

OUCH!

NË KËTË NUMËR..

- Çfarë është malware
- Kush i krijon
- Si të mbrohemi

Çfarë është Malware

Sfondi

Me siguri i keni dëgjuar për termat si virus, trojan, ransomware apo rootkit kur diskutohet për sigurinë kibernetike. Të gjithë këto fjalë përshkruajnë të njëjtën gjë: lloje programesh me të cilët kriminelët infektojnë kompjuterët dhe pajisjet. Termi që përdoret rëndom për t'i përmbledhur të gjitha këto fjalë është malware. Ky buletin shpjegon çfarë është malware, kush e krijon dhe pse, si edhe si të mbrohemi.

Botuesi i ftuar

Lenny Zeltser punon NCR Corp me mbrojtjen e operacioneve IT të klientëve dhe jep mësim në SANS Institute se si të luftohen malware-t. Lenny është aktiv në Twitter me emrin [@lennyzeltser](https://twitter.com/lennyzeltser) dhe shkruan një blog sigurie në zeltser.com.

Çfarë është malware?

E thënë thjeshtë, malware është softuer - program kompjuteri - që përdoret për të kryer veprime dashakeqe. Në fakt, termi malware është kombinim i fjalëve malicious dhe software (dashakeq dhe softuer). Kriminelët kibernetikë instalojnë malware në kompjuterët apo pajisjet tuaj që të marrin nën kontroll ato ose informacionin që përmbajnë. Gjithashtu, ju spiunojnë se ku lundroni në internet, ju vjedhin fjalëkalimet apo skedarët, apo përdorin sistemin tuaj për të sulmuar të tjerët. Malware mund t'ju pengojë hapjen e skedarëve tuaj dhe sulmuesi mund t'ju vendosë një gjobë që t'jua kthejë.

Shumë njerëz kujtojnë se malware është problem vetëm për kompjuterët Windows. Malware mund të infektojë çdo pajisje, edhe kompjuterët Mac, smartphone-t apo tabletët. Sa më shumë kompjuterë dhe pajisje të infektojnë, aq më shumë para mund të bëjnë kriminelët kibernetikë. Prandaj, të gjithë janë nën rrezik, edhe ti.

Kush e krijon

Malware nuk krijohet më nga thjesht kuriozë apo hakera amatorë, por nga kriminelë kibernetikë të sofistikuar. Qëllimi i tyre është të fitojnë para nga kompjuterët apo pajisjet e infektuara, me shitjen e të dhënave që ju kanë vjedhur, me dërgimin e-maileve spam, me sulme për refuzim shërbimi, ose me zhvatje. Personat që krijojnë, shpërndajnë dhe përfitojnë nga malware mund të jenë individë që veprojnë vetëm, organizata kriminale të strukturuar, madje edhe organe shtetërore.

Çfarë është Malware

Sot, personat që krijojnë malware të sofistikuar e kanë bërë këtë si punë me kohë të plotë. Madje, pasi krijojnë malware, shpesh ua shesin individëve apo subjekteve të tjera, duke i furnizuar këta “klientë” me mbështetje dhe përditësime periodike.

Si të mbroheni

Masa më e zakonshme është instalimi i softuerëve anti-virus të blerë nga shitës të besuar. Këto softuerë që shpesh quhen anti-malware synojnë të diktojnë dhe të ndalojnë malware. Ama, anti-virusi e ka të pamundur të bllokojë apo të heqë të gjitha programet dashakeqe. Kriminelët kibernetikë po zhvillojnë maslware gjithnjë e më novatorë dhe të sofistikuar që të mos diktohen. Nga ana tjetër, fabrikuesit e anti-viruseve përforcojnë produktet e tyre me aftësi të reja për të diktuar malware. Kjo është bërë si një luftë, ku secila palë përpiqet të tregohet më e zgjuar.

Fatkeqësisht, të këqijtë janë shpesh një hap më para. Meqë anti-virusi nuk ju garanton sigurinë e plotë, më poshtë keni disa hapa shtesë se si të mbroheni:

- Kriminelët kibernetikë shpesh infektojnë kompjuterët apo pajisjet duke shfrytëzuar dobësitë e këtyre të fundit. Sa më i fundit të jetë softueri juaj, aq më pak dobësi kanë sistemet tuaja dhe aq më vështirë infektohen. Prandaj, sigurohuni që sistemet operative, aplikacionet dhe pajisjet tuaja janë aktivizuar që të instalojnë përditësimet automatikisht.
- Një mënyrë e zakonshme infektimi është edhe krijimi i aplikacioneve të rreme për celularë, postimi në internet dhe shkarkimi e instalimi nga njerëzit. Prandaj, shkarkoni dhe instaloni vetëm nga burime të besuara. Gjithashtu, instaloni aplikacione celulari që janë postuar në internet prej një kohë të gjatë, që janë shkarkuar nga shumë njerëz dhe që kanë feedback pozitiv.
- Në kompjuter, përdor llogari standard me privilegje të kufizuara dhe jo llogari të privileguara si “administrator” apo “root”. Kjo nuk lejon shumë lloje malware që të instalohen vetë në pajisjet tuaja. Kriminelët shpesh ju mashtrojnë që ju ta instaloni vetë malware. Për shembull, ju dërgojnë një e-mail me dokument bashkëngjitur, që ngjan sikur e dërgon banka apo një mik. Por, sapo e klikoni, aktivizoni pa dashje instalimin e malware në sistemin tuaj. Nëse një e-mail duket shumë urgjent, ose shumë i bukur për të qenë i vërtetë, ai mund të jetë sulm. Jini dyshues. Frika ruan vreshtin.



Mbrohu prej malware: (i) jini skeptik ndaj mesazheve të dyshimta; (ii) përditëso pajisjet; (iii) instalo versionin më të fundit të antivirusit, kur është e mundur.

Çfarë është Malware

- Bëjini rregullisht sistemit dhe skedarëve back up në shërbimet cloud, ose ruajini në drive pa akses në internet.
- Kështu i mbron materialin, nëse malware tenton t'i inkriptojë apo t'i fshijë. Backup shpesh është e vetmja mënyrë që të shpëtoni materialet pas një infektimi me malware.

Mbrojtja më e mirë është ta mbani softuerin sa më të përditësuar, të instaloni anti-viruse cilësorë nga shitës të mirënjohur dhe të jeni vigjilentë ndaj tentativa për infektim.

Mëso më shumë

Regjistrohuni në buletin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen

<http://www.securingthehuman.org>.

Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyesë profesioniste e gjuhës angleze në OSBE.

Burimet

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Securely Using Mobile Apps:	https://securingthehuman.sans.org/ouch/2015#january2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

OUCH! botohet nga SANS Securing The Human dhe shpërndahet nën licencën [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Lejohet ta shpërndani këtë buletin ose ta përdorni për programet tuaja vetëdijësuese, për sa kohë nuk e modifikoni përmbajtjen e buletinit. Për përkthimet apo më shumë informata, ju lutemi na kontaktoni në ouch@securingthehuman.org.

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



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.org/gpl