



UNIVERSITÀ
DEGLI STUDI
FIRENZE

Da un secolo, oltre.



HR EXCELLENCE IN RESEARCH

Ransomware: Analisi tecnica e considerazioni giuridiche alla luce del caso Conti

Giulio Morandini

Relatore: Stefano Pietropaoli

Correlatore: Rosario Pugliese

Ransomware:

Classe di malware utilizzata per estorcere digitalmente alle vittime il pagamento di una tariffa specifica, manomettendo il dispositivo attaccato e rendendolo talvolta inutilizzabile. Deriva dal termine “ransom”, che in inglese significa “riscatto”.

Tipologie generali:

- Ransomware crittografico;
- Ransomware con blocco dello schermo;

Sistemi colpiti: Windows, Linux, iOS, ma anche i sistemi dei dispositivi mobili come Android

Vettori di infezione principali:

- E-mail di phishing o siti online
- Vulnerabilità del sistema operativo o dei software
- Furto di credenziali
- Trojan



Evoluzione dei ransomware

Inizialmente l'obiettivo dei criminali era limitato alla criptazione dei dati e alla successiva richiesta di pagamento per la chiave di decriptazione verso individui o aziende indistintamente. L'approccio era inoltre basato su una diffusione casuale del virus.

Oggi gli obiettivi vengono scelti secondo studi specifici, selezionando quindi le possibili aziende da colpire, definendo inoltre in base al fatturato e ad altri indicatori finanziari un possibile valore per il riscatto. Fenomeno noto come **Big game hunting**.

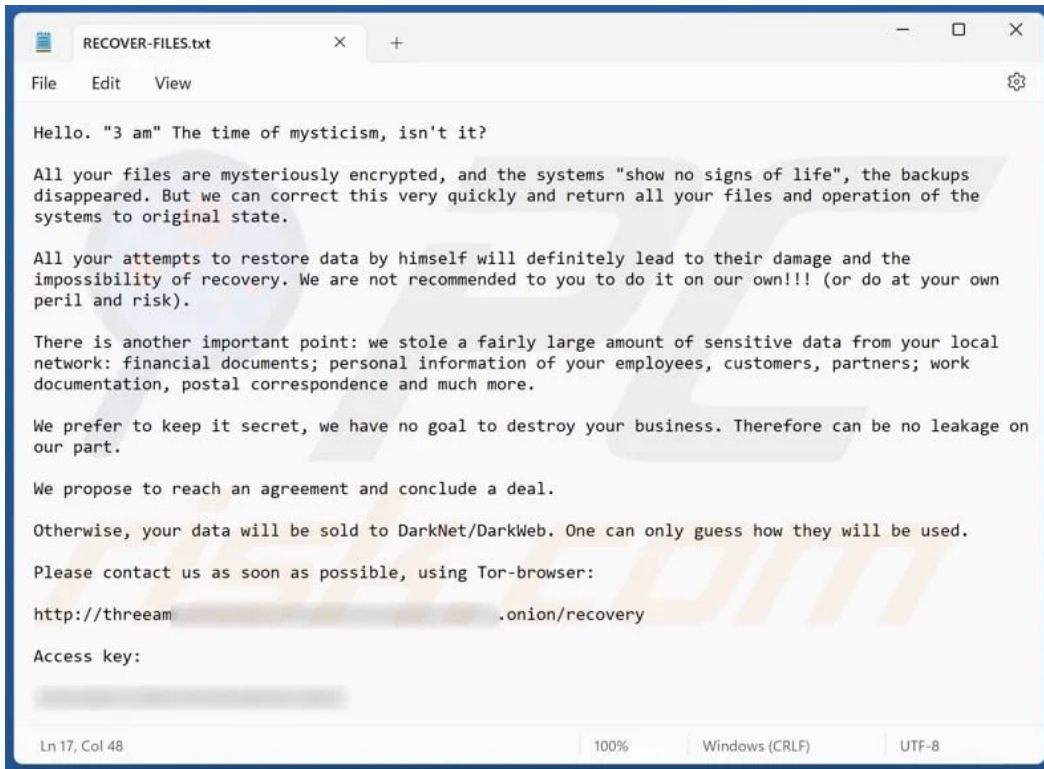
Inoltre i ransomware, come gli altri virus, si sono evoluti secondo il modello **MaaS**: Malware as a Service.

Linguaggi di programmazione:

Inizialmente veniva utilizzato il linguaggio a basso livello Assembly, poi si è passati a linguaggi di livello più alto, come C e C++. Le tecniche di programmazione si sono evolute e chi scrive un ransomware ha bisogno di semplificare e ottimizzare il lavoro, vengono quindi usati linguaggi moderni come Python, Rust e Golang.

Questi ultimi preferiti per la vocazione verso le prestazioni e realizzazione di codice forte e sicuro. Inoltre la loro natura focalizzata sulla programmazione concorrente facilita il controllo di condizioni di competizione tra processi e altri problemi comuni riscontrabili quando si ha a che fare con *thread* multipli e la programmazione concorrente.

Caso Recente: 3AM



```
RECOVER-FILES.txt
File Edit View
Hello. "3 am" The time of mysticism, isn't it?

All your files are mysteriously encrypted, and the systems "show no signs of life", the backups
disappeared. But we can correct this very quickly and return all your files and operation of the
systems to original state.

All your attempts to restore data by himself will definitely lead to their damage and the
impossibility of recovery. We are not recommended to you to do it on our own!!! (or do at your own
peril and risk).

There is another important point: we stole a fairly large amount of sensitive data from your local
network: financial documents; personal information of your employees, customers, partners; work
documentation, postal correspondence and much more.

We prefer to keep it secret, we have no goal to destroy your business. Therefore can be no leakage on
our part.

We propose to reach an agreement and conclude a deal.

Otherwise, your data will be sold to DarkNet/DarkWeb. One can only guess how they will be used.

Please contact us as soon as possible, using Tor-browser:
http://threeam.onion/recovery

Access key:
[redacted]
```

Il ransomware 3AM è un eseguibile a 64bit scritto in Rust. Il malware compie una sequenza di azioni ben definita:

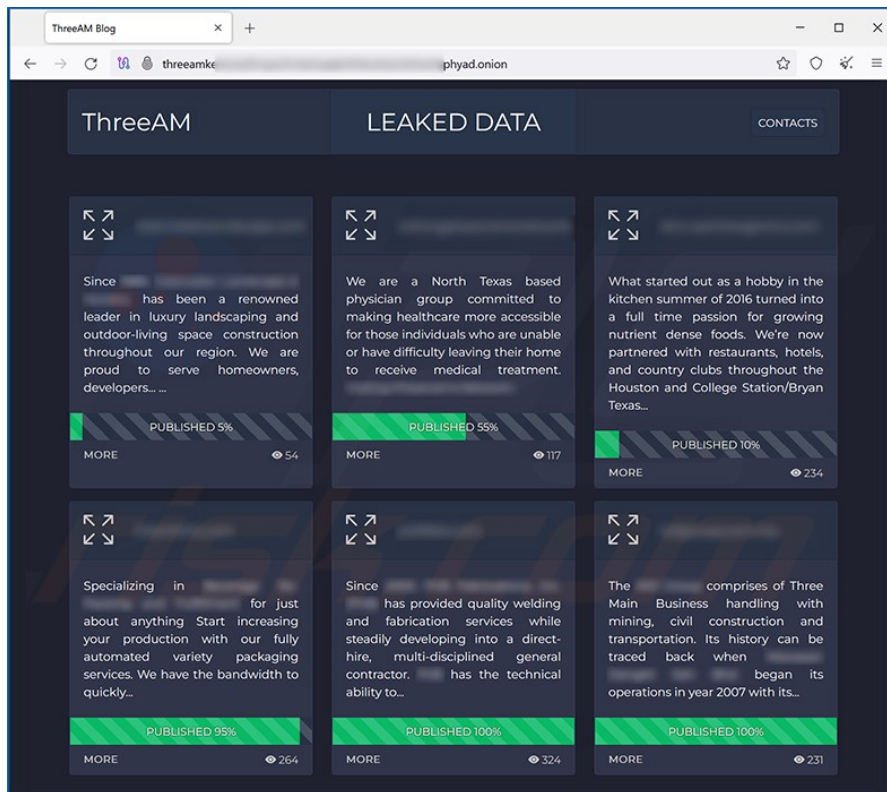
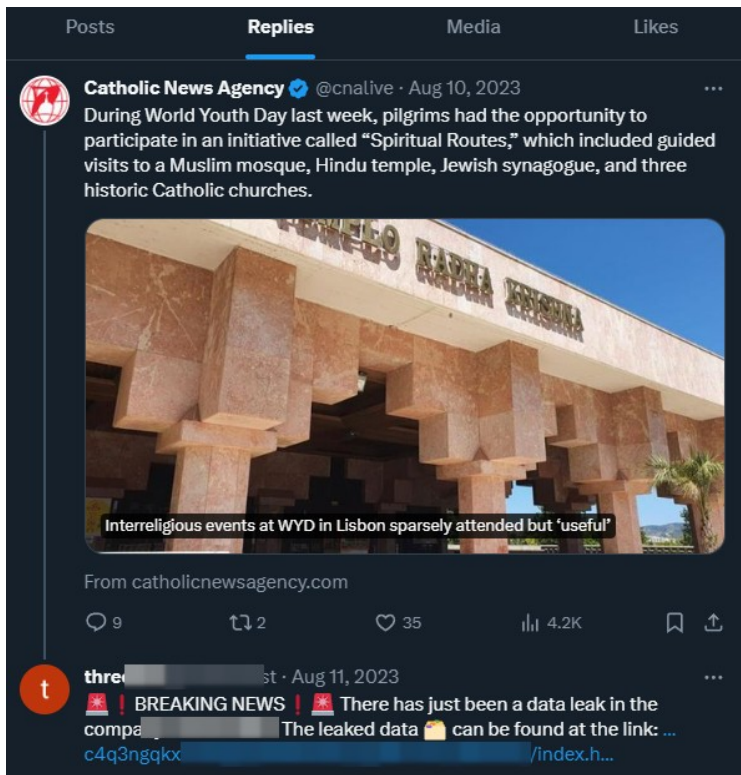
inizialmente il ransomware tenta di interrompere numerosi servizi, tra cui i software di sicurezza e i tool per il backup dei dati.

Per quanto riguarda la criptazione, il ransomware scansionerà il disco, cripterà tutti i file che corrisponderanno a criteri predefiniti e infine eliminerà i file originali.

Il malware creerà inoltre un file *RECOVER-FILES.txt* in tutte le cartelle colpite.

Questo software lavora in maniera simile al ransomware del gruppo Conti, come afferma la ricerca del team Intrinsec, per esempio nell'uso dei canali di comunicazione, delle infrastrutture e delle tattiche, delle tecniche e delle procedure.

Nuove tecniche per l'estorsione



Caso Conti

Gruppo di haker criminali che si ritiene abbia preso parte a numerosi e distruttivi attacchi di tipo ransomware tra il 2020 e il 2022 finchè non è stato chiuso, a seguito di una diffusione di dati nota come *Conti Leaks*.

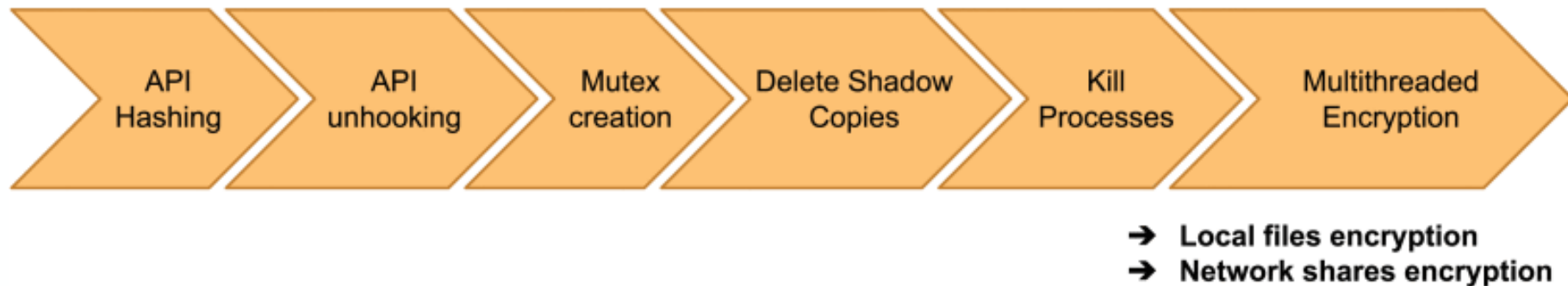
Il gruppo sfruttava soprattutto tecniche di *double-extorsion*, supportate da un *data leak site*, vendendo oltre ai dati anche le modalità di accesso ad essi.

Formato da un collettivo di un centinaio di persone che avrebbero raccolto oltre 170 milioni di euro, spesso sotto forma di bitcoin. Si presentava ben organizzato, con gerarchie interne e un modus operandi ben definito. L'organizzazione era suddivisa in diversi dipartimenti, con al vertice un vero e proprio amministratore delegato, conosciuto con lo pseudonimo di Stern

Degno di nota è l'attacco alla Costa Rica del 2022, che ha causato danni a tutta l'infrastruttura informatica ministeriale.

Succesivamente alla diffusione dei dati durante *Conti Leaks*, il gruppo ha effettivamente cessato la sua attività. I criminali affiliati al gruppo però non hanno smesso di operare, infatti si pensa che molti dei suoi membri collaborino con altre organizzazioni, rendendo lo sviluppo dei nuovi ransomware più metodico e dannoso possibile.

Ransomware Conti: fasi dell'esecuzione:



Analisi del codice: Offuscamento API e stringhe

La maggior parte delle stringhe del ransomware è cifrata per motivi di sicurezza, per evitare che con tecniche di reverse engineering si possa risalire al codice sorgente. La loro cifratura e decifratura segue uno schema di tipo *lazy*.

L'algoritmo di cifratura delle stringhe fissa due chiavi k_1 e k_2 e cifra in C_i ogni byte X_i della stringa secondo la seguente formula:

$$C_i = (k_1 X_i + k_2) \bmod 127$$

L'algoritmo di decifratura deve quindi risolvere la seguente equazione per poter riottenere i byte X_i della stringa in chiaro:

$$k_1 X_i \equiv C_i - k_2 \pmod{127}$$

k_1 e k_2 saranno inoltre generate pseudo-casualmente ogni volta per ogni stringa, che verranno quindi crittografate in modi differenti.

Le API vengono anch'esse risolte dinamicamente e sempre con un approccio *lazy*, ma questa volta sfruttano un'unica funzione custom chiamata *GetProcAddressEx2* che restituisce il puntatore alla funzione richiesta:

```
GetProcAddressEx2(<dll_id>, <function_name_hash>, <cache_index>)
```

Il primo parametro della funzione *<dll_id>* è un ID interno al ransomware che identifica la libreria *DLL* in cui è presente la funzione richiesta.

Analisi del codice: Crittografia

Conti utilizza una tradizionale combinazione tra crittografia simmetrica (*Chacha8*) e asimmetrica (*RSA*) per cifrare i file, inoltre ogni file del sistema viene crittografato con una chiave diversa, per evitare un *pay once decrypt many*. Le chiavi sono generate pseudo-casualmente e hanno la dimensione di 32 byte.

Per bilanciare efficienza ed efficacia dell'attacco il software adotta una strategia di cifratura che varia con le dimensioni e con il formato del file da cifrare:

- **File piccoli** (1MiB): cifrati completamente
- **File medi** (2-5 MiB): viene cifrato solo il primo MiB
- **File grandi** (>5 MiB): file suddiviso in chunk, vengono cifrati solo alcuni chunk

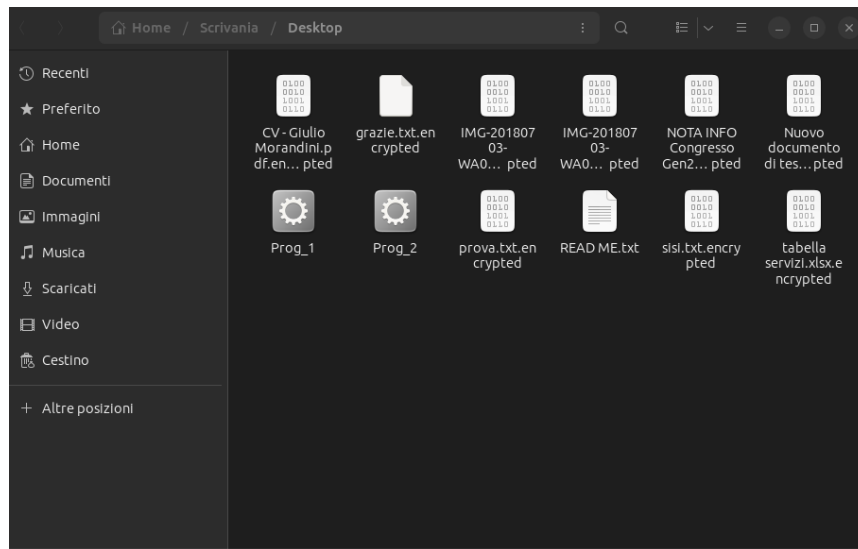
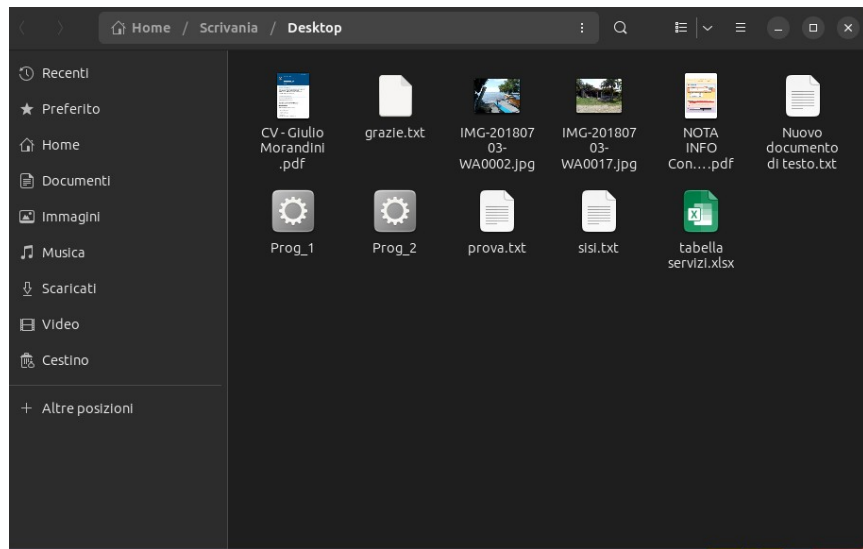
Formule di suddivisione in chunk:

$$ChunkSize = \frac{7}{100} FileSize = 7\%$$

$$ChunkOffset = \frac{1}{2} (FileSize - 3 * ChunkSize) = \frac{79}{200} FileSize$$

I chunk cifrati saranno quelli ai seguenti offset: $\{0, ChunkOffset, 2 * ChunkOffset\}$

Esempio di Ransomware: esecuzione di Prog_1 e Prog_2



Conclusioni

Abbiamo analizzato cosa significa subire un attacco ransomware, le conseguenze e la loro significativa evoluzione.

Considerando ciò le contromisure da prendere dovranno essere precise e metodiche, per cercare di prevenire un attacco di questo tipo, ed evitare i danni che tutto ciò può provocare.

È inoltre utile sottolineare che curare i danni causati da un ransomware non è mai facile e conveniente, per questo è consigliabile preferire contromisure che prevengano l'attacco piuttosto che il ripristino successivo dei dati.