HP Wolf Security: Infractorii cibernetici folosesc servicii de solutionare a litigiilor, obligatiuni si plati escrow

Noul raport HP Wolf Security arata ca, în mod ironic, exista un fel de "onoare" între hackeri, deoarece infractorii cibernetici folosesc servicii de solutionare a litigiilor, obligatiuni în valoare de 3.000 de dolari pentru furnizori si plati escrow - totul pentru a se asigura ca tranzactiile sunt corecte, potrivit unui comunicat al HP Inc, remis, vineri, AGERPRES.

HP Inc. a lansat cel mai recent raport HP Wolf Security - "Evolutia criminalitatii cibernetice. Cum amplifica Dark Web amenintarile si cum putem riposta". Studiul arata ca existenta unor kituri malware de tipul "plug and play" faciliteaza mai mult ca niciodata lansarea atacurilor cibernetice. Sindicatele înfiintate de organizatiile de hackeri colaboreaza cu atacatori amatori pentru a viza companii si institutii, punând în pericol întreaga activitate online.

Echipa HP Wolf Security a colaborat cu Forensic Pathways pentru o investigatie de trei luni în Dark Web, în cadrul careia au fost analizate peste 35 de milioane de marketplaces si mesaje publicate pe forumurile infractorilor cibernetici, pentru a întelege modul în care acestia opereaza, câstiga încrederea victimelor si îsi creeaza reputatia.

Principalele constatari arata ca programele malware sunt ieftine si usor de gasit. Peste trei sferturi (76%) dintre reclamele malware listate si 91% dintre codurile care ofera atacatorilor controlul asupra sistemelor, profitând de erori software, se vând cu mai putin de 10 dolari. Costul mediu al acreditarilor compromise pentru Remote Desktop Protocol este de doar 5 dolari. Furnizorii vând produse la pachet, cu kituri malware de tipul plug and play, malware-as-a-service, tutoriale si servicii de mentorat, reducând astfel nivelul de pregatire si experienta pentru cei care vor sa lanseze atacuri complexe si tintite.

De fapt, doar 2-3% dintre infractorii cibernetici de astazi sunt programatori cu cunostinte avansate.

La fel ca în lumea comertului online legal, încrederea si reputatia sunt, în mod ironic, elemente esentiale si ale tranzactiilor în domeniul criminalitatii cibernetice. 77% dintre pietele online analizate, în care activeaza hackerii, solicita o garantie de vânzator - o licenta de vânzare - care poate costa pâna la 3.000 de dolari. 85% dintre acestea utilizeaza plati escrow, iar 92% au un serviciu de solutionare a litigiilor asigurat de o terta parte. Fiecare piata ofera scoruri de feedback pentru furnizori. De asemenea, infractorii cibernetici încearca sa fie cu un pas înaintea fortelor de ordine transferând reputatia de la un site la altul - în conditiile în care durata medie de viata a unui site Tor în Dark Net este de numai 55 de zile.

Programele software populare le ofera infractorilor cibernetici ocazia de a lansa atacuri: infractorii cibernetici încearca sa gaseasca în software lacune care sa le permita sa preia controlul asupra sistemelor, vizând erori si vulnerabilitati deja cunoscute. Printre exemple se numara sistemul de operare Windows, Microsoft Office, sistemele de gestionare a continutului web si serverele web si de e-mail. Kiturile care exploateaza vulnerabilitatile din sistemele de nisa au preturile cele mai mari (de obicei, între 1.000 si 4.000 de dolari). Zero Days, adica vulnerabilitatile care nu sunt înca cunoscute public, se vând cu zeci de mii de dolari pe pietele Dark Web.

"Din pacate, nu a fost niciodata mai usor sa fii un infractor cibernetic. La început, atacurile complexe necesitau abilitati, cunostinte si resurse serioase. Acum, tehnologia si expertiza sunt disponibile de la doar 5 dolari. Şi, fie ca este vorba de expunerea datelor companiei si ale clientilor, de întârzierea livrarilor sau chiar de anularea unei programari la spital, înmultirea atacurilor cibernetice ne afecteaza pe toti", precizeaza autorul raportului, Alex Holland - Senior Malware Analyst la HP Inc.

"Totul este despre ransomware, care a creat un nou ecosistem al criminalitatii cibernetice unde sunt recompensati cu o parte din profituri si jucatorii mai mici. Acest lucru faciliteaza lansarea de atacuri care cu greu pot fi contracarate, iar companiile si institutiile pe care ne bazam cu totii devin tinte", a adaugat Alex Holland.

HP a consultat un grup de experti din domeniul securitatii cibernetice si din mediul academic - inclusiv pe fostul hacker Michael "Mafia Boy" Calce si pe Dr. Mike McGuire - pentru a întelege cum a evoluat criminalitatea cibernetica si ce pot face companiile pentru a se proteja mai bine împotriva amenintarilor prezente si viitoare. Acestia au avertizat ca lumea ar trebui sa se pregateasca pentru campanii din ce în ce mai bine tintite si infractori cibernetici care folosesc tehnologii emergente, precum inteligenta artificiala.

Raportul include câteva recomandari, precum însusirea elementelor de baza pentru a reduce sansele infractorilor cibernetici. Adoptarea celor mai bune practici, cum ar fi autentificarea cu mai multi factori si gestionarea patch-urilor. Suprafata de atac trebuie redusa din principalii vectori, cum ar fi e-mailul, navigarea pe internet si descarcarile de fisiere. De asemenea, hardware-ul cu functia self-healing creste rezistenta în fata unui potential atac.

"Este necesara realizarea unui plan de actiune, inclusiv pentru cel mai rau scenariu. Riscul reprezentat de angajati si de parteneri poate fi limitat prin instituirea unor procese de verificare a securitatii furnizorilor si de educare a fortei de munca în ceea ce priveste securitatea cibernetica. Scenariile de raspuns la eventuale atacuri trebuie testate, pentru a putea identifica problemele si, astfel, îmbunatati masurile de securitate", sustine compania.

Criminalitatea informatica este un sport de echipa. De aceea, securitatea cibernetica trebuie sa fie la fel. Este important schimbul de informatii despre amenintari, în timp real. Astfel de informatii ajuta orice utilizator sa fie proactiv.

"Cu totii trebuie sa facem mai mult pentru a lupta împotriva masinariei tot mai sofisticate care este criminalitatea cibernetica. Pentru persoanele fizice, acest lucru înseamna ca oamenii trebuie sa devina constienti din punct de vedere cibernetic. Cele mai multe atacuri încep cu un click, asa ca este întotdeauna important sa analizati înainte de a da click. Dar, este si mai bine sa beneficiati de o plasa de siguranta prin achizitionarea de tehnologie care poate atenua efectele nedorite ale unui click gresit", spune Ian Pratt, Global Head of Security for Personal Systems la HP Inc..

"Pentru companii, este important sa fie pregatite si sa elimine cât mai multe cai comune de atac. Multe dintre cele mai comune categorii de amenintari, cum ar fi cele transmise prin e-mail si pe internet, pot fi complet neutralizate prin tehnici precum izolarea amenintarilor, reducând astfel foarte mult suprafata de atac a unei organizatii, indiferent de existenta unor vulnerabilitati care au fost sau nu remediate", adauga Pratt.