AUTO, FAKE NEWS & SOCIAL LE NUOVE ROTTE DEI PIRATI

Dalle vetture connesse ai gadget tecnologici da indossare: gli oggetti più a rischio di cyber attacco. Nel dark web i finti profili costruiti rubando dati si vendono a duemila euro

di **Umberto Torelli**

Anno nuovo, virus informatici vecchi. O meglio, diffusi in Rete dopo essere stati modificati per diventare più letali delle versioni precedenti. È questa la strategia che metteranno in atto gli hacker per attaccare computer e dispositivi mobili. A dirci da dove arriveranno le maggiori insidie dei prossimi mesi è il report *Previsioni sulla sicurezza 2018* di Trend Micro, che verrà reso pubblico a Milano tra due giorni. *L'Economia* ha avuto un'anteprima.

Le tendenze

Parliamo per esempio di auto. Quelle nuove che usciranno dai concessionari saranno sempre più connesse. Gartner stima che entro due anni circoleranno nel mondo oltre 250 milioni di veicoli collegati al web. I pirati informatici lo sanno. Così dobbiamo aspettarci *malware* studiati per violare i sistemi di intrattenimento e sicurezza di bordo, ma anche per catturare le informazioni private dei guidatori. Specie nel segmento *car sharing*: le app e i mezzi utilizzati dalle flotte, oltre ad avere sistemi di geo localizzazione, contengono molti dati personali del guidatore.

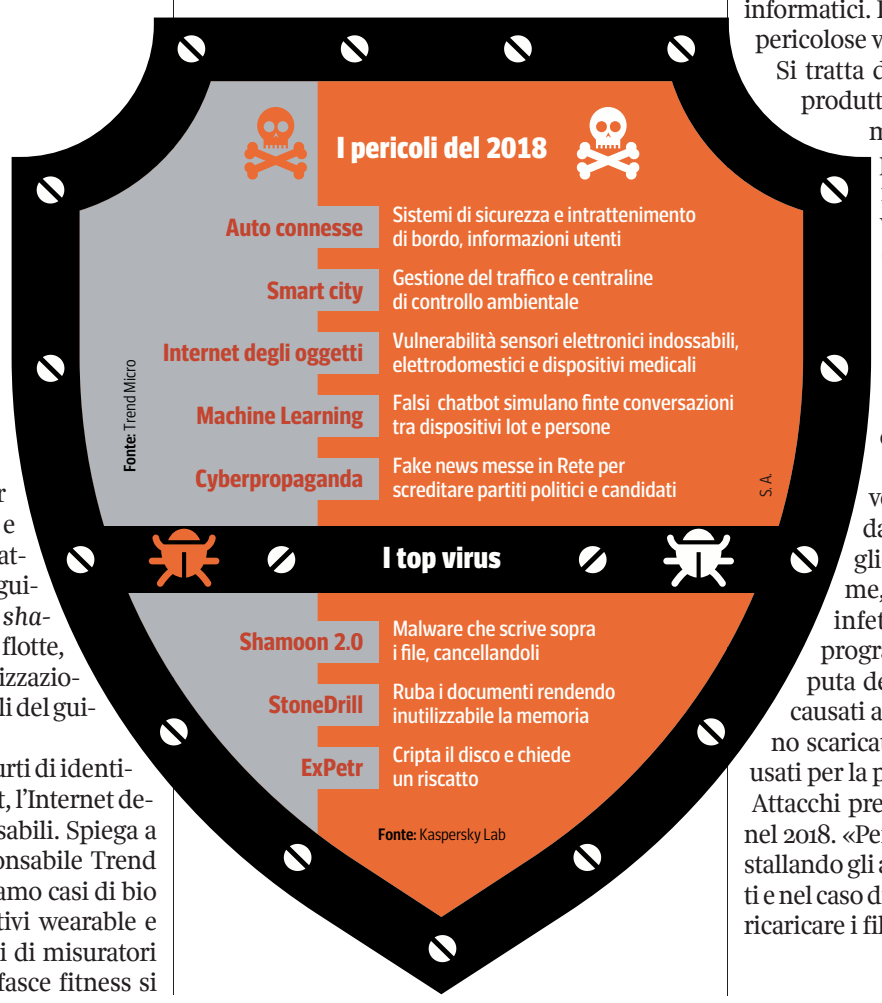
Protezione
Gastone Nencini, responsabile di Trend Micro Italia: ogni anno elabora un report sulle insidie informatiche

In modo analogo, nell'ambito di furti di identità, i pericoli arrivano dal mondo Iot, l'Internet degli oggetti, e dai dispositivi indossabili. Spiega a proposito Gastone Nencini, responsabile Trend Micro Italia: «Per il 2018 ci aspettiamo casi di bio hackeraggio effettuati da dispositivi wearable e medicali. Ad esempio, i parametri di misuratori biometrici, frequenza cardiaca e fasce fitness si possono intercettare per catturare informazioni riservate».

Vulnerabilità a disposizione dei pirati informatici, per successivi attacchi ai dispositivi elettronici dell'utente. A rischio anche le *smart cities*, soprattutto nella gestione dei sistemi di trasporto intelligenti. In questo caso il nervo scoperto riguarda la connessione online di semafori, segnaletica stradale, telecamere di sorveglianza e centraline di controllo ambientali. Tutte dotate di sensori e gestite da app in tempo reale, dunque facili prede dei cybercriminali che possono catturare informazioni in modalità remota, chiedendo poi riscatti per sbloccare i virus.

Attenzione anche al proliferare delle fake news. «In Italia per le prossime elezioni aumenteranno i rischi di manipolazione di dati sui social e sui siti istituzionali», avverte la ricerca.

Già lo scorso anno Trend Micro aveva individuato nel dark web un tariffario che consentiva di ordinare notizie false come fossero una merce qualsiasi. Ad esempio, la campagna per screditare una personalità può costare 45 mila euro. Mentre per allestire un finto profilo social completo di 300 mila follower bastano duemila euro.



Le tecniche

In fatto di virus i web pirati mettono in atto tecniche sempre più sofisticate per violare i dispositivi informatici. Per il 2018 sono già state individuate pericolose varianti di attacchi alle *supply chain*. Si tratta dei canali distributivi delle aziende produttrici di applicazioni e programmi. Il meccanismo di attacco è tanto semplice quanto letale. Gli hacker violano i server dei produttori, inserendo virus maligni in programmi e app che sono in vendita. «Così l'utente acquista in tutta tranquillità il software e si trova il virus nel computer — spiega Giampaolo Dedola, ricercatore al GReAT team dei Kaspersky lab —, inclusa la regolare licenza d'uso *virus free*».

È successo per Shadowpad, un server gestionale per aziende prodotto dalla coreana NetSarang. Lo scorso luglio al labs Kaspersky è scattato l'allarme, perché migliaia di aziende vennero infettate da un malware nascosto nei programmi originali. Ovviamente all'insaputa del produttore. Ben più gravi i danni causati a oltre due milioni di utenti che hanno scaricato CCleaner, un applicativo tra i più usati per la pulizia di file e dischi del pc.

Attacchi previsti ancora con pericolose varianti nel 2018. «Per proteggersi bisogna intervenire installando gli aggiornamenti dei programmi infetti e nel caso di danni letali formattare i computer e ricaricare i file di lavoro da precedenti backup».

@utorelli

Pit Spot

Innocenti evasioni (telefoniche)

a cura di **Aldo Grasso**
pitspotcorriere@gmail.com
in collaborazione con
Massimo Scaglioni

Le tariffe telefoniche come un carcere da cui cercare di evadere il più rapidamente possibile. La metafora è calzante. Gioca sull'ironia la campagna di Fastweb, che si propone un obbiettivo chiaro: «Quello che vedi è quello che paghi». Fin quanto ci si può spingere nel prendere in giro i costi nascosti dei concorrenti?

Fino a un certo punto, ha decretato il Giurì della pubblicità, che ha censurato un paio di spot (per altro piuttosto divertenti: nel primo i passeggeri di un aereo sono avvertiti che tutti i servizi sono a pagamento, toilette compresa; nel secondo il rapporto con le telefoniche è descritto come una dipendenza alcolica…).

Fatto sta che ora resta in onda soltanto il film «carcerario». In questo vediamo un ragazzo circondato da agenti armati, come se fosse un pericoloso terrorista.

Arrivato alla sala dei colloqui, la compagna lo avverte delle «brutte notizie»: «Connessione di casa? Questa promo è da ergastolo…», commenta lui, guardando l'ultima bolletta. Didascalia: «Quando una promozione finisce, è sempre una brutta notizia…». Lei però non si lascia scoraggiare: «Dobbiamo trovare il modo di evadere!». Alla fine la coppia è riunita, la fuga è avvenuta. Tutta la campagna, sottolineando il «triple play» (fibra, wifi e mobile) dell'azienda, punta sulla trasparenza dei costi, senza dubbio un valore apprezzabile dai consumatori di servizi di rete.

Ma come sempre la comunicazione è un'arma da maneggiare con cautela, calibrando ironia e chiarezza del messaggio.

Moneta digitale

Arriva WeChat Pay, si paga alla cinese

WeChat Pay arriva in Italia.Il comunicato ufficiale è atteso oggi, il servizio è previsto partire nei prossimi giorni. Il sistema di pagamento digitale con l'app cinese sarà aperto solo ai cittadini del Dragone rosso nel nostro Paese per turismo o lavoro: nel 2016 erano la bellezza di 3,7 milioni, sono in crescita costante. Stime di fonte cinese parlano di oltre 20 milioni di persone che nei prossimi cinque anni si muoveranno per turismo, in direzione dell'Europa. Per l'Italia quindi, il beneficio sarà indiretto: hotel, ristoranti, centri commerciali, negozi, retailer di catene dalla moda al design, dentro gli aeroporti o nelle città d'arte potranno ricevere pagamenti in mobilità. E i cinesi non avranno bisogno di cambiare la valuta: sono già abituati a pagare così. L'anno scorso da WeChat Pay sono passate oltre un milione di transazioni al minuto.

Internet company
Andrea Ghizzoni, direttore per l'Europa di Tencent: è la società che ha sviluppato WeChat, app cinese per i pagamenti

Ma come funziona? I merchant italiani potranno dotarsi di un apposito Pos o aggiungere WeChat ai circuiti di pagamento per cassa. Il cliente con uno smartphone e un account su WeChat vi collega il proprio conto corrente per creare un portafoglio digitale. Al momento di pagare, inquadra il QR Code, il codice fa accedere al *wallet* e così scatta il pagamento in valuta.

La transazione arriva al negoziante in euro. Due i partner tecnologici coinvolti per l'Italia: Digital Retelex (consulenza sul marketing digitale) e Docomo, piattaforma per il passaggio del denaro virtuale.

Dopo lo sbarco in Francia e Regno Unito, a curare le regia anche per l'Italia è stato Andrea Ghizzoni, Europe director di Tencent, l'Internet company a cui fa capo la app. «WeChat per i cinesi è un luogo dove vivere esperienze e fare acquisti, non solo una chat. Ai merchant offriamo questo: un pubblico coinvolto, amante del lusso e dell'*Italian style*. E un nuovo metodo di pagamento digitale integrato con tutti i servizi della piattaforma».

Fabio Sottocornola