# Kaspersky Lab svela il gruppo Poseidon: la malware boutique commerciale attiva in terra, aria e mare

**Date :** 10 febbraio 2016


**La prima campagna di cyber spionaggio in lingua portoghese-brasiliana resa pubblica prende di mira le istituzioni finanziarie, oltre ad aziende di telecomunicazioni, manifatturiere, energetiche e i media.**

Il Global Research and Analysis Team di Kaspersky Lab ha annunciato la scoperta di Poseidon, un gruppo APT attivo nello spionaggio informatico a livello mondiale almeno dal 2005. Il tratto distintivo di Poseidon è il fatto che si tratta di un'entità commerciale, i cui attacchi sfruttano malware personalizzati firmati digitalmente con certificati falsi usati per rubare informazioni sensibili dalle vittime allo scopo di obbligarle ad avviare una relazione d'affari. Inoltre, il malware è progettato per operare specificatamente su macchine Windows in lingua inglese o portoghese-brasiliana, per la prima volta coinvolte in un attacco mirato.

Sono state identificate almeno 35 aziende colpite, che costituiscono obiettivi primari come istituzioni finanziarie e governative, aziende di telecomunicazioni, manifatturiere, energetiche e altre società di servizi pubblici, oltre che media e aziende di relazioni pubbliche. Gli esperti di Kaspersky Lab hanno inoltre rilevato attacchi a società di servizi che curano il catering per i maggiori manager aziendali. Le vittime di questo gruppo sono state trovate nei seguenti Paesi:

- Stati Uniti
- Francia
- Kazakistan
- Emirati Arabi Uniti
- India
- Russia

Tuttavia, le vittime sono maggiormente concentrate in **Brasile**, dove molte di loro hanno joint venture o partner commerciali.

Una delle caratteristiche del gruppo Poseidon è l'esplorazione attiva delle reti aziendali basate su un dominio. Secondo il report di analisi di Kaspersky Lab, il gruppo Poseidon fa uso di email di spear-phishing con file RTF/DOC, solitamente con un'esca per le risorse umane, che, una volta cliccati, scaricano un codice binario nocivo nel sistema preso di mira. Un'altra scoperta essenziale è la presenza di stringhe in lingua portoghese-brasiliana. La preferenza espressa dal gruppo per i sistemi portoghesi, come svelato dai campioni, è una pratica che non è mai stata vista precedentemente.

Una volta infettato il computer, il malware fa rapporto ai server di comando e controllo prima di iniziare una fase complessa di movimenti laterali. Questa fase sfrutta spesso un tool specializzato che raccoglie automaticamente e in modo aggressivo una vasta gamma di informazioni tra cui credenziali, policy di gestione dei gruppi e persino i registri di sistema per perfezionare al meglio ulteriori attacchi e garantire l'esecuzione del malware. Così facendo, i criminali scoprono quali applicazioni e comandi possono usare senza allertare l'amministratore di rete durante i movimenti laterali e la fuoriuscita dei dati.

Le informazioni ottenute vengono quindi sfruttate da un'impresa di copertura per convincere le aziende prese di mira ad assumere il gruppo Poseidon in qualità di consulente di sicurezza, dietro la minaccia di sfruttamento delle informazioni rubate con una serie di loschi affari a vantaggio di Poseidon.

*"Il gruppo Poseidon è un team di lunga data che opera in ogni luogo: terra, aria e mare. Alcuni dei suoi centri di comando e controllo sono infatti stati trovati all'interno di ISP che forniscono servizi internet a barche in mare, connessioni wireless e carrier tradizionali"*, ha commentato **Dmitry Bestuzhev, Direttore del Global Research and Analysis Team di Kaspersky Lab per l'America Latina**. *"Inoltre, si è scoperto che molti dei suoi impianti hanno un ciclo di vita molto breve, il che ha aiutato il gruppo a operare così a lungo senza essere rilevato"*.

Dato che il gruppo Poseidon è stato attivo per almeno dieci anni, le tecniche usate per progettare i propri impianti si sono evolute, rendendo difficile per molti ricercatori correlare gli

indicatori e mettere insieme i pezzi. Tuttavia, racogliendo con attenzione tutte le prove, lavorando sulla “calligrafia” del gruppo criminale e ricostruendo la cronologia degli eventi, gli esperti di Kaspersky Lab sono stati in grado di stabilire, a metà 2015, che le tracce precedentemente rilevate ma non identificate appartenevano in effetti allo stesso gruppo criminale: Poseidon.

I prodotti Kaspersky Lab rilevano e rimuovono ogni versione conosciuta dei componenti del gruppo Poseidon.

È possibile leggere il report completo sul gruppo Poseidon con una descrizione dettagliata dei tool dannosi e le statistiche, oltre agli indicatori di compromissione, su Securelist.com.

Per scoprire quanto sia sofisticata l’analisi degli attacchi mirati,
visitare: http://www.youtube.com/watch?v=FzPYGRO9LsA

Altre informazioni sulle operazioni di cyber spionaggio sono disponibili al seguente link:
https://apt.securelist.com/