New Version of Flame Malware Platform Discovered

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tgQbtaKbaRc/new-version-flame-malware-platform-discovered

---

Duqu Remained Active After Operations Were Exposed in 2011

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/VUqgOMsKlw4/duqu-remained-active-after-operations-were-exposed-2011

Cybersecurity, Tofalo (Difesa): 'Presto defiscalizzazioni per le PMI'

"*La sicurezza informatica è in cima all'agenda del Governo la cui azione combinata punta a investire sullo sviluppo delle nuove tecnologie e la sensibilizzazione degli utenti attraverso la diffusione della cultura della sicurezza e la formazione*". Lo ha detto il sottosegretario alla Difesa **Angelo**

Tofalo intervenuto ieri al convegno '*Cyber Security, un problema non solo tecnico*" organizzato a Milano con la **Regione Lombardia** e l'Associazione 'Tra il Dire e il Fare'.

"*La sicurezza* – ha aggiunto il sottosegretario – *è un bene comune, deve essere quindi considerata un investimento per la nostra comunità e non un costo, nell'ottica di Sistema Paese. Per questa ragione stiamo lavorando a una proposta per la defiscalizzazione dei costi per la sicurezza per le grandi ma soprattutto piccole e medie imprese*".

Per **Tofalo** quello di Milano "*e' stato un appuntamento che ha richiamato l'attenzione sui rischi e sulle opportunità del dominio cibernetico e su cosa fare per non incorrere nei pericoli della rete. Un tema che riguarda tutti, a ogni livello, dal singolo alle società e alle amministrazioni pubbliche*"

Esperti cyber cercasi

Nel frattempo l'Italia è alla ricerca di risorse interessate a far parte del personale del Comparto Intelligence e che intendono dare un concreto contributo alla missione del **DIS**, dell'**AISE** e dell'**AISI** a tutela degli interessi strategici nazionali in campo politico, militare, economico, scientifico e industriale.

La ricerca è rivolta alle eccellenze con una **formazione specifica in alcuni settori**, tra cui le discipline umanistiche, economiche, giuridiche, e internazionali. Così come rientrano anche le figure tecniche con elevate conoscenze linguistiche, che abbiano capacità di analisi, o esperienze maturate in aree, organizzazioni e/o organismi esteri.

Inoltre, a sostegno delle più recenti iniziative avviate dal

governo in materia di protezione cibernetica e sicurezza informatica nazionali, la selezione include profili con qualificate competenze nei vari ambiti della **cybersecurity**, come ad esempio la ricerca, il **monitoraggio, l'analisi ed il contrasto alla minaccia cyber.**

Per presentare i curricula bisogna registrarsi nella pagina Lavora Con Noi di sicurezzanazionale.gov.it. Per candidarsi c'è tempo fino alle 12:00 del **10 maggio 2019**.

https://www.key4biz.it/cybersecurity-tofalo-difesa-presto-defiscalizzazioni-per-le-pmi/253439/

New Module Suggests Fourth Team Involved in Stuxnet Development

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CMoJuHDVMzA/new-module-suggests-fourth-team-involved-stuxnet-development

---

Payment Card Data Stolen From AeroGrow Website

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/BuzXgd8

fpT4/payment-card-data-stolen-aerogrow-website

Ex-Senate Employee Pleads Guilty to Theft of Personal Data

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Ouh65BlQMSo/ex-senate-employee-pleads-guilty-theft-personal-data

---

Researchers unearth 74 Facebook cybercrime groups with 385,000 members

Enlarge / A post from one cybercrime group deleted by Facebook.

reader comments

114 with 47 posters participating

Share this story

Add spam, phishing, and payment-card fraud to the scourges

Facebook helps foster. The company is already under the microscope for the role it plays in spreading disinformation promoting white nationalism, conspiracy theories, and opposition to life-saving vaccinations. Now, a report published Friday says Facebook also helps criminals peddle a variety of cybercrime services.

Over the past few months, researchers with Cisco's Talos security group compiled a list of 74 Facebook groups whose members promised to carry out a variety of unethical, if not outright illegal, activities. Some groups acted as bazaars for the buying, selling, or trading of stolen payment-card data and hacked account credentials. Others served as forums for selling spamming and phishing tools. In all, about 385,000 users were members.

According to the Talos report:

> *These Facebook groups are quite easy to locate for anyone possessing a Facebook account. A simple search for groups containing keywords such as "spam," "carding," or "CVV" will typically return multiple results. Of course, once one or more of these groups has been joined, Facebook's own algorithms will often suggest similar groups, making new criminal hangouts even easier to find. Facebook seems to rely on users to report these groups for illegal and illicit activities to curb any abuse.*
>
> *Talos initially attempted to take down these groups individually through Facebook's abuse-reporting functionality. While some groups were removed immediately, other groups only had specific posts removed. Eventually, through contact with Facebook's security team, the majority of malicious groups was quickly taken down, however new groups continue to pop up, and some are still active as of the date of publishing. Talos continues to cooperate with Facebook to identify and take down as many of these groups as possible.*

Craig Williams, a senior technology leader and global outreach manager at Talos, told Ars that, as of Thursday, all 74 of the Facebook groups had been taken down. But he said it was entirely plausible that new groups pursuing the same unethical and illegal activities had taken their place. Indeed, less than two minutes of searching on Facebook turned up groups that appeared to offer the same services. One group called Carding Secured offered an array of services related to stolen payment-card data. Others carried names such as Spam Professional, Spammer and Hacker by Z0tlob, and Spam 2019, although it wasn't immediately clear if they violated Facebook terms of service barring the offering of illegal products or services.

Friday's report makes it clear that some of the groups Talos studied were brazenly offering illegal services. A screenshot from one group shows a Facebook user peddling credit card data for as little as $7. For cards with verified-by-Visa protection, the cost was $15. Other screenshots show users selling credit card data including CVV numbers, email addresses exposed in database breaches, and services for creating fake IDs. Most of the time, sellers seek payments in the form of cryptocurrencies.

In multiple cases, Talos was able to confirm that the illegal items or services sold in Facebook groups were being used in real crimes taking place online. In one post, a Facebook user advertised a service that landed Apple-themed phishing emails in inboxes belonging to Hotmail and Yahoo Mail users. The post contained the following image, demonstrating the spammed messages received in one such inbox:

Cisco Talos
Talos researchers were then able to locate the same phishing message sent to users in the wild. An analysis showed the messages attached a malicious PDF file that claimed to be an invoice for an Apple-related purchase. Clicking on a link to either view or cancel the order sent users to a phishing website that was associated with a well-known phishing kit that targets Apple users.

Friday’s report comes a year after journalist Brian Krebs reported Facebook had deleted almost 120 groups with more than 300,000 members total after Krebs provided documentation they were flagrantly promoting a host of illicit activities on the social media network’s platform. Williams, the Talos outreach manager, said Facebook faces an uphill battle ridding its platform of cybercrime groups.

“These users are dedicated to Facebook,” he said in an interview. “It’s a lot like trying to kill cockroaches. If you kill 10 of them, there’s probably 20 more.”

A Facebook spokesperson issued a statement that read: “These Groups violated our policies against spam and financial fraud and we removed them. We know we need to be more vigilant and

we’re investing heavily to fight this type of activity.”

On background, the spokesperson said Facebook employees deleted the groups after confirming the Talos findings. The employees also identified the users running the deleted groups and blocked their ability to create new groups on Facebook in the future. Facebook, the representative said, has 30,000 people around the world working on safety and security, three times as many as 2017. They use a combination of reports from users, technology, and human review to enforce policies.

https://arstechnica.com/?p=1486793

US Colleges Halt Work With Huawei Following Federal Charges

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tNef1KEAQkA/us-colleges-halt-work-huawei-following-federal-charges

---

New ‘Xwo’ Malware Looks for Exposed Services, Default

Passwords

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/sT5uduRELZo/new-xwo-malware-looks-exposed-services-default-passwords

---

Hundreds Targeted in Recent Roaming Mantis Campaign

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/w0Zz05IXo0o/hundreds-targeted-recent-roaming-mantis-campaign