29 Gen 2015

Nuovo attacco del malware Crypto-Ransomware
Cos'è e come proteggersi

La nuova variante si chiama **CTB-locker**, dopo l'attacco di Dicembre l'Italia è nuovamente sotto attacco del malware crypto-ransomware.
Qui di seguito troverete le informazioni su questo malware, come prevenirne un attacco e cosa fare in caso d'infezione.

DETTAGLI

Crypto-Ransomware si riferisce ad una classe di malware che tiene in "ostaggio" un computer, se così possiamo dire, fino a quando l'utente paga un determinato importo in denaro così da ricevere istruzioni specifiche sullo sblocco.
Crypto-Ransomware una volta eseguito, ha la capacità di infettare qualsiasi sistema Windows criptando quasi immediatamente dopo tutti i dati presenti sul disco rigido richiedendo poi un pagamento all'utente per ottenere una chiave di decriptazione. Molti dicono di non pagare, ma non offrono alcun modo per recuperare i file, altri dicono che pagare sia l'unico modo per recuperare i file di cui non si disponga di un backup non compromesso.

Come si diffonde CTB-locker?

CTB-locker di solito si diffonde tramite un allegato di posta elettronica che utilizzano approcci di "social engineering" e che solitamente proviene da fonti legittime oppure tramite una botnet. Adotta un metodo di camuffamento e si presenta tramite un allegato di tipo ZIP che di solito contiene un file eseguibile .
Il file non è visibile come "**<nomefile>.exe**" ma in realtà come "**<nomefile>.<pdf><docx><ecc.>.exe**" perchè l'attaccante si avvale del fatto che i sistemi Windows non mostrano di default le estensioni dei file e un file così creato verrebbe visualizzato come "**<nomefile>.pdf**" nonostante sia un eseguibile, inducendo gli utenti ad aprirlo ed eseguirlo, o come un semplice file **.zip**.
Quando viene eseguito per la prima volta, il software si installa nella cartella "**Documents and Settings**" (o "**Users**", nei sistemi operativi Windows più recenti) con un nome casuale e aggiunge una chiave al registro che lo mette poi in avvio automatico.

A questo punto tenta di connettersi a uno dei server di comando e controllo, una volta connesso il server genera una chiave **RSA a 2048 bit**, manda la chiave pubblica al computer infetto.
Il server di comando e controllo può essere un proxy locale ma anche residente altrove così da renderne difficile il tracciamento.
Quindi il malware inizia a cifrare i file del disco rigido e delle condivisioni di rete mappate localmente con la chiave pubblica, e salva ogni file cifrato in una chiave di registro. Il processo cifra solo dati con alcune estensioni, tra queste: Microsoft Office, Open document, immagini ed altri documenti.
Il software quindi informa l'utente di aver cifrato i file e richiede un pagamento di **dai 200 ai 500 USD o Euro** con un voucher anonimo e prepagato (es. MoneyPak o Ukash), o 0.5 Bitcoin per decifrare i file. Il pagamento deve essere eseguito in **72 o 100 ore**, o altrimenti la chiave privata viene cancellata definitivamente e "mai nessuno potrà ripristinare i file". Il pagamento del riscatto consente all'utente di scaricare un software di decifratura con la chiave privata dell'utente già precaricata.
Se CTB-locker viene rimosso, e la cifratura è iniziata, i file già cifrati rimarrebbero irrimediabilmente cifrati e quindi l'unica soluzione è quella di cercare di alzare delle difese adeguate per non far entrare il malware.
Il malware è conosciuto anche come:

- TROJ_CRYPCTB.SMD
- TROJ_CRYPCTB.SME

Azioni preventive e proattive nell'immediato su prodotti gateway ed endpoint Trend Micro.

La protezione migliore è sempre la prevenzione. Alcuni malware si presentano come allegato e-mail di messaggi spam che come detto in precedenza utilizzano approcci di "social engineering" per indurre gli utenti ad eseguire il file, i più noti malware che utilizzano questa tecnica sono spesso identificabili in **WORM_BAGLE** e **TROJ_UPATRE**. Quest'ultimo scarica **ZBOT**, che successivamente scarica **Ransomware.CryptoLocker** o **FakeAV**.
Nelle KB di seguito possono essere trovate informazioni su come individuare questi malware:
Best Practice per allegati di posta elettronica, attraverso i prodotti di messaggistica:

- Filtering and blocking email attachments using Trend Micro's Messaging products
- Detecting attached password-protected files in InterScan Messaging Security

Best Practice per prodotti endpoint:

- Preventing Ransomware infection using OfficeScan

Cosa si può fare in caso di infezione?

Anche se i prodotti di sicurezza sono progettati per trovare questa minaccia, può capitare che CTB-locker non venga individuato, o magari venga individuato solo dopo che la cifratura è iniziata o addirittura è stata completata.
Se si sospetta un attacco o è ancora al primo stadio, poiché è necessario un po' di tempo perché sia completata la cifratura, la rimozione immediata del malware prima del completamento della cifratura può almeno ridurre la perdita di dati ma ovviamente non risolve completamente il problema.
Quindi vanno assolutamente implementate politiche di sicurezza molto restrittive che impediscano che CTB-locker venga eseguito usando al meglio i prodotti Trend Micro e laddove possibile, prevedere un adeguamento infrastrutturale che permetta l'implementazione di prodotti di scansione attiva del traffico cone IWSVA e Deep Discovery Inspector.
Queste minacce devono essere considerate con un approccio olistico ed essere consapevoli che ogni bisognerà considerare ogni strato coinvolto nella consegna delle e-mail.
Di seguito alcune domande che possiamo porci per la valutazione del grado di protezione:
1. Sto usando politiche di blocco degli allegati al gateway di posta o la soluzione di messaggistica?
2. Sto usando l'Email Reputation Service?
3. Sto usando la soluzione Anti-Spam (scansione e-mail)?
4. Sto usando il servizio di reputazione Web?
5. Sto usando il Monitoraggio del comportamento?
6. Sto usando prompt che richiedono conferma agli utenti prima di eseguire il programma appena ricevuto?
7. Sto usando lo Smart Scan **(OSCE, DS, IMSVA, IWSVA, etc.)**?
La risposta dovrebbe essere affermativa per ogni domanda per avere un livello di sicurezza almeno allineato.

Come trovare il computer infettato:

- Il PC dell'utente finale contiene file con estensione "**.encrypted**"
Come misura proattiva, isolare immediatamente il computer togliendolo dalla rete.
- Per individuare l'origine dell'infezione, se i file su server NAS/SAN sono infetti, controllare l'ultimo utente che ha modificato i file o le attuali sessioni aperte ai file crittografati.

Se l'audit NAS/SAN è abilitato, controllare i registri di log per sapere quale utente sta crittografando i file.
Isolare la sorgente che esegue la crittografia cercando poi quali utenti/aree aziendali hanno accesso alle condivisioni.

Suggerimenti specifici per quanto riguarda alcuni prodotti Trend Micro:

OfficeScan:

WRS abilitato
C&C abilitato
Behaviour Monitoring – Process Injections e Suspicious Behaviour (Comportamento sospetto).
Smart Scan Pattern abilitato

Altri prodotti:

ATSE abilitato (*SMEX, Scan mail for Lotus Domino, IWSVA, IMSVA, DDA*)
Integrazione con DDAN (*SMEX, IWSVA, IMSVA, etc.*)
DDEI

Altre utili informazioni

Dal nostro blog si possono reperire maggiori informazioni e sempre costantemente aggiornate:

- http://blog.trendmicro.com/trendlabs-security-intelligence/ctb-locker-ransomware-includes-freemium-feature-extends-deadline/

Alcuni spunti e focus su come affrontare al meglio una protezione adeguata può essere reperibile di seguito:

- http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-cryptolocker/
- http://esupport.trendmicro.com/solution/en-us/1099423.aspx

Maggiori informazioni dalla nostra threat encyclopedia:

- http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3136/goz-and-cryptolocker-malware-affecting-users-globally
- http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3132/ransomware-raises-the-stakes-with-cryptolocker

*****