Università degli Studi di Camerino

Scuola di Scienze e Tecnologie
Corso di Laurea in Informatica (Classe L-31)

Ransomware: Analisi, Crescita e Sviluppo

Laureando
Flavio Pocari

Relatore
Fausto Marcantoni

Matricola 105057

A.A. 2020/2021

Indice

Abstract

Gli attacchi ransomware sono ormai da anni frutto di campagne automatizzate e industrializzate, che non seguono alcuna pianificazione reale, e il cui unico vero scopo è quello di colpire più target possibili, alla ricerca di un ingresso nei sistemi informativi.

L’evoluzione dei malware è in costante miglioramento, si intende iniziare descrivendo cosa sia un Ransomware e come funziona l'attacco, cercando di mettere in guardia le persone provando a prevenire e ad evitare il pagamento del riscatto.
Verrà illustrata la loro evoluzione, illustrando il primo attacco conosciuto ed alcuni dei più grandi attacchi, come WannaCry [1], ed il più recente che ha colpito la regione Lazio.

Viene illustrato il concetto di RAAS [2], e come le organizzazioni criminali traggono beneficio dalla vendita di ransomware in larga scala.

Scriverò il mio ransomware, chiamato "Some", dove verranno illustrate le tecniche utilizzate nella realizzazione di esso ed un ambiente più o meno veritiero in cui è possibile essere tratti in inganno per scaricarlo ed eseguirlo.
Verranno illustrati possibili sviluppi futuri di esso, magari impedendo il reverse engineering dell'eseguibile oppure offuscando il codice.

Ransomware

Il ransomware è stato ed è tuttora una minaccia importante per le imprese sin dalla metà degli anni 2000.
Nel 2017, l'IC3 (Internet Crime Complaint Center) [3] dell'FBI ha ricevuto 1783 denunce di ransomware che sono costate alle vittime più di 2 milioni di euro.

Queste però sono solo le denunce segnalate a IC3.
Il numero effettivo di attacchi e costi è molto più elevato, solo l'anno scorso sono stati stimati 180 milioni di attacchi ransomware.
Secondo l'FBI, ogni giorno si verificano più di 4.000 attacchi ransomware.

Cosa è?

Il ransomware è un tipo di malware [4] che ottiene accesso ai file o sistemi e blocca l'accesso degli utenti a tali file o sistemi.
Quindi tutti i file, o interi dispositivi vengono cifrati e tenuti in ostaggio fino a quando la vittima non paga un riscatto e vengono decifrati.
La chiave consente all'utente di accedere ai file o ai sistemi crittografati dal programma.

Sebbene il ransomware sia in circolazione da decenni, le varietà di ransomware sono diventate sempre più avanzate nelle loro capacità di diffusione, elusione del rilevamento, crittografia dei file e costrizione a pagare un riscatto.
Il ransomware New Age comporta una combinazione di sforzi di distribuzione avanzati come infrastrutture precostruite utilizzate per distribuire facilmente e ampiamente nuove varietà e tecniche di sviluppo avanzate come l'utilizzo di crypter per garantire che il reverse engineering [5] sia estremamente difficile.

Il ransomware si conferma una delle minacce più significative che oggi le aziende e gli individui devono affrontare, non sorprende che gli attacchi stiano diventando sempre più sofisticati, più difficili da prevenire e più dannosi.

Come funziona l’attacco?

Il termine "ransomware" descrive la funzione del software, ovvero cifrare file ad utenti o aziende a scopo di lucro. Tuttavia il malware deve ottenere l'accesso ai file o al sistema, questo avviene tramite infezione o vettori di attacco.
Ci sono molti modi in cui i sistemi possono essere corrotti, e mediante un vettore di attacco o infezione il ransomware ottiene l'accesso.

Esempi di vettori includono:

1. Allegati email, metodo comune, le aziende aprono malware mascherati da allegati. Se una fattura arriva a un imprenditore o ad un ufficio è probabile che venga aperta, e si ottenere l'accesso a file e/o sistemi.

2. Messaggi, inviare messaggi alle vittime sui social media. Uno dei più utilizzati è Messenger. Vengono creati account Facebook che imitano gli "amici" attuali della vittima. Questi vengono utilizzati per inviare messaggi con file allegati, ed una volta aperto il ransomware potrebbe accedere e creare danni.
3. Popup, classici popup che appaiono su siti di streaming pirata, dove viene consentito l'accesso a scaricare file e/o visitare siti di dubbia provenienza.

Posso recuperare i file?

Utilizzando la crittografia [6] simmetrica [7] e asimmetrica [8], i ransomware possono rendere i file nuovamente accessibili solo se decifrati mediante chiave privata del server. Viene utilizzata la crittografia simmetrica per cifrare i file, grazie alle velocità elevate, e la crittografia a chiave pubblica per cifrare le chiavi AES e la comunicazione con il server.
Utilizzando entrambe le combinazioni, il ransomware può essere veloce e funzionare offline.

Utilizzo della rete Tor

Poiché i ransomware utilizzano la rete Tor [9] per lo scambio di chiavi/informazioni tra il server e la macchina infetta, la posizione del server è praticamente irrintracciabile.
La rete Tor garantisce la crittografia dell'IP, il che significa che l'IP del server è crittografato a ogni hop della rete.
C'è solo un modo per trovare la posizione del server, trovandosi tra l'ultimo nodo Tor e il server, come mostrato nella prima scena del primo episodio di Mr Robot.
Non essendo in grado di trovare la posizione del server, non c'è modo di ottenere la chiave privata del server.

Metodi di pagamento

Bitcoin [10] è la criptovaluta più sicura, con un tasso di hash così alto da eclissare quello di tutte le altre monete proof-of-work messe insieme. Ma le transazioni effettuate sulla blockchain [11] di bitcoin sono trasparenti e possono essere viste da chiunque utilizzi siti Web di blockchain.
Per ora qualsiasi transazione bitcoin può essere potenzialmente ricondotta alla sua fonte. Ciò ha portato gli sviluppatori a cercare di creare una criptovaluta più privata .
Bytecoin [12], che si basa sulla tecnologia CryptoNote [13], afferma di essere la "prima valuta privata non rintracciabile". CryptoNote è stato creato con l'obiettivo di rendere le transazioni sia non tracciabili che non collegabili.
Non tracciabile significa che gli osservatori non possono dire chi ha inviato una transazione a un destinatario specifico, mentre non collegabile significa che gli

osservatori non possono dire se due transazioni sono state inviate o meno alla stessa fonte. L'aspetto irrintracciabile si realizza attraverso le Ring Signature [14].
Le Ring Signature rendono opache le sue transazioni, il che significa che gli osservatori non possono vedere chi ha inviato la transazione, quanto è costato o chi l'ha ricevuta. Fondamentalmente mettono insieme le transazioni in un modo che rende difficile (ma non del tutto impossibile) distinguerle l'una dall'altra.

Per ottenere transazioni non collegabili, CryptoNote utilizza chiavi una tantum. Con le Ring Signature, è ancora possibile vedere le transazioni in entrata su una singola chiave pubblica (indirizzo del portafoglio). Per risolvere questo problema, CryptoNote genera automaticamente chiavi una tantum ogni volta che qualcuno riceve btc. Si basa su un metodo di crittografia noto come Diffie-Hellman Key Exchange [15], che consente la condivisione di dati segreti tra due parti.
Quando qualcuno invia Bytecoin a un altro indirizzo Bytecoin, il mittente crea un codice univoco che viene utilizzato nella transazione. Questo codice univoco fa sembrare che le monete siano state inviate a un portafoglio diverso ogni volta.

Monero [16] è una criptovaluta privata che ha funzionalità di privacy integrate in tutte le sue transazioni. XMR (Monero) è in realtà un hard fork di BCN (ByteCoin). Ciò significa che Monero utilizza la stessa tecnologia di privacy di Bytecoin e condivide la maggior parte delle caratteristiche sottostanti.
Quando Bytecoin è stato creato nel 2012, l'80% dell'offerta totale era già esistente, a differenza della maggior parte delle criptovalute estraibili che iniziano con pochissima offerta esistente.
Ciò ha portato sette degli sviluppatori che lavorano su Bytecoin a creare una nuova moneta biforcando duramente la rete BCN. Hanno chiamato questa nuova moneta Bitmonero, che è stata poi cambiata semplicemente in Monero, che significa "moneta" in esperanto.
Monero è diventata una delle criptovalute private più utilizzate, come dimostra il fatto che la moneta è tra le prime 20 monete per capitalizzazione di mercato. Per questo motivo, l'IRS [17] una volta ha offerto un contratto da $ 625.000 a chiunque potesse violare le funzionalità di privacy di Monero.
Monero è la 14a più grande criptovaluta per capitalizzazione di mercato, con un valore di oltre $ 2,05 miliardi con un volume di scambi giornaliero di circa $ 1,6 miliardi.

E’ una criptovaluta nata infatti per risolvere i problemi di privacy e garantire dunque l’anonimato delle transazioni e wallet.

Monero nasce nell’aprile del 2014 ed è tutt’ora basata sul protocollo CryptoNote con le dovute personalizzazioni del progetto.
Monero è nata da un fork dalla criptovaluta ByteCoin. ByteCoin, infatti, a quel tempo era stata lasciata quasi all’abbandono ed era stata già ampiamente minata, suscitando poco interesse da parte del mercato.
Le feature chiave di Monero che ne consentono di garantire l’anonimato derivano dal protocollo CryptoNote. In particolare, l’uso della Ring Signature e

l’implementazione modificata di Diffie-Hellman, abbinata a tante altri protocolli, ne permettono la garanzia della privacy.
La Ring Signature, infatti, prevede che tutte le transazioni siano firmate a nome del gruppo di appartenenza degli individui. In questo modo durante il processo di verifica risulta praticamente impossibile risalire al creatore originale, in quanto tutte le firme degli appartenenti al gruppo sono tra loro indistinguibili.
Sempre per contribuire alla privacy, in modo tale da garantire che nessuno possa ricostruire tramite le transazioni le identità degli autori, ogni volta che viene eseguita una transazione gli indirizzi vengono rigenerati. Risultano dunque essere sempre diversi seppure associati alle medesime entità. Questo meccanismo è stato introdotto grazie ad una rivisitazione del protocollo di Diffie-Hellman.

Il primo Ransomware della storia?

Il primo attacco ransomware noto si è verificato nel 1989 e ha preso di mira il settore sanitario, che rimane tutt'ora uno dei principali obiettivi.
Ha far partire questo attacco è stato Joseph Popp, PhD, un ricercatore sull'AIDS, che ha effettuato l'attacco distribuendo 20 mila dischi ad altri ricercatori sull'AIDS in più di 90 paesi, sostenendo che i dischi contenevano un programma che analizza il rischio di un individuo di acquisire l'AIDS attraverso l'uso di un questionario. Tuttavia il disco conteneva anche un malware che inizialmente è rimasto inattivo nei PC, veniva attivato solo dopo che un PC veniva acceso 90+ volte. Dopo che è stata raggiunta questa soglia il malware ha visualizzato un messaggio che richiede un pagamento di 189$ iniziali ed altri 378$ per un leasing software, questo attacco passa alla storia come AIDS Trojan o PC Cyborg.

La loro evoluzione.

Durante gli anni '90, mentre i metodi di crittografia continuavano ad avanzare, anche gli attacchi ransomware diventavano più sofisticati e impossibili da decifrare. Intorno al 2006, gruppi di criminali informatici hanno iniziato a sfruttare la crittografia RSA [18] per rendere i loro attacchi ancora più impossibili da contrastare.

Ad esempio, il Trojan Archiveus ha utilizzato la crittografia RSA per crittografare i contenuti nella cartella "Documenti" dell'utente. Il riscatto richiedeva alle vittime di acquistare beni tramite una farmacia online in cambio di una password di 30 cifre che avrebbe decifrato i file.

Il primo attacco naturalmente era abbastanza rudimentale, ma ha posto le basi per l'evoluzione del ransomware negli attacchi sofisticati di oggi.
I primi sviluppatori di ransomware in genere scrivevano il proprio codice di crittografia. Molti ora usano librerie già pronte che sono sicuramente più difficili da decifrare, e sfruttano metodi di consegna più sofisticati come le campagne di spear phishing [19], piuttosto che le tradizionali email che sono spesso filtrate da filtri antispam.

Alcuni aggressori stanno sviluppando toolkit [20] che possono essere scaricati e distribuiti da aggressori con meno competenze tecniche.
Alcuni dei criminali informatici piu avanzati stanno monetizzando il ransomware offrendo programmi RAAS (ransomware as a service), il che ha portato all'aumento dell'importanza di noti ransomware come CryptoLocker, CryptoWall, Locky e TeslaCrypt, questi sono esempi comuni di advanced malware.

I malware avanzati, a volte indicati come Advanced Persistent Threats (APT), sono ceppi di malware progettati con funzionalità avanzate per l'infezione, la comunicazione e il controllo, il movimento o l'infiltrazione di dati/esecuzione del payload. L’ advanced malware è spesso creato per la furtività o la persistenza ed

è in grado di evitare il rilevamento da parte delle soluzioni antivirus tradizionali. Negli ultimi anni si è assistito a un aumento degli attacchi che coinvolgono questi malware, mettendo a rischio le aziende a causa delle sofisticate capacità di attacco del malware e della velocità con cui si evolve per stare al passo con il rilevamento.

COME FUNZIONA L'ADVANCED MALWARE

Gli attacchi malware avanzati in genere seguono una sequenza di attacco comune:

Figura 1: Sequenza di Attacco.

1. Pianificazione: questa fase prevede la selezione di un bersaglio e la ricerca dell'infrastruttura del bersaglio per determinare come verrà introdotto il malware, i metodi di comunicazione utilizzati durante l'attacco e come/dove verranno estratti i dati. In questi attacchi, questa fase include in genere la pianificazione di attacchi di social engineering [21] mirati (come lo spear phishing) per l'introduzione iniziale del malware.
2. Introduzione del malware: in questa fase, il malware inizia l'infezione iniziale. Esso viene comunemente distribuito tramite attacchi di social engineering o tramite attacchi drive-by online.
3. Comando e controllo: il malware deve comunicare con gli aggressori per inviare le informazioni scoperte e ricevere istruzioni aggiuntive. Invierà informazioni sull'utente, sulla rete e sulla macchina agli aggressori e riceverà nuove istruzioni su quali identità o macchine infettare successivamente.
4. Espansione: gli aggressori esploreranno la rete e provano a diffondere il malware lateralmente cercando di infettare macchine o sistemi che hanno accesso ai dati mirati. Un advanced malware ha spesso solide capacità di autopropagazione per identificare e infettare rapidamente i bersagli.
5. Identificazione del target: una volta che l'attaccante ha acquisito un punto d'appoggio iniziale ed esplorato la rete, il/i target verranno identificati per la fase finale della propagazione del malware. In questa fase il malware viene diffuso per infettare macchine o sistemi che contengono o hanno accesso ai dati mirati.
6. Evento di attacco/esfiltrazione: viene eseguito il payload del malware; in un attacco incentrato sul furto di dati, questa è la fase in cui i dati mirati vengono compilati e scaricati in una posizione controllata dall'aggressore. Il malware avanzato utilizza tecniche per nascondere le esfiltrazione e altre attività, come la crittografia o la compressione di file.

7. Ritiro: dopo che un attacco è stato completato, il malware spesso si ritira e si nasconde all'interno di una rete di computer o si autodistrugge, a seconda dell'organizzazione di destinazione e della probabilità di essere scoperto dai sistemi di sicurezza.

TIPI COMUNI DI ADVANCED MALWARE

Il ransomware, essendo una minaccia sempre più comune, può essere considerato una forma di malware avanzato. Il ransomware limita o talvolta impedisce completamente agli utenti di accedere al proprio sistema attraverso una serie di metodi come il blocco dello schermo o la limitazione dell'accesso/crittografia dei file fino al pagamento della somma richiesta. I nomi familiari CryptoWall e CryptoBlocker sono varietà di ransomware, così come il precedente CryptoLocker e i più recenti Locky e TeslaCrypt. Con le vittime che pagano per riottenere l'accesso a sistemi e dati vitali, il ransomware si dimostra una tattica redditizia, incoraggiando solo un'ulteriore proliferazione.

CryptoWall ha generato 320+ milioni di dollari di profitto.
Dopo il primo attacco documentato, questo tipo è rimasto raro fino alla metà degli anni 2000, quando gli attacchi hanno iniziato ad utilizzare algoritmi di crittografia più sofisticati e difficili da decifrare, popolari in quel periodo erano Gpcode, TROJAN.RANSOM.A, Archiveus, Krotten, Cryzip e MayArchive.
Un altro attacco ransomware in quel periodo è stato l'attacco GPcode. GPcode era un Trojan distribuito come allegato di posta elettronica mascherato da domanda di lavoro. Questo attacco ha utilizzato una chiave RSA a 660 bit per la crittografia. Diversi anni dopo, Gpcode.AK, il suo predecessore, è passato al livello di utilizzo della crittografia RSA a 1024 bit. Questa variante ha preso di mira più di 35 estensioni di file.
Nel 2011 appare un worm ransomware che imitava l'avviso di attivazione del prodotto Windows, rendendo difficili distinguere le notifiche legit da quelle pericolose.

Entro il 2015, ancora più varianti stavano creando scompiglio.
SecureList e Kaspersky riportano che da Aprile 2014 a Marzo 2015 le minacce ransomware più importanti sono state CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, TorrentLocker, Fury, Lortok, Aura e Shade.

I più grandi attacchi ransomware e varianti

Dato il progresso, non sorprende che il più grande attacco si sia verificato negli ultimi anni.
In questi ultimi anni le richieste di riscatto sono aumentate, inserendo anche un timer, che provoca il raddoppio della richiesta o la distruzione di tutti i file.
CryptoLocker è stato uno dei ceppi più redditizi del suo tempo.
Tra Settembre e Dicembre del 2013 ha infettato 250.000+ sistemi.
Successivamente è stato analizzato il suo modello di crittografia e ora è disponibile uno strumento online per recuperare i file crittografati.

Nel 2015 un gruppo chiamato Armada Collective ha effettuato una serie di attacchi contro le banche greche, verso 3 istituzioni finanziarie greche crittografando file importanti e chiedere un riscatto di 7 milioni di euro a ciascuna banca. Le banche anziché pagare il riscatto hanno intensificato le difese ed evitato ulteriori interruzioni, nonostante i successivi tentativi.

Per gli attacchi alle aziende più grandi i riscatti sono stati segnalati fino a 50.000$, anche se hanno provato a chiedere un riscatto di 3,4 milioni ad un sistema ospedaliero di Los Angeles. Portando l'ospedale a non avere l'accesso alla rete, posta elettronica e a dati cruciali dei pazienti.

Nel Marzo 2016, l'ospedale di Ottawa è stato colpito da un Ransomware che ha colpito più di 10.000 macchine, ma l'ospedale ha risposto cancellando le unità, grazie a processi di backup e ripristino evitando così di pagare il riscatto.

Sempre nel Marzo del 2016, arriva la comparsa della variante Petya, ransomware avanzato che crittografava la tabella master di un computer e sostituisce il record di avvio principale con una richiesta di riscatto.
Petya è stato tra le prime varianti ad essere offerte come parte di un'operazione RAAS.

Una delle prime varianti di ransomware a colpire Apple OS X è emersa nel 2016, KeRanger ha colpito principalmente gli utenti che utilizzano l'applicazione Transmission colpendo circa 6.500 pc in 36 ore. Apple ha rimosso il ransomware da Transmission il giorno dopo che è stato scoperto.
Il 2016 è stato un anno importante, si stima che i criminali informatici abbiamo totalizzato 1 miliardo di dollari.

Nel 2018 un nuovo RAAS soprannominato GandCrab è apparso a metà mese. Questo è il ransomware più importante del 2018, infettando circa 50.000 computer, la maggior parte dei quali in Europa, in meno di un mese chiedendo a ciascuna vittima riscatti tra $ 400 e $ 700.000 in criptovaluta DASH [22]. Yaniv Balmas, un ricercatore di sicurezza presso Check Point, paragona GandCrab alla famigerata famiglia Cerber, ha anche aggiunto che gli autori di GandCrab stanno adottando un approccio di sviluppo software agile completo per la prima volta nella storia dei ransomware.

WANNACRY

Nel 2017, il ransomware WannaCry è diventato uno degli attacchi informatici più devastanti mai visti. Ha spazzato il mondo intero, bloccando i sistemi critici in tutto il mondo e infettando oltre 230.000 computer in più di 150 paesi in un solo giorno.

National Health Service (NHS) del Regno Unito, FedEx, Telefonia spagnola o Renault-Nissan sono solo alcuni dei nomi che sono diventati vittime di questo ransomware.

WannaCry è un crypto-ransomware, un tipo di software dannoso utilizzato dagli aggressori nel tentativo di estorcere denaro alle loro vittime. A differenza del ransomware locker (che blocca i target fuori dal loro dispositivo in modo che non siano in grado di utilizzarlo), il crypto-ransomware crittografa solo i dati su una macchina, rendendo impossibile l'accesso all'utente interessato.
Proprio come qualsiasi tipo di crypto-ransomware, questo è esattamente ciò che fa WannaCry: prende in ostaggio i file delle vittime, affermando di ripristinarli solo se hanno pagato un riscatto.

WannaCry è un worm ransomware che si è diffuso rapidamente attraverso una serie di reti di computer nel maggio del 2017. Dopo aver infettato un computer Windows, crittografa i file sul disco rigido del PC, rendendone impossibile l'accesso agli utenti, quindi richiede un pagamento di riscatto in bitcoin per decifrarli.
Una serie di fattori ha reso particolarmente degna di nota la diffusione iniziale di WannaCry: ha colpito una serie di sistemi importanti e di alto profilo, inclusi molti nel servizio sanitario nazionale britannico; ha sfruttato una vulnerabilità di Windows che si sospettava fosse stata scoperta per la prima volta dalla National Security Agency (NSA) degli Stati Uniti; ed è stato provvisoriamente collegato da Symantec [23] e altri ricercatori di sicurezza al Lazarus Group, un'organizzazione di criminalità informatica che potrebbe essere collegata al governo nordcoreano.
Il ransomware WannaCry è costituito da più componenti. Arriva sul computer infetto sotto forma di “contagocce”, un programma autonomo che estrae gli altri componenti dell'applicazione incorporati al suo interno.
Tali componenti includono:

1. Un'applicazione che crittografa e decifra i dati.
2. File contenenti chiavi di crittografia.
3. Una copia di Tor.

Il codice del programma non è offuscato ed è stato relativamente facile da analizzare per i professionisti della sicurezza.

Il vettore di attacco per WannaCry è più interessante del ransomware stesso. La vulnerabilità sfruttata da WannaCry risiede nell'implementazione di Windows del protocollo Server Message Block (SMB) [24]. Il protocollo SMB aiuta vari nodi su una rete a comunicare e l'implementazione di Microsoft potrebbe essere

ingannata da pacchetti appositamente predisposti nell'esecuzione di codice arbitrario.
Si ritiene che la NSA statunitense abbia scoperto questa vulnerabilità e, anziché segnalarla alla comunità infosec, abbia sviluppato un codice per sfruttarla, chiamato EternalBlue. Questo exploit è stato a sua volta rubato da un gruppo di hacker noto come Shadow Brokers.
Anche se un PC è stato infettato con successo, WannaCry non inizierà necessariamente a crittografare i file. Questo perché, come notato sopra, prima di andare al lavoro cerca di accedere a un URL molto lungo e incomprensibile . Se riesce ad accedere a quel dominio, WannaCry si chiude da solo. Non è del tutto chiaro quale sia lo scopo di questa funzionalità.

Hutchins non solo ha scoperto l'URL hard-coded, ma ha pagato 10,96 $ per registrare il dominio, aiutando così a smussare, anche se non a fermare, la diffusione del malware. Poco dopo essere stato acclamato come un eroe, Hutchins è stato arrestato per aver presumibilmente sviluppato diversi malware nel 2014 .

Ironia della sorte, la patch necessaria per prevenire le infezioni da WannaCry era effettivamente disponibile prima dell'inizio dell'attacco.

CRYPTOWALL

Cryptowall è un ransomware aggressivo con i sistemi Windows. Il ransomware colpisce il sistema e RSA a 2048 bits, rende inaccessibili tutti i file e i dati che trova sul suo cammino: l'utente non riuscirà più ad accedervi in alcun modo, fattorizzare una chiave pubblica RSA 2048 è tuttora impossibile.
Dal 2014 al 2016 CryptoWall è stata la variante piu utilizzata, riuscendo ad estorcere 18+ milioni di dollari, spingendo l'FBI a rilasciare un avviso sulla minaccia.

Esistono 4 modi di contrarre l'infezione CryptoWall:

1. Email: oltre il 75% degli attacchi CryptoWall vengono veicolati da normalissime email (almeno in apparenza). Gli utenti quasi sempre ci cascano.
2. Navigazione incontrollata: possiamo trovare CryptoWall scaricando allegati direttamente dai siti internet infetti. Quante volte vi è già capitato di effettuare il download di un file da pagine web: un documento word, pdf...
3. Software scaricati: "vorrei scaricare un software gratuito che mi permetta di convertire in mp3 le canzoni di YouTube" oppure "vorrei scaricare un programma che mi permetta di estrarre i file .zip". Detto fatto, basta scaricare il file di installazione del software infetto e dopo qualche secondo si attiva il virus CryptoWall.
4. Collegamento RDP [25]: difficile ma non impossibile. Persino le connessioni con desktop remoto possono essere il vettore perfetto per un'infezione ransomware letale.

I più grandi flop

Se implementati male, i ransomware possono essere invertiti e i file possono essere recuperati.
Ecco alcuni esempi di ransomware che hanno implementato in modo errato le funzionalità di base.

Linux.Encoder.1 ransomware

```
time_seed = time(0);
srand(time_seed);

// IV generation
do
    IV[idx++] = rand();
while ( idx != 0x10 );

//AES key generation
char alphabet[] = "abcdefghijklmnopqrstuvwxyz\
ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789,.-#'?!";
sz = 16;
while ( i < sz )
    key[i++] = alphabet[rand() % 69];
```

Figura 2: Snippet di Linux Encoder Ransomware.

Utilizzando il tempo come seed per la generazione delle chiavi, il ransomware è vulnerabile al ripristino delle chiavi, poiché si possono indovinare le chiavi.

Jigsaw Ransomware

```
// Encrypted files will have this file extension added
internal const string EncryptionFileExtension = @".fun";

// Maximum filesize that is going to be encrypted in bytes
// Default is 10MB, probably anything works
internal const int MaxFilesizeToEncryptInBytes = 10000000;

/* Password for encrypting and decrypting encrypted files.
 * Change it to something random, preferably every time before you spread your software
 * Leave the same lenght and don't touch the "==" in the end!
 * (You don't need to remember it.)
 */
internal const string EncryptionPassword = @"OoIsAwwF23cICQoLDA0ODe==";
//LULADASILVA
```

Figura 3: Snippet di Jigsaw Ransomware.

La chiave si trova in chiaro all'interno del ransomware.

Altro

I ricercatori del ransomware Bad Rabbit hanno scoperto che la chiave di decrittazione non è stata cancellata dalla memoria e non ha eliminato le copie shadow, consentendo alle vittime di ripristinare i file tramite la funzionalità di backup di Windows.

Attacchi recenti?

Quest'anno, Colonial Pipeline [26], il più grande operatore di gasdotti negli Stati Uniti, è stato compromesso. I primi rapporti indicano che questo incidente esemplifica molti dei motivi per cui gli attacchi ransomware sono aumentati.
Successivamente è stato riferito che Colonial Pipeline aveva circa 100 GB di dati rubati dalla loro rete e che l'organizzazione avrebbe pagato quasi $ 5 milioni di dollari a un affiliato di DarkSide.

Lazio

L'attacco ransomware che ha colpito la regione Lazio [27] era a scopo di lucro, come confermato dalla stessa Regione, per lo più banale da quanto è stato riferito. Dall'analisi del link Tor lasciato dai criminali alla Regione Lazio, risulta che il malware è RansomExx. Si tratta di una gang già nota per violazioni di diversi Governi (Brasile, Texas) e grandi aziende.
Regione Lazio ha confermato che l'attacco è partito da un computer di un dipendente in smart working (senza dare dettagli sulle cause principali).

Una delle ipotesi investigative è stata che l'attacco fosse arrivato tramite un fornitore di servizi di sicurezza alla Regione, compromesso da un ransomware da mesi. Tramite questa compromissione sono state rubate varie password VPN dei clienti di questo fornitore, tra cui quella di un utente LazioCrea. Con la password i criminali hanno installato un ransomware sul suo computer.
Al momento la versione ufficiale è che il dipendente sia stato contagiato dal malware (forse per aver cliccato un link dannoso).
Fatto sta che ci sono stati errori di gestione privilegi o di password in Regione se è stato possibile per gli attaccanti passare dal computer del dipendente ad account con privilegi di admin con cui criptare il tutto.
A essere criptati sono stati in particolare dati presenti su VM-Ware: applicativi (di cui il down di siti e piattaforme) e documenti regionali (non database principale, né dati sanitari).
Bloccata la piattaforma vaccini, ma i dati sanitari erano al sicuro su un database separato, dice la Regione, che quindi ha potuto ripristinarla in pochi giorni.

Ma di eccezionale in questo attacco, vale la pena ripeterlo, non c'è nulla. Secondo l'ultimo Rapporto Clusit il settore pubblico è tra gli obiettivi più colpiti dal cybercrime nel 2020.

Toscana

L'infrastruttura informatica dell'Agenzia Regionale di Sanità (ASR) della Toscana [28] è stata interessata da un attacco perpetrato nei giorni scorsi. Fortunatamente, rispetto a quanto avvenuto qualche settimana fa nel Lazio, le conseguenze non sembrano altrettanto gravi.
I dettagli riportati da ANSA fanno riferimento alla distruzione di numerosi dati epidemiologico-statistici, ma i tecnici si sono subito messi al lavoro in modo da recuperarli e ripristinarli, grazie ai backup effettuati. Non c'è stato alcun furto di informazioni e non sussistono rischi inerenti la privacy, poiché l'ARS non impiega dettagli di natura personale nell'ambito dei propri studi.

RAAS

Cosa è?

Ransomware as a Service è un modello di business utilizzato dagli sviluppatori di ransomware, in cui affittano varianti di ransomware nello stesso modo in cui gli sviluppatori di software legittimi affittano prodotti SaaS [29]. RaaS offre a tutti, anche alle persone senza molte conoscenze tecniche, la possibilità di lanciare attacchi ransomware semplicemente registrandosi a un servizio.
I kit RaaS consentono ai malintenzionati che non hanno le capacità o il tempo per sviluppare le proprie varianti di ransomware di essere operativi in modo rapido e conveniente. Sono facili da trovare nel dark web, dove vengono pubblicizzati nello stesso modo in cui le merci vengono pubblicizzate sul web legittimo.

Un kit RaaS può includere supporto 24 ore su 24, 7 giorni su 7, offerte in bundle, recensioni degli utenti, forum e altre funzionalità identiche a quelle offerte dai fornitori SaaS legittimi. Il prezzo dei kit RaaS varia da $ 40 al mese a diverse migliaia di dollari – importi insignificanti, considerando che la richiesta media di riscatto nel terzo trimestre del 2020 è stata di $ 234.000.

Come acquistarlo?

Esistono quattro modelli di entrate RaaS comuni:

1. Abbonamento mensile a tariffa fissa.
2. Programmi di affiliazione, che sono gli stessi di un modello di canone mensile ma con una percentuale dei profitti (tipicamente 20-30%) che va all'operatore RaaS.
3. Canone di licenza una tantum senza partecipazione agli utili.
4. Pura partecipazione agli utili.

Un cliente accede semplicemente al portale RaaS, crea un account, paga con Bitcoin, inserisce i dettagli sul tipo di malware che desidera creare e fa clic sul pulsante di invio. Gli abbonati possono avere accesso al supporto, alle community, alla documentazione, agli aggiornamenti delle funzionalità e ad altri vantaggi.

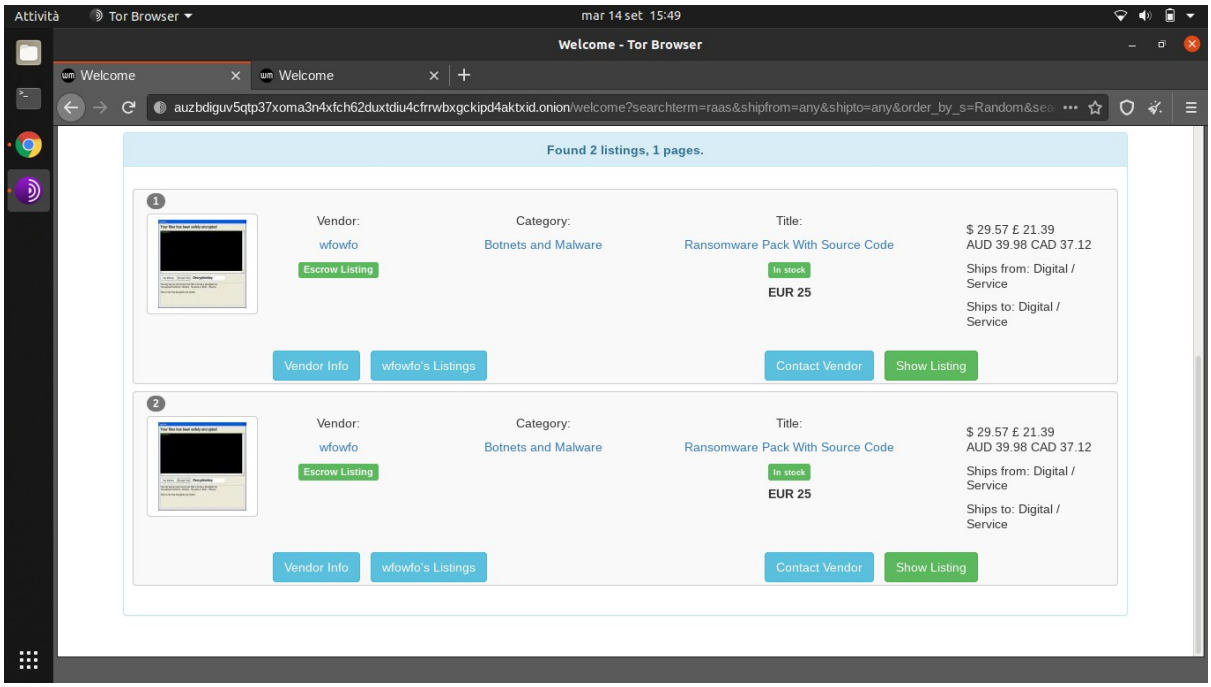
Il mercato RaaS è competitivo. Oltre ai portali RaaS, gli operatori RaaS eseguono campagne di marketing e dispongono di siti Web che assomigliano esattamente alle campagne e ai siti Web della tua azienda. Hanno video, white paper e sono attivi su Twitter. RaaS è business, ed è un grande business: i ricavi totali del ransomware nel 2020 sono stati di circa $ 20 miliardi nel 2020, rispetto a $ 11,5 miliardi dell'anno precedente.

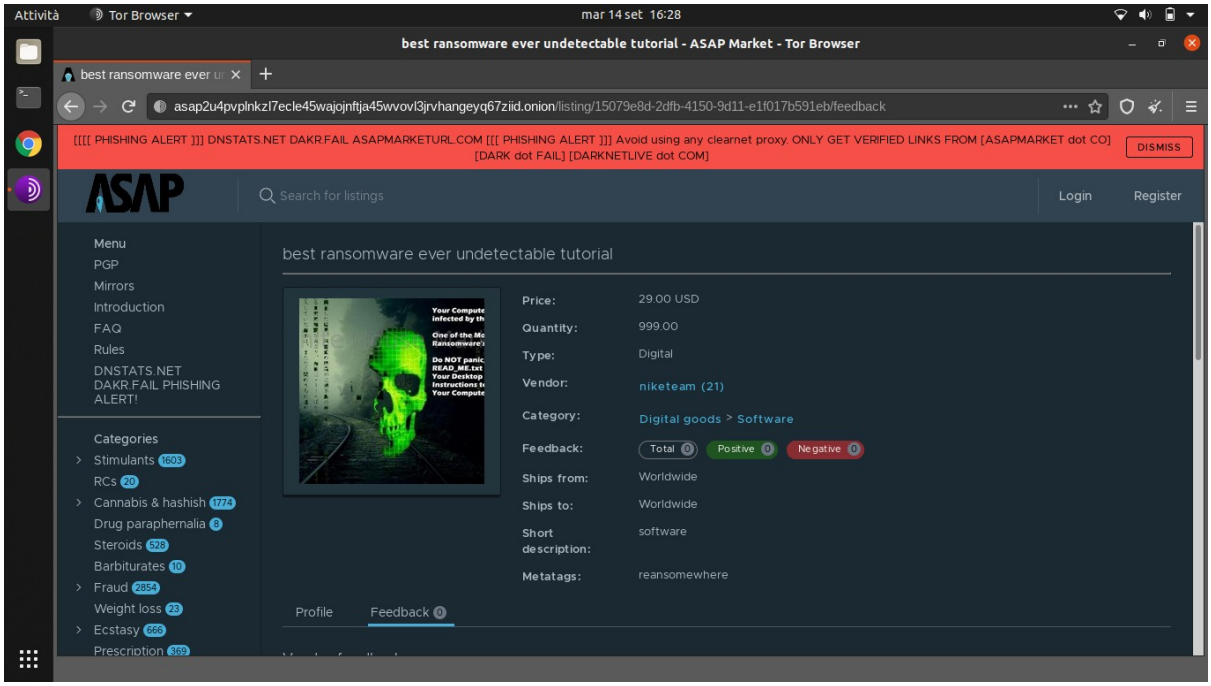
Simulazione acquisto RaaS

L’acquisto di un RAAS è molto facile mediante la rete TOR, basta scaricare il browser di tor, semplici ricerchi come “best deep web forum” per trovare già i primi link da visitare, come:
`auzbdiguv5qtp37xoma3n4xfch62duxtdiu4cfrrwbxgckipd4aktxid.onion`
`asap2u4pvplnkzl7ecle45wajojnftja45wvovl3jrvhangeyq67ziid.onion`

Possibile trovare siti chiusi, tipo questo.

Basta continuare a cercare ed arriviamo qui.





Questo ad esempio riporta sotto nella descrizione:

This is by far the best ransomware ever (100% UNDETECTABLE) 2021 + Tutorial. This is by far the best ransomware ever. Best Tool ever to Make HUGE money.

Promotion: For now price is 55$, after 10 sales price will be 1500$, hurry up get it while its cheap.
You can send it to all big companies, commerce, and hospitals.
For educational purposes Only , i'm not responsible for what you will do.

You will receive a Tutorial how to use it FOR FREE (Usually darknet ransomware sellers dont give you Tutorial, only download link), how to send it by email, how to put the desired amount and how to spread it (many spreading methods).

100% Undetectable. It's a ransomware-like file crypter sample which can be modified for specific purposes.

Features:
- Uses AES algorithm to encrypt files.
- Sends encryption key to a server.
- Encrypted files can be decrypt in decrypter program with encryption key.
- Creates a text file in Desktop with given message.
- Small file size (12 KB).
- NOT detected by antivirus programs.

WARNING DO NOT OPEN THE FILE WITHOUT READING THE TUTORIAL FIRST!!! YOU CAN INFECT YOURSELF, I WILL NOT BE RESPONSIBLE.
+ 2 other undetectable ransomware 2020.

DarkSide

DarkSide, apparso per la prima volta sui forum di hacking in lingua russa nell'agosto 2020, è una piattaforma Ransomware as a Service. DarkSide afferma che si rivolge solo alle grandi aziende e vieta agli affiliati di rilasciare ransomware su organizzazioni in diversi settori, tra cui sanità, servizi funebri, istruzione, settore pubblico e organizzazioni non profit.

Come altre piattaforme ransomware, DarkSide aderisce all'attuale best practice della doppia estorsione, che prevede la richiesta di somme separate sia per una chiave digitale necessaria per sbloccare file e server, sia per un riscatto separato in cambio della promessa di distruggere tutti i dati rubati da la vittima.

Il gruppo ransomware DarkSide ha fatto notizia nel 2021 a causa dei suoi obiettivi di alto valore come la Colonial Pipeline e le sue elevate quantità di riscatto. È considerato uno dei gruppi di ransomware più prolifici del settore. Nell'agosto 2020, il team di DarkSide ha lanciato il proprio blog pubblico, "DarkSide Leaks", per intimidire le vittime, vantarsi dei suoi attacchi e pubblicare informazioni rubate da vittime che non hanno pagato il riscatto.

DarkSide ha recentemente raggiunto una vasta notorietà come presunto colpevole dell'attacco ransomware Colonial Pipeline. Il gruppo ransomware DarkSide si distingue per la sua professionalità, compresa l'attenzione al prodotto, al servizio clienti e al "codice etico". Questa professionalità rende DarkSide un gruppo ransomware particolarmente pericoloso e capace.

Nel novembre 2020, l'autore "darksupp" ha creato dei thread su due forum del dark web di alto livello in cui ha annunciato il lancio di un RaaS, mentre nel marzo 2021, lo stesso ha creato un nuovo thread annunciando il lancio di DarkSide Ransomware v2.0.

Se una vittima non contatta DarkSide per pagare il riscatto, il gruppo criminale si offre di lanciare attacchi DDoS (Distributed Denial-of-Service) [30] contro l'azienda per esercitare ancora più pressione su di essa così da contattare DarkSide.

Vettori di attacco

Poiché il ransomware DarkSide è pubblicizzato come RaaS, gli autori che noleggiano il ransomware potrebbero utilizzare vari vettori di attacco che vanno dalle campagne di phishing allo sfruttamento di applicazioni vulnerabili.
Dopo aver ottenuto l'accesso alla rete interna della vittima, gli operatori DarkSide stabiliscono una connessione RDP con il proprio server di comando e controllo tramite la porta 443 (HTTPS), instradando il traffico Internet attraverso la rete Tor.

Per condurre ricognizioni sulla rete interna, eseguire comandi, eseguire il dump dei processi e rubare credenziali, gli aggressori utilizzano strumenti come Advanced IP Scanner [31], PSExec [32], Mimikatz [33].

Con una completa comprensione della rete e delle risorse interne, gli operatori DarkSide iniettano un eseguibile ransomware dannoso in un processo di sistema esistente tramite CMD, dopo di che avvengono diverse procedure preparatorie: rilevamento della presenza di meccanismi anti-forensi e anti-debug, rimozione delle copie shadow del volume e arresto dei processi di sistema che possono interferire con la crittografia. Dopo che la crittografia viene eseguita utilizzando gli algoritmi crittografici Salsa20 + RSA 1024 per il sistema operativo Windows e ChaCha20 + RSA 4096 per il sistema operativo Linux aggiungendo un'estensione di 8 caratteri ai file crittografati e lasciando una richiesta di riscatto intitolata "REDME.victimsID.text".

Alla fine di marzo, DarkSide ha introdotto un'innovazione del "servizio di chiamata" che è stata integrata nel pannello di gestione dell'affiliato, che ha permesso agli affiliati di organizzare le chiamate spingendo le vittime a pagare i riscatti direttamente dal pannello di gestione.

DarkSide si è dimostrato abbastanza spietato con le aziende vittime che hanno tasche profonde, ma con cui si può ragionare. La società di intelligence sulla sicurezza informatica Intel 471 ha osservato una negoziazione tra l'equipaggio di DarkSide e una società vittima degli Stati Uniti da $ 15 miliardi che è stata colpita da una richiesta di riscatto di $ 30 milioni nel gennaio 2021, e in questo incidente gli sforzi della vittima per negoziare un pagamento inferiore alla fine riducono la richiesta di riscatto di quasi i due terzi.

DHarma

L'operazione ransomware Dharma ha una storia lunga e sinuosa. Inizialmente è iniziato sotto il nome di CrySiS nell'estate del 2016.
CrySis era una cosiddetta operazione Ransomware as a Service (RaaS). L'autore di CrySiS ha creato un servizio in cui i clienti (altre bande criminali) potevano generare le proprie versioni del ransomware da distribuire alle vittime, di solito tramite campagne di spam, exploit kit o attacchi di brute force sugli endpoint RDP.

Per anni, c'è stato un flusso costante di nuove versioni di Dharma, poiché il ransomware ha ricevuto aggiornamenti e nuovi clienti si sono iscritti per distribuirlo in tutto il mondo, ognuno diffondendo la propria variazione unica di Dharma.

Nella primavera del 2019, è emerso online un nuovo ceppo di ransomware chiamato Phobos, utilizzato principalmente in attacchi mirati. I ricercatori di sicurezza di Coveware e Malwarebytes hanno rapidamente sottolineato che

Phobos era quasi identico a Dharma. Ma Dharma non si è estinto una volta che il nuovo ramo di Phobos è stato rilasciato.
Jakub Kroustek, responsabile delle informazioni sulle minacce presso Avast, ha individuato tre nuove versioni di Dharma in una settimana, il che significa che i gruppi criminali trovano ancora affidabile il codice di Dharma e continuano a utilizzarlo anche oggi, a più di 4 anni dal suo lancio.

RDP

RDP è un protocollo di comunicazione e consente a qualcuno di connettersi a un dispositivo e vedere il suo desktop, quindi il computer remoto può essere utilizzato come se fosse locale. Ciò è particolarmente utile per i dipendenti che sono spesso sul campo, come il personale di vendita o consulenti.
Microsoft ha creato il Remote Desktop Protocol (RDP) ed è integrato in Windows. Ciò significa che Dharma è stato specificamente progettato per attaccare i computer che hanno il sistema operativo Windows .

Il protocollo RDP si connette alla porta TCP 3389 [34]. Pertanto, durante il funzionamento, l'amministratore deve attivare RDP sul computer host. Questo avvia un programma di ricezione che esegue un ciclo continuo, monitorando le richieste di connessione in entrata con il numero di porta 3389 su di esse.
Sono disponibili opzioni di sicurezza. L'amministratore può impostare una password che deve essere immessa dall'utente remoto prima che l'accesso possa procedere. Sfortunatamente, molti amministratori non si preoccupano di questa funzione. All'utente verrà comunque richiesta una password, ma accede semplicemente premendo invio. Questa configurazione insicura è esattamente ciò che sta cercando il ransomware Dharma.
Il ransomware Dharma può essere facilmente bloccato semplicemente impostando una password per l'accesso RDP. Tuttavia, la protezione con password deve essere attivata, ma la password deve essere complessa e non facile da indovinare.
Gli attacchi ransomware automatizzati Dharma interromperanno semplicemente il flusso di lavoro se incontra un requisito di password. Tuttavia, gli attacchi guidati manualmente non devono fermarsi qui. L'hacker può provare una serie di password di uso comune o ingannare uno degli utenti del computer di destinazione facendogli rivelare la password.

I ransomware Dharma sono stati attribuiti a un gruppo iraniano motivato finanziariamente. Questo RaaS è disponibile sul darkweb dal 2016 ed è principalmente associato agli attacchi del protocollo desktop remoto (RDP).

Dharma non è controllato centralmente, a differenza di REvil.
Le uniche differenze erano le chiavi di crittografia, l'email di contatto e poche altre cose che possono essere personalizzate tramite un portale RaaS.

L'FBI, in un discorso alla conferenza sulla sicurezza RSA del 2020, ha classificato Dharma come la seconda operazione ransomware più redditizia degli ultimi anni, dopo aver estorto oltre 24 milioni di dollari di pagamenti alle vittime tra novembre 2016 e novembre 2019.

La maggior parte degli attacchi Dharma Ransomware sfrutta RDP come vettore di attacco. Ciò è dovuto alla prevalenza di porte RDP scarsamente protette e alla facilità con cui i distributori di Ransomware sono in grado di eseguire brute force o acquistare credenziali su siti del dark web. Le aziende che consentono a dipendenti di accedere alle proprie reti tramite accesso remoto senza adottare le adeguate protezioni corrono un grave rischio.

Gli aggressori possono violare RDP tramite alcuni metodi diversi:

1. Utilizzando la scansione delle porte tramite siti Web come Shodan e successivamente sessioni RDP di brute force fino a quando le credenziali non vengono compromesse.
2. Acquisto e utilizzo di credenziali su siti come XDedic (rimosso dalle forze dell'ordine).
3. Phishing di un dipendente dell'azienda per ottenere l'accesso e il controllo della propria macchina. Utilizzando tale accesso per elevare l'autorizzazione degli utenti utilizzando altri malware per la raccolta delle credenziali. Questo accesso elevato consente all'aggressore di spostarsi nella rete.

Ci sono decine di migliaia di credenziali RDP disponibili per la vendita a soli 3 $ sui marketplace del dark web. L'ampia disponibilità di credenziali RDP incoraggia i criminali informatici che cercano di lanciare attacchi ransomware.

REvil

REvil, noto anche come Sodinokibi, è stato identificato come il ransomware dietro una delle più grandi richieste di riscatto mai registrate: $ 70 milioni. È venduto dal gruppo criminale PINCHY SPIDER, che vende RaaS.

Questo gruppo, ha portato a termine un altro attacco ransomware, dopo quelli contro Travelex, Acer. Il bersaglio recente è stato Kaseya VSA, una piattaforma cloud per la gestione dei servizi IT. Il ransomware è stato installato tramite un aggiornamento software.

Sfruttando una vulnerabilità in Kaseya VSA, i cybercriminali hanno distribuito un finto aggiornamento contenente il ransomware. Il malware esegue anche uno script PowerShell per disattivare varie funzionalità di Microsoft Defender.

I ricercatori olandesi hanno scoperto sette vulnerabilità in Kaseya VSA durante una ricerca avviata all'inizio aprile. L'azienda statunitense è stata informata il 6 aprile. Quattro bug sono stati corretti tra il 10 aprile e l'8 maggio. Per gli altri tre

si dovrà attendere la versione 9.5.7 del software. La vulnerabilità identificata con CVE-2021-30120 è quella sfruttata dal gruppo REvil per aggirare l'autenticazione a due fattori e installare il ransomware.
Come spesso capita in questi casi, alcuni malintenzionati hanno avviato una campagna di spam per distribuire un malware.

I ricercatori di sicurezza hanno collegato i creatori del malware REvil/Sodinokibi agli autori del ransomware GandCrab, che è stato notato per la prima volta nel 2018. Gli hacker affiliati a GandCrab hanno preso di mira le aziende sanitarie, incluso il fornitore di servizi di fatturazione medica Doctor's Management Service.

Nel 2019, i membri di questo GandCrab hanno dichiarato che si sarebbero ritirati e si sono vantati di aver raccolto $ 2 miliardi di riscatti dopo solo un anno. Un anno dopo, il ministro degli Interni della Bielorussia ha dichiarato di aver arrestato un hacker legato a GandCrab.

In cambio dell'utilizzo dei servizi di REvil, REvil, come altri gruppi simili, prendono il 20% di qualsiasi pagamento, mentre chi lo utilizza l'altro 80%.

Futuro del Ransomware?

Questi avvenimenti hanno catapultato il ransomware in una nuova era, portando criminali informatici a replicare attacchi più piccoli contro aziende più grandi e chiedendo riscatti maggiori.
Alcuni sono in grado di mitigare gli attacchi e ripristinare i propri file senza pagare, ma basta una piccola percentuale di attacchi così da produrre entrate sostanziali. Anche perché pagare un riscatto non garantisce che ti verrà concesso l'accesso ai tuoi file.

Inoltre nel 2017 è stato visto il primo attacco ransomware segnalato su dispositivi connessi, 55 telecamere sono state infettate dal ransomware WannaCry, bisogna essere a conoscenza del fatto che tutti i dispositivi IoT [35] sono vulnerabili.

Anche un'infrastruttura critica rappresenta un altro obiettivo preoccupante per futuri attacchi ransomware, dove ad esempio i servizi idrici e infrastrutture simili potrebbero costituire obiettivi praticabili e di alto valore per gli aggressori.

Nel 2020, gli attacchi ransomware sono aumentati del 150%, con un aumento della dimensione media dei pagamenti di oltre il 170%. Alcune delle vittime degne di nota includono United Health Services , Orange e Acer.

La criminalità informatica è un settore in crescita, di grande successo e redditizio. Secondo Cybersecurity Ventures, i costi della criminalità informatica cresceranno del 15% all'anno per raggiungere i 10,5 trilioni di dollari entro il 2025: la terza "economia" più grande al mondo, dopo quelle degli Stati Uniti e della Cina.
Dall'inizio della pandemia, gli attacchi ransomware sono aumentati del 500%.

Come proteggersi?

Se un attacco riesce, significa che qualcosa poteva essere fatto per evitarlo.
Ma questo non implica che siano stati fatti errori facilmente evitabili o che ci sia incompetenza.
In una grande organizzazione, può essere troppo complesso e costoso gestire un backup offline o applicare sistemi di autenticazione a doppio fattore.

L'unico modo per prevenire un attacco ransomware è essere preparati prima che accada. Ciò richiede la creazione di backup offline regolari su un dispositivo che non rimane connesso a Internet. Il malware, incluso il ransomware, può infettare allo stesso modo le unità di backup e le unità USB. È fondamentale assicurarsi di mantenere i backup offline.

Per proteggersi basta seguire le best practice fondamentali per la sicurezza informatica così da ridurre al minimo i danni del ransomware e di qualsiasi altro malware:

1. Backup frequenti e testati, backup di tutti i file e sistemi è una delle difese più potenti contro il ransomware. Tutti i dati possono essere ripristinati in un punto di salvataggio precedente.
2. Aggiornamenti strutturati e regolari, dato che questi possono includere patch per rendere il software più sicuro contro le minacce note.
3. Restrizioni sensate, alcune limitazioni dovrebbero essere poste a dipendenti che lavorano con dispositivi che contengono file.
4. Tracciamento delle credenziali adeguato, qualsiasi dipendente a cui viene concesso l'accesso ai sistemi crea un potenziale punto di vulnerabilità.

Nonostante queste best practice siano abbastanze note, molte persone non riescono a eseguire regolarmente il backup dei propri dati ed alcune aziende lo fanno solo all'interno della propria rete, il che significa che i backup possono essere compromessi da un singolo attacco ransomware.

L'istruzione sui segni rivelatori delle tattiche di distribuzione del ransomware, come attacchi di phishing, drive-by download e siti Web fittizi, dovrebbe essere una priorità assoluta per chiunque utilizzi un dispositivo connesso oggi.

Tipi di Backup

Un backup completo, o full backup [36], consiste nella copia di tutti i blocchi di cui è composto il file, quindi anche i blocchi non modificati vengono copiati: è una copia totale. Ogni file è fatto da 'mattoncini', i blocchi, di dimensioni predeterminate; la modifica di un file consiste nella modifica di uno o più blocchi. Un backup completo è rappresentato da questa immagine.

Un backup completo, essendo una copia totale dei file, richiede sempre il massimo dello spazio su disco (pari alla somma delle dimensioni di ciascun file), del tempo necessario per l'esecuzione e delle risorse computazionali.

Il backup incrementale copia solo i blocchi cambiati rispetto all'ultimo backup disponibile. Per eseguire il ripristino occorrono sia il backup completo di riferimento che ciascun backup incrementale fino al giorno scelto: se ad esempio servono i dati aggiornati al giorno 4, allora serve il backup di riferimento e i backup incrementali dei giorni 2, 3 e 4. Tra i vantaggi di questo tipo di backup troviamo la velocità di esecuzione e le dimensioni contenute in relazione al backup completo: solo le differenze rispetto al precedente backup sono copiate.

Lo svantaggio principale è che per il ripristino necessità di tutti i backup intermedi, quindi se un backup risulta corrotto, anche i successivi lo sono.

Similmente al backup incrementale, il backup differenziale esegue una copia solo dei blocchi cambiati, ma cambia il riferimento: il backup incrementale copia i blocchi cambiati rispetto all'ultimo backup eseguito, il backup differenziale copia i blocchi cambiati rispetto al backup completo di riferimento. Come il backup incrementale, i vantaggi del backup differenziale consistono nella rapidità di esecuzione e nelle ridotte richieste di spazio rispetto al backup completo; tuttavia richiede risorse maggiori e più tempo rispetto al backup incrementale, ma il ripristino è più veloce dal momento che sono richieste solo due copie - il backup completo di riferimento e quello differenziale - e non tutte le copie intermedie e quello di riferimento.

Di conseguenza, la corruzione di un backup determina l'impossibilità di ripristinare solo quel backup e non anche i successivi.

Bruteforce

I ransomware utilizzano algoritmi troppo complessi come AES256 ed RSA per lo scambio di chiavi, che per essere decriptati, richiedono una potenza di calcolo elevatissima, quasi infinitesimale, ma con il progredire delle tecnologie e con la comparsa dei computer quantistici, anche questi algoritmi potrebbero diventare obsoleti.

L'unico modo per recuperare i files è trovare qualche vulnerabilità nella fase di encrypt, nel caso di RSA potrebbe essere:

- Esponente pubblico (**e**) troppo piccolo o troppo elevato.
- **p** e **q** vicini tra loro, oppure troppo piccoli.

Problematiche che si possono verificare ma che accadono raramente, solo nel caso non si conosce il sistema RSA.

Nel caso di AES:

- Utilizzare stessa IV e KEY per ogni encrypt.
- Utilizzare stessa IV.
- Side channel attack.

Qui è più facile avere il "sistema" di encrypt vulnerabile, dato che per comodità sei tentato ad utilizzare sempre la stessa KEY ed IV, magari salvarsi ed utilzzarli quando occorrono.

Formazione

Bisogna investire un po' di tempo nella lettura dei ransomware e dei metodi di phishing più diffusi. Senza avere fretta di fare clic e aprire gli allegati, la disattenzione e la fretta costeranno molto di più.
Le aziende dovrebbero fornire formazione sulla sicurezza informatica ai propri dipendenti. Il CEO di ogni azienda deve prepararsi al ransomware.

La formazione si può classificare in:

1. Formazione fisica, come ad esempio evitare di inserire una chiavetta non ti appartiene, oppure una chiavetta che trovi “solo perché sei curioso”, devi sempre prestare attenzione a quello che si inserisce nel proprio computer.
2. Formazione online, prestare attenzione ai siti che si visitano, rimanere sempre nel https e controllare il dominio di esso, anziche “facebook.com” potrebbe essere “face.book.com”, verificare l’affidabilità del sito mediante recensioni.
3. Formazione aziendale, diffidare maggiormente da email, controllando sempre da chi provengono e verificando le informazioni contenute in esse prima di scaricare qualsiasi informazione contenuta in essa.

Come difendere o essere difesi da Google Drive

Google Drive [37] consente agli utenti di creare, condividere e accedere senza problemi ai propri documenti, moduli, video e immagini da qualsiasi luogo, su qualsiasi dispositivo abilitato a Internet in tempo reale dato che ha tutti i tuoi dati salvati nel cloud.

Per proteggere Google Drive dai ransomware, bisogna sapere come può raggiungerlo. Come qualsiasi altro servizio cloud, Google Drive è soggetto ad attacchi ransomware.

Backup e sync è uno strumento di sincronizzazione gratuito di Google. Sincronizza i computer locali con Google Drive e crea una copia dei file dal tuo Google Drive al tuo computer. Qualsiasi modifica su Google Drive si riflette sul tuo computer locale e viceversa.
Questa sincronizzazione comporta dei rischi se scarichiamo un file dannoso che effettua l encrypt dei file sul computer, inclusi i documenti sincronizzati nella cartella Google Drive. Backup e sync interpreterà la crittografia come una normale modifica dei file e li sincronizza automaticamente con Google Drive.
La soluzione è avere sempre un backup recente.
Backup e sync è uno strumento di sincronizzazione, non una soluzione di backup. Questo strumento non salva i tuoi file: li sincronizza.
L'unico modo per evitare la perdita di dati è avere sempre un backup selettivo di Google Drive.

Se elimini dei file, i file eliminati vengono archiviati automaticamente nel Cestino di Google Drive.

Ad esempio se il ransomware elimina il file originale, questo viene eliminato dal mio computer. Tuttavia, se hai installato l'app Backup e sync di Google Drive, i file eliminati verranno archiviati automaticamente nel Cestino di Google Drive, così da trovare i file originali nel Cestino di Google Drive e ripristinarli, senza dover pagare il riscatto ed eliminare tranquillamente quelli crittografati.

Some

Framework e Tecnologie utilizzate?

Python

Python è un linguaggio di programmazione interpretato, orientato agli oggetti e di alto livello con semantica dinamica. Le sue strutture dati integrate, lo rendono molto utile per lo sviluppo rapido di applicazioni, nonché per l'uso come linguaggio di script o colla per collegare insieme componenti esistenti. La sintassi semplice e facile da imparare di Python enfatizza la leggibilità e quindi riduce i costi di manutenzione del programma. Python supporta moduli e pacchetti, il che incoraggia la modularità del programma e il riutilizzo del codice. L'interprete Python (nel mio caso Cpython [38], anche il più comune utilizzato dato che Pypy non è compatibile con alcuni package) e l'ampia libreria standard sono disponibili gratuitamente in formato sorgente o binario per tutte le principali piattaforme e possono essere distribuiti liberamente.
Invece, quando l'interprete scopre un errore, solleva un'eccezione. Quando il programma non rileva l'eccezione, l'interprete stampa una traccia dello stack.

Ngrok

Ngrok [39] è un'applicazione multipiattaforma che consente di esporre un server di sviluppo locale con il minimo sforzo. Il software fa sembrare che il tuo server web ospitato localmente sia ospitato su un sottodominio di ngrok.com, il che significa che non è necessario alcun IP pubblico o nome di dominio sulla macchina locale.

Ngrok è in grado di aggirare la mappatura NAT [40] e le restrizioni del firewall creando un tunnel TCP di lunga durata da un sottodominio generato casualmente su ngrok.com (es. aa45-185-138-216-36.ngrok.io) alla macchina locale. Dopo aver specificato la porta su cui il tuo server web è in ascolto, il programma client ngrok avvia una connessione sicura al server ngrok e quindi chiunque può effettuare richieste al tuo server locale con l'indirizzo univoco del tunnel ngrok.

Per impostazione predefinita, ngrok crea endpoint sia HTTP che HTTPS, rendendolo utile per testare le integrazioni con servizio API [41] di terze parti che richiedono domini SSL/TLS validi.

Pyinstaller

PyInstaller [42] legge uno script Python. Analizza il codice per scoprire ogni altro modulo e libreria di cui lo script ha bisogno per essere eseguito. Quindi raccoglie copie di tutti quei file, incluso l'interprete Python attivo e li mette con il tuo script in una singola cartella, o facoltativamente in un singolo file eseguibile.
Per i tuoi utenti, l'app è autonoma. Non è necessario installare alcuna versione particolare di Python o alcun modulo. Non hanno affatto bisogno che Python sia installato.
PyInstaller trova tutti gli import nel tuo script. Trova i moduli importati e cerca in essi le import, e così via in modo ricorsivo, finché non ha un elenco completo di moduli che il tuo script può usare.

PyInstaller può raggruppare il tuo script e tutte le sue dipendenze in un singolo eseguibile denominato myscript.
Il vantaggio è che gli utenti ottengono qualcosa che capiscono, un singolo eseguibile da avviare. Uno svantaggio è che tutti i file correlati come README devono essere distribuiti separatamente. Inoltre, il singolo eseguibile è un po' più lento da avviare.

MySQL

MySQL [43], il più popolare sistema di gestione di database Open Source, è sviluppato, distribuito e supportato da Oracle.

Un database è una raccolta strutturata di dati. Può essere qualsiasi cosa, da una semplice lista della spesa a una galleria di immagini o alla grande quantità di informazioni in una rete aziendale.
Per accedere ed elaborare i dati archiviati in un database, è necessario un sistema di gestione del database.

Un database relazionale archivia i dati in tabelle separate anziché mettere tutti i dati in un unico grande magazzino. Le strutture del database sono organizzate in file fisici ottimizzati per la velocità. Il modello logico, con oggetti come database, tabelle, viste, righe e colonne, offre un ambiente di programmazione flessibile. Si impostano regole che regolano le relazioni tra diversi campi di dati, come uno a uno, uno a molti, univoco, obbligatorio o facoltativo e "puntatori" tra tabelle diverse. Il database applica queste regole, in modo che con un database ben progettato, l'applicazione non veda mai dati incoerenti, duplicati, orfani, non aggiornati o mancanti.

La parte SQL di “MySQL” sta per “Structured Query Language”. SQL è il linguaggio standardizzato più comune utilizzato per accedere ai database.

MySQL Database Server è molto veloce, affidabile, scalabile e facile da usare. Se è quello che stai cercando, dovresti fare un tentativo. MySQL Server può essere eseguito comodamente su un desktop o laptop, insieme ad altre

applicazioni, server Web e così via, richiedendo poca o nessuna attenzione. Se dedichi un'intera macchina a MySQL, puoi regolare le impostazioni per sfruttare tutta la memoria, la potenza della CPU e la capacità di I/O disponibili. MySQL può anche scalare fino a cluster di macchine, collegate in rete.

MySQL Server è stato originariamente sviluppato per gestire database di grandi dimensioni molto più velocemente rispetto alle soluzioni esistenti ed è stato utilizzato con successo in ambienti di produzione altamente esigenti per diversi anni. Sebbene in costante sviluppo, MySQL Server offre oggi un ricco e utile set di funzioni. La sua connettività, velocità e sicurezza rendono MySQL Server particolarmente adatto per l'accesso ai database su Internet.
MySQL Server funziona in sistemi client/server o embedded.
Il software MySQL Database è un sistema client/server costituito da un server SQL multithread che supporta diversi backend, diversi programmi e librerie client, strumenti amministrativi e un'ampia gamma di interfacce di programmazione delle applicazioni (API).
Forniamo anche MySQL Server come libreria multithread incorporata che puoi collegare alla tua applicazione per ottenere un prodotto autonomo più piccolo, più veloce e più facile da gestire.

Flask

Flask [44] è un framework web, è un modulo Python che consente di sviluppare facilmente applicazioni web. Ha un nucleo piccolo e facile da estendere: è un micro framework che non include un ORM (Object Relational Manager) [45] o simili funzionalità.
Ha molte funzioni interessanti come il routing degli URL, il motore dei modelli. È un framework di app Web WSGI [46]. È progettato per mantenere il nucleo dell'applicazione semplice e scalabile.

Ghidra

Ghidra [47] è un software di reverse engineering (SRE) è un framework creato e gestito dalla NSA Research Directorate. Questo framework include una suite di strumenti di analisi software di fascia alta e completi che consentono agli utenti di analizzare il codice compilato su una varietà di piattaforme tra cui Windows, macOS e Linux. Le funzionalità includono disassemblaggio, assemblaggio, decompilazione, creazione di grafici e script, insieme a centinaia di altre funzionalità. Ghidra supporta un'ampia varietà di set di istruzioni del processore e formati eseguibili e può essere eseguito sia in modalità utente interattiva che automatizzata. Gli utenti possono anche sviluppare i propri componenti di estensione Ghidra e/o script utilizzando Java o Python.

Ghidra è open-source su GitHub, incluso il decompilatore.

Ghidra ha la capacità di caricare più binari contemporaneamente in un progetto, ciò significa che puoi tracciare più facilmente il codice tra un'applicazione e le sue librerie.
Il disassemblatore di Ghidra ha un'analisi del flusso di dati integrata, che mostra da dove possono venire i dati quando si fa clic su un registro o una variabile.
Ghidra ha progetti di disassemblaggio/decompilazione collaborativi incorporati in base alla progettazione.
Ghidra sembra avere un supporto migliore per immagini firmware [48] molto grandi (1GB+) con prestazioni decenti. Inoltre, non ha problemi con l'analisi delle immagini del firmware che dichiarano grandi regioni di memoria.
Ghidra per disassemblare i binari del sistema operativo Windows (es. kernelbase.dll) è attualmente interrotto a causa di alcuni bug con il decodificatore di istruzioni x86.

Gobuster

Gobuster [49] è un tool usato per fare bruteforce, tra le tante funzionalita che offre, quella che a noi interessa di più è quella che riguarda gli URI:

- URIs (trova tutti i file e directory che ritornano status code positivo) presenti in un sito web.

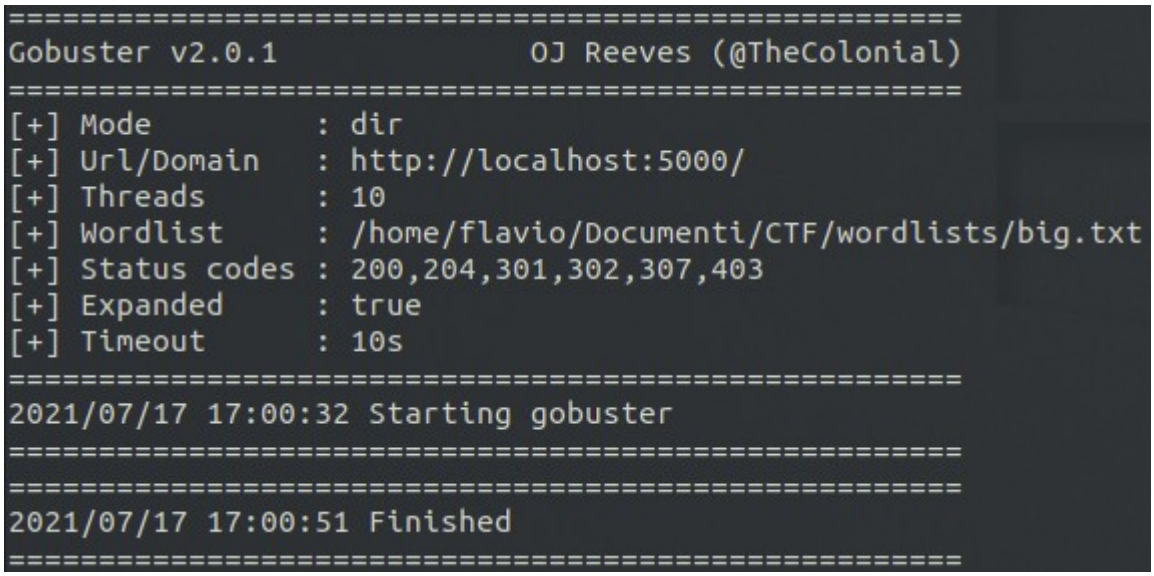
API

Flask supporta le chiamate REST [50], sono state predisposte delle route, con dei path speciali, se si cerca di enumerare le directory presenti nel sito si ha un riscontro negativo.
Infatti se si prova con **gobuster**, ad esempio con il comando:

```
~$ gobuster -e -u http://localhost:5000/ -w .../wordlists/big.txt
```

Il file big.txt contiene 20.000 record con nomi di directory o file comunemente presenti all'interno di una pagina web.

Il risultato sarà:



Non è stata trovata nessuna directory o file come si può vedere, si potevano utilizzare altri tool come **dirbuster** [51] o **wfuzz** [52] ottenendo sempre lo stesso risultato.
Il Server risponde a 6 route:

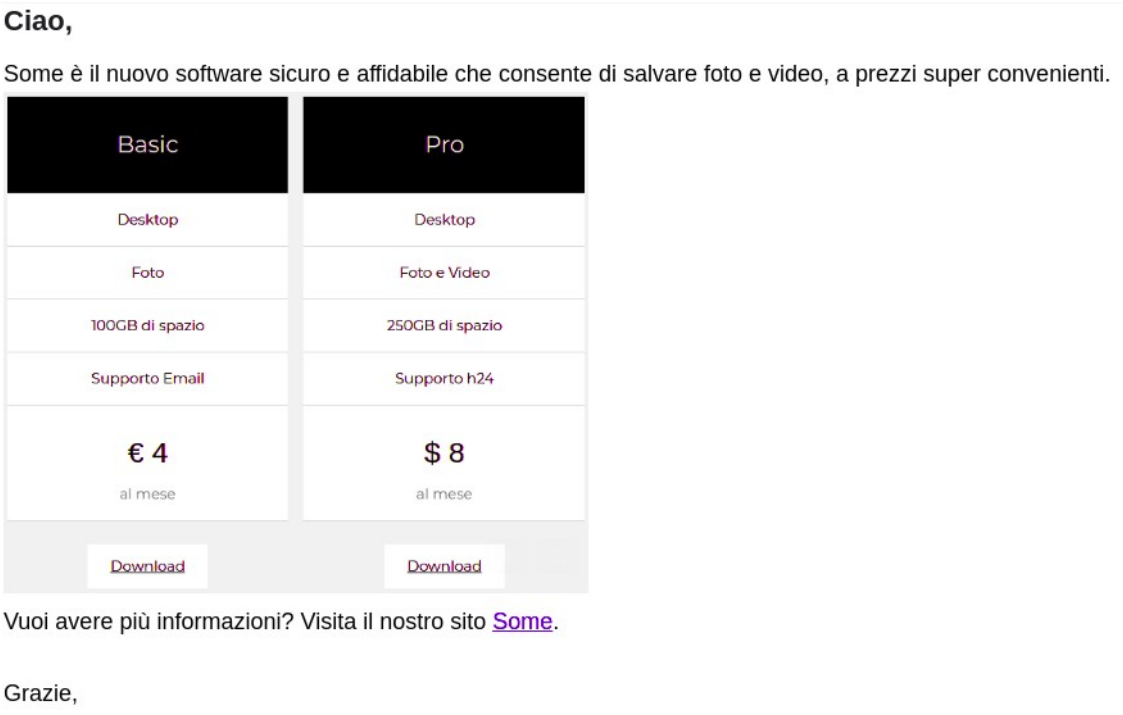
1. `/`, la home principale, dove viene mostrato l'index.html, che ha il compito principale di fare credere che il sito sia veritiero, così da trarre in inganno le persone e far scaricare il software malevolo.
2. `/afc0db1a93d34ebf844b3808e749e7ff/some`, mostra la pagina che contiene le informazioni che servono per effettuare il decrypt, appare non appena è stato iniziato l' encrypt, all'interno della pagina ci sono delle info che riguardano l'interruzione del software oppure la possibilità di chiuderlo e riaprirlo.
3. `/f6c2c6976c0d1155384b6090376c25fe/add`, POST utilizzata per inserire un User formato da id, aes, pass, che verrà salvato all'interno di un file.
4. `/181b01247a7c602897e927c7395b0507/get/<user_id>`, POST che ritorna la key per fare il decrypt dei file, necessita di un parametro all'interno del body, ovvero pass, se la pass è corretta ritorna la key, altrimenti ritorna 'None'.

5. `/b899e033e3b761f6f96d0c26b1b15d7e/remove/<user_id>`, GET che rimuove un User, viene chiamata dopo il decrypt, se si chiama questa GET, ad esempio quando il client non ha ancora pagato il riscatto, il recupero dei dati è impossibile.
6. `/c3be40a118e451381f85da18f3112023/exist/<user_id>`, GET che ritorna True o False nel caso un User esistesse già, nel caso non esistesse viene creato.

Tutti gli altri path, es. `/login` avranno uno status code 404, con relativa pagina dove segnala il mancato ritrovamento di essa.
Si può notare che una richiesta ha un path differente, lungo 32 byte, fare bruteforce, conoscendo solo la lunghezza e i caratteri presenti richiederebbe 16^32 tentativi, il che la rende un'opzione impossibile.

Come funziona?

Ora vediamo come funziona Some, supponiamo riceverete un email spam lievemente convincente, tipo questa.



Una semplice mail innocua che vi consiglia un software per conservare foto e video, il sito a primo impatto si presenta ben fatto, così decidiate di scaricarlo.

SOME

Una volta scaricato, lo avviate, aspettate, pensando di trovarvi una pagina iniziale di login, oppure una intro, ed invece niente, siete fregati.
La prima cosa che Some farà sarà prendere l'utente loggato (quello in sessione) in quel momento e l'hostname, questa coppia formerà l'id dell' User.
Viene creato l'oggetto File e vengono trovate tutte le cartelle che si trovano all'interno della home, la mia home è '/home/flavio' ed otteniamo: Documenti, Immagini, Modelli, Musica, Pubblici, Scaricati, Scrivania, Video.

Questa lista di cartelle viene filtrata mediante una lista apposita (lista che contiene nomi semplici di cartelle frequenti) e vengono effettuati dei controlli parziali, ad esempio se io ho 2 cartelle che contengono immagini, chiamate 'Immagini Vacanza' e 'Foto Mare' vengono prese entrambe dato che viene fatto un semplice 'contains' tra i nomi presenti nella lista e quelli trovati nella home.
In questo modo otteniamo una lista che contiene tutti i path dei file presenti nelle molteplici cartelle, ma che rispettano tutti i requisiti.

Dopo aver creato l'oggetto File, si passa a creare l'oggetto Server, che come prima cosa fà richiama la variabile `server_public_key` che contiene la chiave pubblica del Server, e viene fatto il load di quella, così non è necessario fare una GET e si evita un eventuale MITM [53]. Con quella chiave verrà cifrato l'User che verrà mandato al Server.

L'unico a poter decifrare il messaggio è il Server grazie alla sua chiave privata.

Per la comunicazione tra Server e Client è stata utilizzata una chiave a 4096 bit, il più grande modulo **n** (dato dal prodotto di 2 numeri primi distinti **p** e **q** diversi tra loro) ad essere stato fattorizzato, era di 829 bit. Quindi possiamo immaginare sia veramente impossibile riuscirci se **p**, **q** ed **e** vengano scelti con attenzione (il che avviene in maniera abbastanza facile).

Dopo aver creato l'id dell'User, viene fatta una GET per vedere se è presente o meno all'interno del Server, così da non procedere di nuovo con l' encrypt ma far

apparire solo la finestra che chiede la password con la possibilità di fare il decrypt, dove si hanno a disposizione 2 soli tentativi.

Viene creato l'oggetto Cipher dove gli viene passato il parametro `key=None` nel caso l'User non esistesse, così viene scelta una key random, mentre nel caso si procede con il decrypt si ha `key=risposta_server`, ma solo nel caso la password fosse corretta e si procede a fare il decrypt.

Nel caso l'User non esistesse ne viene creato uno con:

1. Id, dato da utente in sessione + hostname.
2. Key, chiave AES usata per fare l' encrypt/decrypt.
3. Password, una password di 4 bytes.
4. IP del pc che viene ricavato facendo una GET ad http://httpbin.org/ip.

Il JSON dell'User che viene mandato al Server è simile a questo.

```
{
    "id": "flavio",
    "key": "Xq4Fr65nD2dN2kJyo1zet4UhP9GzrZCDae5ObOGsGhE=",
    "pass": "5d6a",
    "ip": "84.214.51.184"
}
```

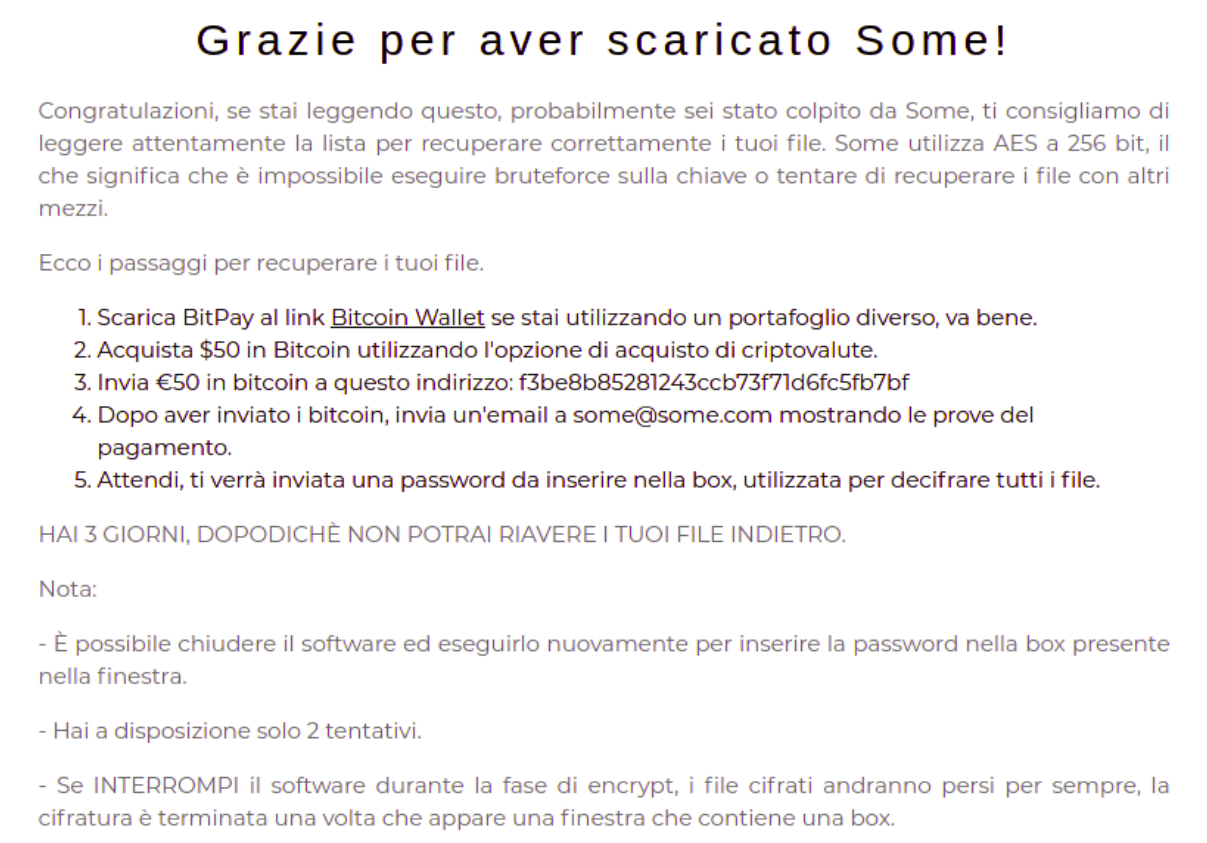
Viene fatta una POST dove nel body vi è il JSON cifrato con la chiave pubblica del Server ottenuta in precedenza, il Server decifra il messaggio e lo salva all'interno del database.

Se analizziamo la POST dell'inserimento di un User, intercettiamo una stringa in base64 [54], fatto il decode di tale stringa si avranno una serie di numeri che rappresentano il messaggio cifrato con la chiave pubblica del Server.

```
POST /f6c2c6976c0d1155384b6090376c25fe/add HTTP/1.1
Host: localhost:5000
User-Agent: python-requests/2.22.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 1236

MzAwMTMyOTI5Mzc0NTc5NTMyNzUxNTIzMjAyNzAxNDcxNDc0NzA2Njg0Mjc0MDY3Mzk1NjQ5Mzg1MTQ5NDI0
NTE0NDkyOTc5NTM2NzY4MjE5MDc5NDM5NTA0MjI5NDcyNzYzNTQzMjM5OTgyMTU1NTc3NzQyMzQ3NDIwMjU3
NTE0MTc2Nzc4Njc2MjMzODQwMTIyNjQ4MTE3MTM4MTYzODIxMDE1MzY3NTQ4NDk3OTE2OTkyMjM4NjYxMTc4
MDY1NDYxMTYyNjA3NDI3NDc4MjYwNTg0MTYxNzUwNzMzNDY4NTYwNDYwNDM5MTQ1Mzg5ODQ1NjczNzI2NDI1
NDg0NDM4NjIxNzI5NDI0ODU3MzI2Mzg4Mjk2NTMyNTMxMzQ3ODkyNDM1NDkxMzE1NTQyMTYxNDcwMzE3ODM4
OTY4OTM0MzgwODEwNTkwOTI3MzY3ODEzMzY1NDk4NTc3OTAyMzU1OTE0MzQxOTgzNzkxMDk5NTY5MDA4NDg0
NTI0NzA0MDA5MjYxMzI3NTc0MDcyMzUxNTEwOTAwNTQ5NDcwMTkwMTQ2MDkxMTMyODEzODQ3NTEyNjk4MDAw
MDA1NjEwNjI5NTg4ODM5Nzc1OTEyOTYxNjQwNDEyNzQ2MzEzNDUxMDMxMjM1ODQ1MTgwMDAyNDQ1MTQyNzcw
MTQwMjcxNTY1MTk1NzgzMTY5MTA1NzMzMzkxMzI4MzUxNTg4ODUyNTg3ODE5NjYzMjA4NTU2MTg1NzEwODYz
NTcyMTkwODkzNDA0Nzc3NDIwNzk2MjIwMDM0NzM1MTMyODc3MzExMjQ1NzYyOTY4MjY3ODMzMjYwNTYzNDMw
NTgwODYzODE1MzgwODQ3MjE4NTUxMTIzNDY3MzE0MzExMzAxODc4NjU5MzI2NzI2MDk1NjczNTA0MDA1Mzg5
Njk4NjkwODIwNTkxODQzMDcyNDkwMDU2ODc5OTU2Njc3MTM1MjcxMDY5NzYyMjA5NTA0NDE2NjQxMDEzOTEx
MTczNTE0OTAyOTUyNzU3ODI2OTQ5ODYzNzczNTgwNzYwMDcwNTc2NjIzNDYxNjk4MzA0NTE2ODI4ODA5NDMw
ODgxMTM5MTU3OTY0MTgxOTI2ODE1NDQ0MzM3ODkwMzM0MDA3ODg3NTk4NjQwMjE5MzY3MjQ1MjE4OTI1NjA5
ODE4MDA3OTUyNjM1MTI3NTM5NjgwNjU2NzQzOTI4NDQyNzgyNTkxNTcxNQ==HTTP/1.0 201 CREATED
Content-Type: text/html; charset=utf-8
Content-Length: 0
Server: Werkzeug/1.0.1 Python/3.8.10
Date: Sat, 17 Jul 2021 18:16:01 GMT
```

Una volta fatta la POST viene aperta una pagina che reindirizza in una pagina all'interno del nostro sito che mostra quello a cui si è andati incontrato, e tutte le procedure per fare il decrypt dei file.



Grazie per aver scaricato Some!

Congratulazioni, se stai leggendo questo, probabilmente sei stato colpito da Some, ti consigliamo di leggere attentamente la lista per recuperare correttamente i tuoi file. Some utilizza AES a 256 bit, il che significa che è impossibile eseguire bruteforce sulla chiave o tentare di recuperare i file con altri mezzi.

Ecco i passaggi per recuperare i tuoi file.

1. Scarica BitPay al link Bitcoin Wallet se stai utilizzando un portafoglio diverso, va bene.
2. Acquista $50 in Bitcoin utilizzando l'opzione di acquisto di criptovalute.
3. Invia €50 in bitcoin a questo indirizzo: f3be8b85281243ccb73f71d6fc5fb7bf
4. Dopo aver inviato i bitcoin, invia un'email a some@some.com mostrando le prove del pagamento.
5. Attendi, ti verrà inviata una password da inserire nella box, utilizzata per decifrare tutti i file.

HAI 3 GIORNI, DOPODICHÈ NON POTRAI RIAVERE I TUOI FILE INDIETRO.

Nota:

- È possibile chiudere il software ed eseguirlo nuovamente per inserire la password nella box presente nella finestra.

- Hai a disposizione solo 2 tentativi.

- Se INTERROMPI il software durante la fase di encrypt, i file cifrati andranno persi per sempre, la cifratura è terminata una volta che appare una finestra che contiene una box.

Contemporaneamente, viene fatto partire l’ encrypt dei file, così mentre l’utente legge si hanno dei file di vantaggio prima di capire bene quello che sta succedendo, così se decide di interrompere quei file andranno persi per sempre.

Durante la fase di encrypt, vengono trovati tutti i file che terminano con le seguenti estensioni.

- Documenti: '.csv', '.doc', '.docx', '.odt', '.ods', '.pdf', '.pps', '.ppsx', '.ppt', '.pptx', '.txt', '.xls', '.xlsx'.
- Foto: '.jpg', '.jpeg', '.png', '.gif'.
- Audio: '.mp1', '.mp2', '.mp3', '.wav', '.mka'.
- Video: '.avi', '.mp4', '.mov', '.mkv'.
- Zip: '.zip', '.rar', '.7z'.

Ho deciso di prendere quelle che sono le estensioni più comuni di un utente medio.

La lista che contiene i path viene iterata, vengono aperti in modalità lettura uno alla volta, viene salvato il contenuto, fatto l’ encrypt di esso e viene riscritto il file in base64 del risultato dell’ encrypt con AES 256 mode CBC.
Tutti i file vengono cifrati con la stessa key da 32 byte, impossibile da fare bruteforce, dato che richiederebbe un totale di 256^32 tentativi.

Per ogni file viene scelto un IV diverso, quindi non si usa lo stesso, altrimenti l’ encrypt sarebbe vulnerabile.

L’ IV è di 16 byte, e viene spezzato in 2 parti, che vengono aggiunte all’inizio del contenuto del file ed alla fine. Quindi si avrà:

```
iv[:8] + aes.encrypt(pad(data, self.BLOCK_S)) + iv[8:]
```

Mandare l’ IV di ogni file al Server risulterebbe dispendioso e poco efficace, dato che bisognerebbe memorizzare a quale IV appartenga il file.

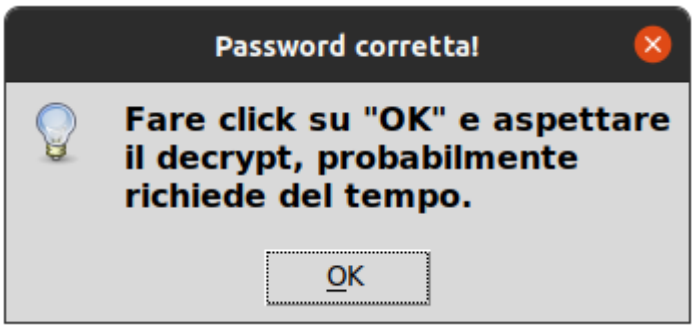
Finito l' encrypt la key dell’oggetto Cipher viene cambiata 1024 volte con stringhe random di 16 byte, insieme a quella dell’User, dato che l’app rimane attiva dato che compare la GUI, sarebbe possibile recuperare la key nelle area di memoria.
Facendo così, viene fatta una free e sovrascritta la variabile rendendo impossibile il recupero della key.

Se si decide di chiudere la GUI, ad esempio mediante chiusura forzata (dato che non è possibile chiuderla mediante la x), è possibile eseguire nuovamente il software senza fare nuovamente l’ encrypt.

Nella GUI è presente una box, dove è possibile inserire una password, che rappresenta la password che viene assegnata ad ogni utente durante la sua creazione, però, ci sta sempre un però, la password che viene scelta all'inizio, quella di 4 byte, è una password fittizia che viene cambiata lato Server con una da 48. Così da avere 16^48 tentativi (16 dato che la password è formata solo da a-f e 0-9), in più, se nessuno conosce la lunghezza e le lettere che la compongono, è praticamente impossibile fare il recovery della password, oppure riuscire a fare bruteforce.

La password viene mandata tramite email, solo se si prova il pagamento effettuato, e dato che si hanno a disposizione solo 2 tentativi, non conviene "tirare ad indovinare", diciamo che abbiamo aggiunto un incentivo per far si che l'utente paghi.

Ogni volta che viene premuto il tasto "Decrypt", viene preso il testo e viene fatta una POST al Server, dove controlla che a quell' User id, corrisponda la password inserita nella box, se è cosi, viene mandata la key in risposta alla POST ed inizia il decrypt, per verificare che la key sia giusta, appare questa finestra di dialogo.



Se la password non è corretta appare un messaggio di errore immediato sotto la box che dice “Password sbagliata!”.

Se l’utente decide di collaborare seguendo le procedure di pagamento del riscatto, inviando una mail, che deve avere come oggetto l’ User id visibile nella GUI così da ottenere la password dell’utente, la scrive nella box e fa la POST, e tutto va nel migliore dei modi, viene fatto il remove dell’User, quindi se lo si esegue nuovamente, ad esempio per sbaglio, parte nuovamente l’ encrypt.

Tutti gli User sono memorizzati all’interno di una tabella chiamata ‘users’. La tabella users è stata costituita nel seguente modo:

```
CREATE TABLE users (
      id VARCHAR(255) NOT NULL,
      aes VARCHAR(255) NOT NULL,
      pass VARCHAR(64) NOT NULL,
      ip VARCHAR(16)
);
```

Il database si chiama ‘some’, che rappresenta il nome del ransomware, sono state utilizzate delle stored procedure per eseguire le query, così da evitare eventuali sql injection che evitano il dump del database consentendo il recupero.

Sono state realizzate 4 stored procedure, una per ogni azione necessaria:

1. addUser, serve ad aggiungere un User all’interno del database.
2. removeUser, rimuove un User dopo che è stato effettuato il decrypt.
3. getUserAes, ritorna la chiave AES nel caso la password inserita nella box della GUI corrisponda a quella dell’User.
4. userExist, utilizzata per vedere se un User è già presente all’interno del database.

Comandi per creare la stored procedure addUser:

```
DELIMITER //
CREATE PROCEDURE addUser(
   IN user_id VARCHAR(255),
   IN user_aes VARCHAR(255),
   IN user_pass VARCHAR(64),
   IN user_ip VARCHAR(16)
)
           -> BEGIN
           -> INSERT INTO users (id, aes, pass, ip) VALUES (user_id,
     user_aes, user_pass, user_ip);
           -> END //
DELIMITER ;
```

Grazie all'utilizzo del database se il Server cade, si hanno tutti gli User salvati, così da garantire il recupero dei file cifrati.

Se l'utente, preso dal panico, interrompe l' encrypt, i file cifrati fino andranno persi per sempre, dato che l'User viene salvato nel Server solo dopo aver terminato la fase di encrypt, ed avendo terminato il software, non è possibile recuperare le key nelle aree di memoria.

Conclusioni

Questa tesi ha cercato di illustrare le possibili via di accesso di un ransomware, come affrontarlo e non farsi cogliere impreparati; come risulta facile farne uno.
Illustrando il funzionamento delle varie tecniche applicabili ad esso per eseguire un “lavoro perfetto”.
Come possiamo vedere, le tecniche e gli strumenti permettono di sfruttare diversi approcci combinati tra loro, mettendo in pratica un attacco vero e proprio.

Sviluppi futuri

Possibili sviluppi futuri che renderebbero questo ransomware ancora più interessante ed innovativo potrebbero essere i seguenti.

Code Obfuscation

Riuscire a fare l’ obfuscation [55] del codice, così quando si va a fare il reverse dell'eseguibile tutte le informazioni saranno difficili da comporre.
È stato provato a farlo, cercando di offuscare tutti i file .py, ma non arrivando a nessuna conclusione, risulterebbe più facile se tutto il ransomware si trovasse all’interno di un unico file .py, così da rendere possibile questa manovra.
Provando a fare l’ obfuscation di tutti i file costruendo in seguito l’eseguibile è risultato più difficoltoso, dato che i metodi e le classi sono divise in file, non veniva trovato il package src (sorgente che contiene tutti i file .py).
È stato provato a fare l’ obfuscate povero, provando a cambiare solo i nomi delle variabili, da `key` ad `oo0o000o0o00o0o0` ma cambiando solo nomi di variabili e metodi è possibile fare il reverse tranquillamente, ma rendendo solo più difficile il ruolo delle variabili / metodi.

Web Interface

Sarebbe interessante fare un interfaccia tipo quelle che mette a disposizione chi ha abbonamenti RAAS, un'interfaccia Web che tiene conto di tutti gli User colpiti, magari inserendoli all’interno di una mappa così da vedere il luogo di provenienza, gestendo così il tutto anche in maniera molto più comoda, vedendo anche gli OS colpiti e fare dei grafici.
Ecco alcuni esempi presi da una repository GitHub.

- https://github.com/leonv024/RAASNet/blob/master/demo/panel1.png
- https://github.com/leonv024/RAASNet/blob/master/demo/new_profile.png

Vulnerabilità

Per evitare ogni tipo di debolezza, sarebbe opportuno creare un file txt, all'interno della cartella tmp oppure nella home, chiamato 'keys.txt', con una struttura tipo dizionario.

```
/.../file.txt, MHcCn07dRy9q6n3tIXwBDf5umnu4pBixI4jQYvmz6ns=
/.../pwd.txt, eRziSpE/hN5uSis1YNNqHR9I2ziRSfMzlGHT4YA0Vpw==
```

Dove da una parte è presente il path del file, mentre dall'altra la chiave AES utilizzata per fare l' encrypt, così si ha una key ed un IV diverso per ogni file.
Poi si procede a fare l'encrypt di quel file con una key diversa dalle altre e si manda l'ultima key al Server come si faceva in precedenza con l'altra key utilizzata per fare l'encrypt di tutti i file.

Reverse Some

Se si prova a fare il reverse, mediante Ghidra, le funzioni apparirebbero così:

```
bool thunk_FUN_001041d0(char *param_1,undefined8 param_2)
{
  int iVar1; char *pcVar2; bool bVar3;
  char acStack4120 [4104];
  iVar1 = snprintf(acStack4120,0x1000,"%s",param_2);
  bVar3 = false;
  if (iVar1 < 0x1000) {
    pcVar2 = dirname(acStack4120);
    iVar1 = snprintf(param_1,0x1000,"%s",pcVar2);
    bVar3 = iVar1 < 0x1000;
  }
  return bVar3;
}

undefined8 FUN_001030d0(FILE **param_1,char *param_2)
{
  int iVar1; size_t sVar2;
  sVar2 = strlen(param_2);
  if (sVar2 < 0x1000) {
    __memcpy_chk(param_1 + 0xf,param_2,sVar2 + 1,0x1000);
    FUN_001041d0(param_1 + 0x20f,param_2);
    *(undefined4 *)(param_1 + 0x80f) = 0;
    __strcpy_chk(param_1 + 0x60f,param_1 + 0x20f,0x1000);
    iVar1 = FUN_00102d90(param_1);
    if (iVar1 == 0) {
      return 1;
    }
    if (*param_1 != (FILE *)0x0) {
      fclose(*param_1);
      *param_1 = (FILE *)0x0;
    }
  }
 return 0;
}
```

A primo impatto potrebbe risultare difficile capire, ma con un po di pazienza è possibile “decifrare” le funzioni, bisogna tenere sempre in considerazione che passare da codice **c → python** non è semplice, ma utilizzare **cpython** come interprete aiuta a favorire il reverse.

Figure

Bibliografia

[1] *WannaCry.* WannaCry

[2] *RAAS. What is it?* RaaS

[3] *IC3.* Wikipedia Internet Crime Complaint Center

[4] *Ransomware. Cos'è e come funziona?* Ransomware

[5] *Reverse Engineering.* Reverse Engineering

[6] *Posso recuperare i file?* Crittografia e Recupero File

[7] *Simmetrica.* Wikipedia Symmetric Key Algorithm

[8] *Asimmetrica.* Wikipedia Asymmetric Cryptography

[9] *TOR.* Tor

[10] *BitCoin.* BitCoin

[11] *BlockChain.* BlockChain

[12] *ByteCoin.* ByteCoin

[13] *CryptoNote.* CryptoNote

[14] *Ring Signature.* Wikipedia Ring Signature

[15] *Diffie-Hellman Key Exchange.* Wikipedia Diffie Hellman

[16] *Monero.* Monero (XMR)

[17] *IRS.* Internal Revenue Service

[18] *RSA.* Wikipedia RSA

[19] *Spear Phishing.* Spear Phishing

[20] *Toolkit.* Wikipedia Toolkit

[21] *Social Engineering.* Social Engineering

[22] *DASH.* Dash

[23] *Symantec.* Wikipedia Symantec

[24] *Server Message Block.* Wikipedia Server Message Block

[25] *RDP.* RDP

[26] *Colonial Pipeline.* Colonial Pipeline

[27] *Attacco Lazio.* Regione Lazio Ransomware

[28] *Attacco Toscana.* ARS Toscana Ransomware

[29] *SaaS.* Wikipedia Software as a Service

[30] *DdoS.* Wikipedia Distributed Denial of Service

[31] *Advanced IP Scanner.* Advanced IP Scanner

[32] *PSExec.* psexec

[33] *Mimikatz.* GitHub mimikatz

[34] *TCP.* Wikipedia Transmission Control Protocol

[35] *IoT.* Internet of Things

[36] *Backup.* Backup Completo, Differenziale, Incrementale

[37] *Google Drive.* Google Drive and Ransomware Protection

[38] *Cpython.* Wikipedia CPython

[39] *Ngrok.* GitHub ngrok

[40] *NAT.* Network Address Translation

[41] *API.* Wikipedia API

[42] *Pyinstaller.* GitHub pyinstaller

[43] *MySQL.* MySQL 8.0, What is MySQL?

[44] *Flask.* Welcome to Flask

[45] *ORM.* Wikipedia Object Relational Mapping

[46] *WSGI.* Wikipedia Web Server Gateway Interface

[47] *Ghidra.* Ghidra, GitHub ghidra

[48] *Firmware.* Wikipedia Firmware

[49] *Gobuster.* GitHub gobuster

[50] *REST.* Wikipedia Representational State Transfer

[51] *Dirbuster.* dirbuster

[52] *Wfuzz.* GitHub wfuzz

[53] *MITM.* Wikipedia Man In The Middle Attack

[54] *base64.* Wikipedia Base64

[55] *Obfuscation, What is it?* Code Obfuscation

Ringraziamenti

Un sentito grazie a tutte le persone che mi hanno permesso di arrivare fin qui e di portare a termine questo lavoro di tesi.

Grazie al mio relatore Marcantoni Fausto, sempre presente e disponibile. Grazie al percorso intrapreso insieme mi ha aiutato a sviluppare capacità di analisi e di reverse engineering.

Non posso non menzionare i miei genitori che da sempre mi sostengono nella realizzazione dei miei progetti. Non finirò mai di ringraziarvi per avermi permesso di arrivare fin qui.

Vorrei ringraziare le persone che ho conosciuto durante questo percorso di studi, chi dal giorno 0 e chi è arrivato più tardi, persone con cui ho avuto l'occasione di stringere un legame.
Un ringraziamento va ad Armando X., che mi ha ospitato, supportato e soprattutto sopportato in questi 3 anni, troppo gentile.