lockbit che ha bloccato per più di un mese la distribuzione internazionale dei pacchi.

Il focus sulla gestione delle crisi provocate dalle intrusioni ransomware ha ridotto l'attenzione ad altri aspetti del fenomeno, fondamentali per capire le ragioni della sua diffusione e della complessità dei rimedi. Una delle linee guida del lavoro è evidenziare sia le caratteristiche delle intrusioni ransomware che le similitudini tra i modus operandi dei vari gruppi criminali (o gang) nell'ecosistema ransomware e delle ragioni per cui crescono e si arricchiscono. Queste similitudini sono alla base delle contromisure per combattere il fenomeno.

Un'ultima avvertenza è che molto spesso le vittime del ransomware non rendono pubbliche le intrusioni che le hanno colpite. Ad esempio, a marzo 2023 vi sono stati 23 attacchi segnalati rispetto a circa 400 attacchi non segnalati. Ciò riduce la significatività dei dati disponibili su intrusioni e riscatti presentati nel seguito o, meglio, indica che essi sono una stima ottimistica dei numeri e degli impatti di questa forma di crimine.

Il cap.2 di questo lavoro discute ciò che caratterizza le intrusioni ransomware rispetto ad altre forme di cyber crime. Il capitolo successivo riassume la storia del ransomware, lo stato attuale del fenomeno e le possibili evoluzioni.

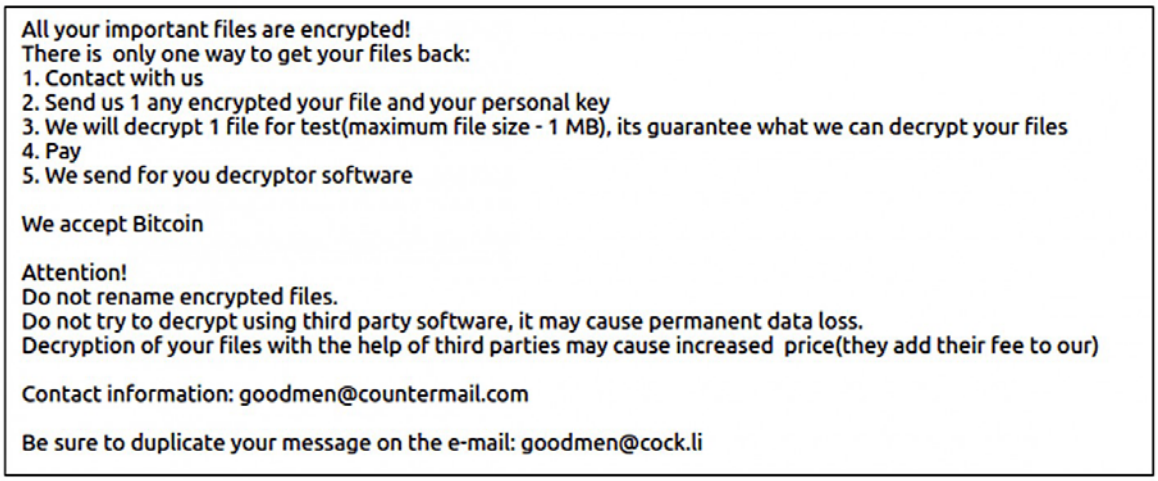
Il cap. 4 discute l'ecosistema ransomware ed alcune gang che vi operano. Il rapporto tra gang e Stati nazionali, fondamentale per capire la difficoltà di reprimere il fenomeno, è discusso nel cap. 5. Infine, il cap. 6 riassume alcune strategie per combattere il fenomeno e gestire il rischio corrispondente. Il capitolo sottolinea anche la necessità di nuove strategie di difesa. L'ultimo capitolo presenta una breve bibliografia per approfondimenti sull'argomento. Vista l'impossibilità di essere esaustivi, rimandiamo a Wikipedia per le informazioni sui singoli ransomware citati nel seguito e sulle loro varianti.

2 - Intrusioni ed intrusioni ransomware: similitudini e differenze

Riassumiamo in breve le caratteristiche del fenomeno ransomware rispetto ad altri crimini informatici.

2.1. Intrusioni ransomware

Nelle intrusioni ransomware, l'attaccante prende il controllo di un sistema ICT e cripta delle informazioni sul sistema attaccato. Le informazioni torneranno ad essere disponibili per gli utenti solo dopo aver pagato un riscatto per ottenere la chiave per decriptare. La Fig. 1 illustra una tipica richiesta di riscatto.


All your important files are encrypted!
There is only one way to get your files back:
1. Contact with us
2. Send us 1 any encrypted your file and your personal key
3. We will decrypt 1 file for test(maximum file size - 1 MB), its guarantee what we can decrypt your files
4. Pay
5. We send for you decryptor software

We accept Bitcoin

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price(they add their fee to our)

Contact information: goodmen@countermail.com

Be sure to duplicate your message on the e-mail: goodmen@cock.li

***Figura. 1**. Richiesta di riscatto*

In alternativa alla cifratura, l'attaccante può bloccare, rubare o cancellare delle risorse del sistema quali file, folders, boot records o master file tables con indici per l'accesso ai file. ENISA riassume le azioni possibili nell'acronimo LEDS, (lock, encrypt, delete, steal). Il ransomware è la forma più innovativa e redditizia di crimine informatico e non solo, visto che alcune analisi indicano un margine di profitto del 98% per le somme investite in intrusioni ransomware rispetto al 92% del traffico di cocaina, con una probabilità di essere arrestati circa 100 volte minore. Da alcuni anni, ogni giorno si registrano intrusioni dovute ad una variante di ransomware ed esistono moltissimi siti dedicati unicamente alla storia o alle statistiche su questo fenomeno.

2.2. Prima del ransomware

Gli obiettivi delle intrusioni informatiche, non legate al ransomware, sono il furto di informazioni o l'installazione di malware. Il bersaglio delle intrusioni per installare un malware sono le infrastrutture critiche. Di solito l'agente che le implementa è sponsorizzato da uno Stato, rappresentando la cosiddetta Advanced Persistent Threat, o APT, ed il malware permette di manipolare e sabotare il funzionamento dell'infrastruttura.

Le intrusioni per furto di informazioni sono più complesse ed hanno come obiettivo o lo spionaggio o la vendita delle informazioni ad altri. Nel caso dello spionaggio, gli attaccanti sono sponsorizzati da Stati, eg agenzie di intelligence, per acquisire informazioni utili per supportare le scelte dei decisori politici o proprietà intellettuali su tecnologie e prodotti legati alla sicurezza nazionale. Le informazioni sono sfruttate in trattative politiche o economiche o ancora per riprodurre tecnologie e prodotti in industrie nazionali. Ad esempio, le intrusioni di APT sponsorizzati dalla Cina contro alcune aziende US sono state descritte da autorevoli membri del congresso USA come "il più grande furto di proprietà intellettuale del XX secolo"[1].

[1] Si veda anche Annual Intellectual Property Report to Congress FY2021, https://www.whitehouse.gov/wp-content/uploads/2022/04/FY21-IPEC-Annual-Report-Final.pdf

I criminali rubano informazioni per rivendere sul dark web informazioni quali numeri di carte di credito, credenziali bancarie, documenti di identità ed analisi mediche. Anche se gli Stati possono essere interessati a queste informazioni, il vero guadagno proviene dalla vendita delle informazioni esfiltrate.

In tutte le intrusioni precedenti, l'attaccante cerca di minimizzare il proprio rumore per impedire la rilevazione dell'intrusione. Ciò permette non solo di esfiltrare una maggiore quantità di informazioni, ma anche di evitare che le informazioni rubate vengano invalidate e quindi perdano di valore. Ad esempio, un numero di carta di credito annullato perde immediatamente ogni valore. Questo porta l'attaccante a preferire bersagli di media grandezza, i cui sistemi informatici memorizzano e gestiscono una ragionevole quantità di dati, ma che non utilizzano strumenti sofisticati per la rilevazione di intrusioni. Ciò offre agli attaccanti un vantaggio rispetto ai difensori. La redditività del furto di informazioni è ridotta perché la loro vendita sul dark web sfrutta degli intermediari per collocare quanto esfiltrato e per nascondere gli autori dell'intrusione. Un altro fattore che riduce la redditività del crimine è il numero elevato di intrusioni che hanno successo e che aumentano le informazioni in vendita, ad esempio i numeri delle carte di credito, e quindi ne diminuiscono il valore. Storicamente, il valore del numero di una carta di credito si è ridotto fino a pochi dollari. Riassumendo: all'aumentare del numero di attaccanti diminuisce la redditività dei furti di informazione, anche se le vittime sono diverse.

Una conferma dell'evoluzione del crimine, dal furto e riciclaggio di informazioni finanziarie al ransomware, è la storia del gruppo FIN7 che è apparso nel 2012 ed inizialmente era attivo nel furto e nella rivendita di numeri di carte di credito. Successivamente è passato alle intrusioni ransomware focalizzandosi inizialmente nel settore del commercio e del turismo per poi passare ad istituzioni finanziarie, trasporti e difesa. Il gruppo è anche attivo nella fornitura di strumenti software ad altri gruppi dell'ecosistema criminale.

2.3. Ransomware: aspetti innovativi

Il diffondersi delle criptovalute ha mitigato in parte il problema della concorrenza tra attaccanti che si sono concentrati, seguendo l'esempio degli hacker della Corea del Nord, sul furto di dette criptovalute. La diffusione delle criptovalute ha però facilitato anche quella del ransomware. Inizialmente, le criptovalute hanno provocato il passaggio del crimine informatico dal furto di informazioni all'installazione di malware per il mining delle criptovalute stesse. L'uso fraudolento di risorse altrui per il mining elimina la concorrenza tra attaccanti che non devono più competere per vendere informazioni in qualche modo equivalenti. Inoltre, le criptovalute permettono di minimizzare gli intermediari perché, ad esempio, non sono più necessari dei "muli" che incassino e trasportino valuta.

La volatilità delle criptovalute mette però a rischio sia la redditività che il capitale accumulato e questo ha spinto il crimine a concentrarsi sul far fruttare non le informazioni e le risorse delle vittime, ma la disponibilità delle proprie informazioni. Il primo ad essere danneggiato dalla non disponibilità delle informazioni è il loro proprietario. Quindi, se impediamo l'accesso alle informazioni, il loro proprietario sarà disposto a pagare per riottenerlo e non occorre trovare altri compratori. Anche questa strategia, come il mining, evita la competizione tra attaccanti. Un modo di impedire l'accesso alle informazioni è di esfiltrarle e cancellarle, ma questo aumenta la complessità dell'intrusione perchè l'esfiltrazione richiede tempo e facilita la rilevazione dell'intrusione. Un modo relativamente semplice, ma estremamente potente, di impedire l'accesso alle informazioni è di criptarle. Inoltre, la crittografia asimmetrica permette di generare una coppia di chiavi sul sistema attaccato e di usare quella pubblica per cifrare tutte le informazioni. In questo modo occorre esfiltrare solo la chiave per decifrare, quella privata, che viene trasmessa ad un sistema controllato dall'attaccante. Ciò minimizza la quantità di informazioni da esfiltrare e trasforma la crittografia, uno degli strumenti di difesa più potenti, in uno strumento di attacco. Inoltre, non è necessario nascondere l'intrusione perché il proprietario del sistema ne è ben cosciente.

Anzi, la diffusione delle notizie sul successo delle intrusioni può convincere altri proprietari a pagare il riscatto per i sistemi già attaccati o che lo saranno. Il fatto che chi ha realizzato una intrusione ransomware abbia tutto l'interesse ad informare la vittima il prima possibile è confermato dalla diminuzione del tempo medio di scoperta di una intrusione, da quando si è verificata all'apparire del fenomeno ransomware, e dal fatto che nel 75% dei casi la scoperta avviene grazie ad una segnalazione esterna.

Un attaccante che riesca anche ad esfiltrare le informazioni criptate può minacciare la loro divulgazione per aumentare la pressione sulla vittima. Infatti, la divulgazione può provocare ulteriori perdite per la pubblicazione di dati finanziari, di proprietà intellettuale o di informazioni personali o sensibili con possibili violazioni delle leggi, eg del GDPR. Ad esempio, la pubblicazione da parte di Lockbit delle chat della negoziazione con Royal Mail mostrano che Lockbit era ben cosciente che il ricatto richiesto, 66 milioni di sterline, era comunque inferiore alla multa massima che le autorità potevano infliggere a Royal Mail per la diffusione dei dati. Nel febbraio 2023, la Security Exchange Commission US ha multato di tre milioni di dollari la software house Blackbaud, che gestisce database su cloud, per non aver informato in modo corretto i suoi clienti sulla esfiltrazione di dati personali dai loro database, provocata da una intrusione ransomware nel maggio 2020. Sempre nel febbraio 2023, la gang Medusa ha pubblicato un video con tutti i dati esfiltrati dalle scuole di un distretto di Minneapolis con più di 35.000 studenti.

Il danno provocato dalla pubblicazione dei dati è alla base della strategia di double-extortion dove, dopo il pagamento del riscatto per rilasciare la chiave, l'attaccante può chiedere un nuovo riscatto per non divulgare le informazioni. Nei casi peggiori, la double-extortion si trasforma in n-extortion perché il ricatto si prolunga nel tempo e nessuna prova è possibile della cancellazione, da parte dell'attaccante, di un dato esfiltrato. Ovviamente, contro gang che adottino double-on-extortion non è possibile difendersi usando backup per ripristinare i dati criptati.

Come tutte le intrusioni, anche quelle ransomware devono accedere inizialmente al sistema da attaccare. Per questo accesso, gli attaccanti possono usare soluzioni che vanno dalle email di phishing ai falsi update di una delle applicazioni o che sfruttano le vulnerabilità del sistema. Questi attacchi sono lanciati da un'infrastruttura, c.d. d'attacco, costituita da una botnet, una rete nascosta che connette nodi di terzi e che la gang ha creato attaccando in modo nascosto tali nodi. Alcune versioni del ransomware si diffondono in modo autonomo, come carico utile di worm che sfruttano vulnerabilità che permettono attacchi remoti. Gang diverse possono usare soluzioni differenti per diffondere la stessa versione di ransomware.

La minore complessità, e la maggiore redditività, contribuiscono a spiegare l'aumento esponenziale delle intrusioni ransomware e la loro evoluzione da strumento usato da Stati a strumento tipico della criminalità organizzata. Come discusso in un prossimo capitolo, separare nettamente il mondo degli attacchi sponsorizzati da Stati da quelli della criminalità è comunque difficile, perché alcune realtà statali possono essere interessate ad acquistare le informazioni esfiltrate o le gang possono offrirle gratuitamente per ottenere una benevola neutralità. Ad esempio, la gang Wizard Spider, che è passata al ransomware dopo essere stata attiva nel settore delle frodi bancarie e finanziare, utilizza strumenti che ricercano ed esfiltrano automaticamente file che contengano termini quali militar, secret, army: un comportamento tipico di APT che lavorano per conto di Stati.

3. Una breve storia

Generalmente, si assume che il primo malware per ransomware sia apparso nel 1989 nella conferenza sull'AIDS dell'Organizzazione Mondiale della Sanità, dove è stato distribuito, mediante floppy disk, un malware che crittografava i nomi dei file dopo novanta avvii del sistema. Il riscatto per la chiave per decifrare era di 189 dollari da pagare ad una casella postale a Panama. Era piuttosto facile neutralizzare il malware tramite strumenti di crittografia disponibili online.

3.1 Gli inizi

Nel 2005 alcune gang hanno iniziato a utilizzare una crittografia asimmetrica che poteva essere invertita con una password di trenta cifre fornita dopo aver pagato il riscatto. Gli strumenti antivirus potevano identificare ed analizzare facilmente questi malware. Nel 2009 sono apparsi malware che sfruttavano le vulnerabilità nei plugin del browser e che venivano installati quando gli utenti cliccavano su alcuni allegati di posta. Un altro malware che attaccava singoli utenti è apparso nel 2010 e bloccava i sistemi Windows fino al pagamento di un piccolo riscatto. Negli stessi anni sono comparsi alcuni ransomware per Mac. La comparsa di Cryptolocker nel 2013 ha portato numerose innovazioni, ad esempio l'accesso iniziale al sistema poteva usare o phishing tradizionale o attacchi lanciati dalla botnet Gameover Zeus. Un'altra innovazione è stata l'adozione di chiavi RSA a 2048 bit con il conseguente aumento della complessità del cracking della crittografia. Il successo di CryptoLocker ha portato ad un aumento significativo delle varietà di ransomware.

Nel 2015 sono apparsi ransomware di tipo locker che impedivano l'accesso al sistema criptando risorse quali i boot record o le master file tables.

Nel 2016 sono apparse ulteriori varianti di ransomware insieme ai primi fenomeni di ransomware-as-a-service (RaaS) nella forma ancora primitiva di una partnership in cui un gruppo di sviluppatori produce il malware che un gruppo di hacker usa nelle sue intrusioni. Altri eventi critici del 2016 e 2017 sono legati alla comparsa di Petya. Inizialmente, questo ransomware ha avuto meno successo di CryptoWall, che riutilizzava il codice di CryptoLocker, ma il 17 giugno 2017 è emersa la variante NotPetya che si diffondeva grazie ad EternalBlue, un exploit che sfruttava una vulnerabilità di Windows scoperta dalla NSA e pubblicizzata da Wikileaks. NotPetya era diffuso da un worm che usava i sistemi già infettati per lanciare altri attacchi e che dall'Ucraina si è diffuso in tutto il mondo provocando danni per 10 miliardi di dollari.

Diversi governi occidentali hanno attribuito alla Russia, ed in particolare al gruppo Sandworm del GRU lo sviluppo di NotPetya[2]. A complicare ulteriormente l'analisi, NotPetya sovrascriveva il Master Boot Record di Windows. Ciò impediva di accedere ai file anche se fossero stati decriptati e quindi la cifratura non poteva essere invertita, visto anche che il malware non trasmetteva informazioni all'attaccante. Nella migliore tradizione di "it is not a bug but a feature", non si è mai chiarito se ciò fosse un errore degli sviluppatori o se, come diversi analisti ritengono, l'obiettivo principale di NotPetya fosse quello di forzare a cancellare i file criptati per nascondere le tracce di altre intrusioni. Questa ipotesi dovrebbe forse essere rivalutata alla luce dei numerosi attacchi wiper portati da Sandworm contro l'Ucraina. Scopo di un attacco wiper è quello di cancellare definitivamente le informazioni su un sistema. Molti analisti definiscono NotPetya "un wiper mascherato da ransomware". Come discusso nel seguito, NotPetya ha prodotto una causa legale non ancora risolta tra alcune vittime e le loro compagnie di assicurazioni che si sono concordemente rifiutate di rimborsare i danni dell'intrusione, asserendo che l'attribuzione alla Russia provava che si trattasse di un atto di guerra, e quindi non coperto dalla polizza. Sempre nel 2017 è comparso WannaCry che, come notPetya, si è diffuso tramite EternalBlue. WannaCry ha causato danni per 4 miliardi di dollari ed ha infettato circa 230.000 computer con sistema operativo Windows che non erano aggiornati, anche se Microsoft aveva già rilasciato una patch da due mesi. L'intrusione più significativa è stata quella al sistema sanitario inglese che ha avuto successo nonostante pochi mesi prima diverse valutazioni del rischio cyber avessero segnalato le vulnerabilità nei sistemi ICT ed il rischio associato.

A partire dal 2018 la criminalità ha sviluppato ed utilizzato versioni di ransomware in grado sia di crittografare che di esfiltrare le informazioni.

[2] https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks
https://home.treasury.gov/news/press-releases/sm0410
https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/

La strategia prevede l'uso delle due funzioni e la creazione di siti, siti name-and-shame, per diffondere le notizie sugli attacchi e pubblicare i dati esfiltrati. Le strategie utilizzate sono sofisticate ed aumentano la pressione sulla vittima, pubblicando il nome dell'azienda vittima con alcune lettere mascherate o il settore commerciale in cui opera l'azienda ed il suo fatturato fino ad arrivare ad un filmato con i dati esfiltrati. Il tempo che passa dall'intrusione alla pubblicazione delle informazioni sul sito varia da due a dieci giorni. Questa strategia, chiamata *doxware* o *leakware*, è diventata molto popolare tra le gang. A sua volta, questa popolarità ha aumentato sia la visibilità che la diffusione del ransomware.

3.2. Gli ultimi anni

Nel 2020 RagnarLocker è stato il primo ransomware ad usare macchine virtuali e sfruttava anche cartelle condivise per raggiungere i file ed eludere i meccanismi per rilevare le intrusioni. Nel 2020 Maze è stato il primo caso noto di ransomware che esfiltrava dati sensibili per ricattare gli utenti. Durante la pandemia del 2020, sono aumentati gli attacchi contro ospedali e centri medici ed è emersa una versione di ransomware chiamata Corona. Nel 2021, il ransomware Conti ha attaccato il sistema sanitario irlandese provocando il blocco delle prenotazioni e delle visite, ma non delle vaccinazioni. Il sistema sanitario non ha pagato il riscatto di 20 milioni di dollari, ma ha ottenuto comunque dalla gang la chiave per decriptare. Secondo molti, questa "buona azione" della gang è stata forzata dalle pressioni di altre gang e del Cremlino. Il ripristino del normale funzionamento dei sistemi colpiti ha richiesto comunque alcuni mesi. Un'altra conseguenza della pandemia è stata un maggior sfruttamento di vulnerabilità in moduli per vpn per ottenere l'accesso iniziale ai sistemi. Sono ormai popolari anche ransomware che usano le soluzioni di wake on lan per riattivare sistemi spenti per cifrare le loro informazioni o cancellare copie di backup.

Dopo il 2020, le gang hanno abbandonato la tecnica “spray and pray” degli attacchi non mirati, in favore di “big-game-hunting” focalizzandosi su aziende più grandi che possono pagare riscatti più elevati con maggiori profitti. Nel 2022 solo la gang Deadbolt ha continuato ad attaccare piccole imprese ed anche singoli individui, utilizzando la blockchain di Bitcoin per automatizzare la spedizione della chiave alle vittime che pagavano il riscatto. Un errore nel codice (smart contract?) per la gestione dei pagamenti ha permesso ad alcune vittime di ottenere la chiave senza pagare. In media il riscatto pagato a Deadbolt è stato di 476 dollari rispetto ad una media complessiva di circa 70.000 dollari, con un incasso complessivo di più di 2 milioni di dollari. L’adozione di big-game-hunting ha portato ad un uso più diffuso di botnet come infrastrutture di attacco per stabilire l’accesso iniziale ad un sistema.

4. Lo stato attuale e le possibili evoluzioni

Gli impatti degli attacchi ransomware sono ancora aumentati e nel 2022 vi sono state più di 2800 vittime con un riscatto medio superiore ai 3 milioni di dollari. Nello stesso anno, il 66% delle intrusioni che avevano come obiettivo il guadagno finanziario sono state legate al ransomware mentre in circa il 20% delle intrusioni che hanno rubato informazioni, il furto era finalizzato a forzare il pagamento di un riscatto. Operando in modo estremamente opportunistico, le gang non sono interessate al tipo di azienda, ma solo al riscatto che può pagare. Alcune gang preferiscono attaccare organizzazioni con maggiori entrate, mentre altre si focalizzano su organizzazioni che operano in settori specifici dove si diffondono più velocemente informazioni sui danni delle intrusioni, favorendo così il pagamento del riscatto. Infine, alcune gang scelgono in base al tipo di dati che possono esfiltrare.

Nel 2022 e nel 2023, le intrusioni di tipo double-extortion sono aumentate complessivamente di circa l’80% ed in alcuni settori, come quello sanitario o della ristorazione, sono triplicate o quadruplicate.

Contemporaneamente sono cresciuti ecosistemi complessi in cui creatori di ransomware convivono con gang specializzate che eseguono una sola operazione come penetrare inizialmente in un sistema, installare il ransomware o trattare il riscatto.

Le gang interagiscono sui dark market. Prima dell'invasione dell'Ucraina, nessun ransomware attaccava sistemi nei paesi della ex CSI controllando o il linguaggio di default del sistema o geolocalizzando l'indirizzo IP. Questo ha spinto Fabian Woser, chief technology officer of Emsisoft, a proporre la contromisura più economica contro il ransomware, quella di cambiare il linguaggio di default a russo o collegare una tastiera russa al sistema. La situazione è cambiata perchè in un rapporto apparso nel Febbraio 2023, Google e Mandiant segnalano alcuni attacchi ransomware contro infrastrutture russe dovute a gruppi di attivisti che hanno anche riciclato malware di gang russe.

Una soluzione tecnica per accelerare le intrusioni è quella dell'intermittent encryption, o encryption parziale, che cifra solo parte di un file. Ciò riduce i tempi senza diminuire l'impatto per le vittime. Altre strategie di accelerazione cifrano solo file in archivi condivisi, ritenuti più critici, o utilizzano versioni parallele del software lanciando fino a 32 thread paralleli.

4.1. Il ransomware con un tocco umano

Attualmente, una intrusione ransomware è caratterizzata da quello che Microsoft ha definito human-operated ransomware. In pratica, tutte le intrusioni prevedono necessariamente alcune fasi: accesso iniziale, esplorazione del sistema e raccolta di informazioni, aumento dei privilegi dell'attaccante ed esecuzione del ransomware per criptare le informazioni. Con l'accesso iniziale l'attaccante entra nel sistema, mentre con l'esplorazione del sistema l'attaccante scopre i collegamenti, il sistema operativo e le applicazioni installate in ogni nodo e le loro vulnerabilità. La fase di aumento dei privilegi sfrutta alcune vulnerabilità che consentono di eseguire uno o più attacchi per controllare un account su alcuni nodi o per diventare amministratore di una macchina.

Una o più fasi possono essere automatizzate, ad esempio usando una piattaforma d'attacco o uno scanner, ed esistono anche ransomware che automatizzano completamente l'intrusione. Invece, nel human-operated ransomware il passaggio tra fasi non è automatizzato ed è guidata da umani che prendono decisioni in base a quanto scoprono esplorando un sistema. In passato, l'intrusione ransomware era spesso semplice ed automatizzata, e quindi operava in modo non mirato ma opportunistico sui sistemi affetti dalle vulnerabilità che il malware poteva sfruttare o tramite gli utenti che cliccavano su link contenuti in e-mail di phishing. Era una strategia pensata per grandi numeri di intrusioni e quindi su singoli riscatti più bassi. Attualmente, ogni gang utilizza strumenti e soluzioni diverse per i vari passi e quindi vi sono diversi livelli di automazione, ma il passaggio fra i vari passi è comunque guidato dalla esplorazione del sistema. In questa fase, gli attaccanti possono scoprire e poi criptare ed esfiltrare i dati più preziosi, aumentando l'importo del riscatto. Ciò permette agli attaccanti non solo di raccogliere informazioni, ma di continuare a rimanere nel sistema. Questa persistenza permette di monetizzare ripetutamente la stessa intrusione, utilizzando anche più varianti di uno stesso ransomware. Vi sono quindi poche garanzie che gli attaccanti lasceranno il sistema dopo il pagamento del riscatto.

Una intrusione human-operated è molto simile ad una intrusione classica con l'unica fondamentale, ma ovvia, analogia che chi paga è sempre il proprietario del sistema. ~~In~~ Con questo modo di operare, il tocco umano può variare sia gli obiettivi che le tecniche e gli strumenti utilizzati in base alle opportunità uniche scoperte dagli attaccanti nel sistema. La raccolta di informazioni permette di profilare l'organizzazione e di scegliere cosa criptare, cosa esfiltrare ed il riscatto da chiedere. Spesso gli attaccanti utilizzano i dati raccolti per invalidare i controlli di sicurezza presenti e per verificare l'efficacia del loro malware "in produzione" cioè nell'ambiente del loro bersaglio. Se alcuni moduli del malware vengono rilevati e bloccati da uno strumento di sicurezza, gli attaccanti possono acquisire sui dark market ed utilizzare una versione diversa degli stessi, modificare il payload oppure usare ransomware diversi in intrusioni distinte che possono anche avvenire contemporaneamente.

Gli attaccanti possono anche manipolare gli strumenti di sicurezza che difendono un sistema per sfruttare gli elevati privilegi necessari a questi strumenti, come terminare applicazioni o rimuovere file. Ad esempio, in alcune intrusioni gli attaccanti hanno usato ai loro fini i privilegi di strumenti di endpoint detection and response. Paradossalmente, anche la rilevazione di alcuni attacchi da parte degli strumenti di difesa può giocare a favore degli attaccanti dando ai difensori, e.g. al Security Operation Center, un falso senso di sicurezza riguardo al fatto che le soluzioni esistenti stiano funzionando.

Nel 2021, il tocco umano si è spinto fino all'utilizzo di phishing mirato, o spear phishing, con chiamate telefoniche per convincere la vittima a concedere un accesso remoto al sistema ad un fantomatico centro remoto di assistenza. Questa strategia, chiamata BazarCall, è stata usata per prima dalla gang Conti e poi si è diffusa perché, dopo lo smantellamento di Conti, descritto nel seguito, alcuni suoi membri sono migrati in altre gang. Nel 2022 si è avuto un elevato incremento delle intrusioni in cui l'accesso iniziale al sistema è stato ottenuto mediante questa tecnica. Si prevede che in futuro verranno utilizzate persone sempre più specializzate sui temi di sicurezza informatica per aumentare il realismo della telefonata ed aumentare così il numero delle vittime. Attualmente i bersagli del phishing sono utenti Windows perché si ritiene che gli utenti Linux abbiano in media una competenza informatica migliore, siano più consapevoli dei rischi informatici e che quindi richiedano più informazioni prima di concedere l'accesso remoto. In generale, la gestione dei call center utilizzati da questa soluzione è in carico a gang specializzate, anche se sono stati usati call center commerciali in India.

Sempre in riferimento al phishing, un altro tocco umano di alcune gang è l'uso di account di posta istituzionali di alcune vittime per inviare mail con attachment malevoli a potenziali nuove vittime. L'idea è che l'uso di account legali riduca le difese dei destinatari e faciliti il download e l'esecuzione del malware.

4.2 Automazione e nuovi linguaggi

Nonostante la diffusione dello human-operated ransomware, alcune gang preferiscono sempre soluzioni a maggiore automazione che, ad esempio, si diffondono sfruttando le risorse condivise tra i vari nodi di un sistema ed operano in parallelo su nodi diversi, riducendo a poche ore il tempo dall'accesso iniziale alla cifratura. Come sempre, la redditività cresce con l'automazione. Queste gang scelgono la versione di ransomware da utilizzare in base al sistema target grazie anche al diffondersi del RaaS che permette di scegliere in una gamma di versioni e famiglie di ransomware.

È anche in corso la riscrittura dei malware mediante linguaggi di programmazione più portabili per ridurre il costo dello sviluppo di più versioni dello stesso malware in grado di attaccare sistemi diversi. Molte gang utilizzano Rust per ridurre i costi della specializzazione rispetto ad un linguaggio come C++. Altri vantaggi sono una migliore gestione del parallelismo che permette prestazioni migliori ed il ridotto numero di strumenti per analizzare software sviluppato con questo linguaggio. Uno strumento ransomwae che è stato riscritto in Rust è HiveLocker, un ransomware efficace contro Windows e Linux usato da almeno 15 gang ed in grado di cifrare anche cartelle condivise in rete e di non cifrare file troppo grandi. Ovviamente, la riscrittura del software è anche una occasione per migliorare le capacità di evadere gli strumenti di difesa e di offuscare il codice per ostacolare eventuali analisi.

4.3 Ricatti senza encryption

In ultima analisi, con human-operated ransomware l'attaccante non deve necessariamente criptare informazioni o esfiltrarle, perché per richiedere un riscatto basta provare la capacità di poterlo fare, elencando ad esempio file e risorse critiche presenti nel sistema. Una intrusione che non riduce la disponibilità può avere come bersaglio un centro di cura o un ospedale e questo varia le regole di ingaggio delle gang ed i possibili riscatti. A conferma di questa evoluzione, alcune gang stanno chiedendo il pagamento di un riscatto con la sola minaccia di bloccare le attività di una organizzazione per un certo periodo.

For most companies we don't use crypt and give to managers the opportunity to decide their security issues without notifying lawyers and government departments.

They have the right to decide themselves because third parties force them to company's suicide.

After these notifications and cooperation company lose reputation and get financial losses in most cases.

So we recommend to write us ASAP and don't lose time"

***Figura 2**. Una richiesta di ricatto senza encryption di BianLin da un post sul blog di Redacted*

Altre gang come BianLian si sono riconvertite ed esfiltrano informazioni senza cifrarle, ~~e~~ chiedendo un riscatto per non pubblicarle. Come mostrato in Fig.2, tra l'altro questo non blocca le attività dell'azienda, non viene notato dai partner dell'azienda e permette trattative più lunghe e forse riscatti più alti visto che l'azienda non deve ripristinare le risorse o con la chiave di decifrazione o dai backup.

Un ulteriore vantaggio per le gang è il minor tempo richiesto da una intrusione che non cripti le informazioni. Nel caso della gang BianLian, il passaggio da encrypt a leak è stato anche facilitato dalla diffusione di uno strumento per decifrare i file criptati dalla gang.

Secondo fonti di threat intelligence, nel 2022 circa la metà delle intrusioni ha esfiltrato informazioni senza criptarle e più di metà dei siti name-and-shame sono apparsi nello stesso anno nel dark web. Altre fonti segnalano però la nascita di gang che operano in modo parassita e sfruttano il diffondersi delle intrusioni ransomware per estorcere riscatti con la minaccia di una intrusione, ma senza possedere le capacità tecniche per realizzare l'intrusione stessa. Alcune utilizzano le informazioni apparse nei siti name-and-shame di altre gang per dimostrare che conoscono le informazioni di una azienda.

L'unica difesa efficace da gang che fondano il tocco umano nella scelta dei bersagli e del malware da utilizzare e che non utilizzi encryption non può essere basata unicamente su copie di back up ma su un aumento di robustezza del sistema da proteggere che minimizzi la probabilità sia di accessi esterni e sia di persistenza degli attaccanti nel sistema.

Una nota positiva sulla situazione attuale dei ricatti pagati viene da Chainanalysis, una società che analizza le transazioni in criptovalute. Secondo un post sul blog di Chainanalysis del gennaio 2023, di fronte ad un aumento delle intrusioni con successo si ha una diminuzione della percentuale di riscatti pagati. Forse, come dimostra il caso del sistema sanitario irlandese, i tempi di ripristino anche una volta ottenuta la chiave, sono così alti che le organizzazioni preferiscono comunque non pagare. Questa situazione potrebbe però cambiare al diffondersi dei ricatti senza encryption. Un effetto sicuramente correlato alla riduzione del numero dei pagamenti è stata l'apertura di nuovi mercati, con un rapido aumento delle intrusioni, nei paesi dell'America Latina. Ovviamente, queste evoluzioni possono avere altre cause oltre a quella citata.

4.4 Ransomware e SCADA

Anche nel mondo del controllo industriale, la diffusione del modello RaaS ha portato ad un incremento significativo sia del numero di gruppi attivi che degli attacchi in cui prima di essere cifrate, le informazioni sono esfiltrate. La capacità di evadere meccanismi di difesa come Windows Defender è una caratteristica che ha contributo alla popolarità di alcuni malware tra cui Lockbit.

Nel corso del 2022 sono state attaccate aziende ed organizzazioni che operano nel settore automotive, nella distribuzione dell'acqua, ~~e~~ del gas e dell'energia, nel settore minerario e alimentare. La sensazione è che non ci sia una strategia precisa ma che gli attaccanti operino in modo opportunistico in base alle occasioni offerte dalle debolezze dei vari sistemi. Nel secondo semestre si è osservata una crescita di nuove gang ma non è chiaro se questo sia dovuto al riciclaggio di persone da altre gang. Gli analisti prevedono che grazie al RaaS ed al leaking di alcuni malware, nuovi gruppi appariranno anche nel 2023.

L'ultima innovazione è del gennaio 2023, quando un gruppo affiliato ad Anonymous ed impegnato nella difesa dell'Ucraina ha pubblicizzato lo sviluppo di una versione malware in grado di criptare direttamente i componenti SCADA usati nel controllo di processi industriali.

In passato, il ransomware coinvolgeva i componenti ICT che interagiscono con il controllo processi ma non bloccava tale controllo. Spesso, non era il ransomware ma il proprietario del sistema che bloccava per precauzione il processo controllato. Ad esempio, nell'intrusione della gang DarkSide alla Colonial Pipeline, la società ha bloccato l'oleodotto che gestiva ma solo perché l'intrusione impediva al sottosistema ICT di misurare, e fatturare, il consumo dei singoli utilizzatori. GhostSec attacca non i moduli ICT che interagiscono con i componenti SCADA, ma direttamente questi componenti. Ciò aumenta significativamente i rischi dell'intrusione perché impedisce il controllo del processo industriale con le ovvie conseguenze di affidabilità e rischio per le vite umane. Questa innovazione potrebbe facilitare la migrazione di strategie già efficaci contro sistemi ICT al mondo del controllo industriale. Comunque, vi sono molti dubbi sulla utilità, se non sulla possibilità, di cifrare i componenti per il controllo industriale. Infatti, la cifratura potrebbe provocare la perdita del controllo sull'impianto generando così rischi elevati di danni irreparabili agli impianti industriali ed alle persone che vi lavorano. Provocare danni irreparabili non è previsto dalla filosofia delle gang ransomware perché il pagamento del riscatto non garantirebbe il ritorno alla normalità. Molti analisti ritengono quindi poco credibile lo sviluppo e la diffusione di famiglie di ransomware che colpiscano direttamente impianti di controllo industriale.

4.5. Il futuro

Premesso che il parlare del futuro è sempre molto complesso, una facile previsione è quella sulla persistenza e la maggiore sofisticazione del RaaS. I servizi sempre più raffinati e le informazioni offerte sui dark market permetteranno una maggiore efficacia delle intrusioni ed una migliore selezione dei bersagli, individuando quelli con una più elevata probabilità di successo. La probabilità di successo aumenterà anche perché le maggiori risorse finanziarie a disposizione delle gang permetteranno loro l'acquisto di vulnerabilità zero day nei dark market che poi utilizzeranno nello sviluppo di malware. Complessivamente, le migliori informazioni ed i migliori malware ridurranno notevolmente il tempo necessario ad una intrusione dopo l'accesso iniziale.

I difensori di un sistema avranno quindi un compito più complesso e meno tempo a disposizione per scoprire e fermare un'intrusione. Inutile evidenziare che questa inferiorità dei difensori potrà essere risolta solo con un aumento degli investimenti necessari per la difesa, come discuteremo nel seguito.

Le gang continueranno nella loro strategia di sfruttare sia vecchie vulnerabilità non ancora eliminate che vulnerabilità appena scoperte o, come già detto, zero-day acquistate grazie ai profitti. Questo comportamento opportunistico è tipico di tutti gli attaccanti e non è limitato alle sole gang ransomware.

Una possibile evoluzione è l'integrazione di wiper nel malware per esfiltrare e cancellare anche delle informazioni in modo da spingere le vittime al pagamento del riscatto. Durante l'invasione russa dell'Ucraina abbiamo assistito ad un numero significativo di attacchi distruttivi condotti mediante wiper che cancellavano invece di cifrare le informazioni. Alcuni di questi attacchi, come quello con il malware Prestige, un altro prodotto di Sandworm, hanno avuto come bersagli altri paesi oltre all'Ucraina. Non è molto chiaro perché con una invasione in atto si senta la necessità di mascherare il wiper come ransomware. Qualcuno lo spiega con la plausible deniability ovvero la possibilità di negare di essere coinvolti nell'intrusione mascherandosi dietro le gang criminali con una strategia di false flag, ma proprio l'invasione in corso indebolisce questa spiegazione. Forse dovremo aspettare ancora qualche tempo per conoscere altri dettagli.

Un'ultima evoluzione riguarda il mondo Apple. Nell'Aprile 2023, la gang Lockbit ha annunciato una versione del proprio ransomware per sistemi Mac ed i possibili bersagli, ovvero i vari tablet e iPhone, sono estremamente popolari tra business men e manager e che si sono, per questo, diffusi anche in infrastrutture aziendali. Un bersaglio comunque diverso dalle infrastrutture informatiche che le varie gang hanno prediletto in passato. Nessuna delle altre gang in passato ha messo sotto tiro il mondo Mac, ma il diffondersi di questi sistemi ed una spiccata preferenza per il mondo Apple nelle giovani generazioni spiega la scelta di Lockbit.

Anche se le prime versioni sembrano ancora primitive ed alcuni meccanismi a difesa della integrità dei file aumentino la complessità dello sviluppo del ransomware, il fatto che una grande gang abbia preso di mira il mondo Mac è senz'altro indice di una tendenza che potrebbe diventare molto redditizia in futuro.

5. Ecosistema Criminale

Nel seguito esaminiamo brevemente il funzionamento dei mercati nel dark web, o dark market, e dell'ecosistema criminale. Esamineremo quindi le offerte di lavoro sul dark web e le poche informazioni disponibili su due delle gang criminali più note. Infine, analizzeremo i rapporti tra gang criminali ed alcuni Stati sovrani.

5.1 Dark market ed ecosistema

I mercati sul dark web, in breve dark market, hanno avuto e continuano ad avere un ruolo fondamentale nel rendere il ransomware una scelta sempre più popolare nel mondo criminale perché facilitano la collaborazione tra gang specializzate nello sviluppo software e gang specializzate in intrusioni. Ciò facilita il RaaS e riduce la barriera d'ingresso all'ecosistema ransomware. Infatti, in passato una intrusione ransomware richiedeva lo sviluppo di un malware che, a sua volta, era possibile solo possedendo significative competenze di sviluppo software, crittografia e capacità di penetrazione nei sistemi target. Di fronte a queste competenze, il profitto finale era moderato. I mercati semplificano le transazioni, diminuiscono le intermediazioni e permettono di acquistare i malware se e quando servono invece di svilupparli a priori.

I dark market influenzano anche le caratteristiche tecniche dei malware che ora possono essere utilizzati anche da chi è poco competente. Quindi le versioni offerte in RaaS sono altamente user friendly, con pannelli di controllo semplici, how-to e supporto tecnico. Un ulteriore vantaggio è che i dark market offrono anche vulnerabilità per lo sviluppo del ransomware.

Ovviamente, l'utilizzo delle criptovalute semplifica i pagamenti al di fuori dei circuiti ufficiali, anche se non sempre garantisce un completo anonimato.

Ciò che completa l'ecosistema, lo alimenta e lo rende autosufficiente, è che i dark market offrono anche accessi iniziali ai sistemi delle potenziali vittime, un'offerta che sta vivendo un momento di boom. Fonti di threat intelligence indicano che nel 2022 sono stati venduti circa 2200 accessi ed ognuno dei primi tre venditori ha ceduto un centinaio di accessi.

E' bene evidenziare come lo human-operated ransomware sia fortemente correlato all'ecosistema perché non vincola una gang ad alcuni strumenti predefiniti, ma le permette di acquistare i migliori e più convenienti una volta esplorato il sistema target. Infine, la presenza di fornitori specializzati in malware rende sempre più trascurabile la probabilità di vulnerabilità o di errori che permettano di decriptare le informazioni. Per ridurre ulteriormente vulnerabilità ed errori, alcuni venditori hanno creato programmi di bug bounty per ricompensare chi segnala errori. Inoltre, nei dark market sono anche in vendita botnet da utilizzare come infrastruttura d'attacco. Queste botnet fanno sempre più ricorso a soluzioni peer-to-peer aumentando significativamente la difficoltà di smantellarle. Inoltre, le gang condividono parti delle loro botnet per meglio resistere agli attacchi.

Cambiamenti nell'ecosistema sono possibili, perché la possibilità di ricattare senza criptare in qualche modo diminuisce l'importanza degli sviluppatori di ransomware rispetto a chi penetra nei sistemi e li esplora per scoprire le risorse e le informazioni critiche. In particolare, aumenta l'importanza delle gang che offrono accessi iniziali ai sistemi target o IAB, initial access broker, ed infatti il numero di gang specializzate in questo servizio è in continuo aumento. In particolare, si sta osservando una maggiore organizzazione della vendita degli accessi dove le gang acquistano con una frequenza regolare da uno IAB un blocco di accessi a sistemi diversi. Tutte le informazioni provenienti sia dalle vittime che dai dark market confermano la crescente specializzazione dei singoli attori e dell'elevato livello professionale dei membri delle gang

5.2 Dark market ed offerte di lavoro

Per approfondire ruolo e funzionamento dei dark market è utile capire come si crea il rapporto professionale tra una persona ed una gang. In un report apparso a fine gennaio 2023, Kaspersky ha analizzato il mercato del lavoro sul dark web dal gennaio 2020 al giugno 2022 a partire da offerte di lavoro e curriculum postati su 155 forum sul dark web. Complessivamente parliamo di circa 200.000 post con un picco a marzo 2020 quando la pandemia ha ridotto fortemente le offerte di lavoro legali. Di questi post, poco meno di 900 erano legati al mondo IT e le offerte di posti di lavoro erano circa il triplo delle richieste. In generale, le persone postavano il loro curriculum in risposta ad offerte.

Le competenze richieste spaziano dallo sviluppo di software per intrusioni alla gestione delle infrastrutture di attacco ed al *reverse engineering*. Dato che il dark web non apprezza le iniziative per formare degli hacker, la professionalità più ricercata è quella dello sviluppatore, circa il 60% delle offerte, con compensi che vanno dai 1.500 ai 2.000 dollari mensili tenuto conto del cambio del rublo. Il compenso medio maggiore è per figure specializzate in reverse engineering. I compensi di un attaccante per l'accesso iniziale sono inferiori e sono molto spesso richieste competenze su piattaforme come Cobalt Strike o Metasploit. Molte offerte hanno come requisito la non dipendenza da alcool o droghe. L'elevato numero di richieste per sviluppatori può indicare degli investimenti sullo sviluppo di strumenti di attacco ed intrusione più sofisticati di quelli attualmente disponibili.

Le procedure di assunzione sono abbastanza standard e molto simili a quelle nel mondo reale. Dopo alcuni test iniziali per verificare le competenze di sviluppo di malware, il processo di reclutamento prevede una intervista ed un periodo di prova. Per gli sviluppatori è ovviamente importante saper sviluppare software che non sia rilevabile dai più diffusi antivirus. Come è ovvio, tra i maggiori vantaggi di un impiego trovato sul dark web vi sono il lavoro remoto e gli orari di lavoro flessibili. Alcune offerte parlano di ferie pagate.

Infine, è interessante notare che sui dark market siano apparse anche offerte di lavoro per posizioni in aziende perfettamente legali e per incarichi altrettanto legali.

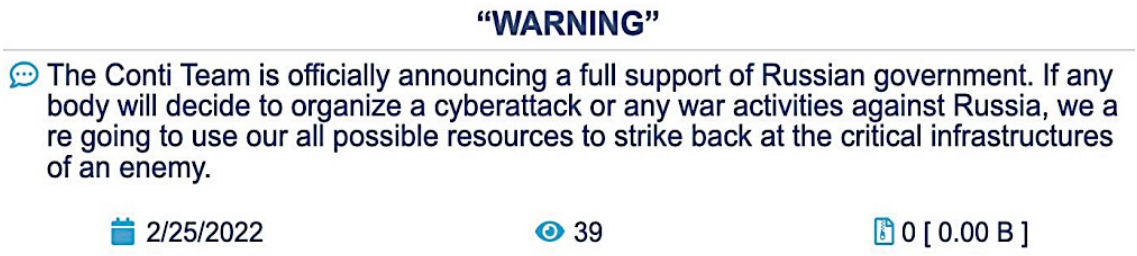


***Figura 3**. La presa di posizione della gang Conti*

5.3 La gang Conti

Nello scorso anno la gang russa Wizard Spider è stata vittima di una fuga di informazioni. Si tratta di una gang che ha incassato riscatti per centinaia di milioni di euro e ha utilizzato ransomware come Conti o Ryuk (e che, per semplicità, nel seguito indicheremo come Conti). Anche se la fuga di informazioni è legata alla invasione russa dell'Ucraina, quanto rivelato è completamente generale e probabilmente valido anche per altre gang.

L'evento che ha scatenato la fuga di informazioni è avvenuto il 25 febbraio 2022, poche ore dopo l'invasione, quando la gang ha pubblicato l'avviso in Fig. 3 schierandosi a fianco degli invasori e minacciando di attaccare chi avesse messo in pericolo le infrastrutture russe. Questa presa di posizione aumenta i sospetti sui legami tra la gang e lo Stato russo, sospetti alimentati anche dal fatto che Conti è l'unica gang che abbia sviluppato software per lo spionaggio di informazioni. La dichiarazione di Conti, definita da alcuni come la mossa più idiota che la gang potesse fare visti i suoi numerosi membri ucraini, è stata poi stemperata, ma ha spinto un membro ucraino della gang a pubblicare più di 60.000 messaggi di una chat interna. Una significativa informazione resa pubblica è che la gang comprende un centinaio di persone con una organizzazione interna simile a quella di una software house. Copiando l'organizzazione di una normale software house, la gang è organizzata con un reparto di amministrazione, uno di ricerca e sviluppo e uno di produzione.

Esistono regole per la gestione del codice dei malware prodotti e per non essere scoperti dalle forze di polizia. La gerarchia interna alla gang è molto rigida e fa capo ad un "presidente" ed un "amministratore". Il presidente, (indicato come Stern o Demon) e l'amministratore (Mango) comunicano molto frequentemente e stabiliscono privatamente le strategie del gruppo e valutano i dipendenti in base alla quantità e qualità del lavoro. Possono anche punire i dipendenti che non rispettano le scadenze o violano le regole della gang, ad esempio attaccando degli ospedali, un comportamento che secondo la dirigenza provoca un notevole danno di immagine. Forse i dipendenti a cui si fa riferimento sono quelli che hanno attaccato il servizio sanitario irlandese.

I programmatori a libro paga della gang hanno uno stipendio fisso mentre coloro che negoziano il pagamento dei riscatti sono incentivati con una percentuale dei profitti. Nel periodo di massima espansione si stima che circa 150 persone lavorassero nella gang con uno stipendio medio mensile di 2000 dollari US. Ciò porta ad un fabbisogno, per i soli stipendi, di 3,6 milioni di dollari US per anno, una quantità non banale di liquidità da reperire.

Le dimensioni della gang variano con un elevato turnover. I neoassunti provengono da normali software house o da forum di hacking. Per accelerare le assunzioni la gang stava valutando l'apertura di uffici di reclutamento a San Pietroburgo o di trasferirsi a Mosca. I dipendenti non possono, come vorrebbero, godersi una vacanza all'estero per il forte rischio di essere arrestati. La gang ha a libro paga dei giornalisti che dovrebbero porre sotto pressione le aziende attaccate per spingerle a pagare il riscatto, non vi sono informazioni sulla nazionalità di questi giornalisti, ma non possono essere russi visto che la gang non può attaccare aziende russe.

La gang utilizza un insieme di strumenti per l'anonimato come Tor, ProtonMail e Privnote con messaggi che si cancellano dopo un certo tempo. Utilizza anche CobaltStrike, una piattaforma di attacco sempre più popolare tra le gang che permette di automatizzare alcuni passi di una intrusione. La gang ha anche tentato di ottenere versioni demo degli antivirus commerciali per verificare che non rilevino i propri malware.

La fuga di informazioni ha anche permesso di accedere ai repository della gang con i vari eseguibili, alcuni dei quali sono stati poi usati per attaccare delle infrastrutture russe. Secondo altre fonti, le informazioni fornite dalla gola profonda ucraina avrebbero permesso di smantellare la botnet che la gang usa come infrastruttura d'attacco, ma la FBI ha chiesto di non rivelare queste informazioni in modo da monitorare le azioni della gang. Invece, la pubblicazione delle informazioni avrebbe forzato l'uso di una infrastruttura, ovvero una botnet, diversa. È comunque molto improbabile che la gang abbia continuato ad usare la stessa infrastruttura.

Le informazioni pubblicate producono la sensazione di una organizzazione strutturata per essere operativa a lungo, come confermato dal fatto che l'organizzazione ha assorbito altre gang e che gli attacchi sono continuati anche dopo il leaking di informazioni sulla sua struttura ed organizzazione. Però, nel maggio 2022, il governo USA ha offerto fino a 10 milioni di dollari per informazioni sulla gang e questo ha provocato il ritiro della gang o forse del solo brand. Tutti i membri di Conti si sono riciclati in altre gang o ne hanno create di nuove. Alla fine del 2022 erano note quattro varianti del ransomware Conti, alcune usate in attacchi contro organizzazioni pubbliche e private ucraine e contro organizzazioni umanitarie e del terzo settore europee. Nel febbraio 2023, la National Crime Agency UK, operando in modo congiunto con il Department of Justice US, ha incriminato sette cittadini russi per le loro attività criminali ed in particolare per lo sviluppo di Trickbot, un malware utilizzato da Conti ed altre gang. Dopo il ritiro di Conti, i sette russi hanno continuato a collaborare con altre gang contribuendo ad attaccare 149 organizzazioni inglesi. Recentemente, è apparso un ransomware che utilizza la backdoor Domino per raccogliere informazioni su un sistema su cui successivamente vengono installati strumenti sviluppati da Conti. Domino è uno strumento sviluppato da FIN7, una gang attiva nel crimine finanziario.

I travagli di Conti hanno suggerito ad altre gang, ad esempio Lockbit, di dichiarare, forse in modo opportunistico, la loro neutralità nel conflitto e il loro unico interesse nella crescita dei ricavi. A posteriori possiamo dire che, ad eccezione di Conti, l'invasione ha avuto effetti limitati se non nulli sulle gang che hanno continuato, con successo, a condurre i propri affari.

Un altro effetto delle vicende di Conti è la riduzione delle dimensioni delle gang perché con la dimensione aumentano anche i rischi di conflitti interni o di fughe di informazioni.

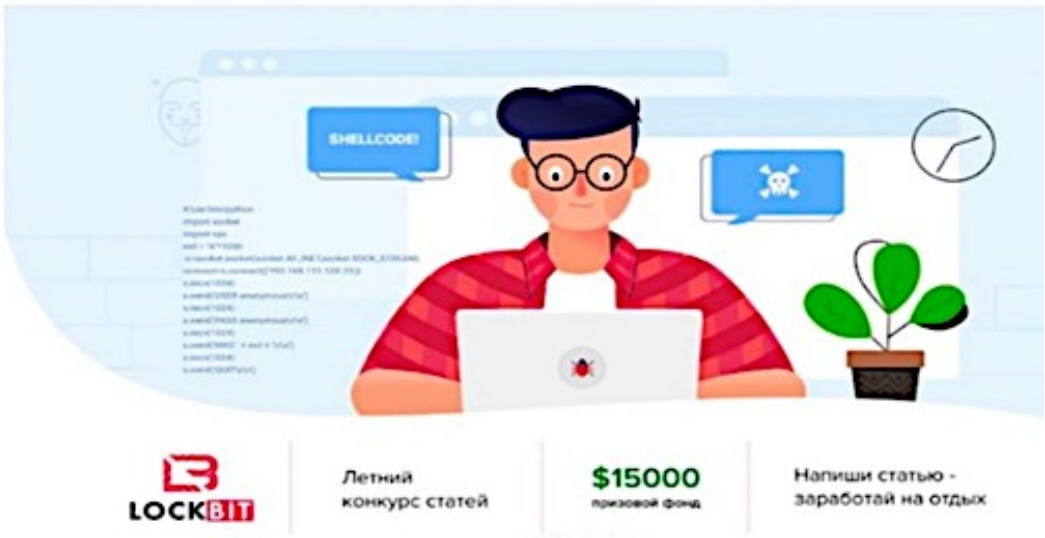


***Figura 4**. Annuncio del premio Lockbit per il miglior articolo*

5.4 La gang Lockbit

Lockbit è una delle gang più attive ed innovative nell'ecosistema criminale del ransomware. E' stata la prima ad automatizzare le proprie intrusioni ed ad usare un tunnel IPSEC per esfiltrare informazioni. Anche dal punto di vista del RaaS, Lockbit ha innovato utilizzando un modello in ~~in~~ cui il riscatto viene trattato ed incassato dalla gang che ha acquistato il ransomware di Lockbit mentre la gang Lockbit riceve a posteriori una percentuale del riscatto. In altri casi è chi fornisce il malware a trattare ed incassare per girare una percentuale a chi ha eseguito l'intrusione. Infine, Lockbit non chiede mai un riscatto ma un compenso per la consulenza nelle trattative per il riscatto e per la scoperta ed eliminazione di vulnerabilità nell'infrastruttura attaccata. Quest'ultima offerta non è però particolarmente innovativa perché il passaggio da membro di gang criminale a consulente di sicurezza non è certo una peculiarità russa o del mondo del ransomware.

Nel gennaio 2023 è apparsa una interessante analisi su Lockbit, la gang che ha attualmente eseguito il massimo numero di intrusioni con successo ed a cui è stato attribuito più del 40% delle intrusioni del 2022. Oggetto dell'analisi sono le notizie su Lockbit nelle chat e nei forum dell'underground russo dove i membri delle gang interagiscono usando Tox, un servizio di messagistica p2p criptato. L'analisi copre il periodo da settembre 2019 a gennaio 2022 e fornisce informazioni per approfondire i rapporti, le fusioni e le scissioni tra gang e le competizioni per offrire il proprio ransomware. Eventi sorprendenti e interessanti sono ad esempio la competizione per il miglior articolo scientifico sponsorizzata da Lockbit con 5000 dollari di premio, il call for paper è in Fig. 4, oppure le campagne diffamatorie contro gang rivali per segnalare il fallimento di intrusioni che usano il ransomware di un concorrente o che rivelano presunte collaborazioni con la FBI o lo Stato russo. Ad esempio, autorevoli membri di Lockbit affermano che le varie incarnazioni della gang Conti lavorino per il Cremlino.

Un altro evento legato alla gang Lockbit conferma l'evoluzione continua dei ransomware utilizzati. Il 16 Marzo 2023, una nota congiunta di FBI e CISA descrive Lockbit 3.0, l'ultima versione del ransomware che la gang fornisce agli affiliati. LockBit 3.0 è configurato al momento della compilazione con molte opzioni diverse che determinano il comportamento del ransomware. Durante l'effettiva esecuzione del ransomware nell'infrastruttura della vittima, è possibile fornire altri parametri per modificare ulteriormente il comportamento del ransomware. Ad esempio, LockBit 3.0 accetta argomenti aggiuntivi per operazioni specifiche in movimento laterale. Se un affiliato LockBit ha accesso a LockBit 3.0 solo con password, la password è un parametro obbligatorio durante l'esecuzione del ransomware. La password è una chiave crittografica che decodifica l'eseguibile LockBit 3.0. Proteggendo il codice in questo modo, LockBit 3.0 può anche ostacolare il rilevamento e l'analisi del malware. Infatti rilevamenti basati su firma potrebbero non riuscire a rilevare l'eseguibile. La porzione crittografata dell'eseguibile varierà in base alla chiave crittografica utilizzata per la crittografia. Quando viene fornita la password corretta, LockBit 3.0, continua a decifrare o decomprimere il suo codice ed eseguire il ransomware.

LockBit 3.0 infetta solo i computer in cui è impostata una lingua per il sistema che non appare in un elenco predefinito. La lingua di sistema viene controllata in fase di esecuzione in base ad un flag di configurazione originariamente impostato al momento della compilazione. Lockbit 3.0 si diffonde nel sistema attaccato usando un elenco di credenziali codificato nel codice, ma anche mediante strumenti come Mimikatz. Le informazioni sono esfiltrate usando o una evoluzione dello strumento di Lockbit 2.0 o un servizio di file sharing o di cloud sharing. L'esistenza di più meccanismi di esfiltrazione conferma l'evoluzione verso il name-and-shame ma anche la potenziale vendita di informazioni sul dark web o a Stati.

Per completezza di informazione, è doveroso aggiungere che dopo l'intrusione ad un ospedale pediatrico a Toronto, il 1° gennaio 2023 la gang si è scusata, ha inviato gratuitamente le informazioni per decifrare i vari file ed ha annunciato di aver terminato la collaborazione con gli affiliati che hanno eseguito l'intrusione. Era la prima volta che questo succedeva, ma poi le scuse, e l'offerta di decifrazione gratuita, si ~~è~~ sono ripetute ad aprile 2023 dopo che la gang ha colpito un distretto scolastico ed un asilo per bambini, il Keystone Smiles Community Learning Center.

5.5 Le gang e le versioni di ransomware

Le informazioni sulle gang e sull'ecosistema sono state arricchite dall'analisi dei flussi ~~di~~ dei pagamenti prodotti dalle varie versioni di ransomware. In particolare, lo stesso post di Chainanalysis che abbiamo già citato e che segnala il calo del numero di pagamenti, suggerisce che non vi è una associazione stretta tra gang e variante di ransomware. Una stessa gang può usare varianti diverse e la stessa variante può essere sfruttata da più gang. La conclusione di Chainanalysis è che l'ecosistema sia formato da un numero ridotto di persone che si muovono tra le varie gang e che usano diverse versioni di ransomware. È l'elevata dinamicità, che si prevede continuerà anche nell'anno in corso, a produrre l'illusione di molte gang ognuna con molti membri. Forse assistiamo ad una nuova versione dei villaggi Potëmkin, falsi villaggi di sole facciate creati per ingannare l'imperatrice Caterina II, o ad una nuova versione della guerra ibrida russa, perché comunque l'elevato numero di gang è un ostacolo per

l'attribuzione delle intrusioni. Il piccolo numero di membri delle gang spiegherebbe l'elevato numero di offerte di lavoro sul dark web.

Infine, alcuni analisti ipotizzano l'esistenza, a partire da maggio 2020, di un cartello che riunisca alcune gang, tra cui Conti e Lockbit. Le gang del cartello si scambiano membri, ransomware ed anche siti web e, probabilmente, infrastrutture d'attacco. Il cartello ha il duplice scopo di ridurre i costi ed aumentare la redditività dell'attività criminale. Probabilmente il termine cartello è esagerato perché non ci sono evidenze di condivisione di costi e profitti fra le gang, ma solo di un aiuto reciproco per la reciproca convenienza e per poter meglio intimidire le loro vittime. Da parte loro, le gang hanno negato l'esistenza del cartello senza approfondire le ragioni della innegabile condivisione di risorse.

5.6. Il rapporto tra le gang e gli Stati

Completiamo la descrizione dell'ecosistema ransomware discutendo brevemente i rapporti tra le varie gang dell'ecosistema ransomware ed alcuni Stati sovrani.

5.6.1. La Russia

Le considerazioni del paragrafo precedente pongono il problema dei rapporti tra le gang e lo Stato russo. Nessuno dubita che questi rapporti esistano ed alcune analisi evidenziano come, in un contesto in cui le relazioni sono flessibili e altamente variabili, vi sono tre principali tipi di rapporto: associazione diretta, affiliazione indiretta e consenso implicito.

Nel caso di associazione diretta, un esponente di una gang criminale viene assunto da un organo di sicurezza o di intelligence. Sono stati documentati casi di assunzioni di esponenti di rilievo di una gang o di importanti parentele tra membri di gang e dei servizi di sicurezza russi. Abbiamo affiliazione indiretta quando vi sono forti indicazioni dell'uso da parte di organi di sicurezza di risorse di una gang. Ad esempio, in passato l'infrastruttura di attacco di una gang creata per il furto di informazioni bancarie e per diffondere ransomware è stata utilizzate da organi di intelligence ~~o~~ per lanciare DDOS in conflitti in atto. Un altro possibile caso è quello scoperto nel materiale pubblicato sulla gang Conti.

Anche se è indubbio che la gang scelga i suoi obiettivi in base a criteri puramente economici e di rendimento, alcuni messaggi scambiati sulla chat indicano una collaborazione di membri della gang per scoprire informazioni su alcuni giornalisti di Bellingcat, agenzia di stampa molto attiva sulla Russia, ed in particolare di quelli che lavoravano sul caso Navalny. In altri messaggi, alcuni membri discutono sull'utilità e la convenienza di aprire un settore dedicato ad "operazioni politiche". Per chiarire l'importanza della affiliazione indiretta, alcuni rapporti di threat intelligence suggeriscono che le azioni della polizia russa contro alcune gang criminali abbiano avuto luogo solo per "spiegare" alle gang l'importanza dell'affiliazione indiretta e che le associate azioni giudiziarie siano state interrotte dopo che le gang hanno accettato di collaborare.

Nel caso di consenso implicito, le attività della gang non sono esplicitamente coordinate con le attività dello Stato russo, ma si integrano naturalmente con tali attività. Un possibile esempio sono intrusioni ransomware delle gang e diffusione di fake news da parte degli organi dello Stato russo. L'obiettivo finale dei vari tipi di rapporto è quello della plausible deniability o negazione plausibile ovvero la possibilità per uno Stato di non essere coinvolto in attività illegali svolte da alcuni suoi cittadini. Il comunicato ufficiale del Department of Justice sulla incriminazione dei sette cittadini russi già citato in precedenza indica, senza alcun dubbio, la gang Conti come controllata dai servizi di sicurezza russi.

Il rapporto non chiarito tra cybercrime e lo Stato russo è particolarmente critico ed importante, come provato dall'arresto per altro tradimento di Ilya Sachkov, fondatore e CEO di Group-IB, una azienda di cybersecurity. Sachkov ha fatto dichiarazioni critiche e molto informative sui rapporti tra cybercrime e Cremlino e sulla protezione offerta da alcune organizzazioni statali ai capi di una gang.

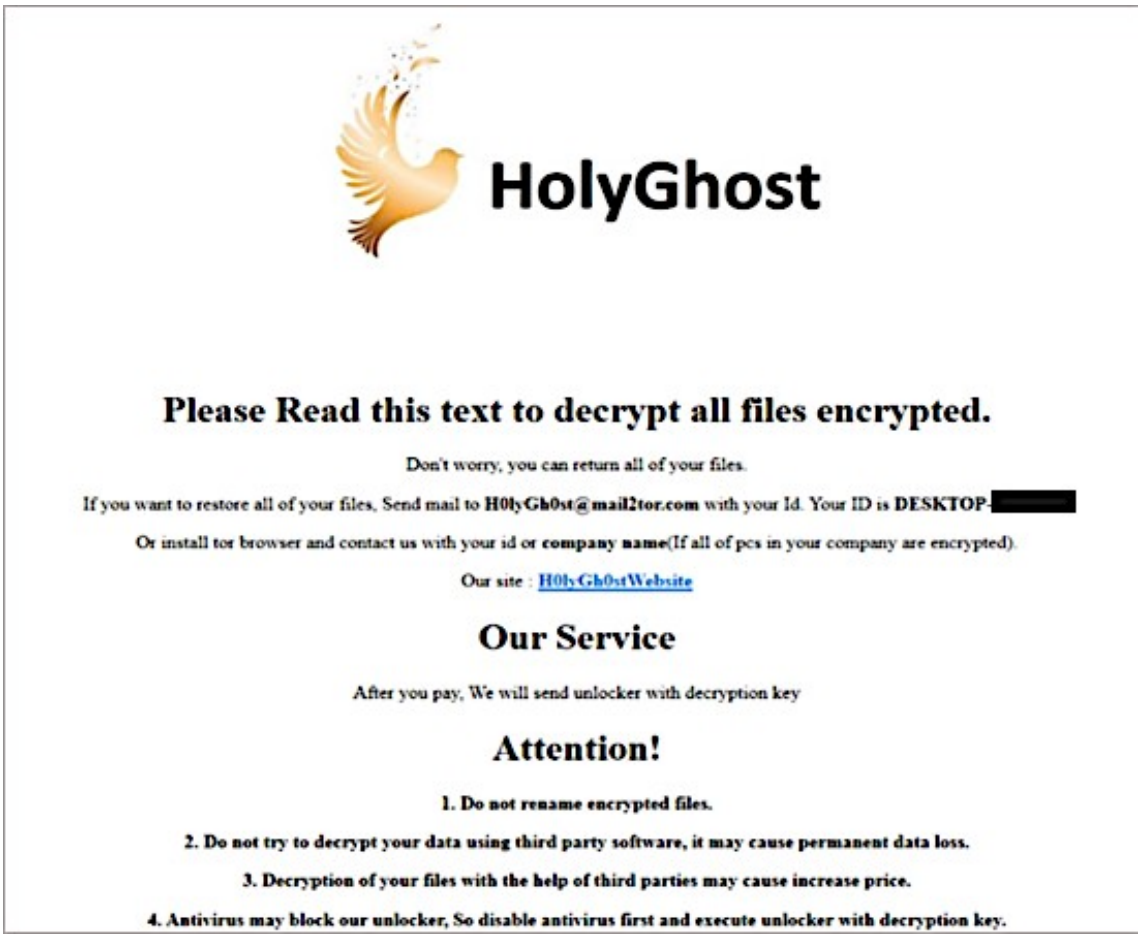


***Figura 5**. Richiesta di riscatto di H0lyGh0st*

Nell'ottobre 2022 è apparsa alla conferenza Cyberwarcon ad Arlington, Virginia, una interessante analisi sui rapporti tra le gang e lo Stato russo. L'analisi di K. Nershi e S. Grossman dello Standford Internet Observatory ha sfruttato la tecnica di double extortion ed ha analizzato i siti nel dark web che pubblicano i dati esfiltrati per valutare il numero di intrusioni in sei paesi democratici: USA, UK, Francia, Canada, Italia e Germania. Complessivamente, sono stati considerate 4,194 vittime di intrusioni ransomware avvenute tra il maggio 2019 e quello del 2022. Gli attaccanti sono stati divisi in due classi, basati in Russia e non basati in Russia. Una delle conclusioni dell'analisi è che gli attacchi dei gruppi basati in Russia aumentano, per ogni paese, nei tre mesi precedenti le elezioni. Un aumento simile non esiste per i gruppi non basati in Russia.

Inoltre, non esistono correlazioni tra il fatto di essere basati in Russia e il settore in cui opera una organizzazione vittima. Il sospetto immediato è quello di un supporto delle gang ransomware alla diffusione di fake news e di post di account fake che hanno tentato di influenzare le varie elezioni. La conclusione degli autori è che la Russia mantenga una relazione lasca, quella che prima abbiamo chiamato affiliazione indiretta, con le gang ransomware che operano come organizzazioni criminali indipendenti ma che non esitano, occasionalmente, a supportare azioni del governo russo in cambio di un riparo sicuro dalle azioni giudiziarie internazionali.

Infine, un possibile altro esempio di affiliazione indiretta sono i numerosi attacchi wiper condotti contro l'Ucraina durante l'invasione russa.

Complessivamente, possiamo riassumere la relazione tra Stato russo e gang ricordando i corsari inglesi che nel XVI secolo depredavano i galeoni spagnoli ma, quando necessario, davano anche una mano contro l'Invincibile Armata.

5.6.2 La Corea del Nord

I rapporti tra lo Stato russo e gang criminali sono di vario tipo, laschi e spesso ambigui, pochi dubbi esistono invece sugli attaccanti nordcoreani che sono sponsorizzati dallo ~~stato~~ Stato per acquisire sia valute tradizionali che cripto valute mediante intrusioni informatiche che utilizzano malware specializzati per il furto di valuta. Nel 2022, queste intrusioni sono diventate prioritarie rispetto a quelle per lo spionaggio ed il furto di informazioni. Stime risalenti a più di 4 anni fa indicano in 2 bilioni di dollari il ricavato complessivo che la Corea del Nord ha investito nello sviluppo di armi nucleari e di hardware per nuove intrusioni. Secondo Anne Neuberger, Deputy National Security Advisor for Cyber, circa un terzo dei fondi che la Corea del Nord investe nella produzione di armi di distruzione di massa proviene da cyber attacchi.

Per quanto riguarda il ransomware, a partire dal 2021 attaccanti nordcoreani hanno realizzato intrusioni contro aziende sanitarie pubbliche e private ed altre infrastrutture critiche usando i malware Maui e H0lyGh0st.

La richiesta di riscatto di H0lyGh0st in Fig. 5 è interessante perché contiene un link ad un sito del dark web dove si giustifica l'attacco spiegandone gli obiettivi scelti per suggerire l'immagine di hacker etici. Infatti, questi obiettivi includono la riduzione del gap tra ricchi e poveri, l'aiuto agli affamati e l'aumento della consapevolezza del cyber risk tra le vittime. Il tutto completato con l'immagine di una colomba.

Gli attaccanti nordcoreani nascondono le loro attività operando con o sotto identità di terze parti, acquisendo altri ransomware sul dark web ed utilizzando intermediari esteri per ricevere i pagamenti dei riscatti. Parte dei profitti sono investiti nei miglioramenti della infrastruttura d'attacco. Gli esperti prevedono un aumento del coinvolgimento di attori nordcoreani nell'ecosistema del ransomware se il valore delle criptovalute e la redditività dei loro furti continuerà a diminuire.

6. Le possibili difese

Come per tutti i problemi complessi con cause molteplici, non esiste una soluzione per il ransomware che sia contemporaneamente semplice, efficace ed economica. In generale, possiamo distinguere tra strategie di difesa tecnica e quelle di tipo sociale o legislativo. Mentre queste ultime cercano di reprimere il fenomeno criminale alla base del ransomware, le misure tecniche operano sui sistemi informativi che sono i bersagli degli attaccanti in modo da ripristinare i dati criptati o contenere l'intrusione prima del suo successo completo. Infine, discuteremo le innovazioni che riteniamo necessarie per una difesa efficace.

6.1 Difese non tecniche

Descriviamo alcune strategie basate sulla repressione del fenomeno e non sull'aumento di robustezza e/o resilienza dei sistemi attaccati.

6.1.1 Difese basate sul contrattacco

Un recente esempio di contrattacco è quello della FBI contro la gang Hive, diventata popolare nell'aprile 2022 quando ha attaccato un grande numero di server Exchange utilizzati da organizzazioni finanziare, no profit e del mondo della sanità.

A partire dal luglio 2022, gli agenti della FBI si sono infiltrati nella infrastruttura d'attacco e nei sistemi della gang rubando chiavi di decriptazione che venivano poi fornite alle vittime della gang. Complessivamente sono state fornite circa 300 chiavi a vittime che erano sotto attacco mentre gli agenti si muovevano nei

***Figura 6**. La pagina web che appare sui nodi di Hive attaccati da FBI*

sistemi di Hive e circa 1000 chiavi alle vittime precedenti, con un risparmio complessivo per le vittime di più di 130 milioni di dollari. La distribuzione delle chiavi è stata un cambio di strategia della FBI che, in precedenza, non ha trasmesso alle vittime informazioni sulle infiltrazioni di una gang per evitare di compromettere le azioni per smantellare l'infrastruttura della gang stessa. Nel gennaio 2023, un'azione congiunta delle forze di polizia di più paesi ha smantellato l'infrastruttura d'attacco ed i sistemi di Hive, vedi Fig. 6. Come la FBI dichiara in alcuni documenti ufficiali, le azioni contro Hive fanno parte della nuova strategia caratterizzata da "un allontanamento continuo" dal semplice arresto dei colpevoli verso una strategia che prevede invece anche l'aiuto alle vittime e lo smantellamento delle infrastrutture informatiche delle gang, uno dei pilastri della strategia complessiva.

Il tutto è coerente con l'annuncio dell'amministrazione Biden di considerare il ransomware non come un fenomeno criminale, ma come un problema di sicurezza nazionale. L'obiettivo della strategia è di ridurre fortemente la redditività del ransomware e le risorse finanziarie a disposizione delle gang. Comunque, anche chi ha smantellato l'infrastruttura prevede che, a breve, i membri della gang si riorganizzeranno sotto un altro nome o in altre gang. Come evidenziato da molti analisti, molte persone lavorano per più gang contemporaneamente e quindi smantellare una gang provoca solo il passaggio di competenze ad altre gang o la nascita di nuove gang. La strategia migliore, e più a lungo termine, per la sconfitta di una gang e dell'intero ecosistema criminale legato al ransomware, non è quella di smantellare una gang, che sarà facilmente sostituita da altre, ma di aumentare la robustezza dei sistemi.

Alcune ore dopo l'operazione della FBI, alcuni siti che pubblicizzavano l'offerta di una taglia per informazioni su Hive sono stato bloccati da un DOS. Secondo molti analisti, il DOS è stato realizzato da agenti che hanno operato per conto del governo russo. Questo può fornire indizi sulla sponsorizzazione delle gang ransomware e sulle relazioni tra gang e Stato.

Una diversa versione di contrattacco, citata per completezza, è quella della sicurezza offensiva privata, cioè la possibilità, non solo per le forze di polizia, ma anche per una organizzazione che scopra di essere attaccata da una gang, di contrattaccare. In pratica, c'è chi propone una innovazione legale che permetta anche ad una organizzazione privata di contrattaccare per smantellare i sistemi delle gang che la stanno attaccando. Ad esempio, Entrust, una grande società di sicurezza informatica, ha eseguito un attacco DOS per impedire l'accesso al sito dove la gang Lockbit aveva minacciato di pubblicare dati esfiltrati da Entrust stessa. L'innovazione è controversa ed estremamente discutibile, visto che le infrastrutture di attacco sono botnet costruite con risorse che non appartengono sicuramente all'attaccante. Anche un semplice attacco DOS come quello eseguito da Entrust ha danneggiato altre organizzazioni oltre alla gang Lockbit perché ha necessariamente saturato la banda di rete in più punti. È abbastanza preoccupante pensare alle ripercussioni complessive di un certo numero di attacchi DOS eseguiti contemporaneamente da alcune vittime.

La proposta della sicurezza offensiva privata evidenzia come anche nel settore civile si possano presentare situazioni che richiedono l'adozione di piattaforme offensive quali la distruzione delle botnet che le gang criminali utilizzano nelle intrusioni ransomware. Esperienze passate hanno dimostrato che l'efficacia delle azioni per smantellare una botnet dipenda dalla capacità di agire simultaneamente su tutta la botnet stessa. Senza tale simultaneità, la tecnologia peer-to-peer che sta alla base delle botnet permette alla parte non smantellata di sopravvivere e di ricreare quella eliminata. Solo l'automazione delle azioni in una singola piattaforma può garantirne la simultaneità.

Le gang non sono rimaste passive di fronte alle operazioni di sicurezza offensiva per smantellare le loro infrastrutture d'attacco ed hanno colto, indubbiamente meglio di molti difensori, i vantaggi offerti da alcune soluzioni tecnologiche. Ad esempio, alcune gang hanno iniziato ad usare i servizi di Emercoin per gestire le loro infrastrutture. Emercoin offre strumenti e servizi basati su blockchain. La sicurezza intrinseca e la completa decentralizzazione dei servizi permessa dalla blockchain aumenta notevolmente la robustezza dell'infrastruttura stessa. Ad esempio, Emercoin offre un servizio di DNS completamente decentralizzato ed in cui i vari record possono essere modificati unicamente da chi possiede la chiave privata associata al record. In precedenza era stato segnalato anche l'uso di Namecoin, una criptocurrency che usava il codice di bitcoin e che permetteva di registrare nomi di dominio nel top-level domain (TLD) ".bit". Il dominio registrato era associato all'hash del nome di chi registrava. Comunque, questa soluzione richiedeva modifiche al proprio DNS, almeno per trasmettere la richiesta ad un qualche proxy in grado di accedere alla blockchain o di averne una copia locale.

Ultima soluzione proposta ma, a quanto risulta, non ancora adottata, è di integrare gli attacchi alle infrastrutture delle gang con la diffusione di fake news nel dark web per ridurre la fiducia tra le varie gang. L'uso congiunto di attacchi e fake news dovrebbe ridurre la disponibilità e la credibilità dei vari servizi offerti sul dark web riducendo l'efficacia della cooperazione e quindi delle gang.

6.1.2. Contrasto al riciclaggio

Il miglioramento della tecnologia per analizzare i flussi di pagamento su strutture dati di tipo blockchain e per de-anonimizzare i soggetti coinvolti in questi flussi, permette di individuare e punire i soggetti coinvolti nel riciclaggio dei riscatti. Sfruttando questa tecnologia, a gennaio 2023, il Department of Justice statunitense ha incriminato ed arrestato Anatoly Legkodymov, fondatore e maggiore azionista di Bitzlato, una società per il cambio di valute. L'accusa a Bitzlato è quella di riciclare i riscatti del ransomware del dark market Hydra smantellato nell'aprile 2022. Questi riscatti comprendono anche quelli generati dal ransomware Conti. Complessivamente, circa il 2% dei fondi gestiti da Bitzlato proveniva da ransomware mentre gli altri erano sostanzialmente legati al mercato della droga.

Il riciclaggio del denaro è uno dei servizi più importanti tra quelli che un dark market può offrire. Dopo lo smantellamento di Hydra, c'è stata una competizione tra i rimanenti dark market ed i vincitori, quelli che hanno attratto più clienti, sono quelli che hanno offerto il servizio di riciclaggio ad un prezzo più basso. Molte delle offerte nei dark market sopravvissuti sono state create da amministratori di Hydra che sono migrati ad altri market. Fanno probabilmente parte di questa competizione la pubblicità di BlackSprut, un dark market specializzato in droghe, apparse su alcuni cartelloni elettronici a Mosca. Non è chiaro se ciò sia dovuto ad un acquisto legale o ad una intrusione informatica nel sito dell'agenzia pubblicitaria. È noto, comunque, che BlackSprut sia un supporter del Cremlino ed abbia finanziato gruppi paramilitari che operano a supporto dello Stato russo[3]. Un altro indizio da considerare nell'analisi dei rapporti tra gang e Stato russo.

[3] https://www.vice.com/en/article/wxnmg5/russia-darknet-market-wars

6.1.3 Mitigazione mediante copertura assicurativa

Altre strategie di mitigazione sono basate sul trasferimento del rischio mediante polizze assicurative. Questo è un meccanismo classico per trasferire il rischio, ma, dopo un entusiasmo iniziale, le assicurazioni sono attualmente molto restie a coprire il rischio cyber perché è governato da correlazioni tra intrusioni e condivisioni di risorse tra gang spesso ignote a priori. Non siamo nel mondo felice delle assicurazioni auto dove il coinvolgimento di un automezzo in un incidente non cambia la probabilità che un altro automezzo lo sia. Nell'ecosistema informatico, la scoperta di una vulnerabilità in un sistema operativo cambia lo scenario di rischio in un numero elevato di sistemi. Il rischio di un singolo evento catastrofico che coinvolga un numero a priori non noto di sistemi informatici preoccupa molto gli assicuratori e soprattutto i riassicuratori che dovrebbero rimediare alle perdite di molte compagnie. La diffusione di NotPetya ha presentato molte delle caratteristiche di un singolo evento catastrofico ed ha provocato, per la prima volta, un numero elevato di cause legali che hanno posto il problema delle intrusioni informatiche come atti di guerra ibrida ovvero un atto di guerra in un periodo di guerra non dichiarata. Una ulteriore conferma del passo indietro delle assicurazioni dalla decisione dei LLyod's di Londra di non assicurare, a partire dal marzo 2023, nessun rischio causato da malware prodotto da attaccanti sponsorizzati da uno Stato e quindi utilizzabile in un conflitto.

Il problema centrale è che, come certificato in numerose audizioni presso il senato US, le compagnie di assicurazione non dispongono di strategie che permettano loro di modulare il costo delle loro polizze in base alla effettiva robustezza del singolo sistema ICT anche se attaccato da cyber crime e non da attaccanti sponsorizzati da Stati, perché non dispongono di metriche che permettano di valutare, a priori, tale robustezza. Ciò produce un approccio "one size fits all" che ovviamente i clienti non amano. Il successo della soluzione assicurativa richiede quindi metriche e test per misurare tale robustezza, così come i crash test misurano quella di un'autovettura. Sorge il problema che ogni sistema informatico può essere molto diverso dagli altri, non esiste come nel mondo delle auto un numero ridotto di modelli la cui robustezza può essere misurata una volta per tutte con un singolo crash test.

Più analisti concordano sul fallimento del contributo delle assicurazioni all'aumento della sicurezza e robustezza dei sistemi. Un altro sintomo del fallimento viene dalla gang HardBit che non fissa un riscatto a priori, ma chiede alle sue vittime la cifra che possono farsi rimborsare dalla propria assicurazione. Sostanzialmente, la copertura assicurativa, invece di essere un incentivo a migliorare la robustezza del sistema assicurato, attrae gli attaccanti perché aumenta la probabilità di incassare il riscatto.

6.2 Difese tecniche

Presentiamo ora le strategie di difesa che operano sui potenziali bersagli delle intrusioni ransomware. Vale la pena ricordare che decifrare le informazioni individuando errori nell'algoritmo di cifratura non è possibile viste le competenze disponibili nell'ecosistema criminale e gli algoritmi di cifratura utilizzati. Le società che promettono di invertire la cifratura individuando fantomatici errori nel software o nella cifratura sostanzialmente non fanno altro che pagare il riscatto, ottenere la chiave e passarla alle vittime ad un prezzo più alto per compensare il loro disturbo. Le uniche soluzioni realistiche sono il ripristino dei dati a partire da copie di backup o aumentare la robustezza dei sistemi per annullare la probabilità di successo delle intrusioni.

6.2.1 Ripristino dei dati

Le strategie basate sul ripristino dei dati sono efficaci solo quando l'attaccante non ricorre a double-extortion o comunque non minaccia la pubblicazione dei dati esfiltrati. La base di queste contromisure sono le copie di backup dei dati. Ovviamente, tali copie vanno difese impedendo che, come quasi sempre accade, l'attaccante le elimini durante la sua intrusione. Difese possibili sono strategie come la 3-2-1 che prevede l'utilizzo di almeno tre copie dei dati, memorizzati su due supporti diversi di cui almeno una non in linea o su un altro sistema. Non in linea vuol dire non collegato ad una rete e non semplicemente spento visto che alcuni ransomware possono forzare il boot di una macchina per criptarne le informazioni.

La strategia 3-2-1 è talmente efficace che la gang Lockbit la usa per proteggere le informazioni sui propri malware. Tuttavia, è difficile garantire l'aggiornamento istantaneo e continuo delle copie, soprattutto di quella non online. Ergo tutti i dati non ancora memorizzati sulla copia non online possono andare persi, aumentando il tempo di ripristino.

Una seconda strategia di difesa prevede l'uso di memorie immutabili. Si tratta di memorie worm, write once read many, in cui ogni operazione può essere scritta, ma non aggiornata. In generale, la proprietà worm viene garantita in modo nativo da CD-r o DvD-r oppure utilizzando degli interruttori o delle chiavi fisiche che impediscono l'aggiornamento del supporto fisico di memoria. Memorie worm, ormai messe comunemente a disposizione dai fornitori di servizi cloud, possono essere usate per memorizzare backup, ma sono anche stati sviluppati file system che utilizzano questi dispositivi e che offrono all'utente una interfaccia completamente standard. Sostanzialmente, ogni scrittura di una pagina fisica del file system provoca non la modifica della stessa, ma l'allocazione e la scrittura di una nuova pagina. In questo modo, il dispositivo conserva tutte le pagine già scritte e la copia di backup è prodotta automaticamente e pertanto non può essere cancellata.

6.2.2 Aumento robustezza dei sistemi

Una soluzione più generale e proattiva cerca di bloccare l'intrusione prima che abbia successo. Ciò richiede l'adozione di difese standard, cioè non specializzate per il ransomware. Tra queste strategie ricordiamo l'aumento della security awarness degli utenti, una politica di patching per le vulnerabilità più critiche, la classificazione delle informazioni, la minimizzazione dei diritti assegnati ad ogni utente, il privilegio minimo e la segmentazione delle reti. In particolare, la segmentazione delle reti e la separazione delle varie sottoreti mediante firewall ~~è~~ sono una delle contromisure più efficaci per il contenimento della diffusione del malware sia nel caso in cui attaccanti usino una piattaforma di attacco automatizzata sia in quello di human operated ransomware. Le strategie che le varie gang usano nelle loro intrusioni dimostrano che la segmentazione delle reti può forzare un aumento significativo del tempo per la raccolta di informazioni e di quello per criptarle, aumentando il tempo a disposizione dei difensori.

Una forma estrema di segmentazione è l'air gap cioè l'impossibilità di due reti di interagire come richiesto dalla strategia 3-2-1 discussa in precedenza. Un'altra contromisura efficace, soprattutto nel caso di ransomware che esfiltri le informazioni, è l'egress filtering cioè il filtraggio delle comunicazioni in uscita per individuare comunicazioni anomale in termini di quantità e/o di destinatari. Tenendo conto che molte gang hanno sfruttato vulnerabilità in sistemi per VPN, in prospettiva, anche soluzioni zero trust potranno essere adottate per respingere intrusioni che sfruttano credenziali rubate o dispositivi infettati al di fuori del perimetro aziendale.

Sostanzialmente, la soluzione più generale per contrastare il ransomware non è diversa da quella per contrastare altre minacce ed è basato su una lista di meccanismi e strategie che gli esperti di sicurezza informatica suggeriscono da tempo, ma che le organizzazioni, dalle più piccole alle più grandi, non riescono a adottare. Se teniamo conto che, in media, passano tre giorni dal momento in cui una intrusione accede ad un sistema a quando tutte le informazioni sono criptate, ci rendiamo conto di quanto deboli siano i sistemi se un attaccante si muove liberamente per tre giorni al loro interno. Questa debolezza può in parte essere dovuta ai meccanismi di scelta dei responsabili della sicurezza che privilegiano persone interne all'organizzazione rispetto al possesso delle competenze necessarie. Delegare a ditte esterne l'installazione, gestione e manutenzione di strumenti per la propria sicurezza può migliorare, anche drammaticamente, le competenze a disposizione, ma pone uno dei problemi più critici nella situazione attuale, quello dei supply chain attacks e delle vulnerabilità condivise tra organizzazioni diverse. Ad esempio, Solarwinds, una azienda che produce strumenti per la sicurezza informatica, è stata vittima di una intrusione che ha permesso all'attaccante di manipolare il codice degli strumenti Solarwinds e quindi ogni utilizzatore di questi strumenti è diventata una potenziale vittima della intrusione. Successivamente, l'intrusione è stata attribuita al SVR, l'organo intelligence russo con competenze sull'estero[4].

[4] https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

Non è difficile pensare che l'obiettivo dell'intrusione sia stato quello di installare una backdoor negli strumenti Solarwinds ed alla vendita sul dark web di accessi ai sistemi che utilizzano questi strumenti. Intrusioni simili potrebbero coinvolgere le ditte che offrono servizi di sicurezza. A questo si affianca la carenza di risorse che le organizzazioni riservano per la propria sicurezza. È singolare come l'alta dirigenza delle organizzazioni, sia pubbliche che private, spinga per l'adozione veloce ed acritica delle tecnologie informatiche emergenti per aumentare la competitività aziendale senza ricordare che ogni adozione aumenti la digitalizzazione dei processi aziendali, ma necessariamente anche la superficie d'attacco e la fragilità dell'organizzazione rispetto ad intrusioni informatiche.

A fronte dei ridotti investimenti per aumentare la robustezza da parte delle vittime, le gang ransomware investono costantemente una parte dei loro profitti per migliorare la qualità dei loro strumenti software e delle loro infrastrutture di attacco. Ad esempio, un anno fa solo poche varianti erano in grado di criptare informazioni su sistemi operativi diversi da Windows, oggi tutte le varianti possono criptare informazioni su qualsiasi sistema Windows o Linux e su macchine virtuali e sono in grado di attaccare un qualsiasi server. Un altro esempio citato in precedenza è la riscrittura di malware in Rust. Queste evoluzioni ridurranno significativamente il tempo medio tra accesso ed encryption e quindi richiederanno un aumento degli investimenti in sicurezza.

6.3 La necessità di una nuova prospettiva

Questa sezione, che è anche una prima conclusione del contributo, evidenzia la necessità di un nuovo approccio per una soluzione stabile al problema del ransomware e più, in generale, del crimine informatico. L'innovazione è necessaria perché, come evidenziano molti ricercatori ed analisti, il fenomeno del ransomware mette in crisi gli strumenti tradizionali di analisi e gestione del rischio e non solo di quello cyber. Infatti, l'elevata dinamicità del fenomeno richiede un approccio altrettanto dinamico in cui lo scenario di rischio può essere completamente rivoluzionato in conseguenza di una nuova strategia di attacco o di una nuova vulnerabilità.

Alcune analisi hanno dimostrato come metodi tradizionali per valutare il rischio generato da nuove vulnerabilità non sono efficaci nel caso del ransomware. Ad esempio, il Common Vulnerability Scoring System associa ad ogni vulnerabilità uno score tra 0 e 10 proporzionale al rischio generato dalla vulnerabilità in esame. Numerose evidenze sperimentali hanno dimostrato l'inutilità di questo scoring nel caso del ransomware. Infatti, ~~se~~ le aziende che utilizzavano lo score per decidere quali vulnerabilità patchare non hanno patchato molte delle vulnerabilità che le intrusioni ransomware sfruttano e che hanno uno score inferiore a 4. Ciò ha ovviamente semplificato il lavoro degli attaccanti.

Alla dinamicità delle strategie di attacco e delle vulnerabilità si associa quello dei sistemi da difendere. Infatti, anche i sistemi da difendere si evolvono per la presenza di nuovi nodi, di nuove applicazioni e di nuovi utenti. È chiaro che tutte queste caratteristiche generano una situazione che è, ad esempio, molto diversa da quelle che le compagnie di assicurazione affrontano tradizionalmente e che hanno tempi di evoluzione molto più lunghi di molti ordini di grandezza. Non si tratta solo della scarsità delle informazioni su intrusioni, ricatti e danni subiti per la naturale ritrosia delle vittime a condividere tali informazioni. Il vero problema è che molte di queste informazioni diventano obsolete e inutilizzabili rapidamente all'apparire, ad esempio, di gang che usano strategie di attacco o diffusione del ransomware diverse. Quindi, la scarsità dei dati è un fenomeno strutturale, sistemico dell'ecosistema informatico e non è legato ad una carenza momentanea a cui si può rimediare creando agenzie che, come per il traffico aereo, raccolgano e facilitino la condivisione di informazioni su incidenti o malfunzionamenti. L'unico modo di superare la carenza è quello di utilizzare dati sintetici ovvero non raccolti durante intrusioni su sistemi reali ma prodotti simulando su piattaforme informatiche il comportamento degli attaccanti e la reazione del sistema. Per garantire l'accuratezza dei dati generati, le simulazioni devono utilizzare dei modelli del sistema da proteggere e degli attaccanti che siano formali ed eseguibili su un sistema informatico. Sostanzialmente, si estende alla sicurezza informatica la strategia dei digital twin che è già molto popolare nell'industria 4.0.

Questa strategia permette di utilizzare il metodo Monte Carlo ed eseguire simulazioni ripetute ed indipendenti che generano in breve tempo un volume di dati che permette di stimare con elevata confidenza le probabilità di interesse, ad esempio quella che una intrusione abbia successo o che un attaccante riesca ad installare un malware in un nodo del sistema
La disponibilità di questi dati permette di reagire in tempi brevi o brevissimi a repentini cambi di scenario sia nei sistemi da proteggere che nelle intrusioni contro di essi.
Possiamo concludere dicendo che la necessità di un approccio dinamico alla valutazione e gestione del rischio generato dal ransomware è corretta, ma parziale perché, in realtà, tutti i rischi cyber richiedono un approccio dinamico e solo accettando e gestendo questa dinamicità possiamo sperare di scoprire solidi strumenti di analisi, prevenzione e gestione anche del rischio ransomware. Citando un rapporto di BlackFog sulle lezioni imparate sul ransomware possiamo dire che occorre spendere per resistere al ransomware ma spendere non basta, occorre anche spendere bene perché le assicurazioni e le soluzioni tradizionali non funzionano.

7. Bibliografia Commentata

È estremamente difficile produrre una lista aggiornata di siti, blog e post con notizie su ransomware sia per il numero estremamente grande di candidati sia per la natura dinamica che caratterizza il fenomeno ransomware ed il web in generale. Vista anche la povertà di riferimenti accademici adeguati, preferiamo segnalare pochi testi che riteniamo più accurati rispetto ad altri riferimenti magari più recenti ma che potrebbero in breve diventare obsoleti.

Alcuni testi interessanti che tracciano la storia del ransomware, delle varianti e delle evoluzioni sono:

- Ryan Matthew. Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Springer, 2021.
- Wolff Josephine. You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches. Mit Press, 2018.

- Jenkinson Andrew. Ransomware and Cybercrime. CRC Press, 2022.

Altri testi discutono i problemi posti da una analisi realistica del rischio ransomware e per la gestione di questo rischio:

- Wolff Josephine. Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks. MIT Press, 2022.
- Adam Barbara, Joost Van Loon, and Ulrich Beck. "The risk society and beyond." The Risk Society and Beyond (2000), pp.1-240.

Sulle tecniche e gli impatti di uno dei più celebri gruppi di hacker dell'esercito russo:

- Greenberg Andy. Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor, 2019.
- Greenberg Andy. "The untold story of NotPetya, the most devastating cyberattack in history." Wired, August 22 (2018).

Sull'ecosistema ransomware e la sua economia, la più recente analisi dei post legati alla gang Lockbit su siti russi:

- Di Maggio, Jon, Ransomware Diaries, Vol. 1 https://analyst1.com/ransomware-diaries-volume-1, Gennaio 2023

Sugli impatti dell'invasione russa sull'ecosistema ransomware

- Brad Smith,. "Defending Ukraine: Early Lessons from the Cyber War." Microsoft on the Issues, June 22 (2022).
- Grossman Taylor, Kaminska Monica, Shires James, and Smeets Max, The Cyber Dimensions of the Russia-Ukraine War, Workshop report, European Cyber Conflict Research Initiative, Aprile 2023

Sui rapporti tra gang e Stato russo sono illuminanti questi contributi:

- Recorded Future, Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine, https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf
- Meduza, The FSB's personal hackers: How Evil Corp, the world's most powerful hacking collective, takes advantage of its deep family ties in the Russian intelligence community, https://meduza.io/en/feature/2019/12/12/the-fsb-s-personal-hackers
- Threat Analysis Group, Mandiant, Google Trust and Safety, Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/
- Nershi Karen, Grossman Shelby Assessing the Political Motivations Behind Ransomware Attacks, CYBERWARCON '22, Nov. 10, 2022 Arlington, VA

Altri articoli e libri sull'ecosistema criminale e sui vari dark market:

- Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. "The Ransomware-as-a-Service economy within the darknet." Computers & Security 92 (2020): 101762.
- Perlroth, Nicole. This is how they tell me the world ends: The cyberweapons arms race. Bloomsbury Publishing USA, 2021.
- Di Maggio, Jon, Ransom Mafia - Analysis of the World's First Ransomware Cartel https://analyst1.com/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel, Aprile 2021
- Chainanalysis Blog, Ransomware Revenue Down As More Victims Refuse to Pay, https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, Gennaio 2023
- SEKOIA.IO Ransomware Threat Landscape – second-half 2022, https://blog.sekoia.io/sekoia-io-ransomware-threat-landscape-second-half-2022/

Un rapporto ENISA con una sintetica ma approfondita analisi del fenomeno con informazioni statistiche di molte varianti

- ENISA Threat Landscape for Ransomware Attacks, July 2022

Un report indipendente sull'intrusione della gang Conti al sistema sanitario irlandese

- Conti cyber-attack on the HSE Indipendent Post Incident Review https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Un report di una commissione del senato US sugli attacchi ad aziende US,

- US CONGRESS SENATE COMMITTEE ON HOMELAND SECURITY AND GOV. AFFAIRS America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies, Mar. 2022, https://www.hsdl.org/c/view?docid=86617

Un'analisi delle varie ragioni per non pagare un riscatto

- Tarah Wheeler and Ciaran Martin Should ransoware payment be banned? https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/

Per gli amanti della crittografia un testo che ne analizza gli usi maliziosi

- Young Adam and Moti Yung. Malicious cryptography: Exposing cryptovirology. John Wiley & Sons, 2004.

Infine, un testo meno tecnico ma comunque ben documentato

- Dudley Renee and Daniel Golden. The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from CyberCrime, Mac Millian, Oct. 2022