la Repubblica

22-GEN-2018
pagina 19
foglio 1

Il mistero dell'ultimo virus

"Non aprite quella mail". Aziende sotto attacco

JAIME D'ALESSANDRO, ROMA

Chi ha confezionato la mail, il fisco italiano lo conosce bene. Ha come oggetto "Codici Tributo Acconti" o anche "F24 Acconti-Codice Tributo 4034", moduli noti alle amministrazioni delle aziende. Solo l'indirizzo è chiaramente fasullo: *info@amber-kate.com* e *info@fallriverproductions.com*. Ma se si commette la leggerezza di non notarlo limitandosi all'oggetto, come accaduto fra gli altri alla Camera o al ministero dell'Interno, le conseguenze possono esser gravi.

«Il virus lo hanno confezionato su misura per le compagnie italiane», spiega Marco Ramilli, a capo della Yoroi di Bologna, la società specializzata in sicurezza informatica che lo ha scoperto. «Non è un attacco a pioggia come è accaduto in passato, ma mirato agli uffici commerciali e a chi ha a che fare con tasse e cartelle esattoriali».

Una volta aperto il link, il virus battezzato "TaxOlolo" si collega ad un server regalando le credenziali del computer del malcapitato. Viene scaricato il file It.exe capace di installarsi da solo e di mettersi in attesa di comandi dall'esterno. Si tratta di un malware imparentato con *GootKit*, che affonda le suc radici in Russia nel 2013 e da allora evolutosi.

«Stiamo approfondendo. Non sappiamo ancora cosa è capace di fare, ma sicuramente è stato lanciato con intenti malevoli» racconta Ramilli. Stando alle indagini, le aziende che sarebbero cascate nel tranello sono circa ottantotto e quasi tutte italiane. Ci sarebbero nomi di peso come quello dell'Aci, Autostrade, Bt Italia, Camera dei deputati, i Comuni di Brescia e Bologna, Fastweb, Fineco, H3G, ministero dell'Interno, Provincia di Reggio nell'Emilia, le Regioni Basilicata, Toscana e Veneto, Telecom Italia, Tiscali, Trenitalia, Università degli Studi di Milano, diversi uffici di Vodafone e di Wind. Ma nel caso dei provider, da Telecom a Vodafone fino a Wind, è probabile che ad essere infettato sia stato qualche loro cliente più che i loro uffici veri e propri.

Mentre scriviamo il server di controllo è ancora attivo. Si trova in Inghilterra, a Lincoln per l'esattezza, nord est di Nottingham. La società che ha affittato il server ai quali i pc infettati si connettono è la Namecheap.com. Vende servizi cloud e accetta pagamenti in bitcoin. Difficile quindi risalire a chi ha sferrato l'attacco, a meno che non abbia commesso errori madornali e pesanti ingenuità.

I punti

"TaxOlolo" ha già colpito ministeri, Comuni e Regioni

1 Come agisce
"TaxOlolo", così è stato battezzato, agisce tramite una mail che somiglia a quelle dell'Agenzia delle entrate.

2 Se si apre il link
Il virus prende possesso del pc regalando le credenziali del computer e si collega ad un server esterno in attesa di ordini

3 Chi c'è nel mirino
Attaccati Aci, Autostrade, Trenitalia, Camera dei deputati, ministero dell'Interno ma anche Comuni e Regioni

4 Che origine ha
Non si sa chi c'è dietro al virus. Il server al quale si collegano i pc infettati si trova in Inghilterra ed è stato affittato da un'azienda che offre servizi online