HeroRAT usa il protocollo di Telegram per controllare i dispositivi Android

Il malware viene distribuito tramite social network e market paralleli. E su Internet è addirittura disponibile il codice sorgente. Per il momento la maggior parte degli attacchi sono stati registrati in Iran, ma la diffusione di HeroRAT potrebbe essere destinata ad aumentare esponenzialmente nel giro di poco tempo. Come spiegano i ricercatori di ESET in […]

L'articolo HeroRAT usa il protocollo di Telegram per controllare i dispositivi Android proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/29/herorat-usa-il-protocollo-di-telegram-per-controllare-i-dispositivi-android/

Intrusione nei sistemi di Ticketmaster. Rubati i dati del 5% degli utenti

L'attacco portato attraverso una società che fornisce servizi al sito per l'acquisto di biglietti. È il primo caso di violazione dopo la partenza del GDPR. Dati anagrafici, indirizzo email, numero di telefono, dettagli di pagamento e credenziali di accesso. Sarebbero questi I dati che ignoti pirati informatici sarebbero riusciti a ottenere attraverso un attacco che […]

L'articolo Intrusione nei sistemi di Ticketmaster. Rubati i

dati del 5% degli utenti proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/28/intrusione-nei-sistemi-di-ticketmaster-rubati-i-dati-del-5-degli-utenti/

Attenti ai nuovi file Windows Settings Shortcut di Windows 10

Introdotti nel 2015 e possono essere usati per avviare l'installazione di malware senza alcun tipo di avviso, ma per Microsoft non è una fala di sicurezza. Non c'è niente da fare: ogni novità introdotta in Windows sembra andare incontro all'inevitabile destino di rappresentare, prima o poi, un problema di sicurezza. A confermare questa sorta di […]

L'articolo Attenti ai nuovi file Windows Settings Shortcut di Windows 10 proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/27/attenti-ai-nuovi-file-windows-settings-shortcut-di-windows-10/

Il malware ruba i dati dal tuo smartphone, ma ti fa

risparmiare batteria

L’app per Android promette di monitorare i consumi della batteria. È vero, ma dentro c’è un trojan che fa tutt’altro. Se negli ultimi anni abbiamo assistito alla crescita numerica dei malware per Android, ora si comincia ad assistere alla comparsa di attacchi sempre più raffinati, che non si limitano a compromettere i dispositivi che colpiscono, […]

L’articolo Il malware ruba i dati dal tuo smartphone, ma ti fa risparmiare batteria proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/26/il-malware-ruba-i-dati-dal-tuo-smartphone-ma-ti-fa-risparmiare-batteria/

Zacinlo, un rootkit che sfrutta i nostri PC per frodare i circuiti pubblicitari

Bitdefender ha rilasciato un white paper su Zacinlo, un malware pensato per frodare i circuiti pubblicitari estremamente complesso e pronto a diventare altro. Bogdan Botezatu, ricercatore di Bitdefender, non si è risparmiato. In un white paper di ben 100 pagine ha sviscerato Zacinlo, uno dei malware più avanzati in circolazione al momento che si […]

L’articolo Zacinlo, un rootkit che sfrutta i nostri PC per frodare i circuiti pubblicitari proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/19/zacinlo-un-rootkit-che-

sfrutta-i-nostri-pc-per-frodare-i-circuiti-pubblicitari/

Ti presento InvisiMole, il software spia in circolazione dal 2013

È in grado di compromettere il PC per rubare informazioni, catturare video e audio. E nessuno lo ha rilevato per cinque lunghi anni… Si tratta molto probabilmente dell'ennesimo software spia "professionale", messo a disposizione di governi e soggetti vari per operazioni di sorveglianza e spionaggio. InvisiMole (la talpa invisibile) però detiene un vero record: è […]

L'articolo Ti presento InvisiMole, il software spia in circolazione dal 2013 proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/14/ti-presento-invisimole-il-software-spia-in-circolazione-dal-2013/

VPNFilter ora fa paura. I ricercatori: "potrebbe essere solo l'inizio"

Un ricercatore di Talos spiega a Security Info perché il malware rappresenta un pericolo che nessuno può permettersi di

sottovalutare. Quando l’FBI ha annunciato il sequestro dei server Command and Control sembrava che la vicenda VPNFilter fosse già conclusa. Le cose, però, non sono andate così e il timore è che il malware possa creare […]

L’articolo VPNFilter ora fa paura. I ricercatori: “potrebbe essere solo l’inizio” proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/08/vpnfilter-ora-fa-paura-i-ricercatori-potrebbe-essere-solo-linizio/

VPNFilter è più pericoloso di quanto si fosse pensato

I ricercatori rendono pubblici nuovi dettagli sul malware. “È in grado di colpire più modelli di router e ha funzioni avanzate per colpire i PC”. Come se non avesse procurato già abbastanza allarme tra gli esperti di sicurezza, su VPNFilter emergono nuovi dettagli che aumentano la preoccupazione per gli attacchi portati attraverso il malware. Come […]

L’articolo VPNFilter è più pericoloso di quanto si fosse pensato proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/07/vpnfilter-e-piu-pericoloso-di-quanto-si-fosse-pensato/

L’endpoint si evolve: dalla protezione al detect and response

I nuovi regolamenti e l’evoluzione delle minacce impongono un cambio di passo che coinvolge la stessa architettura degli antivirus. Il primo impatto dello tsunami GDPR ha riguardato, in buona sostanza, la comunicazione nei confronti degli utenti e l’adempimento degli obblighi burocratici. I suoi effetti, però, non finiscono qui e la parte più interessante deve ancora […]

L’articolo L’endpoint si evolve: dalla protezione al detect and response proviene da Securityinfo.it.

https://www.securityinfo.it/2018/06/05/lendpoint-si-evolve-dalla-protezione-al-detect-and-response/

Vulnerabilità zero-day in Windows prende di mira JScript

Il componente del sistema operativo Microsoft vulnerabile ad attacchi che possono portare all’esecuzione di codice in remoto. L’azienda lavora alla patch. Se dovessimo assegnare un trofeo per il componente che crea più grattacapi agli esperti di sicurezza, ci sarebbero pochi dubbi sul fatto che JavaScript sarebbe in grado di stracciare la concorrenza a mani basse. […]

L’articolo Vulnerabilità zero-day in Windows prende di mira JScript proviene da Securityinfo.it.

https://www.securityinfo.it/2018/05/31/vulnerabilita-zero-day-in-windows-prende-di-mira-jscript/