Un atac cibernetic masiv, cu ajutorul unor instrumente de hacking care ar fi fost furate de la Agenția Națională de Securitate din SUA (NSA) a lovit organizații din întreaga lume. În Germania a fost lansată o investigație.

Procurorii DIICOT au deschis un dosar penal in rem pentru infracțiuni contra siguranței și integrității sistemelor și datelor informatice, în legătură cu atacul cibernetic din ultimele zile.

Potrivit unor oficiali ai DIICOT, procurorii s-au autosesizat în acest caz și au deschis un dosar penal pentru săvârșirea infracțiunilor de acces ilegal la un sistem informatic (art. 360 Cp), alterarea integrității datelor informatice (art. 362 Cp) și perturbarea funcționării sistemelor informatice (art. 363 Cp), scrie Agerpres.

Procurorii așteaptă să primească informații de la SRI pe această temă, dar și ca instituțiile afectate să depusă plângeri penale.

***

Atacul cibernetic masiv declanșat vineri la nivel mondial a făcut "200.000 de victime, în special companii, în cel puțin 150 de țări", a declarat duminică, într-

un interviu pentru postul britanic de televiziune ITV, directorul Europol, Rob Wainwright, potrivit AFP.

"Desfășurăm operațiuni împotriva a circa 200 de atacuri cibernetice pe an, însă până acum nu am mai văzut un astfel de atac", a subliniat șeful Europol, oficiul european de poliție, conform Agerpres.

El a mai spus că cel mai probabil numărul victimelor va crește, când "oamenii se vor întoarce luni la muncă și își vor deschide calculatorul". Anchetatori și experți informatici internaționali încercau duminică să îi identifice pe hackerii care s-au aflat la originea atacului informatic, ce ar putea lovi din nou în zilele următoare.

+++

Printre cele 99 de țări vizate de atacul de tip ramsonware se numără și România. Momentan, se știe că au fost țintă ale atacului Ministerul de Externe și Uzinele Dacia Mioveni.

Atacul asupra MAE român a fost anunțat de cyberscoop.com, potrivit căruia un grup de hackeri - APT28 / Fancy Bear - ce are legături cu Rusia s-a dat drept reprezentant NATO pentru a trimite un val de emailuri de phishing către organizaţii diplomatice din Europa, inclusiv către Ministerul de Externe de la București.

În cursul zilei de vineri, SRI a anunţat că Centrul Național Cyberint, structură aflată în coordonarea sa, a reușit să contracareze tentativa de atac cibernetic derulată, cel mai probabil, de entitatea asociată grupului de criminalitate cibernetică APT28 / Fancy Bear. Acțiunea SRI s-a derulat la sesizarea Serviciului de Informații Externe.

Sâmbătă, activitatea a fost întreruptă parțial la Uzinele Dacia de la Mioveni, în urma unui atac cibernetic care a afectat unele dintre sistemele informatice, potrivit unui comunicat al companiei.

Măsura a fost luată pentru a preveni extinderea disfuncționalităților care, la prima vedere, sunt o consecință a atacului cibernetic ce a avut loc la nivel global, se precizează în comunicat.

Pe platforma de la Mioveni a fost convocată o celulă de criză care urmărește evoluția situației.

Atacul nu a afectat doar Dacia Mioveni, ci și uzinele Renault din Franța și Slovenia.

Producția a fost oprită în Franța și în Slovenia, a precizat un oficial al Renault S.A., potrivit AFP.

Probleme au fost și la Nuclearelectrica, dar conducerea a negat că ar fi avut legătură cu atacul cibernetic global.

Atacurile ransomware afectează orice dispozitiv conectat la Internet

Ministrul Comunicațiilor și Societății Informaționale, Augustin Jianu, a declarat, sâmbătă, pentru Agerpres, că atacurile ransomware, de tipul celui raportat recent de mai multe organizații din întreaga lume, afectează orice dispozitiv conectat la Internet și, implicit și România, însă nu are date privind instituțiile din țară care ar fi fost ținta acestei amenințări.

> **”Cea mai bună metodă de a contracara această amenințare este prevenția, și anume actualizarea sistemului de operare acum și, bineînțeles, a aplicațiilor pe care folosesc pe acel sistem de operare. De asemenea, să utilizeze un sistem antimalware puternic, fie și unul gratuit, decât nimic. În plus, să-și realizeze în mod repetat backup pentru datele sensibile și importante. Este foarte important de știut și faptul că atacurile cibernetice nu se propagă doar prin e-mailuri, ci și prin rețelele de socializare. Majoritatea acestor atacuri, de tip ransomware, sunt atacuri globale și afectează, repet, orice persoană conectată la Internet”,**

a explicat Augustin Jianu.

Producătorul român Bitdefender a precizat că WannaCryptor, folosit în atacul început vineri, e primul ransomware care se instalează fără implicarea utilizatorului.

Astfel, ransomware-ul convențional se răspândește prin emailuri cu documente periculoase atașate, browsere și exploit-uri în aplicatiile web, în timp ce atacul de vineri folosește o vulnerabilitate prezentă în majoritatea versiunilor sistemului de operare Windows.

Recomandările CERT-RO

Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) a atras atenția, într-o postare pe Facebook, asupra faptului că un atac de tip ransomware se răspândește cu rapiditate în Europa.

Specialiștii notează faptul că Microsoft a oferit deja o soluție de rezolvare a problemei, însă aceasta depinde de utilizatorii dispuși să-și actualizeze sistemul de operare.

”Un atac de tip #ransomware ce poarta denumirea «WannaCry» se răspândește cu rapiditate în Europa. Conform companiei de securitate Kaspersky Lab, atacatorii exploatează o vulnerabilitate cunoscută a sistemului de operare Windows, ce a fost publicată recent în mediul online de un grup de hackeri (Shadowbrokers). Microsoft a oferit un patch care soluționează problema încă din 14 martie, dar rezolvarea depinde de disponibilitatea utilizatorilor de a-și actualiza sistemul de operare”, informează CERT-RO.

Echipa CERT-RO recomandă aplicarea de urgență a update-ului, care poate fi descărcat de aici: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Suspiciuni privind Kaspersky

Specialiștii producătorului de soluții de securitate Kasperky Lab a anunțat că Rusia a fost de departe cea mai afectată de atacul de vineri, în timp ce România este pe locul 9 în topul țărilor lovite de hackeri. Producătorul de soluții de securitate cibernetică Avast a precizat că sâmbătă dimineața erau afectați peste 57.000 de utilizatori din 99 de țări.

Trebuie reamintit că, joi, responsabili cu rang înalt ai securității și serviciilor americane de informații și-au exprimat public temerile cu privire la gigantul din securitatea informatică Kaspersky Lab, din cauza presupuselor legături ale acestuia cu Moscova, relatează AFP.

Această societate privată cu sediul la Moscova propune antiviruși și alte software-uri menite să protejeze calculatoarele împotriva pirateriei, însă unii se tem că, din contră, aceste instrumente servesc la spionaj.

Ce ținte au mai fost vizate

ForcePoint Security Labs, o altă unitate de securitate informatică, evocă, la rândul său, "o campanie majoră de difuzare a unor emailuri infectate", cu circa cinci milioane de emaluri trimise în fiecare oră răspândind virusul numit WCry, WannaCry, WanaCrypt0r, WannaCrypt și Wana Decrypt0r.

Organizații în Spania, în Australia, în Belgia, Franța, Germania, Italia și Mexic au fost, de asemenea, afectate, potrivit analiștilor.

În SUA, compania de livrare a coletelor FedEx a recunoscut că a fost și ea afectată.

Ministerul de Interne rus a anunțat și el că a fost afectat de un virus informatic vineri, chiar dacă nu a precizat dacă este vorba despre același atac.

Aceste atacuri informatice au afectat în special Serviciul public de sănătate (NHS) din Marea Britanie, notează AFP, preluată de Agerpres.

Atac de tip ransomware

Centrul Național Spaniol criptologic (CCN) — divizie a serviciilor de informații însărcinată cu securitatea tehnologiei informației — a vorbit de un "atac masiv de tip ransomware", cryptoware, de tip WannaCry.

Atacul "atinge sistemele Windows criptând toate fișierele și pe acelea din rețelele partajate", a explicat CCN.

Ransomware este un tip de programe malware care blochează computerele victimelor sau le criptează datele, solicitând plata unei răscumpărări, în schimbul recuperării controlului asupra dispozitivului sau a fișierelor afectate.