Attacchi mirati alle aziende USA con il trojan LookBack

Set 25, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, Minacce, News, RSS 0

I pirati hanno utilizzato tecniche di spear phishing puntando a compromettere i sistemi di 17 società di servizi. Gli esperti: "lavorano per uno stato estero".

Una campagna orchestrata per ottenere l'accesso ai sistemi informatici di almeno **17 società di servizi attive negli Stati Uniti**, condotta utilizzando un trojan che avrebbe permesso ai pirati informatici di sottrarre informazioni sensibili e compiere azioni di sabotaggio.

È questo il quadro tratteggiato da un report di **Proofpoint** in un report che approfondisce una segnalazione pubblicata dalla stessa società di sicurezza a inizio agosto.

L'attività dei pirati, che secondo i ricercatori farebbero parte di un gruppo collegato a uno stato estero, è iniziata a luglio e si è protratta per pochi giorni. Una seconda ondata di attacchi è invece stata rilevata tra il 21 e il 29 agosto.

La tecnica è sempre la stessa e utilizza come vettore di attacco un'email che contiene una serie di allegati. Il messaggio di posta, realizzato con grande cura, sembra provenire da organizzazioni di certificazione e, nel caso del secondo attacco, i ricercatori sottolineano alcune "finezze" utilizzate dai pirati per rendere più credibile l'email.

Gli ultimi messaggi, infatti, sono confezionati in modo da apparire provenienti da un ente pubblico chiamato **Global Energy Certification (GEC)** e, oltre al documento Word che

contiene il malware, contengono come allegato un PDF assolutamente innocuo “estratto” dalla documentazione originale del GEC.

Anche la tecnica utilizzata per indurre la vittima ad aprire il file in formato .DOC che contiene il trojan è decisamente brillante. Il documento ha come nome **Take the exam now.doc** e lascia quindi supporre che si tratti di un test interattivo.

Un trucchetto che, negli obiettivi dei pirati, dovrebbe permettere di superare eventuali sospetti riguardo alla richiesta di attivare le funzionalità Macro del documento. **L’attivazione avvia in realtà una serie di comandi VBA concatenati, che portano all’installazione del trojan LookBack**.

Per offuscare questo tipo di attività, i cyber-spioni hanno adottato una tecnica piuttosto elaborata. All’apertura del file, infatti, vengono memorizzati sul computer dei file PEM (privacy-enhanced mail) e un file chiamato **Temptcm.tmp**.

Quest’ultimo viene utilizzato per decodificare i file PEM (memorizzati in formato TXT) per trasformarli nei moduli

utilizzati dal malware. Nel dettaglio, **Tempgup.txt** diventa **GUP.exe**, un tool proxy utilizzato per mascherare il traffico del trojan, mentre **Tempgup2.txt** si trasforma in libcurl.dll che agisce come loader.

Tempsodom.txt, infine, viene decodificato come **sodom.txt**, al cui interno sono memorizzate le impostazioni per il collegamento al server Command and Control.

Una volta installato, LookBack consente di eseguire un gran numero di operazioni in remoto, tra cui la possibilità di esaminare i processi attivi sul PC, terminarli, eseguire comandi, copiare o cancellare file, catturare schermate del computer e simulare l'attività del mouse.

Abbastanza per garantire ai pirati informatici il **completo accesso alla macchina** e la possibilità di eseguire movimento laterale all'interno dei sistemi delle aziende colpite.

Considerata la tipologia dei bersagli e il livello tecnico degl istrumenti di attacco, dalle parti di Proofpoint non hanno dubbi riguardo il fatto che gli attacchi siano opera di un gruppo legato a un governo straniero. I ricercatori, però, non si spingono oltre. Per un'eventuale attribuzione bisognerà aspettare ancora un po' di tempo.

Condividi l'articolo

Da Google Alert a Google Calendar: pirati all'attacco

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/25/attacchi-mirati-alle-az

iende-usa-con-il-trojan-lookback/