Assange Charged in US With Computer Hacking Conspiracy

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/nCdiGYYOFlo/assange-charged-us-computer-hacking-conspiracy

---

U.S. Attributes New Trojan to North Korean Hackers

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ZHm52t-mJ9w/us-attributes-new-trojan-north-korean-hackers

---

Assange Arrested in London After Ecuador Withdraws Asylum

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/zEmjPZFAd78/assange-arrested-london-after-ecuador-withdraws-asylum

TajMahal APT Can Steal Data From CDs, Printer Queues

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5kL4K80DLjE/tajmahal-apt-can-steal-data-cds-printer-queues

---

Over 60,000 Stolen Profiles Sold on Underground Marketplace

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Vhv0K9osNCE/over-60000-stolen-profiles-sold-underground-marketplace

---

Czech Court: Rights of Alleged Russian Hacker Violated

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ct4n404

WttA/czech-court-rights-alleged-russian-hacker-violated

Hackers Behind Triton ICS Malware Hit Additional Critical Infrastructure Facility

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/BL-eh9yLcuM/triton-hackers-focus-maintaining-access-compromised-systems-fireeye

---

Minnesota State Agency Breach May Have Put Thousands at Risk

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/P_GcRnmYffQ/minnesota-state-agency-breach-may-have-put-thousands-risk

---

Microsoft Patches Windows Privilege Escalation Flaws Exploited in Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/VvVneoKEmVg/microsoft-patches-windows-privilege-escalation-flaws-exploited-attacks

---

Yoroi mette a disposizione gratis la piattaforma Yomi per individuare e bloccare i malware

Yoroi ha deciso di aprire 'Yomi' al pubblico per mettere a disposizione della comunità i propri strumenti più avanzati per rilevare, analizzare e bloccare i software dannosi. Come dice il nome, "**Yomi: The Malware Hunter**", è infatti una piattaforma online per la rilevazione e la gestione in sicurezza di malware informatici. Basato su tecnologia open source italiana, Yomi da oggi può essere usata anche dai singoli individui, gratuitamente.

Già soprannominata dalla stampa come "Il cimitero dei virus" all'epoca del suo lancio in versione beta, la piattaforma Yomi, ulteriormente perfezionata, è in grado di "digerire" e detonare nel suo recinto di sabbia (*sandbox*) documenti dannosi, file eseguibili, installatori e script senza alcun

pericolo. La “detonazione” avviene infatti in una maniera controllata, registrando il comportamento di ogni file potenzialmente dannoso dentro un **ambiente personalizzato** e **progettato per sconfiggere le tecniche di evasione** più avanzate messe in atto da chi diffonde il malware.

“*Compito di Yomi è di contribuire a rendere il cyberspace più sicuro per tutti* – ha detto **Marco Ramilli** di Yoroi -, *e per questo ne facciamo dono alla comunità italiana di info-security.*”

Il **malware** rappresenta un potente strumento per il cybercrime in tutto il mondo e, con oltre 856 milioni di campioni identificati durante l’ultimo anno è, senza dubbio, **uno dei principali tipi di minaccia** che aziende e organizzazioni affrontano ogni giorno per gestire la propria attività con grande impegno di tempo, risorse e denaro, mettendo a rischio la propria reputazione e gli asset dei loro clienti.

Le minacce malware hanno sviluppato in questi anni la capacità di eludere ogni rilevamento, scavalcando le barriere di sicurezza e rimanendo in silenzio fino a scatenare il loro potenziale malevolo, consentendo ad hacker malvagi, cyber-criminali e spie di rubare segreti, dati, beni digitali e denaro, compromettendo processi aziendali e persino vite umane quando colpiscono le infrastrutture critiche. Per divertimento e profitto.

“*Per tutti questi motivi ‘Yomi’ è il contributo italiano alla battaglia contro il malware dedicato ai professionisti della sicurezza, alle comunità di intelligence, ai CERT e ai CSIRT che vorranno usarlo.*” Ha dichiarato **Marco Castaldo**, amministratore delegato del Gruppo **Cybaze Spa** di cui Yoroi è parte.

Il software di Yomi è in grado di condurre un’analisi

multilivello sui software malevoli: statica, dinamica e comportamentale, per aiutare gli analisti umani a comprendere la dinamica dell'esecuzione del codice dannoso risparmiando tempo e denaro.

Yomi può analizzare una grande varietà di tipi di file, per ogni tipo di esigenza, sia privata che aziendale, per realtà di piccole e di grandi dimensioni, "Compresi i pericoli che preoccupano di più i gli utenti comuni e che derivano dal trattamento di documenti PDF, Office, Powerpoint, Word o Excel, anche nei formati compressi." sottolinea Marco Ramilli.

Yomi è anche capace di ispezionare gli indirizzi e i domini di rete e presenta funzionalità di analisi SSL, per consentire ai cacciatori di malware di riconoscere le minacce nascoste che sfruttano la protezione crittografica.

La piattaforma creata da Yoroi presenta diverse caratteristiche innovative nel panorama dell'analisi delle minacce informatiche. Mentre è possibile condividere con la comunità le proprie scoperte 'Yomi' rende anche possibile decidere – per questioni di privacy o di segretezza – di richiedere report privati per i campioni analizzati attraverso la sua piattaforma.

"Yomi: The Malware Hunter" non è solo uno strumento di analisi automatizzato e gratuito con avanzate capacità di analisi delle minacce, rappresentate graficamente, ma è pensato per coinvolgere tutti gli attori interessati attraverso contest personalizzati. La piattaforma è infatti progettata secondo i principi della gamification, cioè come un gioco e un concorso a premi a cui tutti possono partecipare per finire nella *hall of fame* dei "Cacciatori di virus".

Per provare "Yomi: The Malware Hunter" clicca qui.

https://www.key4biz.it/yoroi-mette-a-disposizione-gratis-la-piattaforma-yomi-per-individuare-e-bloccare-i-malware/253497/