Buletini mujor për vetëdijësimin mbi sigurinë e përdoruesve të kompjuterëve

OUCH!

NË KËTË BOTIM..

- Çka është Heartbleed?
- Çka duhet të bëj?
- Kujdes nga sulmet Phishing

Heartbleed – Pse të brengosem?

Përmbledhje

Të hënën më 7 prill, një mangësi serioze është identifikuar në një nga implementimet më të njohura të protokolit SSL, të quajtur OpenSSL. SSL është një protokol shumë i rëndësishëm i përdorur nëpër gjithë internetin. SSL jo vetëm që bën enkriptimin e komunikimeve online, por ndihmon të siguroheni që po lidheni me faqe të besueshme kur bëni blerje apo banking online. Në këtë broshurë ne do të japim një përmbledhje të thjeshtë se çka nënkupton kjo dobësi dhe çka duhet të bëni që të vetëmbroheni.

Botuesi i ftuar

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) është udhëheqës i shkencëtarëve në CSRgroup Computer Security Consultants. Ai është poashtu bashkëautor i kurseve Memory Forensics (FOR526) dhe Malware Reverse Engineering (FOR610) në SANS.

Çka është Heartbleed?

Mangësia me emrin Heartbleed i jep mundësinë një hakeri të lidhet në një webserver dhe të mbledhë informata të ndieshme, që mund të nënkuptojnë edhe emrin e përdoruesve dhe fjalëkalimet. Nëse një sulmues ia del të mbledhë informata të tilla, ata mund ta përdorin atë informacion për t'u qasur në ndonjë nga llogaritu tuaja duke përdorur emrin e përdoruesit dhe fjalëkalimin e njejtë. Edhepse kjo mangësi ka ekzistuar qysh para 2 vjetësh, vetëm me 7 prill u zbulua dhe u bë publike. Heartbleed nuk i afekton kompjuterët me Windows apo Mac; por ndikon në web faqe në Internet që ju mund të përdorni, sikurse janë Facebook dhe Gmail. Për t'i komplikuar gjërat, nuk e afekton çdo web faqe në Internet, por shumë prej tyre.

Ju mund të verifikoni nëse një web faqe që përdorni është apo ishte i cënueshëm nga kjo mangësi duke përdorur faqen Lastpass dhe një aplikacion në linkun https://lastpass.com/heartbleed/.

Çka duhet të bëj?

Për t'u vetëmbrojtur janë disa hapa që duhet të ndërmerren. Këta hapa jo vetëm që do të ndihmojnë kundër dobësisë Heartbleed, por do t'ju ndihmojnë nga shumë sulme tjera në të ardhmen.

- Së pari, ndërroni fjalëkalimet në webfaqet që ju e dini që kanë qenë të cënueshme dhe janë rregulluar ndërkohe, duke filluar nga llogaria juaj më e rëndësishme. Nëse nuk e dini se a ka qenë një webfaqe e cënueshme, ndërrojeni fjalëkalimin gjithsesi. Kjo është një kohë e përshtatshme që ta ndryshoni fjalëkalimin dhe të rrisni sigurinë online.
- Sigurohuni që kur e ndryshoni fjalëkalimin tuaj ju përdorni një fjalëkalim të fortë dhe të vështirë për t'u qëlluar. Gjithashtu nëse webfaqja ofron shërbimin e ashtuquajtur "verifikimi në dy hapa" (ang. two-step verification), atëherë aktivizojeni. Ky është një hap shtesë që ndihmon ta bëni këtë llogari online më të sigurt.
- Sigurohuni që përdorni fjalëkalime të ndryshme për çdo llogari online që keni. Në këtë mënyrë nëse ndodh njëra nga web faqet dëmtohet atëherë llogaritë tjera janë të sigurta. Nuk mund t'i mbani mend të gjithë fjalëkalimet

Jam hakuar, çka të bëj?

tuaja? Urime, kjo do të thotë që ju përdorni fjalëkalime të forta. Ne ju rekomandojmë që të shfrytëzoni këtë rast që të filloni të përdorni një menaxhues fjalëkalimesh (ang. Password manager) që ruan të gjithë fjalëkalimet tuaja. Këto janë aplikacione shumë të dobishme që jo vetëm e thjeshtësojnë aktivitetin tuaj online, por i bëjnë shumë më të sigurta.

- Mos i harroni klientët e emaileve. Nëse klienti juaj, si p.sh. Outlook ose Apple Mail, përdor SSL për t'u lidhur me serverin e emaileve, ju duhet t'i ndërroni edhe ata fjalëkalime.

Nëse keni nevojë për më shumë informata mbi këto hapa, shihni seksionin Burimet në fund të kësaj broshure.

Hapi më i mirë të vetëmbroheni është të ndërroni fjalëkalimet në llogaritë kryesore dhe sigurohuni që përdorni fjalëkalime të veçanta dhe të forta për secilën llogari.

Kujdes nga sulmet Phishing

Për fat të keq, njerëzit dashakëqinj janë oportunistë. Ata e dinë që Heartbleed ka qenë teme kryesore në lajme dhe shumë njerëz, duke ju përfshirë edhe juve, kanë lexuar për të. Duke ditur këtë, ata do të krijojnë emaila mashtrues që duken sikur janë nga faqe të besueshme që ju përdorni (sikurse janë bankat online apo dyqane). Mund edhe të pretendojnë që janë nga kompani sigurie që ofrojnë aplikacione falas për të kontrolluar rrezikun nga Heartbleed.

Kjo mënyrë (që zakonisht quhet phishing) nuk është ndonjë risi. Sulmuesit provojnë të ju mashtrojnë që të klikoni në ndonjë link që ju dërgon në ndonjë webfaqe të dëmshme ose t'ju detyrojnë të hapni ndonjë dokument të bashkangjitur të infektuar. Nëse bini viktimë e këtyre sulmeve, kompjuteri juaj mund të infektohet. Për t'u mbrojtur, nëse keni nevojë të ndërroni fjalëkalimin, atëherë thjesht shkruajeni emrin e webfaqes (që shpesh njihet me emrin URL) në shfletuesin e Internetit dhe ndërrojeni fjalëkalimin online. Në këtë mënyrë ju e dini që po lidheni në një web faqe të besueshme.

Burimet

Cilat faqe janë të cënueshme?:	https://lastpass.com/heartbleed/
OUCH! Fjalëkalimet:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Menaxhuesit e fjalëkalimeve:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Verifikimi në dy hapa:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Detajet teknike:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano