COMUNICATO STAMPA

Cyber spionaggio: l'operazione Potao Express smascherata dai ricercatori di ESET

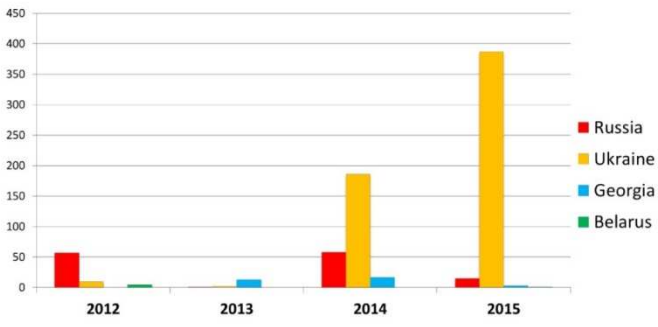
I cyber criminali spiavano target governativi e militari in Ucraina, Russia e Bielorussia
Nel mirino anche importanti organi di informazione ed organizzazioni finanziarie

Roma, 3 agosto 2015 - ESET, uno dei principali produttori di software per la sicurezza digitale, ha presentato oggi l'operazione Potao Express, che analizza in maniera approfondita un potente gruppo di cyberspionaggio operante attraverso la famiglia di malware Win32/Potao. Potao è stato rilevato principalmente in Ucraina ed in altri paesi della CSI tra cui Russia, Georgia e Bielorussia; tra le vittime finora identificate ci sono obiettivi governativi e militari ucraini, insieme ad una delle principali agenzie di stampa, sempre in Ucraina. Potao è stato utilizzato anche per spiare i vertici di MMM, un noto sistema di marketing multilivello operante in Russia e in Ucraina.

Come il malware BlackEnergy, Potao è un trojan appositamente progettato per rubare le password e le informazioni sensibili delle vittime ed inviarle ad un server remoto controllato dai cyber criminali. Le tecniche di adescamento utilizzate hanno evidenziato attacchi mirati, consistendo principalmente nell'invio di messaggi SMS personalizzati contenenti link fraudolenti: i cybercriminali conoscevano dunque i nomi delle vittime ed il numero di cellulare ad esse associato.

I ricercatori di ESET hanno individuato anche una connessione tra Potao ed una versione russa del popolare software di crittografia open source ormai fuori produzione, TrueCrypt a sua volta collegato al sito *truecryptrussia.ru*; quest'ultimo non solo ha fornito in alcuni casi una versione del software infetta da malware, ma è anche servito come centro di comando e controllo (C&C) per la backdoor.

La famiglia di malware Potao non è nuova, considerato che è stata utilizzata per la prima volta in attacchi del 2011/12, rimanendo poi silente fino al 2013. Un aumento significativo nell'utilizzo del malware è stato però registrato dalla piattaforma ESET Live Grid® nel 2014 e 2015.



Per ulteriori informazioni sull'operazione Potao Express è possibile consultare l'approfondita analisi di ESET al link http://www.welivesecurity.com/2015/07/30/operation-potao-express/ su WeLiveSecurity.com

Ufficio Stampa: Elisabetta Giuliano
Email: elisabettagiuliano@yahoo.it
Mobile: 328.9092482

ESET, fondata nel 1992, è uno dei fornitori globali di software per la sicurezza informatica di pubbliche amministrazioni, aziende e utenti privati. Il software ESET NOD32 Antivirus fornisce una protezione in tempo reale da virus, worm, spyware e altri pericoli, conosciuti e non, offrendo il più elevato livello di protezione disponibile alla massima velocità e con il minimo impiego di risorse di sistema. NOD32 è l'antivirus che ha vinto il maggior numero di certificazioni Virus Bulletin 100% e dal 1998 non ha mai mancato l'individuazione di un virus ItW (in fase di diffusione). ESET NOD32 Antivirus, ESET Smart Security e ESET Cybersecurity per Mac rappresentano le soluzioni per la sicurezza informatica più raccomandate a livello mondiale, avendo ottenuto la fiducia di oltre 100 milioni di utenti. L'azienda, presente in 180 Paesi, ha il suo quartier generale a Bratislava e uffici e centri di ricerca a San Diego, Buenos Aires, Singapore, Praga, Cracovia, Montreal, Mosca. Per quattro anni di seguito ESET è stata inclusa fra le aziende Technology Fast 500 EMEA da Deloitte e per dieci anni consecutivi fra le aziende Technology Fast 50 Central Europe. Per maggiori info: **www.eset.it**

FUTURE TIME è il distributore esclusivo dei prodotti ESET per l'Italia, nonché suo partner tecnologico. Fondata a Roma nel 2001, Future Time nasce dalla sinergia di due preesistenti aziende attive da anni nel campo della sicurezza informatica. Future Time, con Paolo Monti e Luca Sambucci, fa parte della **WildList Organization International**, ente no profit a livello mondiale composto da esperti e aziende antivirus che hanno il compito di riportare mensilmente tipologia e numero dei virus diffusi in ogni Paese. Per maggiori info: **www.eset.it**