Î.S. CENTRUL DE TELECOMUNICAŢII SPECIALE

CENTRUL PENTRU SECURITATEA CIBERNETICĂ CERT-GOV-MD

FII **INFORMAT**, RĂMÎI **PROTEJAT**.

Noiembrie 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 noiembrie 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

În acest număr:

Atenție la atacuri de tip STARTTLS downgrade

Doi ingineri de la Golden Frog (furnizorul internațional de servicii IT), au descoperit că unii furnizori de servicii Internet șterg informația despre suportul opțiunii STARTTLS din traficul de email care astfel forțează serverul să transmită emailul spre Internetul public în formă de text simplu, în cazul în care aceasta este supus monitorizării sau interceptării.

STARTTLS este o extensie folosită la scară largă pentru protocoale de comunicare de text simplu, care permite transmiterea securizată a mesajelor de e-mail, între serverele de trimitere și primire. În circumstanțe ordinare, înainte ca mesajul să fie transmis, clientul verifică dacă serverul destinatar suportă criptarea din mesaj. Dacă acesta suportă criptarea - este inițiată o sesiune TLS în caz contrar, mesajul va fi transmis prin-un text simplu. Un atac de tip STARTTLS downgrade are loc atunci când un atacator modifică răspunsul serverului, astfel încât să nu conțină o opțiune STARTTLS. Problema este următoarea: utilizatorul nu va fi notificat că mesajul a fost trimis necriptat, ce pune în pericol confidențialitatea și integritatea mesajului.

Cu toate că nu este întotdeauna posibil să preveniți atacurile de tip STARTTLS downgrade, se recomandă să utilizați Pretty Good Privacy (PGP) sau Secure / Multipurpose Internet Mail Extensions (S /MIME) pentru criptarea e-mailului și semnarea digitală a mesajului, în scopul de a rămâne securizat în mediul virtual.

Citiți mai mult pe:
https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks

Membrii Grupului Informal de Lucru OSCE s-au întâlnit pe data de 7 noiembrie 2014, pentru a discuta implementarea setului de măsuri de consolidare a încrederii (CBM)

Întâlnirea, organizată de Președinția Elvețiană OSCE, a avut loc la Viena, Austria, și a reunit experți în securitatea informațională și reprezentanți din peste 50 de țări.

CBM sunt măsurile concepute pentru reducerea riscurilor în scopul de a spori transparența, a reduce percepția eronată, escaladarea, și a crește cooperarea și stabilitatea interstatală în domeniul securității cibernetice. Setul inițial de măsuri CBM a fost adoptat în 2013. Statele au convenit de asemenea să se întâlnească o dată pe an, în scopul de a rezuma rezultatele și pentru a discuta etapele viitoare de dezvoltare a CBM.

În timpul întâlnirii, participanții au evaluat eforturile securității cibernetice la nivel sub-regional și au negociat dezvoltarea unui al doilea set de măsuri CBM.

Citiți mai multe pe:
http://www.osce.org/cio/126475

"Pe măsură ce lumea devine tot mai interconectată, este responsabilitatea fiecăruia să asigure securitatea spațiul cibernetic". - Newton Lee, savant în domeniul informaticii.

Cazul CryptoPHP. Administratorii de sistem sunt ținta unor atacuri de tip inginerie socială

Echipa de securitate din Fox-IT – companie olandeză de securitate informațională, a descoperit un pericol, denumit CryptoPHP, care înșela administratorii de sistem prin instalarea unui backdoor pe serverul lor.

Autorii amenințării găzduiau câteva site-uri web care propuneau teme piratate și plugin-uri „gratuite" pentru sistemul de management al conținutului Joomla, WordPress și Drupal. După ce tema sau plugin-ul malițios a fost instalat, acesta stabilea o conexiune criptată cu serverul de comandă și control pentru a primi instrucțiunile ulterioare.

Actualmente CryptoPHP este folosit pentru a insera link-uri în text care duc spre anumite pagini web. Aceasta a permis autorilor softului să mărească ratingul link-urilor inserate în cele mai populare motoare de căutare.

Estimativ CryptoPHP a compromis mai mult de 20 000 de site-uri web.

Administratorilor de sistem le este recomandat să utilizeze următoarele scripturi pentru a depista infecția CryptoPHP: https://github.com/fox-it/cryptophp/tree/master/scripts

Citiți mai mult pe:
https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf

Wirelurker: o nouă eră în software malițios pentru iOS

Echipa de cercetare Palo Alto Networks a descoperit un program dăunător care vizează dispozitivele iOS conectate la calculatoarele Mac infectate. Malware-ul a fost numit "Wirelurker", deoarece se răspândește prin intermediul cablului USB.

WireLurker a fost folosit pentru a trojanizarea aplicațiilor piratate Mac, încărcate din App Store Maiyadi - site bine cunoscut pentru găzduirea aplicațiilor premium piratate pentru Mac, iPhone și iPad. Victimele descărcau aceste aplicații, le instalau pe sistemele OS X și le executau. Odată pornit malware-ul executa transparent codul de intrare WireLurker, mai apoi răspândea fișierele malware executabile, biblioteci dinamice și fișierele de configurare, și într-un final rula aplicația piratată.

După instalare WireLurker monitoriza orice dispozitiv iOS conectat prin USB la calculatorul infectat și instala aplicațiile malițioase pe dispozitiv, indiferent dacă acesta avea jailbreak sau nu.

Interesant este faptul că malware-ul utilizează metode de atac nevăzute anterior pe platformele iOS:

- Acesta este capabil să genereze automatizat aplicații iOS malițioase, prin înlocuirea fișierelor de tip binar;
- Poate infecta aplicațiile iOS instalate similar cu un virus tradițional;
- Instalează aplicații terțe pe dispozitivele iOS care nu au jailbreak prin provizionarea de întreprindere.

Mai jos găsiți recomandările noastre pentru întreprinderi și utilizatori, în scopul de a preveni infectarea cu virusul sus menționat sau/și atenua acesta și a alte aplicații malițioase similare iOS:

- Instalați o protecție de securitate sau antivirus pentru sistemul Mac OS X și păstrați aplicațiile actualizate;
- În secțiunea "Security & Privacy" a panoului de preferințe OS X, asigurați-vă că opțiunea "Allow apps downloaded from Mac App Store (or Mac App Store and identified developers)" este setată;
- Nu descărcați și nu rulați aplicațiile sau jocurile Mac din magazinele App Store terțe, site-uri de download sau alte surse care nu prezintă încredere:
- Păstrați versiunea iOS a dispozitivului Dvs actualizată;
- Nu acceptați profiluri necunoscute a unor oarecare companii de provizionare, cu excepția cazului când de exemplu, birou de ajutor IT corporativ vă recomandă în mod explicit să faceți acest lucru;
- Evitați alimentarea dispozitivul iOS prin încărcătoarele de la sursele nesigure sau necunoscute;
- Nu este recomandat să efectuați jailbreak a dispozitivului Dvs iOS.

Citiți mai mult pe:
https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Analiza pieței negre a programelor malware în Brazilia

Compania Japoneză specializată în crearea softurilor de securitate Trend Micro Inc., a publicat un studiu recent care analizează situația curentă, prețurile și trendurile pieței negre a programelor malițioase din Brazilia.

Raportul a dezvăluit că piața tenebră braziliană a programelor malițioase de regulă reprezintă o postare pe site-urile Facebook, YouTube, Twitter, Skype, sau WhatsApp unde sunt propuse spre comercializare produse și servicii ilegale. De asemenea s-a constatat că piața programelor malware din Brazilia actualmente este specializată mai mult pe domeniul bancar. Din acest motiv există o ofertă foarte mare a diferitor softuri malițioase precum Trojan bancar, verificator ai cardurilor de credit, cryptere și altele. Unele oferte includ și instrumente care au fost create în special pentru atacuri împotriva produselor și serviciilor locale. De asemenea, piața neagra de malware din Brazilia este unica în lume care oferă servicii de training pentru viitorii criminali cibernetici.

Un criminal cibernetic poate procura următoarele produse/servicii oferite de piața neagră braziliană:

- ***Trojan Bancar***. Acesta este creat în special pentru a intercepta credențialele cardurilor de credit sau/și a redirecționa plățile spre criminalul cibernetic. Pentru a reuși aceasta, softul de tip Trojan Bancar, folosește tehnici precum otrăvirea Sistemului de nume de domene, ferestre false a browser-ului web, sau modul malițios specializat denumit - Boware, care poate modifica codul de bare al chitanței spre plată a magazinului online în felul în care banii vor fi transferați spre atacator și nu spre vânzătorul destinat. Prețurile pentru seturile Bolware pentru construirea Trojanului Bancar oscilează între 155$ - 386$
- ***Crypter***. Crypterele sunt soft-uri specializate pentru a modifica malware-ul în așa mod încât acesta să nu fie depistat de antivirus. Crypterele care previn toate produsele existente de securitate în detectarea malware-ului sunt considerate "100% complet nedetectabile (FUD)." Dacă lucrează împotriva la câteva soluții de securitate, acestea sunt disponibile pe piață sub denumirea de " Cryptere parțiale". Prețul pentru Crypterele FUD oscilează între 19$ și 39$ pentru licență de 1 lună.
- ***Verificator ai cardurilor de credit***. Un astfel de program funcționează în felul următor: o mică sumă de bani este sustrasă din cont pentru a verifica dacă numărul de card este valid și eligibil pentru tranzacții. Prețul mediu pentru astfel de soft se încadrează între 31-135$ în dependență de limitele cardului de credit.
- ***Pagini de Phishing***. Paginile de Phishing permit criminalilor cibernetici furtul de date personale, redirecționarea victimelor spre paginile originale și transmiterea informației furate prin email atacatorului cibernetic. Prețul pentru pagini de Phishing în mediu este de 39$.
- ***Rețelele sociale: fani/vizualizări/like-uri***. Din motiv că numărul de vizualizări, fanii sau nr. de like-uri este un factor cheie care influențează impactul postării, tweet-ului sau video-ului, precum și rezultatele în motorul de căutare, piața tenebră braziliană a soft-urilor malițioase oferă fani contra plată. Prețul pentru like-uri Facebook variază între 8$ pentru 1000 like-uri și 62$ pentru 10 000 like-uri. Fanii Instagram costă în mediu de la 35$ pentru 5000 fani. 200 de abonați la YouTube costă 8$, același preț este și pentru 1000 de vizualizări YouTube sau 1000 fani Twitter.

Piața neagră braziliană oferă de asemenea și servicii precum:

- ***Verificarea rezistenței malware-ului față de soft-urile de securitate***. Criminalii cibernetici trebuie să se asigure că creațiile lor malițioase sunt nedetectabile pentru soluțiile de securitate existente în prezent. Autorii fraudelor cu experiență utilizează rar serviciile publice de scanare a softului, deoarece de obicei aceste servicii transmit fișierele scanate la companiile de securitate pentru analiză. Astfel, criminalii cibernetici oferă servicii de verificare a malware-ului la doar 12$ pentru licență de o lună.
- ***Serviciul de SMS spam***. Unii spammeri utilizează servicii outsourcing de spam la prețuri de 155$ pentru 5.000 de mesaje text și 1.159$pentru 100.000 mesaje.
- ***Servicii de training***. Cea ce diferențiază piața neagră din Brazilia de celelalte piețe este faptul că aici se oferă training-uri pentru oricine își dorește să devină criminal cibernetic. Majoritatea cursurilor sunt focusate pe programarea scripturilor nedetectabile și training-uri de fraude. Atacatorii cibernetici vând video materiale cu instrucțiuni, iar în caz de necesitate cumpărătorul poate primi suport prin Skype.

Citiți mai multe pe:

http://www.trendmicro.ca/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf

"Darkhotel", capcană pentru șefii de mari companii cazați la hoteluri de lux

Echipa de cercetare Kaspersky a publicat un raport cu privire la amenințările informaționale existente, acest raport a dezvăluit apariția unei noi amenințări avansate ce vizează clienții a mai multor hotele de lux.

Atacatorii acționează când victimele se conectează la rețeaua Wi-Fi a hotelului, introducând numărul camerei şi numele de familie pentru logare. Metoda de atac implica redirecționarea la o pagină Web malițioasă pentru a ademeni victimele să instaleze programe false precum GoogleToolbar, Adobe Flash player sau Windows Messenger și a infecta calculatorul cu o programă spyware.

De asemenea, s-a constatat că doar anumiți oaspeți au fost ținta infractorilor, astfel aceștia vizau doar funcționarii guvernamentali și personalul din industria de apărare, ceea ce înseamnă că atacatorii știau data exactă și destinația călătoriei. Odată ce atacul a reusit toate urmele erau șterse. Se estimează că înainte de a fi descoperită, amenințarea a existat de mai mult de cinci ani.

Utilizați următoarele sfaturi pentru a rămâne securizat în timpul călătoriilor:

- ***Înainte de a călători***: hotărâți din timp de ce dispozitive și date aveți de fapt nevoie, străduiți-vă să limitați la maxim ceea ce luați cu Dvs; nu luați cu Dvs dispozitivele care le utilizați de zi cu zi; utilizați conturile și dispozitive temporare precum un laptop ieftin sau un telefon mobil prepaid cumpărat pentru unică folosință.
- ***În timpul călătoriei dumneavoastră***: nu utilizați rețeaua din acest hotel sau oarecare altă rețea publică, sau calculatoare care nu prezintă încredere pentru nevoile de afaceri; nu trimiteți informații sensibile; site-urile pe care le vizitați (chiar camere de hotel) pot fi monitorizate.
- ***După ce vă întoarceți din călătorie***: ștergeți toate informațiile personale din dispozitivele și conturile temporare; schimbați parolele - faptul care va face informația furată inutilă; resetați dispozitivele temporare la setările prestabilite de fabrică pentru a elimina orice tip de malware instalat.

Citiți mai multe pe:
http://securelist.com/blog/research/66779/the-darkhotel-apt/

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**

Ghid de securitate pentru utilizatorii iOS. Partea 1

Acest ghid este destinat utilizatorilor finali care posedă dispozitive de tip iOS 7.x or iOS 8.x și doresc să facă schimbări benefice în practicile de securitate în dispozitivele deținute, pentru a îmbunătăți experiența generală în ceea ce privește securitatea și siguranța.

Instrucțiuni de îmbunătățire a securității. Mai jos sunt prezentați pașii care urmează a fi respectați pentru a îmbunătăți nivelul securității pe dispozitivul Dvs.

- ***Utilizați doar ultima versiune a softului***. Bug-uri și vulnerabilități de securitate sunt inevitabile, de aceea este important să se utilizați cea mai recentă versiune de software disponibilă pentru dispozitivul dumneavoastră. Multe dispozitive vă vor informa când o actualizare este disponibilă, însă Dvs puteți iniția și manual o verificare a actualizărilor. Pentru a verifica dacă dispozitivul rulează cea mai recentă versiune de software mergi la "Settings" -> "General" -> "Software Update"; Notă: Este preferabil să utilizați o rețea Wi-Fi pentru a descărca actualizările în scopul de a economisi traficul internet.
- ***Activați parolă pe dispozitivul Dvs***. Acest lucru previne accesarea datelor de pe dispozitiv în lipsa Dvs. Pentru a seta parolă navigați la "Settings" -> "Passcode" (sau "Touch ID & Passcode");
- ***Activați blocarea cartelei SIM***. Această funcție împiedică un hoț să abuzeze de serviciu mobil și să vă utilizeze banii din contul Dvs mobil. Pentru a seta acest serviciu, accesați "Settings" -> "Phone" -> "SIM PIN" (va trebui să introduceți parola implicită pentru SIM, care de obicei este "1111"). După ce serviciul SIM LOCK este activat alegeți "Schimbare PIN", pentru a vă asigura că nimeni nu poate trece de această măsură de securitate. Asigurați-vă că rețineți noul cod PIN.
- ***Activați pe dispozitivul Dvs auto-blocarea***. Auto-blocarea presupune blocarea automata a ecranului dispozitivul după ce acesta nu a fost utilizat o perioadă de timp. Această funcție împiedică accesarea datelor dumneavoastră. Pentru a activa auto-blocarea navigați la "Settings" -> "General"-> "Auto-Lock";
- ***Activați restricțiile***. Această funcție vă permite să preveniți achiziția aplicațiilor fără introducerea în prealabil a unei parole. Acest lucru poate fi util pentru controlul parental sau în cazul în care, nu doriți ca rudele, care pot accesa dispozitivul, să facă mult decât ar trebui. Pentru a activa această funcție mergeți la "Settings" -> "General" -> "Restrictions";
- ***Atenționare despre situ-rile frauduloase în browser-ul Safari***. Safari are capacitatea de a vă avertiza în cazul în care un site web este suspectat a fi un corupt sau un site fraudulos conceput pentru a vă convinge să divulgați informații personale. Pentru a seta această funcție accesați "Settings" -> "Safari", bifați “on” alături de “Fraudulent Website Warning”.

Citiți mai mult pe:
https://bluebox.com/ios-user-security-guide/