WannaCryptor

- Quando il Ransomware diventa un Worm -

19 maggio 2017

Nel pomeriggio del 12 Maggio, diversi ospedali inglesi, sono stati colpiti da un "attacco hacker" senza precedenti: un virus informatico ha preso in ostaggio i dati dei computer, chiedendo un riscatto per la loro "liberazione". Nelle ore successive, la diffusione del virus, identificato come ransomware WannaCryptor (WannaCry), si è trasformata in epidemia globale, evento che ha attirato l'attenzione dei media di tutto il mondo.

Ma cos'è un ransomware? Come ha fatto questo virus a diffondersi così rapidamente e capillarmente? In cosa si distingue questo particolare attacco? E come si è scatenata questa crisi?

Per rispondere a queste domande dobbiamo fare un piccolo percorso, e spiegare nel dettaglio gli attori e gli eventi che hanno contribuito alla nascita di WannaCry. In questo viaggio incontreremo virus informatici, sedicenti gruppi hacker, agenzie di spionaggio, programmi dai nomi esotici.

A sorpresa, in questa vicenda ha un ruolo determinante (e inconsapevole), uno dei più importanti personaggi sulla scena mondiale mondiali: il presidente degli Stati Uniti, Donald Trump.

Cosa sono i Ransomware

Si parla di virus quando in realtà oggi si dovrebbe parlare di malware, di cui il virus non è che una tipologia, neppure tra le più diffuse.

Il ransomware è un particolare tipo di malware, che prende in ostaggio i file (cifrandoli) e chiede un riscatto (in inglese ransom), in genere alcune centinaia di dollari; il metodo di pagamento preferito è il Bitcoin.

Questo tipo di malware, che si diffonde principalmente attraverso messaggi di posta elettronica, o tramite siti appositamente infettati e trasformati in distributori di malware (Exploit Kit), esiste da tempo, ma è diventato la principale minaccia informatica, e la principale fonte di profitto per il cybercrime solo negli ultimi due/tre anni. Esistono diverse famiglie e varianti di ransomware, ma tutte hanno in comune la caratteristica di "sequestrare" i file della vittima cifrandoli.

Se la tecnica crittografica utilizzata è particolarmente sofisticata, come accade nella maggior parte dei casi, e se i criminali non hanno commesso errori di programmazione, la decrittazione dei file risulta praticamente impossibile.

Al pagamento del riscatto, in genere effettuato in Bitcoin (e tramite una connessione Tor nel darkweb), i criminali inviano alla vittima la chiave necessaria per decrittare, e quindi "liberare", i file "sequestrati".

Cosa sono i Worm

I worm sono particolari tipi di malware che hanno la capacità di auto replicarsi attraverso le reti locali o tramite Internet. A differenza di attacchi di tipo phishing o attacchi portati attraverso siti "Exploit Kit", dove l'utente deve compiere un'azione per infettare il proprio dispositivo (aprire un allegato, visitare una pagina web), i worm si propagano autonomamente, aggirandosi per la rete a caccia di computer vulnerabili.

Nel 2008, una grave vulnerabilità nel protocollo di condivisione file SMB di Windows (MS08-067), molto simile alla vulnerabilità attualmente sfruttata da WannaCry (MS17-010), fu alla base della propagazione del worm Conficker,

worm che a distanza di 10 anni si aggira tuttora per la rete. Ma 10 anni fa non esistevano i ransomware.

Quando il Ransomware incontra il Worm

Come si può capire leggendo le righe precedenti, quando un ransomware ha le caratteristiche di un worm, la situazione diventa molto pericolosa: è quello che è avvenuto con WannaCry.

Se fino a oggi le infezioni ransomware erano "limitate" alla diffusione tramite phishing/spam, tramite Exploit Kit, ovvero con metodi che richiedono l'interazione dell'utente, l'avvento di un ransomware con le caratteristiche di un worm mette nelle mani del cybercrime uno strumento estremamente più veloce e aggressivo. La vera novità di WannaCry è questa: la mutazione di un ransomware in worm, o meglio la fusione tra un ransomware e un worm.

Ma com'è potuto accadere questo? Quali sono le cause che hanno favorito questa "mutazione"?

La risposta è: lo spionaggio svolto da ShadowBrokers ed Equation Group (NSA).

Secondo Kaspersky, Equation Group è uno dei più sofisticati (se non addirittura il più sofisticato) gruppo di cyber spionaggio esistente al mondo. Questi gruppi vengono definiti Advanced Persistent Threat, APT. Alcune similitudini con un celebre malware denominato Stuxnet, che alcuni anni addietro fu utilizzato per attaccare le centrali nucleari iraniane, e la cui paternità secondo Edward Snowden sarebbe da attribuire alla National Security Agency americana (NSA), lascia supporre che Equation Group non sia che una struttura direttamente legata alla NSA.

Chi sono gli ShadowBrokers?

Nell'estate del 2016, è apparso sulla scena mondiale un gruppo di hacker denominato The Shadow Brokers. Specialità di questo gruppo è la diffusione di materiale sottratto alla NSA e/o Equation Group. Questo materiale consiste in

strumenti di hacking estremamente sofisticati, strumenti utilizzati dall'agenzia di spionaggio USA tramite il fantomatico Equation Group, per incrementare la propria capacità di accedere a qualsiasi tipo di informazione. Di fatto Shadow Brokers rende pubbliche "armi cibernetiche segrete" molto efficaci e pericolose che sarebbero a disposizione della più potente organizzazione di spionaggio mondiale (la NSA appunto).

Geopolitica: Trump, la Siria, Eternal Blue

A questo punto entra in scena Donald Trump. Il 7 Aprile 2017, il Presidente degli USA ordina un'azione militare contro la Siria. Decine di missili da crociera Tomahawk, partiti da alcune navi di stanza nel Mediterraneo, si abbattono su una base aerea siriana (utilizzata anche dai russi), dalla quale sarebbe partito un attacco chimico ordinato dalle autorità siriane contro la popolazione civile. Passano solo pochi giorni, e a sorpresa gli Shadow Brokers, in segno di protesta contro l'azione militare intrapresa dagli USA contro la Siria, pubblicano la chiave crittografica necessaria per decodificare il materiale trafugato dalla NSA, già pubblicato ma in versione criptata.

Questo evento mette in subbuglio la comunità della cybersecurity mondiale. Infatti l'archivio pubblicato da Shadow Brokers contiene hacking tools potentissimi, tra i quali spiccano:

- Fuzzbunch, una piattaforma di hacking simile a Metasploit (uno strumento utilizzato dagli hacker di tutto il mondo) impiegato per realizzare attacchi informatici;
- DoublePulsar, una sofisticata backdoor (tecnicamente un rootkit ringo), utilizzata per accedere ai computer precedentemente infettati;

e soprattutto:

- EternalBlue, un exploit (codice d'attacco) che utilizzando una vulnerabilità sconosciuta del protocollo di condivisione file SMBv1, permette l'accesso remoto senza autenticazione a qualsiasi sistema non protetto (tutte le versioni non aggiornate, tranne Windows 10).

Il vaso di Pandora è stato aperto.

L'attacco: WannaCryptor (WannaCry)

Paradossalmente l'elemento meno interessante di tutta questa vicenda è il protagonista che sta monopolizzando i media di tutto il mondo da venerdì 12 Maggio: WannaCry.

Gli autori di questo malware non hanno fatto altro che assemblare un ransomware esistente, le cui caratteristiche non si discostano dalla stragrande maggioranza di ransomware oggi diffusi, con il sofisticato exploit della NSA, EternalBlue, questo sì molto interessante e pericoloso.

Non solo WannaCryptor, non solo ransomware

Il vero problema non è il ransomware ma la vulnerabilità MS17-010, scoperta e sfruttata dalla NSA e svelata da Shadow Brokers in aprile, vulnerabilità che è già attivamente sfruttata sia da varianti di WannaCry, sia da altri ransomware in diffusione attiva.

Ma non solo. È noto un altro malware distribuito tramite EternalBlue, un malware (denominato “Adylkuzz”) già attivo da due settimane prima di WannaCry, che si insinua silenziosamente nel sistema in maniera del tutto trasparente per l'utente. Esso trasforma il computer della vittima in uno strumento per generare monete virtuali simili al Bitcoin, operazione detta "mining" che necessita di notevole potenza di calcolo.

La stessa vulnerabilità potrebbe essere utilizzata per dispiegare in modo clandestino strumenti di spionaggio (spyware), e infettare migliaia di computer di utenti ignari, con la finalità di spionaggio industriale, politico, economico e finanziario.

Attribuzione: chi c'è dietro?

Sebbene i media attribuiscano perentoriamente e con certezza matematica a questa o quella entità la paternità di ogni attacco informatico (gli hacker russi, gli hacker cinesi, la NSA, la CIA...), è difficile o addirittura impossibile affermare chi si nasconda dietro un attacco hacker se non dopo una investigazione complessa e laboriosa, che necessiterebbe della collaborazione tra diversi attori pubblici e privati (agenzie governative, forze di polizia, providers globali, aziende di sicurezza...).

Nel caso WannaCry sono coinvolti certamente gli ShadowBrokers, responsabili della pubblicazione dell'exploit EternalBlue, la cui identità è attualmente ignota, i quali sostengono di aver trafugato i tools dalla NSA (cosa che andrebbe verificata) e da un gruppo denominato Equation Group, la cui vicinanza alla NSA è probabile, ma non accertata definitivamente.

Il ransomware vero e proprio potrebbe avere avuto origine in Russia, tradizionalmente specializzata in questo genere di attività, ma alcuni ricercatori avrebbero trovato analogie con codici utilizzati in precedenza da un altro fantomatico gruppo hacker denominato "Lazarus", vicino (forse...) alla Corea del Nord.

Da non sottovalutare l'utilizzo della tattica cosiddetta "false-flag", ovvero l'utilizzo di diversivi "travestimenti" finalizzati a sviare e confondere le indagini dai veri autori, per indirizzarle verso piste false o addirittura verso gruppi antagonisti.Insomma, la situazione è tutt'altro che chiara, se non per la stampa e i creatori di romanzi anche perché probabilmente il confine tra tutti questi soggetti è più sfumata di quello che potrebbe indicare una lettura superficiale del fenomeno cybercrime.

Prospettive

Per quanto tempo avremo a che fare con EternalBlue? Probabilmente per molto tempo: una vulnerabilità simile, risolta da Microsoft con un aggiornamento distribuito nel 2008 (MS08-067) è stata utilizzata per diffondere il worm Conficker, che ancora oggi si aggira e infetta computer non aggiornati.

Queste vulnerabilità ormai sono di dominio pubblico, e quindi fanno parte dell'arsenale di qualsiasi hacker ethical e non ethical, 'whitehat' e 'blackhat', cyber-criminali e smanettoni della porta accanto.

Prevenzione e contromisure

Sebbene lo scenario possa apparire apocalittico, il rimedio contro EternalBlue è banale: basta infatti installare l'aggiornamento Microsoft MS17-010, disponibile addirittura dal 14 Marzo 2017 (un mese prima della pubblicazione di EternalBlue). Si precisa che tutti gli utenti che hanno attivato l'aggiornamento automatico (WindowsUpdate) dovrebbero averlo ricevuto.

A seguito dell'apparizione di WannaCry, Microsoft ha rilasciato in via del tutto straordinaria gli aggiornamenti per WindowsXP e Windows 2003 Server, sistemi non più supportati da diversi anni.

Chi per qualche motivo non potesse aggiornare il computer, può comunque mitigare la minaccia disabilitando il protocollo SMBv1, o utilizzando un firewall per filtrare le porte interessate dall'exploit (Tcp 139 e 445).

Infine, gli utenti di Windows 10, immuni a EternalBlue, possono dormire sonni tranquilli.

Almeno fino alla prossima mossa di Shadow Brokers e soci.

Angelo Righi

(Ethical Hacker)