Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

COMPUTER EMERGENCY RESPONSE TEAM
PUBBLICA AMMINISTRAZIONE
CERT - PA
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Bollettino: SSH TCP Attack - Sottratte credenziali su numerosi server italiani

ID: CERT-PA-B005-170306 Data: 06/03/2017

AVVERTENZE

Il documento ha lo scopo di fornire alle Amministrazioni accreditate il quadro di riferimento degli scenari di minaccia rilevati dal CERT-PA, al fine di consentire loro di avviare tempestivamente valutazioni di impatto sui propri sistemi informativi e implementare le misure di contrasto/contenimento dei rischi correlati.

Il CERT-PA, nell'erogare al meglio questo servizio, si avvale di propri fornitori e di fonti pubbliche disponibili in Rete, individuati e selezionati tra i più autorevoli organismi di sicurezza, aziende specializzate e fornitori di tecnologie, al fine di garantire alla comunità di riferimento – con la massima accuratezza, affidabilità e tempestività possibile – le informazioni utili per la prevenzione e la gestione degli incidenti di sicurezza informatica.

Non è consentito far uso di queste informazioni per finalità differenti da quelle sopra indicate.

La presenza di rinvii operati mediante tecniche di ipertesto (link) non costituisce una raccomandazione del CERT-PA verso il soggetto richiamato, ma unicamente uno strumento per facilitare il rapido recupero di informazioni utili.

Indice

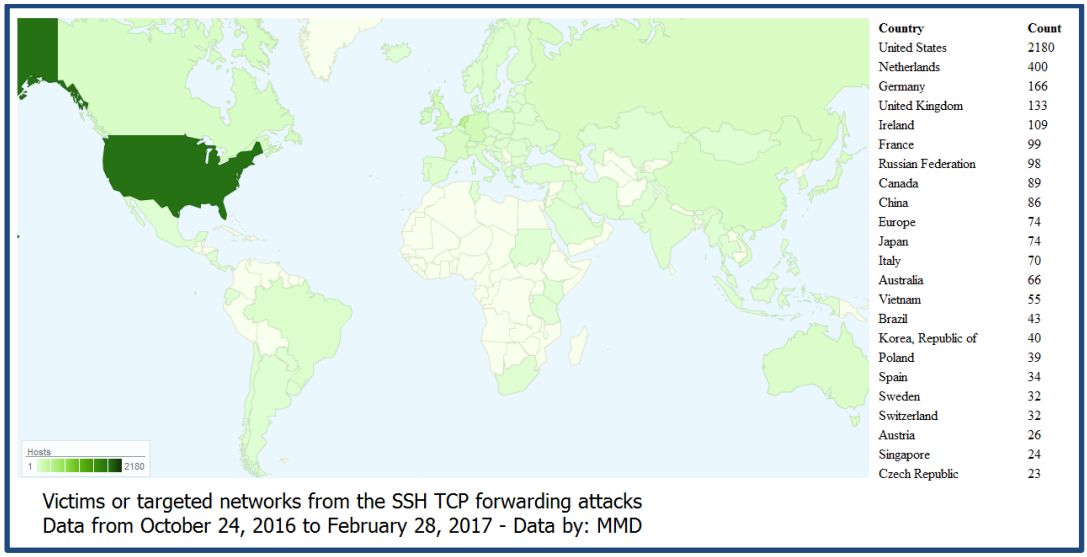
Sommario

Questa sezione contiene l'elenco delle minacce oggetto del presente bollettino. Dalle segnalazioni e dal monitoraggio delle fonti, il CERT-PA evidenzia la seguente minaccia:

SSH TCP Attack - Sottratte credenziali su numerosi server italiani

I ricercatori di MalwareMustDie! hanno individuato una botnet utilizzata da gruppo di criminali per collezionare credenziali e numeri di carte di credito sottratti da numerosi siti sparsi in tutto il mondo abusando di una tecnica denominata *SSH TCP forward*.

La botnet



Country	Count
United States	2180
Netherlands	400
Germany	166
United Kingdom	133
Ireland	109
France	99
Russian Federation	98
Canada	89
China	86
Europe	74
Japan	74
Italy	70
Australia	66
Vietnam	55
Brazil	43
Korea, Republic of	40
Poland	39
Spain	34
Sweden	32
Switzerland	32
Austria	26
Singapore	24
Czech Republic	23

Figura 1 - Paesi coinvolti nell'attacco

Il CERT-PA è entrato in contatto con Odisseus, uno dei ricercatori di MalwareMustDie! (MMD), che in collaborazione con Securityaffairs ha estrapolato la lista dei target italiani che ha condiviso con il CERT-PA. La botnet coinvolge circa 140 host afferenti Enti ed organizzazioni italiane. Secondo Odisseus, il malware che è stato utilizzato per compromettere i dispositivi IoT è probabilmente una variante del codice di Mirai.

Descrizione dell'attacco

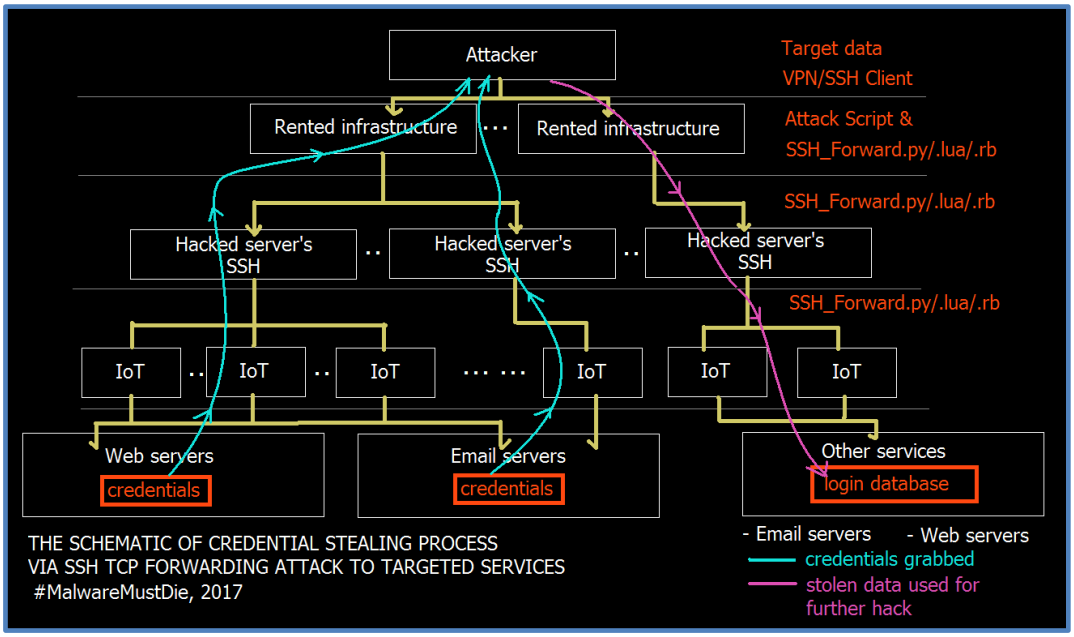


Figura 2 - Schema di attacco

Il malware che si occupa di compromettere i dispositivi con credenziali deboli è sotto osservazione dai ricercatori MalwareMustDie! già da mesi e stando alle evidenze riportate sul sito MMD le forme di attacco utilizzate per compromettere i siti non sono del tutto nuove.

L'attaccante, tramite attacchi manuali o automatizzati, compromette i target che di conseguenza entreranno a far parte della botnet e ne acquisisce le credenziali. Una volta guadagnato l'accesso e reindirizzato il traffico SSH dei dispositivi IoT verso la botnet, gli aggressori riutilizzano le credenziali per compromettere altri siti e/o servizi web tramite attacchi, manuali o via script, lavorando su protocollo TCP, nello specifico HTTP / HTTPS e SMTP.

Le evidenze raccolte da MMD mostrano che l'attacco è stato effettuato utilizzando differenti modalità: inviando richieste (HTTP GET) malformate e tramite script ad-hoc che hanno lo scopo di compromettere versioni del noto CMS Wordpress non aggiornate o sui quali sono installati plugin obsoleti. Per quanto riguarda i server di posta elettronica, invece, si ha evidenza di scansioni automatiche di server mail esposti su Internet raggiungibili su porte più o meno note (in particolare sulla porta 25).

Provenienza degli attacchi

Generalmente gli attacchi analizzati risultano provenienti da servizi SSH di dispositivi IoT violati o compromessi da malware di tipo ELF/Linux di cui è disponibile un archivio aggiornato sul blog MMD; altri attacchi risultano generati da server web già compromessi che a loro volta vengono riutilizzati per attaccare ulteriori servizi.

Mitigare gli attacchi

Al fine di verificare se si è stati compromessi e quindi procedere con la mitigazione degli attacchi, gli amministratori di rete hanno a disposizione il comando *netstat*. Una volta lanciato il comando ed individuate le sessione SSH sospette, indicate come "ESTABLISHED", è opportuno procedere con il blocco della minaccia. Utilizzando i comandi unix "iptables" per sistemi LINUX o "ipfw", "pf", o ancora "IPF" per sistemi FreeBSD sarà possibile inibire l'accesso a indirizzi puntuali con i quali la macchina ha precedentemente stabilito una connessione.

Di seguito un esempio:

// iptables (linux) sudo iptables -A INPUT -s 5.45.72.0/22 -j DROP sudo iptables -A INPUT -s 5.45.84.0/22 -j DROP sudo iptables -A INPUT -s 5.45.76.0/22 -j DROP sudo iptables -A INPUT -s 5.45.64.0/21 -j DROP
// ipfw (freebsd) ipfw add deny from 5.45.72.0/22 to any ipfw add deny from 5.45.84.0/22 to any ipfw add deny from 5.45.76.0/22 to any ipfw add deny from 5.45.64.0/21 to any

Si consiglia inoltre di leggere il documento pubblico "Security Awareness – Footprinting, Scanning & Enumaration nell'era di IoT (Internet of Things)" già citato nella news del sito CERT-PA, emesso in data 11/08/2016 e relativo alle tecniche di "*Information Gathering*" che precedono un attacco informatico, con particolare riferimento alla fasi di "*Footprinting*", "*Scanning*" e "*Enumeration*".