# Promettono di eliminare il ransomware, ma sono complici del pirata

Dic 04, 2018 Marco Schiaffino In evidenza, Malware, Mercato, News, RSS, Scenario 0

---

***La società si chiama Dr.Shifro e prometteva di recuperare i file crittografati dal ransomware. In realtà avevano un accordo coi cyber-criminali.***

Non basta guardarsi dai cyber-criminali e dai loro malware: nell'anno di grazia 2018 bisogna fare molta attenzione anche quando si sceglie la società di sicurezza a cui si chiede aiuto per limitare i danni di un attacco.

A impararlo a loro spese sono stati gli sventurati clienti di **Dr.Shifro**, una società russa che promette di fornire assistenza nel caso di attacchi di ransomware, aiutando le vittime a recuperare i file senza dover pagare il riscatto.

Si tratta di un'attività piuttosto comune, che alcuni soggetti (come il consorzio di società di sicurezza che si raccolgono intorno al progetto No More Ransom) offrono gratuitamente.

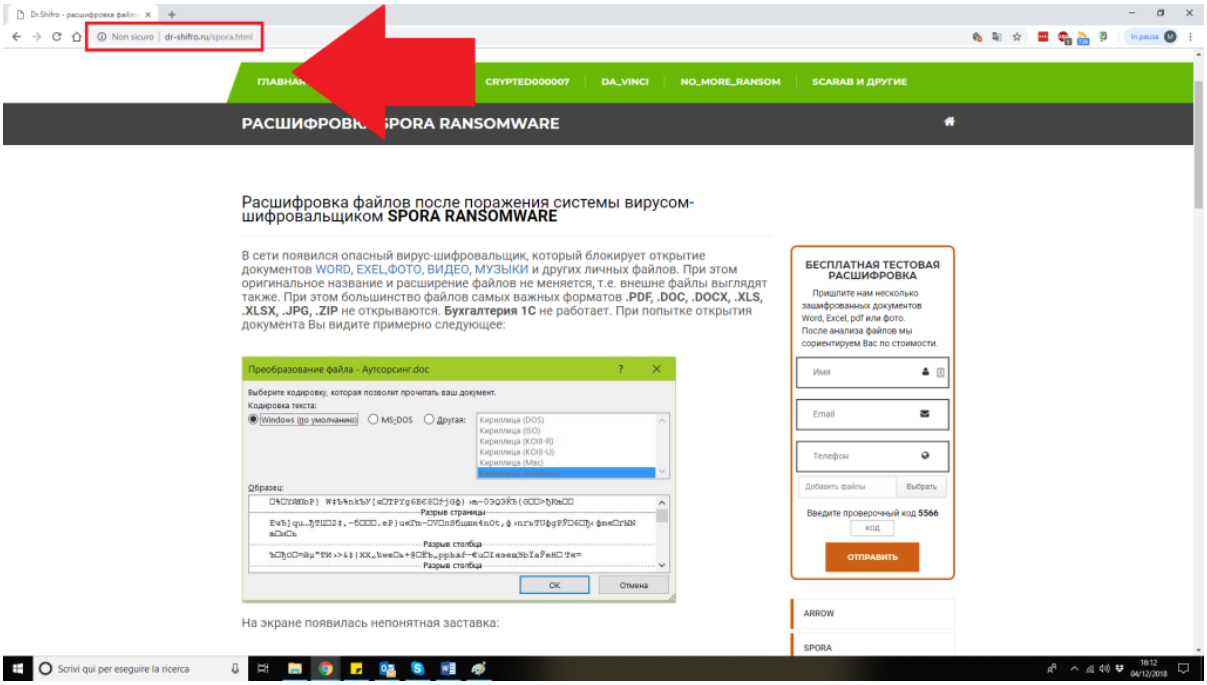
In alcuni casi, infatti, gli analisti sono in grado di aggirare i sistemi usati dai ransomware per crittografare i file. In altri sono gli stessi pirati informatici che, dopo un certo periodo di tempo, rendono pubbliche le chiavi crittografiche che hanno usato.

Come spiegano i ricercatori di **Check Point** in un comunicato, nel caso di Dr.Shifro c'era però qualcosa di strano. La società, infatti, offriva assistenza anche per **Dharma/Crisis**,

un ransomware che in questi mesi va per la maggiore.

**Peccato, però, che secondo i ricercatori di sicurezza non esista alcun modo per spezzare il sistema crittografico utilizzato dal ransomware in questione**.

Siamo di fronte a dei geni della crittografia? No. Solo a dei farabutti. **Dr.Shifro aveva infatti stipulato un accordo con i pirati informatici per truffare i clienti**.




Il sito di una società di sicurezza senza certificato digitale? Cominciamo male…

Il meccanismo era semplice: Dr.Shifro girava parte del compenso ai cyber-criminali, che in cambio gli fornivano la chiave per decrittare i dati del cliente.

Secondo la ricostruzione fatta da Check Point, la "parcella" di 2.300 dollari veniva divisa in parti quasi uguali: **1.300 all'autore del ransomware e 1.000 ai titolari di Dr.Shifo**.

Secondo gli esperti, non si tratta di un caso isolato. Sarebbero molte le società di sicurezza che, promettendo un intervento "tecnico", agirebbero in realtà come mediatori tra le vittime e gli estorsori, in molti casi mentendo

spudoratamente ai loro clienti lasciandogli credere che il riscatto non sia stato pagato.

Please follow and like us:




---

Kaspersky lancia Security Cloud: “La protezione deve diventare flessibile”

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2018/12/04/promettono-di-eliminare-il-ransomware-ma-sono-complici-del-pirata/

---

# Con l’iperconvergenza la sicurezza è più facile

Dic 03, 2018 Marco Schiaffino Approfondimenti, In evidenza, RSS, Tecnologia 0

---

***Syneto usa la convergenza per offrire strumenti di backup e recupero dei dati che normalmente sbarcano solo a livello enterprise.***

Quando si parla di iperconvergenza, di solito, ci si riferisce a sistemi a livello di grandi aziende, che puntano

all’integrazione di più funzionalità in ambiente virtuale per migliorare la versatilità degli strumenti.

L’iperconvergenza, però, può avere un impatto notevole anche in ambito sicurezza. “Uno degli aspetti dell’iperconvergenza è che tutto può essere fornito in una singola appliance senza che ci sia bisogno di creare dal nulla un eco-sistema complesso” spiega **Vadim Comanescu**, CEO di **Syneto**.

“Questo significa che non serve l’implementazione di sistemi complessi, ma è possibile avere a disposizione strumenti efficaci che sono immediatamente attivi e abbordabili anche per le piccole e medie imprese”.

Ma di cosa stiamo parlando esattamente? Facciamo un passo indietro al concetto di iperconvergenza. In termini estremamente sintetici può essere definita come **un’architettura software in cui convergono risorse di calcolo, di memorizzazione, di networking e di virtualizzazione**. Tutto in unico hardware.

L’interpretazione dell’iperconvergenza fatta da Syneto aggiunge un tassello, quello della sicurezza. Guardando ai risultati, si possono riassumere in un sistema di **backup e disaster recovery** che permette di ripristinare tutti i sistemi nel giro di un massimo di 15 minuti.

[embedded content]

Sotto un profilo tecnico, le appliance di Syneto sono sostanzialmente dei server (progettati dall’azienda stessa) sul quale gira un sistema operativo proprietario con un hypervisor (stiamo comunque parlando di sistemi virtuali) basato su **VMware**.

L’aspetto della sicurezza, in **Syneto OS**, fa leva su un file system specializzato. “Il file system è strutturato su più layer” spiega Comanescu. “Il primo sfrutta dei metadata che permettono di riconoscere e taggare concetti come macchina

virtuale o NAS. **In questo modo il sistema può capire se il dato che sta trattando è una replica e da dove arriva**”.

A un secondo livello, spiega Comanescu, ci sono due engine a cui sono affidati, rispettivamente, **la gestione dell’iperconvergenza e i processi di data protection e restore**. L’ultimo livello è rappresentato dall’interfaccia, che consente di gestire il tutto da browser.

Chi lo usa, però, non  si accorge praticamente di nulla ed è proprio questo che, secondo Vadim Comanescu, rappresenta il punto di forza di questa soluzione.

“Il nostro obiettivo è **offrire strumenti avanzati riducendo il livello di complessità per gli utenti**. Una soluzione immediatamente funzionante con caratteristiche del genere permette a tutti di utilizzare strumenti evoluti senza dover impazzire con impostazioni e creazione dell’architettura infrastrutturale”.

Insomma, quello dell’iperconvergenza sarà anche un nome (e un concetto) a prima vista complicato, ma il suo obiettivo è di rendere tutto molto più semplice. Soprattutto nel mondo della sicurezza.

Please follow and like us:

Follow

---

Identificati gli autori del ransomware SamSam

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2018/12/03/con-liperconvergenza-la

-sicurezza-e-piu-facile/

---

# Hacker rubano i dati di 500 milioni di clienti degli hotel Marriott-Staroowd

Nov 30, 2018 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, Privacy, RSS 0

---

***Gli hacker sarebbero riusciti a infiltrarsi nella rete di Starwood nel 2014, ma gli amministratori di sistema se ne sono accorti solo lo scorso settembre.***

Nomi, indirizzi email, estremi del passaporto e (in alcuni casi) i dati della carta di credito: i pirati informatici che hanno violato i sistemi della catena di hotel **Starwood**, acquisita da **Marriott** nel 2016, hanno decisamente fatto il colpo grosso.

Il bilancio delle vittime di questo mega-hack è infatti di **500 milioni di clienti della catena**, che comprende nomi conosciuti come **W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton e Design Hotels**.

Nel comunicato pubblicato su Internet da Starwood si conferma il furto di tutti i dati per circa **327 milioni di clienti** e per alcuni di essi, appunto, la sottrazione anche dei dati di carta di credito che sarebbero però protetti da crittografia AES 128.

La proprietà, però, mette le mani avanti spiegando che **non possono avere la certezza che i pirati non abbiano messo le mani anche sulle chiavi che ne consentono la decrittazione**.




D’altra parte, stando a quanto riportato sempre nel comunicato, **l’intrusione sarebbe avvenuta nel 2014** e gli hacker avrebbero potuto agire indisturbati per la bellezza di 4 anni prima che qualcuno se ne accorgesse.

Gli analisti stanno ora cercando di decrittare la copia dei dati creata dai pirati informatici (a quanto si capisce rinvenuta sui server) per capire quali informazioni siano state esattamente esfiltrate dai sistemi.

Ora Marriott ha cominciato a contattare via email tutti i clienti rimasti vittima del breach e intende offrire loro anche **un servizio gratuito di monitoraggio contro il furto di identità**.

Vista la timeline e la quantità siderale di tempo trascorsa tra il primo attacco e il suo rilevamento, viene però da chiedersi quanti siano già stati vittima di truffe, attacchi

di phishing o furto di identità.

Please follow and like us:




---

AI di nuova generazione contro le tecniche di mimetizzazione dei malware

---

**Articoli correlati**

**Altro in questa categoria**

---

https://www.securityinfo.it/2018/11/30/violati-i-sistemi-degli-hotel-marriott-staroowd-rubati-i-dati-di-500-milioni-di-clienti/

---

# AI di nuova generazione contro le tecniche di mimetizzazione dei malware

Nov 30, 2018 Marco Schiaffino In evidenza, News, RSS, Tecnologia 0

---

***Le tecniche di offuscamento usate dai pirati richiedono nuovi strumenti per individuare il codice malevolo.***

## *L’esempio di G Data DeepRay.*

La velocità con cui i cyber-criminali sviluppano e distribuiscono varianti dei loro malware è in continua ascesa e le tecniche tradizionali di rilevamento automatico (dalle signature ai sistemi di analisi gestiti dal software) faticano a stare al passo.

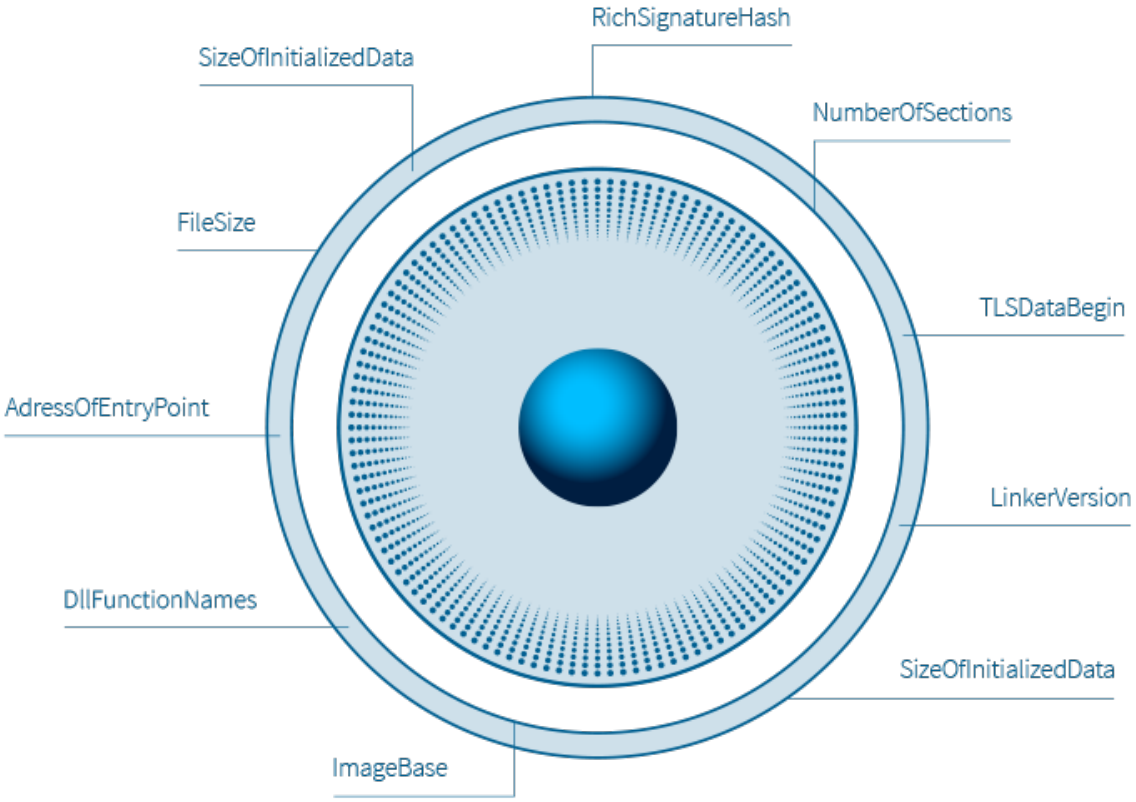
Risultato: sempre più spesso diventa necessario ricorrere all’intervento umano, **indubbiamente più efficace ma anche meno tempestivo**. La soluzione per compensare questo gap esiste e ha un nome che riempie sempre più spesso le pagine Internet dei siti di sicurezza: **Intelligenza Artificiale**.

Il concetto di Intelligenza Artificiale (AI), però, è qualcosa di estremamente ampio e la sua implementazione a livello di sicurezza può avvenire in modo diverso.

L’uso più comune dell’AI è infatti quello di utilizzarla in maniera centralizzata per analizzare i campioni “a monte” per catalogare i sample individuati dagli endpoint ed estrarre indicatori che vengono utilizzati in seguito per rilevare i malware sugli endpoint.

Dalle parti di Bochum, dove ha sede **G Data**, hanno deciso però di forzare i tempi e utilizzare l’Ai in maniera decisamente più spinta, integrando il sistema di intelligenza artificiale **direttamente sul motore dell’antivirus**.

La tecnologia si chiama **DeepRay** e, spiegano i ricercatori, è “un sistema proprietario di self-learning basato sull’AI, capace di individuare anche i malware meglio camuffati direttamente sul computer dell’utente”.




Insomma: la tecnica messa a punto da G Data consente in buona sostanza di **tagliare un passaggio** e consentire all'antivirus di utilizzare tecniche di analisi che prendono in considerazione diversi parametri per "imparare" a riconoscere i malware anche quando adottano sofisticate tecniche di offuscamento.

Nel dettaglio, G Data spiega che il sistema sfrutta una **rete neurale** composta da numerosi percettroni che identificano e analizzano i processi sospetti.

Un'innovazione che **Andreas Lüning**, fondatore e CEO di G DATA considera rivoluzionaria: "Con DeepRay, abbiamo stravolto le regole del gioco e privato i cybercriminali dei loro profitti economici" ha dichiarato.

"Grazie a questa nuova tecnologia siamo in grado di analizzare il vero contenuto di file che contengono malware camuffati e respingiamo in modo efficace i nuovi attacchi".

Please follow and like us:

Follow

Cyber-Security: cosa ci aspetta nel 2019?

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2018/11/30/ai-di-nuova-generazione-contro-le-tecniche-di-mimetizzazione-dei-malware/

# Cyber-Security: cosa ci aspetta nel 2019?

Nov 29, 2018 Marco Schiaffino Hacking, In evidenza, Malware, Minacce, News, RSS, Scenario 0

***Intelligenza artificiale, attacchi alla cloud e ai sistemi di assistenza vocale. Per gli esperti di McAfee il prossimo anno proporrà minacce inedite.***

Il 2018 si avvia alla conclusione ed è normale che ci si scateni nelle previsioni per il prossimo anno. Un hobby che nel settore della sicurezza informatica si traduce immediatamente in previsioni catastrofiche.

Visto che l'esercizio è comunque divertente (e in molti casi si finisce per azzeccarci) preferiamo non tirarci indietro e cominciare da subito a rendere conto di ciò che gli esperti di

sicurezza si aspettano di vedere nel 2019.

I primi a cimentarsi nelle previsioni sono i ricercatori di **McAfee**, che hanno pubblicato un post sul blog della società di sicurezza in cui elencano le possibili minacce in arrivo per il nuovo anno.

La prima preoccupazione riguarda **l'ecosistema del cyber-crimine**, che secondo gli esperti di McAfee potrebbe evolvere e irrobustirsi nei prossimi 12 mesi.

Il tema non è nuovo: già negli ultimi anni, infatti, lo scambio di know-how e la compravendita di malware nei bassifondi di Internet è uno degli aspetti che ha alimentato il fenomeno della pirateria informatica a livello globale.

Gli strumenti di hacking, così come i singoli exploit, circolano con una facilità disarmante e possono essere usati da chiunque abbia la possibilità di recuperarli e le competenze per trasformarli in malware.

In particolare, però, le preoccupazioni si concentrano sul traffico di accessi attraverso account di **Remote Desktop Protocol (RDP)** che vengono venduti o scambiati sui forum di hacking o nel Dark Web e utilizzati spesso per portare avanti campagne mirate che utilizzano ransomware.

Non solo: i forum attivi nei bassifondi di Internet secondo McAfee saranno anche il luogo di scambio di informazioni sulle **nuove vulnerabilità nel settore mobile**, un ambito in cui i cyber-criminali stanno concentrando la loro attenzione e che nel 2018 è risultato particolarmente fruttifero.

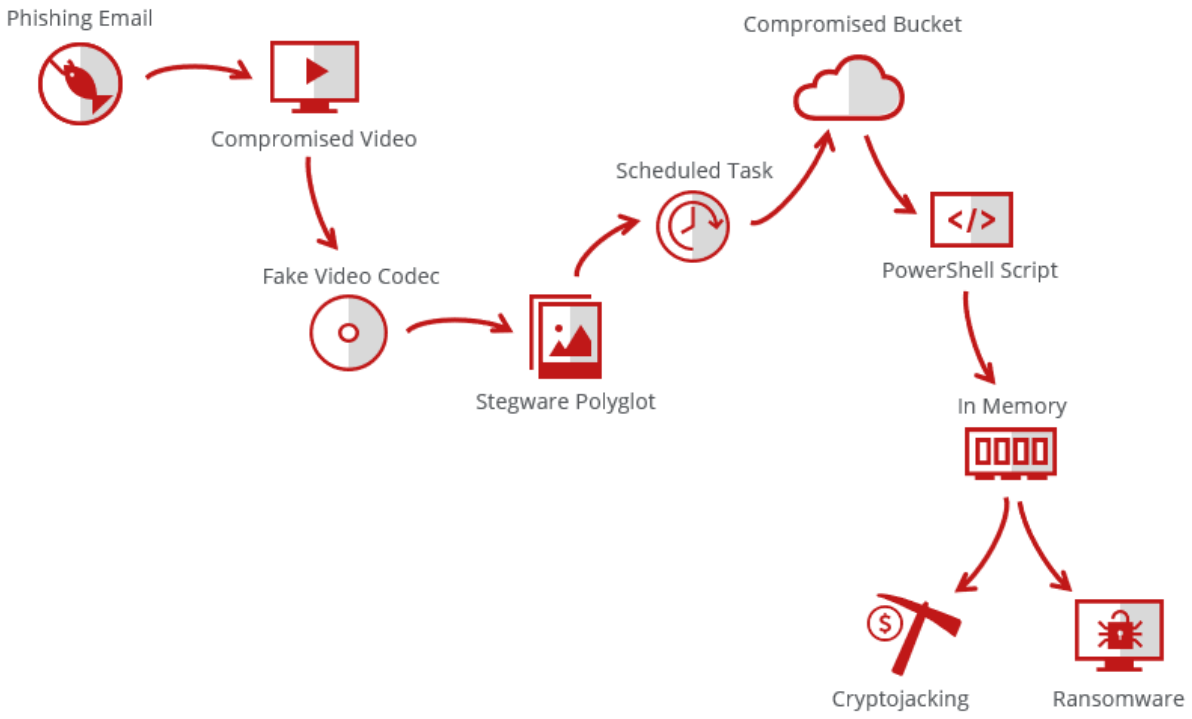
Da un punto di vista più tecnico, ciò che ci si aspetta per il futuro prossimo è l'impiego anche da parte dei "bad guys" dell'intelligenza artificiale.

La tecnologia, finora appannaggio degli esperti di sicurezza e utilizzata principalmente per individuare con maggiore

precisione e tempestività le nuove minacce, ha infatti anche un altro possibile utilizzo: quello di mettere a punto **tecniche di evasione più sofisticate e complesse** rispetto a quelle a cui siamo abituati.

Secondo gli esperti, quello degli strumenti progettati per aggirare gli antivirus rischia di diventare un vero e proprio mercato che sfrutta i sistemi di intelligenza artificiale per mettere a punto strumenti di evasione che vengono poi venduti al mercato nero.

L'altra tendenza che ci si aspetta subisca una crescita esponenziale è quella della differenziazione delle modalità di attacco. Se fino a oggi ci siamo abituati a poter classificare gli attacchi in base a categorie "fisse", come ransomware, trojan, phishing e simili, in futuro la tendenza sarà quella di "mixare" le tecniche, partendo dalla prima compromissione per poi adottare payload diversi a seconda delle situazioni.



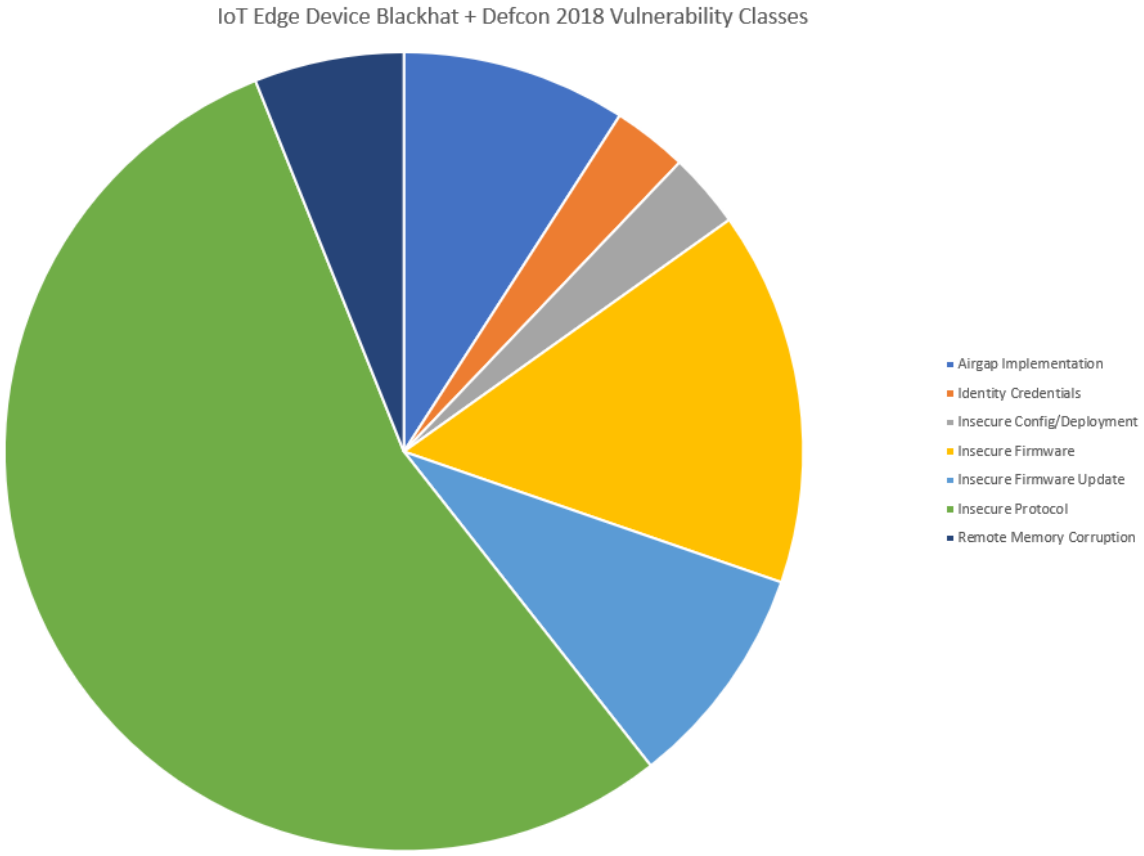

Fino a qui ci siamo occupati della "normale" criminalità informatica, ma gli analisti prevedono anche un'espansione che andrà a coprire nuovi settori che fino a oggi sono stati interessati solo marginalmente dagli attacchi.

Un esempio? **La possibilità che i pirati informatici avviino campagne di sabotaggio dei brand commerciali, sulla sica di quanto accaduto negli ultimi mesi nel caso degli appuntamenti elettorali**.

Una campagna di disinformazione (o un bombardamento di fake news) che prende di mira un brand commerciale ha effetti potenzialmente devastanti e nell'ottica di chi agisce in un quadro di "attacco su commissione" rappresenta un possibile business che in futuro potrebbe diventare un vero problema.

Tornando agli scenari conosciuti, McAfee prevede un aumento esponenziale degli attacchi che mirano all'acquisizione di dati conservati nella cloud. Il ragionamento su cui si basa la previsione è semplice: stando alle ricerche della società di sicurezza, **il 21% dei dati conservati su cloud sono rappresentati da informazioni "sensibili"** il cui furto può essere monetizzato facilmente.

Un ragionamento simile riguarda il settore dell'IoT, in cui è probabile che gli attacchi crescano allo stesso (forsennato) ritmo con cui crescono il numero di dispositivi della Internet of Things sul mercato. Tanto più che le vulnerabilità e gli exploit per IoT (si veda il grafico qui sotto) sono in costante crescita.




L’elemento di novità, stando al report, potrebbe riguardare gli attacchi rivolti agli assistenti vocali (in primis quelli di **Apple e Google**) la cui diffusione sta aumentando di pari passo con la diffusione dei dispositivi “smart”.

La logica, qui, è quasi banale: puntando direttamente al sistema di controllo che gestisce tutti i dispositivi, i pirati prenderebbero una sorta di “scorciatoia” che gli permetterebbe di compromettere l’intero sistema in un solo colpo.

Quante di queste previsioni si avvereranno? Difficile dirlo, ma in passato gli esperti che si sono lasciati andare a questo esercizio non hanno sbagliato di molto. Eventuali errori, poi, in questo caso si trasformerebbero in semplici sospiri di sollievo.

Please follow and like us:

Follow

AI di nuova generazione contro le tecniche di mimetizzazione dei malware Smantellata una mega-frode pubblicitaria che sfruttava 2 milioni di PC

**Articoli correlati**

**Altro in questa categoria**

https://www.securityinfo.it/2018/11/29/cyber-security-cosa-ci-aspetta-nel-2019/

# Smantellata una mega-frode pubblicitaria che sfruttava 2 milioni di PC

La botnet si chiamava 3ve e ha permesso ai suoi autori di incassare denaro vendendo miliardi di click su pubblicità che non vedeva nessuno. Secondo Google si tratta della più sofisticata e complessa frode pubblicitaria mai individuata, smantellata in questi giorni grazie alla collaborazione tra aziende IT, forze di polizia e società di sicurezza. Le […]

L'articolo Smantellata una mega-frode pubblicitaria che sfruttava 2 milioni di PC proviene da Securityinfo.it.

https://www.securityinfo.it/2018/11/28/smantellata-una-mega-frode-pubblicitaria-che-sfruttava-2-milioni-di-pc/

# Germania: ecco come cambio il nome sulla carta d’identità elettronica

Una vulnerabilità nei documenti con chip RFID permette di alterare i dati quando ci si registra online. La scoperta di un ricercatore tedesco. Utilizzare la tecnologia per sostituire i classici documenti è una di quelle suggestioni che affascinano le pubbliche amministrazioni da anni. Le cose, però, non vanno sempre per il verso giusto e le […]

L’articolo Germania: ecco come cambio il nome sulla carta d’identità elettronica proviene da Securityinfo.it.

https://www.securityinfo.it/2018/11/22/germania-ecco-come-cambio-il-nome-sulla-carta-didentita-elettronica/

---

# Attacchi Magecart: ora la lotta è tra diversi gruppi di hacker

I cyber-criminali hanno cominciato una competizione a suon di “sabotaggi” nei confronti dei concorrenti. A rimetterci, come al solito, sono solo le vittime. Gli attacchi tramite Magecart (lo script che consente di rubare i dati delle carte di credito sui siti e-commerce di cui abbiamo parlato in questo

articolo) non accennano a diminuire e, secondo […]

L’articolo Attacchi Magecart: ora la lotta è tra diversi gruppi di hacker proviene da Securityinfo.it.

https://www.securityinfo.it/2018/11/21/attacchi-magecart-ora-la-lotta-e-tra-diversi-gruppi-di-hacker/

---

# Hackerare un bancomat? Bastano 20 minuti

Uno studio di Positive Technologies mette a nudo il (pessimo) livello di sicurezza dei bancomat. Le tecniche di attacco sono tante e i modelli vulnerabili… quasi tutti. Non c’è bisogno di avere poteri da supereroe per rubare i soldi da un bancomat. Per farlo basta avere qualche (buona) conoscenza tecnica e gli strumenti adatti. Parola […]

L’articolo Hackerare un bancomat? Bastano 20 minuti proviene da Securityinfo.it.

https://www.securityinfo.it/2018/11/16/hackerare-un-bancomat-bastano-20-minuti/

---

# Sorpresa! Il 60% delle VPN

# free per smartphone sono… cinesi!

Le più diffuse Virtual Private Network per Android e iOS sono di società con sede in Cina, il paese in cui usare una VPN è reato. E la privacy… Chi installa una VPN (Virtual Private Network) lo fa per un unico motivo: garantire la privacy della sua navigazione. Gli utenti Android e iOS che ricorrono […]

L’articolo Sorpresa! Il 60% delle VPN free per smartphone sono… cinesi! proviene da Securityinfo.it.

https://www.securityinfo.it/2018/11/15/sorpresa-il-60-delle-vpn-free-per-smartphone-sono-cinesi/