La Sicurezza Informatica

di CANOVI NINO – UTIU Matr. *3453HHHCLDIPSI* -

email: **n.canovi@students.uninettunouniversity.net**

E' nuovamente alla ribalta in questi giorni il tema della SICUREZZA INFORMATICA a causa del diffondersi a macchia d'olio del malware "NotPetya"

Il fenomeno NotPetya

Il **malware NotPetya** si presenta sicuramente come lo stato dell'arte dei malware (parola composta dai termini inglesi "malicious+software" – programma dannoso). A poche settimane dalla diffusione del malware **Wannacry**, ecco ritornare agli onori della cronaca mondiale, a causa dei danni provocati, il fenomeno dei ransomware.

Il **ransomware** (dall'inglese "ransom"=riscatto) è un malware di tipo "**troian**", ovvero un tipo di software "malevolo", che infettando il computer/dispositivo blocca l'accesso ai dati, chiedendo un riscatto all'utente per ripristinarne le funzionalità.

Diverse sono le similarità tra i due malware, la richiesta di riscatto, che nel caso di Notpetya è l'equivalente di $300 in **BitCoin** (criptovaluta), la capacità di infettare il dispositivo criptando i dati, e la diffusione in maniera capillare sfruttando delle falle del S.O. Windows.

Ma molte sono anche le differenze che emergono tra i due malware, innanzitutto NotPetya non si limiterebbe a crittografare il contenuto del dispositivo infettato file per file come il predecessore

1 Screenshot di un pc infettato da NotPetya

Wannnacry, ma rende inaccessibile il **Master File Table**, ovvero rende inutilizzabile criptandola la tabella contenente i riferimenti ai file conservati sul computer, Non essendoci più nessun riferimento ai file questi risultano di fatto illeggibili. Per potersi installare partendo da quello che si presenta spesso come un innocuo file (allegato spesso ad una e-mail) con estensione .doc .xls .ppt .txt, ma anche .pdf, necessita di un **dropper,** che porterà con l'apertura ad avviare il download del malware vero e proprio, il quale provvederà a sovrascrivere innanzitutto il Master Boot Loader (quella porzione di disco fisso che permette l'avvio del sistema operativo). Al primo riavvio dopo una schermata iniziale simile al checkdisk dell'ambiente DOS, momento in cui di fatto il malware agisce, la schermata successiva sarà quella (vd fig.1 Screenshot di un pc infettato da NotPetya)che comunica la crittografia dei dati e le istruzioni per il pagamento del

“riscatto”. Con la famigerata ed ormai sin troppo tristemente nota frase: “***Ooops, your important files are encrypted***”.

La particolarità di questo ransomware è che con si limita semplicemente alla crittazione dei files, ma a rendere di fatto inutilizzabile il computer da parte dell’utente inoltre al suo interno contiene “**Loki-bot**” (od un qualcosa di molto simile al punto di far pensare agli stessi sviluppatori) un malware sviluppato un paio di anni fa per rubare agli utenti password, dati personali, account Bitcoin.

Un’altra particolarità di Notpetya è che agendo direttamente sul boot loader è come se di fatto rendesse inaccessibile la “porta di ingresso” del computer infettato.

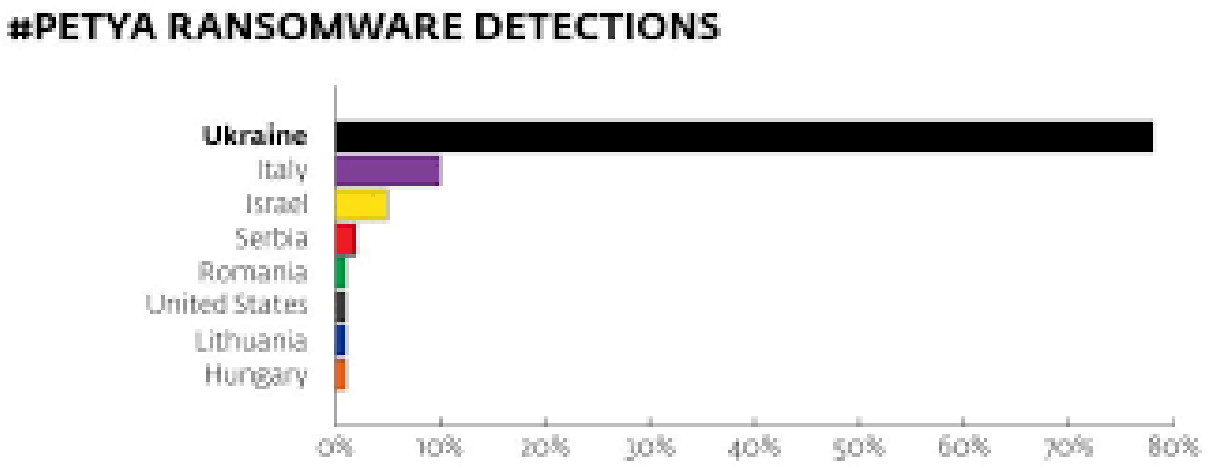
Un altro codice inserito nel ransomware è di tipo **worm**, basandosi sulla tecnologia software di “**Eternal Blue**” (sottratta qualche mese addietro alla **NSA** da parte di un gruppo di hackers), rende il malware, che sfrutta una particolare vulnerabilità del sistema operativo, capace di diffondersi tramite la rete interna di cui fa parte il dispositivo infettato e quindi ai contatti. Questo tipo di worm è in grado di adattarsi nello sviluppare la propria diffusione, capendo se sta agendo su un elaboratore isolato oppure su un “domain server”. Queste sono le caratteristiche che hanno permesso una così rapida ed endemica diffusione del malware.

Notpetya ransomware o wiper?

E’ di questi giorni il sospetto che in realtà NotPetya non sia in un ransomware, analisi da parte di esperti di CyberCrime e da parte di analisti delle Software House di Antivirus, hanno evidenziato come le stringhe di caratteri di cifratura sembrano essere completamente casuali. D’altra parte il pagamento del riscatto, come in tutti i casi di ransomware non dà alcuna garanzia di ricevere l’eventuale chiave di decrittazione. Inoltre nella fattispecie di NotPetya l’account di Posteo (che è indicato come destinatario del pagamento) è stato immediatamente bloccato dal Provider.

A questo punto e visti gli altri codici malware riportati al suo interno si fa strada tra gli esperti l’ipotesi che in realtà NotPetya non sia un ransomware (ovvero che punti ad un riscatto), ma che sia in realtà, già nell’intento dei suoi sviluppatori un “**wiper”**, un malware che punta a bloccare il dispositivo che infetta, a rendere di fatto i dati inaccessibili, a renderli inservibili.

A questo punto sorge spontanea la domanda: se non si punta ad un guadagno, ma ad un danno informatico chi ha interesse a sviluppare tali malware?



2-Grafico sulla diffusione di NotPetya

Come si evince dall'analisi dei dati di diffusione del malware oggetto dell'analisi (vd 2-Grafico sulla diffusione di NotPetya) il paese maggiormente colpito con ampie ricadute economiche e sulla vita quotidiana (ormai ampliamente controllata dagli elaboratori) risulta essere l'Ucraina.

Si fa quindi strada negli esperti il sospetto, peraltro difficilmente dimostrabile, che il malware sia stato sviluppato sotto l'egida del governo russo per colpire proprio l'Ucraina, viste le tensioni tra i due paesi. D'altra parte sempre più spesso malware e virus informatici sono stati utilizzati come vere e proprie "armi". Come nei bombardamenti reali, un ignaro e neutrale utente non è null'altro che un "**danno collaterale**".

Difendersi da Notpetya

Sicuramente alcune precauzioni per difendersi da qualsiasi tipo di malware valgono a priori.

Il consiglio è quello di tenere sempre aggiornato il Sistema Operativo, ad esempio l'ultimo aggiornamento di Windows 10, andava di fatto a rendere inoperativo lo script del malware "Eternal Blue". Importante è anche avere installato sul proprio elaboratore un valido programma antivirus e tenere anche quest'ultimo costantemente aggiornato. Un programma firewall (spesso incluso nell'antivirus) che blocchi l'accesso a minacce provenienti dalla rete quando si è connessi. E' molto utile anche tenere comportamenti cauti, in particolar modo nell'apertura di eventuali allegati.

3- Vaccino NotPetya

Il ricercatore israeliano **Amit Serper**, della compagnia di sicurezza informatica israelo-statunitense **CyberReason** ltd, studiando il codice del ransomware, ha potuto creare una sorta di "vaccino", ovvero ha scoperto che la creazione di un file denominato "perfc" (di sola lettura) nella directory C:\Windows; blocca di fatto la possibilità di azione del malware. Operazione abbastanza semplice. Viene ingannato il malware: prima di installarsi il ransoware controlla di non essere già presente in una "libreria" (file con estensione .dll) nella directory del sistema operativo, Ad oggi questa semplice operazione "immunizza" l'elaboratore dall'attacco di NotPetya. Anche se di fatto non si può essere certi sino a quando questo accorgimento si rivelerà efficace, stante le misure che i cybercriminali creatori di NotPetya, sicuramente, metteranno in atto per mantenere efficace il proprio ransomware e massimizzare i danni, che puntano ad effettuare.

Per rendere semplice l'operazione di immunizzazione del proprio computer il ricercatore **Lawrence Abrams** esperto di sicurezza informatica della **Bleeping Computer**, ha reso disponibile tramite **Twitter** un file batch (autoinstallante) con cui "vaccinare" automaticamente il proprio computer. Il file batch che è stato chiamato: "**notpetyavac.bat**", è disponibile per il download al seguente indirizzo internet: https://download.bleepingcomputer.com/bats/nopetyavac.bat.

L'Aspetto della Sicurezza nell'Informatica

Analizzando in precedenza il fenomeno dei malware e dell'ultima minaccia di NotPetya, è stato possibile vedere quanto sia importante per la tecnologia informatica l'aspetto della sicurezza.

Come detto in precedenza oltre alla necessità di tenere costantemente aggiornato il Sistema Operativo ed installare eventuali patch o tools di rimozione malware, è di fondamentale importanza anche servirsi di un buon Antivirus (ovviamente da tenere costantemente aggiornato).

Spesso si tende a sottovalutare la minaccia delle varie tipologie di malware, ma in un mondo sempre più interconnesso e con una forte dipendenza dalla tecnologia informatica per quanto riguarda la conservazione dei dati (spesso sensibili o di interesse economico), forte è l'interesse di riuscire a carpire dati o cagionare danno o tornaconto economico.

Frequentemente si sente dire “a me non capita utilizzo linux” oppure “utilizzo un mac”, ma orami nessun sistema operativo risulta immune. Statisticamente risulta più colpito Windows perché è il più diffuso. Basti pensare che alcuni sistemi d’arma utilizzano interfacce basate su Windows XP piuttosto che su Windows Server.

Nemmeno chi utilizza unicamente lo smartphone può dirsi al sicuro, recentemente si sono diffusi due malware che hanno colpito molti dispositivi con S.O. **Android**: il malware **Xavier** avrebbe infettato molti ignari utenti di App di Google Play Store, in quanto contenuto in circa 800 applicazioni presenti sullo Store della casa di Mountain View; ed il malware **JUDY,** quest’ultimo malware (generato in Corea) molto particolare in quanto destinato a creare milioni di falsi clic su banner pubblicitari, quindi introiti non dovuti per traffico pubblicitario.

Frequentemente dagli utenti, ma anche dagli addetti ai lavori, la importanza della sicurezza informatica viene sottovalutata e si assiste ad utilizzo di software non aggiornati, alla disinformazione più totale. Basti pensare che statisticamente le password più utilizzate risultano essere: “01234”, “password”. Gli utenti devono considerare delle regole basilari di sicurezza nella creazione di una password: utilizzare almeno un carattere speciale, utilizzare un mix di lettere e numeri, utilizzare sia minuscole sia maiuscole, infine non utilizzare mai nomi e date che abbiano riferimenti personali e familiari. Attualmente si sta diffondendo ed ampliando la tecnologia di accesso tramite dati biometrici, assistiamo quindi sempre più frequentemente a lettori di impronte digitali per accedere al proprio dispositivo (smartphone, laptop, etc.) oppure direttamente alle singole app (banca online, security- ad esempio Knox sella Samsung). Ancora agli albori (ma già applicata su alcuni dispositivi) perché più sicura e quindi apprezzata (in ambito biometrico) è la tecnologia di scansione dell’iride, mentre maggiori problemi sono stati riscontrati nell’utilizzo del riconoscimento vocale.

Ogni utente della tecnologia informatica deve adoperarsi per un utilizzo accorto e diligente degli strumenti informatici e delle risorse della rete WEB. Senza diventare paranoici, ma senza trascurare il fatto che è necessario adottare alcune precauzioni e comportamenti per evitare di diventare un bersaglio di qualche cybercriminale.

Savona, 02/07/17

Bibliografia – Sitografia :

- www.wired.it
- www.ilsole24ore.com
- www.theguardian.com › Technology › Cybercrime (lingua inglese)
- http://thehackernews.com/ (Not)Petya ransomware-wiper (lingua inglese)
- Twitter profile Amit Serper - @0xAmit (lingua inglese)
- https://www.cybereason.com/ (lingua inglese)
- https://www.bleepingcomputer.com/ (lingua inglese)

Risorse rese disponibili nell’articolo:

- ✓ Link per il download del file batch creato da Lawrence Abrams