Ransomware

COSA SONO – COME DIFENDERSI


MALWARE

Malware

Software creato per uno scopi malevoli:
Rubare informazioni
Rendere la macchina infetta veicolo di traffico malevolo (mail bombing, DoS, Botnet …)
Mostrare pubblicità indesiderata
…

I più comuni veicoli di malware sono:

- Virus
- Trojan Horses
- Worms

Come cascarci

Gli utenti vengono indotti nell'eseguire il **malware** utilizzando tecniche di **Ingegneria Sociale**

Per esempio può convincere l'utente

- pretendendo di essere qualcun altro come per esempio
  le poste, amazon, ebay o addirittura le forze dell'ordine, oppure mascherandosi da aggiornamento di sistema
- pretendendo di fare del bene (carità, donazioni, …)
- Millantando guadagni sfruttando l'avidità dell'utente
- Inducendo una paura (il tuo computer è infetto, usa questo tool per ripulirlo)
- ecc..

Ieri:

Lo scopo principale del malware era l’infezione in sé.

Oggi:

Lo scopo principale del malware è quello di generare un profitto

Ransomware

Particolare tipo di malware il cui scopo è quello di indurre chi è colpito al pagamento di un riscatto (ransom).

Prime versioni di questi software cercavano di impedire il funzionamento del computer colpito.

Spesso cercando di ricondurre l'accaduto ad un presunto reato commesso dall'utente promettendo redenzione attraverso il pagamento di una multa.

Cryptolocker

Chiamiamo così (è in realtà il nome della variante più comune di questo malware) un particolare tipo di ransomware il cui effetto è quello di criptare i files del computer infettato rendendoli inacessibili.

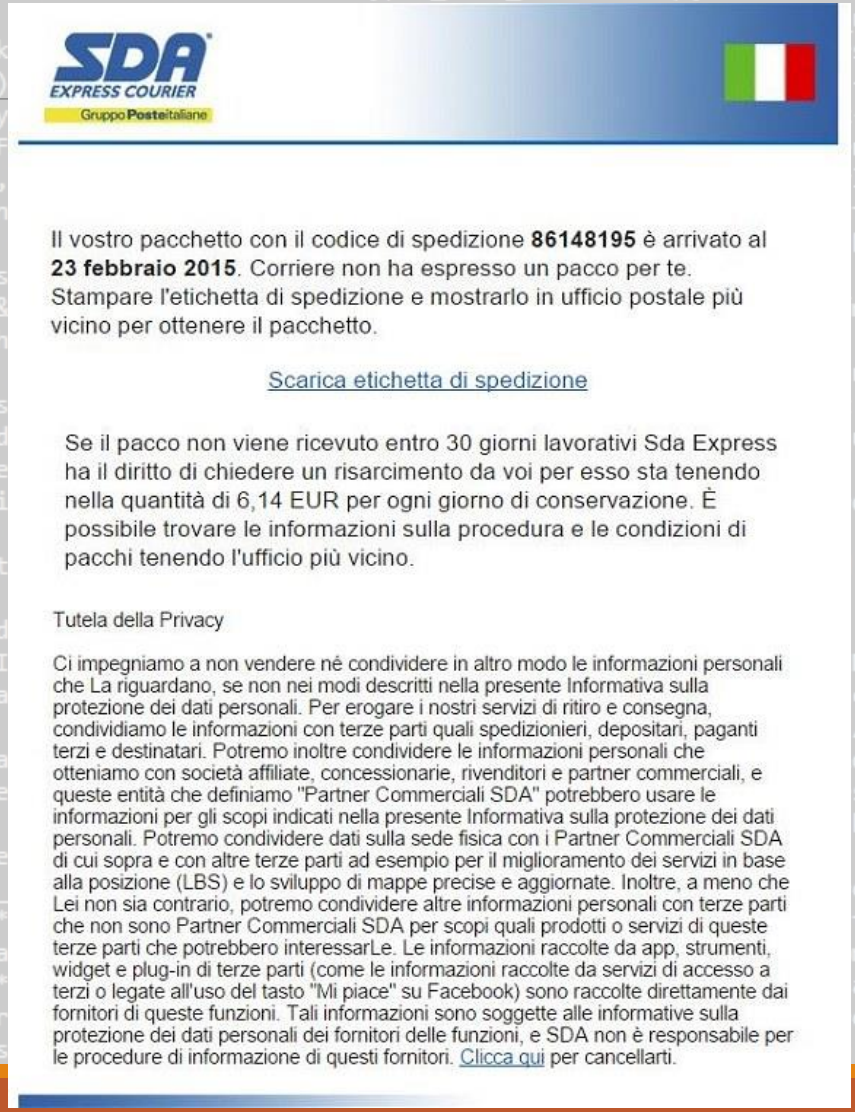
Mediante il pagamento del riscatto viene offerta la chiave di decriptazione.

In molte varianti di questo malware non è possibile decifare i dati con altri metodi

Criptolocker: come funziona un attacco

L'utente viene **indotto ad eseguire** un software, il metodo più comune è attraverso un **email** che invita a scaricare un documento (tipicamente una **bolletta** o un documento di **spedizione**)

Non è l'unico veicolo, un altro metodo comune è il **malwaretising**, cioè pubblicità ingannevoli iniettate in siti legittimi dove l'utente viene per esempio invogliato a scarica un coupon.



SDA EXPRESS COURIER
Gruppo Posteitaliane

Il vostro pacchetto con il codice di spedizione **86148195** è arrivato al **23 febbraio 2015**. Corriere non ha espresso un pacco per te. Stampare l'etichetta di spedizione e mostrarlo in ufficio postale più vicino per ottenere il pacchetto.

Scarica etichetta di spedizione

Se il pacco non viene ricevuto entro 30 giorni lavorativi Sda Express ha il diritto di chiedere un risarcimento da voi per esso sta tenendo nella quantità di 6,14 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

Tutela della Privacy

Ci impegniamo a non vendere né condividere in altro modo le informazioni personali che La riguardano, se non nei modi descritti nella presente Informativa sulla protezione dei dati personali. Per erogare i nostri servizi di ritiro e consegna, condividiamo le informazioni con terze parti quali spedizionieri, depositari, paganti terzi e destinatari. Potremo inoltre condividere le informazioni personali che otteniamo con società affiliate, concessionarie, rivenditori e partner commerciali, e queste entità che definiamo "Partner Commerciali SDA" potrebbero usare le informazioni per gli scopi indicati nella presente Informativa sulla protezione dei dati personali. Potremo condividere dati sulla sede fisica con i Partner Commerciali SDA di cui sopra e con altre terze parti ad esempio per il miglioramento dei servizi in base alla posizione (LBS) e lo sviluppo di mappe precise e aggiornate. Inoltre, a meno che Lei non sia contrario, potremo condividere altre informazioni personali con terze parti che non sono Partner Commerciali SDA per scopi quali prodotti o servizi di queste terze parti che potrebbero interessarLe. Le informazioni raccolte da app, strumenti, widget e plug-in di terze parti (come le informazioni raccolte da servizi di accesso a terzi o legate all'uso del tasto "Mi piace" su Facebook) sono raccolte direttamente dai fornitori di queste funzioni. Tali informazioni sono soggette alle informative sulla protezione dei dati personali dei fornitori delle funzioni, e SDA non è responsabile per le procedure di informazione di questi fornitori. Clicca qui per cancellarti.

Cryptolocker: Anatomia di un attacco

Command an Control C&C

RSA Key exchange

Domain Generation Algorithm

il malware genera un grandissimo numero di contatti verso domini fittizi in modo da camuffare il reale contatto con la rete C&C

In questo momento il malware inizia a criptare i dati

Operazione molto veloce ed eseguita in maniera sempre più intelligente

Lo scopo è quello di rendersi invisibile per il maggior tempo possibile.
Per esempio cercando di criptare per ultimi i files più vicini all'utente.

Vengono disabilitate le shadow copies, criptati per primi i files di rete, delle periferiche collegate al computer ed infine i files dell'utente.

Nuovi tipi di criptovirus sono particolaremente abili nel non saturare le risorse del computer, non criptare files contigui nello stesso tempo e inserire operazioni diverse tra le operazioni di cifratura per cercare di ingannare antivirus e programmi antimalware specifici per i cryptovirus.

Molte varianti di cprytolocker includono il trojan ZeuS, famoso dal 2007.
Si tratta di un malware in grado di recuperare dati bancari dai form internet.

Ransomware: difese di base

La prima linea di difesa per qualsiasi minaccia informatica è sicuramente:

IL BACKUP

Che deve soddisfare alcune caratteristiche:

- Essere inaccessibile ai sistemi vulnerabili
- Avere un versioning adeguato e un retention consona ai dati protetti
- Deve essere veloce da ripristinare
- Seguire il principio 3-2-1 (almeno 3 copie - in 2 formati differenti - 1 delle quali offsite)

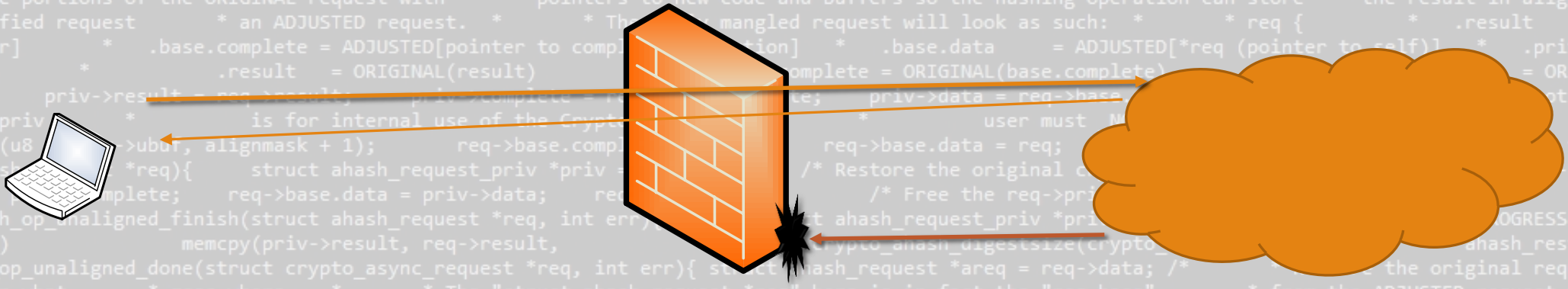
Ransomware: le difese di base

- Diffidenza
- Utilizzo dei sistemi di protezione di base del pc:
- Patch di sicurezza
- Antivirus aggiornato
- Windows smartscreen, UAC, altri software Application Control
- Snapshot dei dischi di rete
- Software restriction policy (cioè impedire tramite policy aziendale che il computer possa eseguire software in determinate posizioni come l'%APPDATA% dell'utente, le cartelle temporanee di programmi zip, rar, arj ecc..)

Ransomware: difese avanzate LA RETE

L’approccio più seguito oggi è una protezione sempre più avanzata attraverso il primo dispositivo di sicurezza di qualsiasi rete:
Il firewall

Tradizionalmente il firewall viene chiamato stateful, cioè è una apparato capace di permettere le comunicazioni di rete solo se sono «iniziate» dall’interno del perimetro protetto, bloccando le comunicazioni che partono dal lato non protetto della rete (internet per esempio)



Ransomware: difese avanzate LA RETE

Oggi sono sempre più diffusi firewall Layer 7 cioè apparati in grado di analizzare il flusso delle comunicazioni permesse e decidere se siano o meno pericolose.

Si tratta di dispositivi avanzati in grado per esempio di:

- Rilevare un eventuale malware prima che entri nella rete e quindi bloccarlo prima che raggiunga il computer che lo ha richiesto
- Bloccare l'accesso a determinate reti (per esempio la rete C&C che per lo più si trova su rete anonima Tor)
- Bloccare l'accesso o il download di files in base alla geolocalizzazione della richiesta
- Individuare pattern di comunicazione e confrontarli con pattern noti (intrusion detection)
- Prevenire tentativi di attacco o intrusione (intrusion prevention)
- DNS sinkholes

Oggi le comunicazioni con molti siti, anche quelli che veicolano malware, avvengono con protocollo https.

Un firewall moderno deve essere in grado di analizzare anche queste comunicazioni decifrandole in tempo reale e poi ri-cifrandole verso il client. Si tratta di una funzione complessa detta ssl-inspection, spesso anche non considerata ortodossa perché di fatto è analoga ad un attacco «man in the middle».

Ransomware domani

RaaS sono kit che possono essere acquistati per creare il proprio malware, sfruttato una botnet già pronta e molto potente, è sempre più facile creare la propria estorsione

SamSam un particolare tipo di attacco verso sistemi distribuiti, si cerca di attaccare direttamente i server piuttosto che gli utenti, questo è il primo ransomware conosciuto che sfrutta tecniche di autopropagazione

Furto di identità

LUCA DE FAZIO

E-MAIL: luca@de-fazio.net
CELLULARE: 3388648383