Î.S. CENTRUL DE TELECOMUNICAŢII SPECIALE

CENTRUL PENTRU SECURITATEA CIBERNETICĂ CERT-GOV-MD

FII **INFORMAT**, RĂMÎI **PROTEJAT**.

August 2014

Buletin Informativ

Dragi colegi,

Centrul pentru Securitate Cibernetică CERT-GOV-MD prezintă buletinul informativ, ca parte a serviciilor sale proactive. Acest buletin compilează articole ce țin de securitatea în sectorul IT pentru luna august 2014 și are drept scop de a vă informa despre cele mai recente știri din domeniul securității informaționale, tendințe, sfaturi și ultimele descoperiri. Sperăm că aceste articole vă vor ajuta în activitățile dumneavoastră de zi cu zi, fie în cazul în care sunteți un specialist tehnic, sau un simplu utilizator de rețea.

FII INFORMAT, RĂMÎI PROTEJAT.
Echipa CERT-GOV-MD

Breșă de securitate identificată în Universal Serial Bus (USB)

Cercetătorii Karsten Nohl și Jakob Lell din organizația Security Research Labs, Berlin, au proiectat un firmware care controlează funcțiile USB, inclusiv chips-urile controler care conectează un USB de un PC. Astfel, cercetătorii au descoperit că acest firmware poate fi reprogramat cu un cod malițios, care este practic, imposibil de a fi detectat de programele antivirus moderne. Această deficiență de securitate a fost numită "BadUSB".

Universal Serial Bus este un standard industrial dezvoltat în mijlocul anilor 1990. Principalul avantaj al USB - este abilitatea de a conecta dispozitivele fără a fi nevoie de repornirea calculatorului - făcându-l cel mai utilizat standard pentru echipamentele portabile și periferice de cele mai diverse tipuri. Sistemul USB este folosit peste tot, acest fapt a sporit semnificativ impactul acestei deficiențe de securitate, deoarece "BadUSB" permite infectarea oricărui tip de dispozitiv, care se conectează la un PC folosind standardul USB, inclusiv tastatura, mouse-ul pentru calculator, precum și unitățile USB utilizate pentru a încărca telefoane și tablete.

Malware-ul, care folosește vulnerabilitatea „BadUSB", este capabil să imite o tastatură și să transmită semnale în modul în care sistemul de operare le va considera ca o activitate normală a utilizatorului, cum ar fi deschiderea fișierelor sau instalarea software-ului. Dispozitivul infectat poate falsifica, de asemenea, cardul de rețea și modifica setările calculatorului pentru a redirecționa traficul web la anumite site-uri.

"Am demonstrat cum un USB poate fi folosit pentru a compromite securitatea calculatorului, precum și posibilitatea creării unui virus USB ce nu poate fi detectat de programele antivirus moderne." - au precizat Karsten Nohl și Jakob Lell.

Cercetătorii menționează ca cel mai bun mod de vă proteja de BadUSB este prudență, astfel utilizatorii trebuie să se asigure că dispozitivul, care urmează fi conectat la PC, este unul de încredere.

Citiți mai mult pe:
http://www.dailymail.co.uk/sciencetech/article-2711802/Is-USB-drive-risk-Invisible-fundamental-flaw-lets-hackers-computers-discovered.html

În acest număr:

Sfaturi utile:

Entuziaștii din Regatul Unit au participat la provocarea în domeniul securității cibernetice "Assignment Flag Drive"

"Assignment Flag Drive" este unul dintre numeroasele concursuri organizate de Cyber Security Challenge în Marea Britanie, și sponsorizate de Sophos, companie de securitate cu sediu în Oxford. Scopul acestui eveniment este în primul rând identificarea și motivarea cetățenilor de a deveni profesioniști în securitatea cibernetică.

Conform scenariului concursului, un grup de teroriști fictivi a avertizat de un viitor atac planificat în Marea Britanie, prin plasarea unui video pe Facebook. Poliția a urmărit locația grupului terorist, dar în momentul în care au ajuns în sediul suspecților, teroriștii deja erau dispăruți, lăsând doar un hard disk criptat. Pe tot parcursul competiției participanții sunt nevoiți să utilizeze competențe IT și logica pentru a decripta hardware-ul suspect și a descoperi cui acest disc ar putea aparține.

Deși concursul a durat 2 zile, pe datele 15 și 16 august, rezultatele încă nu a fost făcute publice.

Citiți mai mult pe:
http://www.dailymail.co.uk/sciencetech/article-2715381/Could-YOU-crack-terrorist-s-hard-drive-Cyber-security-challenge-

"Când vine timpul să acționezi, timpul pentru a te pregăti deja a trecut" - Steven Roberts

Lista hărților cu atacurile cibernetice din toată lumea

Sandro Suffert fondatorul APURA Cyber Intelligence a creat pe blog-ul său o listă cu atacurile cibernetice globale, acestea sunt reprezentate într-o formă grafică pe hărți.

Lista, include următoarele surse:

1. Harta Războiului cibernetic în timp real de la Kaspersky
   http://cyberwar.kaspersky.com/
2. Topul zilnic al atacurilor DDoS de la Google
   http://www.digitalattackmap.com/
3. Harta Cyberfeed live Botnet de AnubisNetworks
   http://globe.cyberfeed.net/
4. Harta live IpViking de la Norse
   http://map.ipviking.com/
5. Honeypots din Proiectul Honeynet
   http://map.honeynet.org/
6. Hărți globale de activitate de la Arbor
   http://atlas.arbor.net/worldmap/index
7. Atacurile DDoS de la Shadowserver
   http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSMap
8. Harți cu activitatea malițioasă de pe Internet de la TeamCymru
   http://www.team-cymru.org/Monitoring/Malevolence/maps.html
9. Harta lumii de la F-Secure
   http://worldmap3.f-secure.com/

Citiți mai mult pe:
http://sseguranca.blogspot.com.br/2014/03/ten-sources-of-global-cyber-attack-maps.html

O privire mai minuțioasă la Adware

Mulți dintre utilizatori s-au obișnuit să folosească softuri gratuite pentru activitățile de zi cu zi. Între timp, tot mai mulți producători de softuri gratuite încep să includă în pachete de instalare, software suplimentar, care a fost numit "Adware". Printre acestea se enumeră: bare de instrumente, plugin-uri, icoane, imagini de fundal, motoare de căutare, precum și alte widget-uri ce țin de activitățile de zi cu zi. Deși cu ajutorul acestor programe producătorii câștigă bani pentru produsele lor, deoarece aceștia sunt plătiți pentru fiecare instalare a adware-ului, utilizatorii au devenit mai expuși la un riscurile de securitate, deoarece un adware ar putea veni cu un set de programe malițioase.

Un Adware poate dăuna calculatorului dvs. în următoarele moduri:

- Deoarece adware-ul se ascunde în software-ul gratuit pe care îl descărcați, dvs nu cunoașteți dacă sistemul rulează adware-ul atunci când începeți instalarea programei gratuite.
- Adware-ul poate avea diverse destinații, spre exemplu: bombardarea cu reclame pop-up (care pot aduce la site-uri nocive sau false), sau să promită eliminarea fictivă a adware-ului, sau oferirea unui antivirus fals, toate într-un final au scopul de a primi accesul deplin la calculatorul dvs.
- Spionarea asupra comportamentului de navigare și adunarea informațiilor private despre utilizator pentru a fi vândute ulterior părților terțe sau unor infractorii cibernetici.
- Adware-ul ar putea deturna click-uri fără știrea dumneavoastră sau fără a fi nevoie de pornirea freeware-ului descărcat, fapt care ar determina calculatorul Dvs să devină insuportabil de lent și instabil.
- În plus, adware-ul poate rula în scopul extragerii bitcoinuri-lor, ceea ce duce la un consum foarte mare de energie electrică.

Pentru a vă proteja împotriva adware-ului utilizați următoarele recomandări:

- Gândiți-vă dublu înainte de a descărca și instala unui software gratuit.
- Pentru a preveni descărcarea și instalarea adware-ului, citiți totul riguros înainte de a semna digital sau de oferi acordul la termenii și condițiile.
- Verificați sistematic calculatorul Dvs și scanați în mod regulat sistemele interne.
- Luați măsuri preventive de bază cum ar fi utilizarea unui software de securitate care vă va asigura protecția în mod constant.

Citiți mai mult pe:
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-exposed-part-2-when-adware-goes-bad-a-closer-look-at-adware/

Campanie de ciber-spionaj dezvăluită

Cercetătorii companiei Kaspersky Lab, susțin că au descoperit o campanie masivă de spionaj cibernetic, numită "Epic Turla", care viza instituțiile guvernamentale din circa 45 de țări ale lumii.

Hackerii colectau foile de calcul, documentele și e-mailurile care conțineau cuvintele cheie precum "NATO", "Budapest" și "dialogul energetic UE." Țintele erau predominant din Europa și Orientul Mijlociu, iar Franța avea cel mai mare număr de victime, circa 25. De asemenea au mai fost atacate țări precum: Germania, SUA, Iran, și chiar Rusia. În total au fost identificate aproximativ 500 adrese de IP virusate.

Victimele erau infectate în diverse moduri, printre care:

- Expedierea e-mailurilor de “spear-phishing” cu fișiere PDF virusate, aceste e-mailuri frauduloase au fost proiectate țintit pentru fiecare victimă în parte.
- Ingineria socială, cu scopul de a manipula utilizatorul făcându-l să instaleze benevol softul malware cu extensie ".SCR", uneori ambalat și în format RAR.
- Folosirea unui atac de tip „watering-hole”, care funcționa bazîndu-se pe faptul că atacatorul, identifica site-urile web vizitate mai des de victimă, după care le “sprăgea”, pentru a instala un program malware care, ulterior, infecta doar utilizatorii site-ului web în care era interesat atacatorul. În total au fost depistate peste 100 site-uri “sparte” cu scripturi periculoase, care se foloseau de vulnerabilitatea softurilor Java, Flash și Explorer 6,7,8.
- Este interesant faptul că în unele cazuri, atacatorii încercau să infecteze utilizatorii site-ului propunând acestora să-și instaleze un “update” pentru “Adobe Flash Player”.

Astfel, după ce Malware-ul se instalează pe calculator, acesta făcea legătura cu Comand & Control (C&C) de pe serverul răufăcătorului, pentru a primi instrucțiunile necesare. Printre instrucțiunile expediate se enumerau următoarele:

- Stabilirea parolelor pentru calculatoarele conectate prin rețea cu calculatorul infectat.
- Elaborarea unei liste de fișiere cu extensia ".doc".
- Căutarea fișierelor unde în denumire figurează cuvintele cheie "*NATO*.msg", "dialogului energetic UE*. *", "EU *.msg", "Budapest *.msg", etc.

După ce malware-ul a primit instrucțiunile, acesta începea instalarea modulelor adiționale, precum „keylogger”, „windows administration utility” și altele. În cazuri mai rare a fost depistat modulul cu denumirea "Carbon system", modulul dat reprezintă un sistem complex, orientat spre mascarea activității virusului și transmiterea neobservată a informației.

Pentru a preveni infectarea calculatorului dumneavoastră, este necesar să respectați următoarele recomandări:

- Nu accesați imaginile sau link-urile din e-mailurile dubioase. Un e-mail poate conține o imagine sau link, care la accesare va aduce utilizatorul pe un site malițios.
- Setați e-mailul dvs. în așa fel, încât acesta să vă afișeze e-mailurile în format de text simplu, și nu în format HTML, astfel veți diminua riscul să fiți trucați cu substituirea link-ului pe altul decât acel afișat în email.
- Asigurați-vă că email-urile partenerului dvs. sunt semnate digital, în scopul de a preveni falsificarea acestora;
- Aveți în vedere că este periculos să deschideți orice atașament, chiar și documentele Microsoft Word și PDF pot conține viruși, nu doar acele care au la sfârșit extensia de".exe".
- În timpul utilizării browser-ului: Nu uitați că mesajele Popup (Ferestrele popup) care cer actualizarea softului "Adobe Flash Player", "Java" sau a altor softuri, pot fi false. Din acest considerent, este important întotdeauna să închideți aceste ferestre, iar toate actualizările necesare trebuie instalate manual de pe site-urile oficiale ale producătorilor.
- Niciodată nu salvați parolele conturilor dvs. în browser-ele web, în cazul în care calculatorul dvs este virusat, acestea pot fi extrase foarte ușor.

Citiți mai mult pe:
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

Ghid pentru utilizarea tehnologiei Whitelisting

Institutul National de Standarde și Tehnologie a elaborat un proiect numit Publicația 800-167 "Ghid pentru utilizarea tehnologiei whitelisting".

Scopul acestei publicații este de a ajuta organizațiile să înțeleagă elementele de bază în utilizarea tehnologiei whitelisting și pașii ce țin de planificarea corectă a implementării acestei tehnologii.

Potrivit Publicației 800-167, tehnologia whitelist este o listă de aplicații și componente de aplicare (biblioteci, fișiere de configurare, etc) care sunt autorizate să fie prezente sau active într-un sistem în conformitate cu cerințele definite anterior.

Utilizarea tehnologiei whitelisting este destinată stopării activității programelor malițioase și a altor softuri neautorizate. Spre deosebire de alte tehnologiile de securitate, cum ar fi programele antivirus, care blochează activitatea recunoscută a softurilor malițioase și permite tuturor celorlalte softuri să activeze normal, tehnologia whitelisting este concepută altfel, aceasta permite activitatea doar programelor "bune" care le cunoaște și blochează restul programelor nerecunoscute.

În conformitate cu Publicația 800-167, organizația ar trebui să utilizeze următorii pași pentru a planifica și implementa tehnologia whitelisting:

1. Inițierea soluției. Prima fază presupune identificarea nevoilor curente și viitoare, precum: cerințele de performanță, funcționalitatea și securitatea.
2. Proiectarea soluției. Această activitate presupune crearea sistemului de management whitelist, politicii de cripto-grafie, și aspectele de securitate ale soluției în sine.
3. Implementarea și testarea unui prototip. Următoarea etapă presupune implementarea și testarea unui prototip al soluției.
4. Implementarea soluției. Odată testarea este terminată, soluția poate fi implementată în mediul de producție.
5. Administrarea soluției. Procesul de management ar trebui să includă întreținerea și suportul aspectelor operaționale.

Citiți mai multe pe:
http://csrc.nist.gov/publications/drafts/800-167/sp800_167_draft.pdf

Despre noi

În vederea executării prevederilor Hotărârii Guvernului Nr. 746 din 18.08.2010 "Cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat", în cadrul Î.S. "Centrul de telecomunicații speciale" a fost creat Centrul pentru Securitatea Cibernetică CERT-GOV-MD.

Punct centralizat de contact

CERT-GOV-MD este punctul central de raportare și coordonare privind incidentele de securitate în sistemele de comunicații și informatice, aflate în administrarea Centrului de telecomunicații speciale.

Pentru raportarea incidentelor cibernetice:

Trimiteți un e-mail la info@cert.gov.md
sau ne puteți contacta la telefon (+373 22) 820-900 (întrebați de CERT-GOV-MD) doar în zilele lucrătoare de la 8:00 la 17:00.

Găsiți-ne pe web:
www.cert.gov.md

FII **INFORMAT**, RĂMÎI **ROTEJAT**

Recomandări pentru efectuarea evaluării de securitate într-o organizație

Lenny Zeltser un expert în domeniul securității tehnologiei informaționale a dat recomandări cu privire la pașii care trebuie luați pentru evaluarea nivelului securității unei organizații.

Conform recomandărilor, managerii ar trebui să urmeze următoarele indicații:

1. ***Identificarea fluxurilor de date*** importate pentru a înțelege mai bine procesele de business ale organizației:
   a) Întâlniți-vă cu oamenii cheie și întrebați care sunt preocupările lor. Aceste persoane pot sprijini eforturile Dvs de îmbunătățire a securității mai târziu;
   b) Încercați sa înțelegeți proveniența datelor, destinația acestora și care sunt componentele de infrastructură care procesează aceste date.
   c) Întrebați despre cerințele contractuale care ar rezulta nevoia companiei de a proteja datele sale.
2. ***Examinarea Interacțiunii utilizator*** pentru a determina cum, cu cine și ce date sunt partajate de personal pe plan intern, cât și pe plan extern cu partenerii și clienții:
   a) Atrageți atenția la nivelul de acces al personalului la date: cine are dreptul doar la vizualizare, și cine are dreptul să modifice datele.
   b) Evaluați care sunt schimbările de acces necesare pentru a preveni modificările neautorizate aduse infrastructurii sau/și a datelor;
   c) Țineți minte că practicile slabe de securizare a informației in contextul partajării datelor operaționale de către angajații companiei pe plan intern, extern cu partenerii și/sau clienții, au adus la numeroase cazuri de scurgeri a informațiilor.
3. ***Examinați perimetrul rețelei*** pentru a explora căi de ieșire și pătrundere în rețea:
   a) Încercați să determinați care sunt punctele slabe care există în perimetrul rețelei;
   b) Verificați ce mecanisme există pentru a detecta și a bloca accesul neautorizat;
   c) Analizați situația în care una din componentele rețelei, presupunem firewall-ul de frontieră, nu a reușit să blocheze atacul, pentru estima urmările pentru mediul de producție, dacă acesta va rămâne nesecurizat;
   d) Examinați conexiunea de Internet, precum și orice legături directe cu partenerii și clienții dvs. Examinați ambele tipuri de conexiuni, wifi și prin cablu.
4. ***Evaluați serverele și stațiile de lucru*** pentru a detecta lipsă de patches-uri sau erori de configurare:
   a) Începeți cu serverele accesibile părților externe. Apoi, treceți la serverele interne.
   b) Nu uitați să evaluați starea calculatoarelor și laptop-uri, deoarece atacurile orientate spre softurile client-side, precum browser-ele web și aplicațiile add-ons sunt foarte răspândite și de succes.
5. ***Analizați aplicațiile*** pentru a determina punctele slabe care ar putea favoriza un atacator să compromită mecanismele de securitate a companiei, și să acceseze datele fără nici o autorizație:
   a) Luați în considerare vulnerabilitățile care pot exista în aplicațiile personalizate accesibile părților terțe și utilizatorilor interni;
   b) Acordați o atenție deosebită la aplicațiile bazate pe web tehnologii, în ultimii ani acestea au fost o țintă răspândită pentru atacatori.

Citiți mai mult pe:
http://zeltser.com/security-assessments/assessments-de-mijlocii-firms.html