Relazione

Virus

Quando parliamo di virus, ci riferiamo a un'applicazione o codice progettato per svolgere attività malevole su dispositivi o reti locali. Tuttavia, il termine "virus" è spesso usato in modo generico per indicare attacchi informatici, mentre sarebbe più corretto analizzare il tipo specifico di minaccia. Ogni categoria di virus ha caratteristiche diverse che ne consentono il riconoscimento. Gli aspetti principali da considerare includono:

- Come esso si comporta e come attacca;
- Come si propaga nel sistema informatico;
- L'ambiente o i dispositivi bersaglio;
- L'obiettivo finale dell'attacco;
  In questa articolo mi piacerebbe approfondire una tipologia specifica di virus, in quanto ci servirà per capire meglio come l'attacco informatico, soggetto di questo articolo, viene progettato.

Stuxnet

Cos'è?

Stuxnet è un virus informatico, nello specifico un worm cioè una particolare categoria di malware in grado di auto-replicarsi. A differenza dei classici virus, esso non necessita di legarsi ad altri programmi eseguibili per diffondersi, ma a tale scopo utilizza le reti, ad esempio tramite mail, dispositivi USB etc.
Un worm sfrutta le vulnerabilità nei sistemi operativi, nei protocollo di rete o nei software per propagarsi rapidamente e infettare altri dispositivi.

Perché è famoso?

Il primo caso di esposizione del worm Stuxnet fu nel 2010, nel quale esso colpì il sistema automatico di controllo delle centrifughe dell'impianto iraniano di Natanz utilizzato per l'arricchimento dell'uranio, mettendo in luce in modo eclatante la vulnerabilità degli ambienti industriali alle minacce informatiche.

Come si è diffuso?

Il metodo di diffusione fu sorprendente, tramite una semplice chiavetta USB che possedeva un ignaro ingegnere iraniano, venne infettato l'intero sistema industriale. Successivamente, si propagò in rete, cercando il software *Step7*, che serviva per controllare i PLC (un computer per l'industria specializzato nella gestione o controllo dei processi industriali). Infatti, l'obiettivo principale di questo worm era colpire questi hardware specializzati che sono programmabili via software, fondamentali per l'automazione degli impianti, in particolare quelli adibiti al controllo delle centrifughe.
Questo malware, tra l'altro, faceva leva su ben 4 vulnerabilità del sistema operativo Windows ancora sconosciute che in termine tecnico vengono chiamate **0-days**, queste informazioni vennero vendute attraverso canali illeciti a cifre esorbitanti.

In un secondo momento il virus informatico ebbe la capacità di diffondersi anche al di fuori dell'impianto di Natanz, a causa di un PC portatile infetto che, tramite la rete, contaminò anche ulteriori nazioni come Giappone, USA e alcuni paesi Europei, da cui provenivano le attrezzature per il programma atomico iraniano. Grazie a questa diffusione esponenziale il worm venne scoperto e poi risolto.

Chi fu l'organizzatore?

Ovviamente i dati personali dell'inventore di questo malware non sono assolutamente noti, in quanto è stata confermata la teoria che fu proprio il governo statunitense in collaborazione con il governo israeliano per favorire l'operazione "Olympic Games", cioè un'operazione segreta

mirata a sabotare il programma nucleare iraniano.
Facendo un breve excursus storico, possiamo dire che l'intento di sabotare la centrale nucleare iraniana da parte dell'Israele e degli USA fu per la paura che l'Iran potesse sviluppare armi nucleari.

Questa tipologia di attacco si può definire come **Cyberwar**, cioè un conflitto tra stati o gruppi organizzati che utilizza attacchi informatici invece di armi tradizionali, questi attacchi mirano a sabotare infrastrutture critiche, rubare informazioni sensibili o destabilizzare un Paese.

Come fu scoperto il virus?

Il malware, come abbiamo già accennato, fu scoperto nel 2010 da l'impiegato Sergey Ulasen di VirusBlokAda, una società di sicurezza informatica bielorussa.
Esso fu chiamato da un loro cliente iraniano che lo informò dell'inaspettato riavvio di una macchina con sistema operativo Windows XP dopo un BSOD (una schermata blu di errore, famosa nel sistema Windows). Dopo un attento intervento da parte del bielorusso, affermò che il problema non era solamente su quella macchina, ma che i diversi PC industriali, con installato anche Windows 7, avevano comportamenti anomali.

A questo punto, venne chiamata in causa Microsoft che doveva risolvere questi 4 problemi di vulnerabilità, che causavano la diffusione di Stuxnet. Microsoft dopo analisi approfondite arrivò a rilasciare patch di sicurezza per correggere queste vulnerabilità, ovvero degli aggiornamenti software.

Come funziona Stuxnet?

Stuxnet è stato progettato per danneggiare solo quei sistemi dotati di particolari requisiti, rimanendo del tutto disinteressato nei sistemi di cui non aveva premura di attaccare. Nello specifico, agisce solo nelle macchine dotate del software Siemens Step7, altrimenti il virus si disattivava in automatico.
Per i suoi scopi il malware è dotato della capacità di effettuare un attacco di tipo ***man in the middle*** (MITM), si tratta di una tecnica in cui un hacker si interpone tra due parti che stanno comunicando, riuscendo a intercettare, modificare o rubare informazioni trasmesse senza che le vittime se ne accorgano. Infatti, l'obiettivo è stato falsificare i dati forniti dai sensori industriali dopo la manomissione degli impianti in modo da non fare insospettire i tecnici, facendogli credere che tutto sesse andando ancora secondo i piani.

Entrando ancora più nello specifico, abbiamo che il virus Stuxnet era talmente complicato che fu in grado di sfruttare le vulnerabilità di ben 3 sistemi diversi già citati, che riporto, il sistema operativo Windows, il software Siemens per la gestione dei PLC (Step7) e i PLC stessi.
Quello che fece, una volta infettati i sistemi, Stuxnet aspettò 13 giorni prima di agire, nel frattempo raccolse tutte le informazioni necessarie per compromettere le centrifughe, per poi

attaccare il 14esimo giorno aumentando la velocità di rotazione di quest'ultime causando una rottura del metallo della centrifuga, successivamente, le rallentò facendole oscillare, con delle vibrazioni, portandole ad un rottura della produzione.
Il worm mandò ai computer della sala di controllo i dati che raccolse nei primi 13 giorni, in modo che i tecnici (almeno in un primo momento) non potessero accorgersi di nulla.

Attacchi dei 3 sistemi

Windows

Stuxnet attaccò il sistema Windows tramite 4 vulnerabilità 0-days, quella ormai nota **CPLINK** (CVE-2010-2568) che riguarda un problema di sicurezza nei collegamenti di Windows (.LNK), i classici file di scorciatoia che permettono di aprire programmi o cartelle con un clic. Il worm sfruttò questa caratteristica per eseguire codice malevolo senza che l'utente debba cliccare sul file.
La seconda vulnerabilità sfruttata fu quella nel servizio Windows Print Spooler (CVE-2010-2729) un servizio che gestisce i processi di stampa in Windows che permette di accodare e inviare i documenti alla stampante, consentendo di stampare anche quando una stampante è temporaneamente occupata. La vulnerabilità consentiva a un attaccante di inviare un file malevolo al servizio Print Spooler, il quale lo eseguiva con privilegi elevati, poiché il servizio girava con diritti elevati, Stuxnet poteva ottenere accesso amministrativo sui sistemi compromessi.
Inoltre, utilizzò anche il worm conosciuto come Conficker (CVE-2008-4250), è un malware che permette di eseguire codice remoto nei sistemi vulnerabili senza bisogno di interazione dell'utente ed esso prova a indovinare le password di amministratore utilizzando un elenco di password comuni (brute-force).
Come già è stato detto, il dispositivo venne infettato tramite una chiavetta USB e si propagò tramite la rete interna degli stabilimenti industriali di tipo *peer to peer RPC* (una rete interna che non ha bisogno di un server centrale per la comunicazione e Remote Procedure Call che consente di eseguire comandi su un altro computer in rete, come se fosse locale). Infatti Stuxnet è in grado di lavorare sia in modalità utente che amministratore, inoltre i suoi driver erano firmati con la chiave privata di due certificati rubati a due aziende molto conosciute ed affidabili, situate a Taiwan. Grazie a queste firme i driver del virus sono stati in grado di installarsi nel kernel di Windows senza destare alcun sospetto, ovviamente dopo la scoperta del worm i certificati sono stati revocati.
Infine, il codice che è stato usato per creare Stuxnet fu scritto con diversi linguaggi di programmazione, questo porta ad enfatizzare l'affermazione di essere state più organizzazioni a collaborare per questo attacco.

Step7

Innescato nel software Windows il worm cercava di infettare i progetti realizzati con il software della Siemens WinCC, PCS7 Step7 per i sistemi SCADA (sistemi informatici utilizzati per monitorare e controllare infrastrutture industriali e critiche) arrivando a sostituire una libreria fondamentale di WinCC `s7otbxdx.dll`. Aiutandosi con questa modifica il governo statunitense e quello israeliano riuscirono a intercettare lo scambio di messaggi tra Windows e i PLC (MITM), così poi fu in grado, Stuxnet, di installarsi su questi dispositivi attuando un attacco di tipo ***replay,*** cioè registrava la comunicazione tra i sistemi per poi riprodurla in un secondo momento per ottenere lo stesso effetto, nascondendo la sua presenza in caso di modifica dei dati.
Il problema reale di Step7 fu proprio che il protocollo S7 non richiedeva l'autenticazione per inviare comandi ai PLC e i dati che venivano trasmessi non erano crittografati, dunque, chiunque in rete poteva intercettarli e modificarli.

PLC

Il worm Stuxnet era talmente intelligente, che fu in grado di colpire solamente i PLC che avevano determinate caratteristiche e che erano fornite da due particolari case produttrici. Esso si installava nel blocco di memoria delle macchine, nell'istante in cui determinate proprietà si verificavano, Stuxnet iniziava a modificare le frequenze di velocità delle centrifughe, lasciando ignari gli operai che lavoravano con i macchinari.

Come fu eliminato? E come proteggersi?

Semplicemente Siemens ha messo a disposizione uno strumento in grado di rilevare e rimuovere gli Stuxnet, ma il vero problema è che l'elevata intelligenza dei worm di riprogrammare le macchine ha complicato la procedura di rimozione dei malware, infatti dopo la rimozione del virus, la minaccia non è del tutto eliminata, ma bensì bisogna fare un'ulteriore analisi delle macchine.
Siemens ha sviluppato S7 Plus, un nuovo protocollo che risolveva i problemi principali che aveva S7 citati precedentemente.
Questo non esclude che alcune aziende ancorano usano il vecchio protocollo del 2010, lasciando i loro impianti vulnerabili ad attacchi simili.

Alcuni consigli che le aziende possono attuare per proteggersi dalle minacce informatiche:

- Isolamento delle reti industriali: è importante utilizzare sistemi di sicurezza come firewall, per impedire la diffusione di malware tra i diversi segmenti della rete;
- Lista di permessi per le applicazioni: implementare una lista di permessi per le applicazioni, in modo da filtrare e controllare il traffico di rete e prevenire l’accesso di attori maligni a sistemi e dati sensibili.
- Gestione rigorosa dei supporti rimovibili: imporre regole ferree riguardo l'uso di dispositivi rimovibili, come chiavette USB, per evitare il collegamento di dispositivi non sicuri ai

sistemi aziendali.

- Hardening dell’host: ovvero disabilitare i servizi e le funzionalità non necessarie per l’operatività dell’azienda. Ciò ridurrà le potenziali vulnerabilità e le superfici di attacco per gli aggressori informatici.
- Utilizzo di comunicazioni criptate: attraverso questa misura di sicurezza, i malintenzionati non saranno in grado di visualizzare in chiaro le attività online di un’organizzazione.

Danni e Denaro

Stuxnet nell'attacco del 2010 ha sabotato circa 1.000 centrifughe dell'impianto di arricchimento dell'uranio di Natanz, si stima che il 10-20% delle centrifughe iraniane siano state danneggiate o distrutte.
Il Costo stimato ammonta a 2-3 miliardi di dollari tra attrezzature distrutte e ritardi nel programma nucleare iraniano.
Oltre alla centrale, ha infettato oltre 100.000 computer in tutto il mondo, aziende e organizzazioni governative hanno dovuto investire ingenti risorse per rimuovere il malware e migliorare la sicurezza informatica.
Dopo Stuxnet, molte industrie hanno dovuto rafforzare le loro difese contro attacchi simili, governi e aziende hanno speso miliardi per migliorare la sicurezza dei sistemi SCADA e ICS (Industrial Control Systems).

Paese	Computer infettati
Iran	62.867
Indonesia	13.336
India	6.552
Stati Uniti	2.913
Austarlia	2.436
Regno Unito	1.038
Malaysia	1.013
Pakistan	993
Finladia	7
Germania	5

Questa tabella riporta il numero di computer trovati infetti alla data del 6 agosto 2010.

Altre varianti di Stuxnet

Hanno constatato su un articolo di giornale (Foreign Policy) scritto nel 2013 che ci fu una versione precedente molto simile a Stuxnet che era più aggressiva e complessa, infatti a differenza di Stuxnet questa non cercava l'attacco diretto a Step7, ma attaccava in modo indiscriminato tutte le macchine.

Duqu

Nel 2011 venne scoperto un nuovo tipo di virus correlato a Stuxnet, infatti attaccava nello stesso modo di quest'ultimo, ma con obiettivi differenti, lo scopo principale era rubare informazioni come chiavi di accesso e dati aziendali sensibili.

Flame

Infine, nel 2012 venne scoperto un ulteriore tipo di worm, anch'esso correlato al malware soggetto di questa relazione, perché Flame utilizzava la stessa vulnerabilità di infezione attraverso la chiavetta USB. Questo malware risultava essere però 20 volte più complesso di Stuxnet, presentando parti di codice scritto anche in linguaggi diversi e capace di auto-eliminarsi senza lasciare traccia del suo passaggio.

Bibliografia

Per redigere al meglio questa relazione ho dovuto fare riferimento ad alcuni link informativi trovati in rete, che cito d seguito:

- Wikipedia
- StormShield
- MalwareBytes
- NordVPN