Fighting Fraud With Threat Intelligence: Debunking Common Misconceptions

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/TD4-BlkD9oQ/fighting-fraud-threat-intelligence-debunking-common-misconceptions

---

The Dark Net, a Major Threat but Also a Resource

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/JwqT8JQO-fg/dark-net-major-threat-also-resource

---

Spain Extradites 94 Taiwanese to China on Phone Scam Charges

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4mLXnOJhCpA/spain-extradites-94-taiwanese-china-phone-scam-charges

Attackers Piece Together Malicious Tools Used for Targeted Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/XuRFJjhlsUU/attackers-piece-together-malicious-tools-used-targeted-attacks

---

Cybercrime, in Italia la sanità resta il settore più colpito. In calo l’hacktivism

Nel 2018 gli attacchi informatici gravi sono aumentati del 38% su base annua raggiungendo la cifra di 1.552, pari a 129 attacchi al mese contro i 94 del 2017. La stragrande maggioranza (1.232 attacchi) è rappresentata dal cybercrime, che “si evolve”. In calo l’hacktivism (hacker attivisti come Anonymous), passato dai 236 attacchi gravi del 2014 a 61 nel 2018.

I dati, elaborati dal **Clusit**, hanno evidenziato il 16% prende di mira gli enti governativi, mentre il 20%, uno su cinque, ha target multipli.

Lo studio evidenzia come i cybercriminali – sempre più attivi

e organizzati che colpiscono target multipli cercando di massimizzare i profitti – prendono di mira soprattutto enti governativi e il settore sanitario, molto appetibile per via dei dati sensibili che custodisce. 1 attacco informatico su 10 infatti è indirizzato al settore, in cui gli attacchi sono raddoppiati tra il 2017 e il 2018.

"*La cybersicurezza non è una sicurezza per addetti ai lavori, oggi e' una sicurezza generale, perché nel mondo digitale, in cui siamo completamente immersi, ci sono tutti gli aspetti della nostra vita. Quando parliamo dei dati come merce pregiata, oramai soggetta ad ogni tipo di trafugamento, sollecitazione e ad appetiti vari (leciti, illeciti, borderline), parliamo di dati nostri di vita, non di dati che hanno solo valore statistico*". Lo ha dichiarato il Direttore del Servizio Polizia Postale e delle Comunicazioni **Nunzia Ciardi** nel corso del suo intervenuta ieri all'evento.

"*Dal 2017 al 2018* – ha ricordato il direttore – *abbiamo avuto un aumento di denunce del 340% di attacchi finanziari a grandi e piccole e medie aziende e un importo di frodi denunciate di +172%. Parliamo quindi di fenomeni che hanno un'incidenza forte sulla nostra economia. Se continuiamo a parlare di sicurezza informatica come di un tema per addetti ai lavori non si fa un favore alla collettivita', ne' restituiamo un'immagine vera. Questo è un attacco sistematico alle infrastrutture di un Paese*".

La Polizia Postale ha siglato recentemente due intese strategiche: **Zecca di Stato** e **Consob**. Gli accordi rientrano nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione alla criminalità informatica con gli operatori che forniscono prestazioni essenziali ed infrastrutture critiche di interesse nazionale.

https://www.key4biz.it/cybercrime-in-italia-la-sanita-resta-il-settore-piu-colpito-in-calo-lhacktivism/260762/

Inside the Operations of a West African Cybercrime Group

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Z_VsW0uM0S8/inside-operations-west-african-cybercrime-group

---

Cybercrime, in Italia la PA è presa di mira da Ransomware, Banking Trojan e Spear Phishing

Gli attacchi informatici che colpiscono di più la Pubblica Amministrazione in Italia? **Ransomware**, **Banking Trojan** e campagne malevole mirate principalmente al furto di credenziali istituzionali chiamate **Sprear Phishing.**

Lo hanno rivelato gli esperti di cybersecurity del *Computer Emergency Response Team della Pubblica Amministrazione* (**CERT-PA**) – l'organo che ha il compito di supportare le amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica – diffondendo i dati

relativi alle minacce cibernetiche monitorate a maggio 2019.

Grafico rappresentativo degli eventi registrati e gestiti dal CERT-PA
I dati del CERT-PA evidenziano come la PA italiana sia stata attaccata con **Trojan**, come Ursnif e Gootkit, insieme al **ransomwame GandCrab** e al malware **Formbook**. In terza posizione si collocano, invece, i numerosi attacchi informatici di tipo Spear Phishing, mirati principalmente al furto di credenziali istituzionali. Non mancano nemmeno, comunque, **AdWare**, **Trojan** di altro tipo, **RAT**, **CryptoMiner**, **Bakdoor**, **Android** e **Infostealer**.

Fonte: CERT-PA

Da queste analisi del CERT-PA sulle minacce in Italia, effettuate anche grazie al monitoraggio dei malware del ricercatore di cyber security **JAMESWT_MHT,** sono emersi elementi interessanti. Ad esempio le campagne di malspam con malware Ursnif si sono rilevate in molti casi "*fallate*": il link nel corpo delle mail era errato o il file allegato, solitamente uno zip, conteneva i file malevoli senza il payload utile a compromettere il sistema.

La cosa più interessante invece riguarda la cadenza, quasi una routine, delle campagne monitorate. Il CERT ha rilevato un'alternanza piuttosto regolare nella diffusione di specifici malware cadenzata nei giorni della settimana. Ad esempio, nello specifico caso di Ursnif, in certi giorni il malware può essere veicolato tramite link presente nel corpo delle mail,

in altri diffuso tramite allegato DOC e giorni in cui viene utilizzato un allegato in formato XLS o VBS.

Attacchi per illeciti economici

Gli esperti hanno evidenziato come questo tipo di campagne cyber siano orchestrate da uno o più gruppi criminali il cui fine è quello di produrre, direttamente o meno, illeciti profitti economici a danno di utenti italiani.

Per massimizzare gli attacchi i cyber criminali abbiano escogitato una metodologia che consente loro di ottimizzare al meglio le operazioni, veicolando malware principalmente nei giorni feriali con una logica organizzativa che prevede una ricorsività nel metodo di diffusione;

Inoltre, gli errori emersi nelle campagne di malspam, nella catena di infezione e nell'utilizzo delle medesime credenziali di accesso ai server di C&C, lasciano presupporre, con buona probabilità, che i criminali non siano gli stessi autori del malware ma utilizzino infrastrutture esistenti, spesso disponibili a noleggio presso i black market, puntando principalmente a compromissioni di tipo massivo.

https://www.key4biz.it/cybercrime-in-italia-la-pa-e-presa-di-mira-da-ransomware-banking-trojan-e-spear-phishing/260475/

LabCorp Says 7.7 Million Patients Caught in AMCA Data

Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/haP6Bx3bIYI/labcorp-says-77-million-patients-caught-amca-data-breach

---

Lotta al cybercrime, al via l'alleanza tra Consob e Polizia di Stato

Continua senza sosta l'impegno della **Polizia di Stato** nella lotta e tutela dei cittadini nel settore della cybersecurity. Oggi è stato firmato un nuovo accordo con la Commissione nazionale per le società e la Borsa **(Consob)** sulla prevenzione e il contrasto dei crimini informatici che hanno per oggetto i sistemi e i servizi informativi di particolare rilievo per il Paese.

La convenzione – che arriva quasi una settimana dopo la firma tra la Polizia postale e **l'Istituto Poligrafico e Zecca dello Stato** – è stata firmata dal Presidente della Consob, **Paolo Savona**, e dal Capo della Polizia **Franco Gabrielli.**

Questa operazione rientra nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento delle attività di prevenzione della criminalità informatica attraverso la stipula di accordi con gli operatori che forniscono prestazioni essenziali.

La Polizia Postale e delle Comunicazioni è, infatti, quotidianamente impegnata a garantire l'integrità e la

funzionalità della rete informatica delle strutture di livello strategico per il Paese attraverso il **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.**

La Consob, nella sua attività di regolamentazione e di vigilanza sui mercati finanziari, ricopre un ruolo determinante e rappresenta un'infrastruttura di interesse nazionale. Pertanto, la protezione dei suoi sistemi informatici è da considerarsi necessaria per assicurare il pieno svolgimento delle sue funzioni.

L'accordo, basato sulla condivisione informativa e sulla cooperazione operativa, ha durata triennale e rappresenta una tappa significativa nel contrasto al *cybercrime.*

Alla firma della convenzione erano anche presenti, per il Dipartimento della Pubblica Sicurezza, il Direttore Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato, **Armando Forgione**, e il Direttore del Servizio Polizia Postale e delle Comunicazioni, **Nunzia Ciardi**; per la Consob il Commissario **Paolo Ciocca**, il Segretario Generale, **Carlo Deodato**, il Responsabile Divisione Infrastrutture Informative, **Paolo Libri**, e il Responsabile Ufficio Sicurezza Informatica, **Claudio Gentili.**

https://www.key4biz.it/lotta-al-cybercrime-al-via-lalleanza-tra-consob-e-polizia-di-stato/260359/

Top Australian University Reports Vast, ‘Sophisticated’ Hack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/34versM7jbk/top-australian-university-reports-vast-sophisticated-hack