AtomBombing - novi(?) vektor napada na Windowse

Nedugo nakon objave vijesti o desetljeće starom sigurnosnom propustu u Linuxovu kernelu, istraživačka tvrtka Ensilo objavila je otkriće dosad neviđenog vektora napada na Microsoft Windowse: AtomBombing [1] kojeg, kako tvrde autori, antivirusni programi i sigurnosne aplikacije još uvijek ne znaju prepoznati, a još manje spriječiti. U srcu napada su atomske tablice [2] koje, iako im naziv sugerira nuklearnu namjenu, nisu ništa drugo već jednostavne (atomske, dakle) tablice koje u sebi sadrže parove informacija: niz znakova (podatak) i 16-bitni integer koji je pokazatelj na niz znakova. Ništa više i ništa manje od toga.

Windowsi (od verzije 2000) koriste atomske tablice za različite namjene, a jedna od njih je i razmjena informacija iz tablica pomoću atomskih brojeva (16-bitnih integer brojeva) kao ključa: sustav tako ubrzava razmjenu informacija među procesima upućujući jednostavnije brojeve umjesto kompleksnijih nizova znakova. Osim samog operacijskog sustava i njegovih atomskih tablica različite namjene, svaka aplikacija može definirati i koristiti svoju privatnu atomsku tablicu, no za komunikaciju informacija sa drugim aplikacijama treba koristiti globalnu, koju nudi operacijski sustav.

I to je grm u kojem, istraživači tvrde, leži zec: spretnom manipulacijom globalne atomske tablice napadač može unijeti informaciju koja sadrži maliciozni kod kojeg zatim "podvali" nekoj legitimnoj aplikaciji na izvršavanje tako što je "nagovori" da prihvati sadržaj koji se nalazi pod atomskim brojem kojeg je napadač dobio unošenjem malicioznog koda u globalnu atomsku tablicu.

Naravno, nagovoriti aplikaciju da prihvati tuđu informaciju pod tuđim atomskim brojem nije trivijalno, no izvedivo je zloupotrebom APC [3] poziva, preciznije zloupotrebom nedokumentiranog *NtQueueApcThread* poziva: kako to u blog [4] postu lijepo dokumentiraju autori, direktnim korištenjem nedokumentiranog poziva umjesto standardnog napadački program može napadnutom podmetnuti maliciozni kod kao niz znakova iz jedne od pozicija u globalnoj atomskoj tablici.

Samo ubacivanje malicioznog koda pomoću globalne atomske tablice nije dovoljno da napadnuti program natjera na na njegovo izvršavanje, radi ugrađenog sigurnosnog sustava DEP [5] kojeg Windows koristi kako bi spriječio upravo ovakve napade: sve što je definirano u bloku memorije označenom za podatke bit će tretirano kao podatak, nikad kao izvršni kod. U teoriji, dakle, sustav bi trebao biti zaštićen od ove vrste napada.

No, tu u igru ubacujemo tehniku razvijenu upravo za zaobilaženje ovih sigurnosnih metoda: ROP [6], odnosno *Return-oriented Programming*, koja lukavo koristi postojeći kod u računalu kako bi se, probranim izvršavanjem povratnih instrukcija u legitimnom kodu aplikacije - izvršio maliciozni kod koji bi inače bio nedostupan.

Maliciozni program koji želi izvršiti AtomBombing napad treba prvo pronaći odgovarajuću poziciju u napadnutom programu, podmetnuti mu maliciozni kod kroz globalnu atomsku tablicu, te spretnom ROP manipulacijom natjerati žrtvu da maliciozni kod izvrši.

Što uspješan napad donosi napadaču, a što odnosi žrtvi? Za razliku od DirtyCOW napada na Linuxu, AtomBombing ne omogućuje napadaču dobivanje većih privilegija od onih koje mu sustav uruči; drugim riječima ovaj propust ne može zaobići UAC [7] i napadač ne može dobiti administratorske ovlasti.

Autori ipak ističu kako ovaj napad nije nimalo bezazlen jer može poslužiti za preuzimanje nadzora nad drugim aplikacijama, pa napadač tako može inicirati MITB [8] (Man-In-The-Browser) napad kojim maliciozna aplikacija može preuzeti nadzor nad preglednikom, zaobilazeći uobičajene sigurnosne rutine poput TLS-a ili 2- ili 3-faktorne autentifikacije; drugim riječima, trenutno najpouzdaniji načini zaštite privatnosti i podataka u preglednicima posve su transparentni napadaču koji se ovakvim napadom uspije domoći kontrole nad napadnutim procesom.

Pažljiviji (ili paranoičniji) čitatelj ovdje će odmah pomisliti na on-line bankarstvo. Tu se krije velika opasnost od ove vrste napada - napadač može ciljano usmjeriti napad na preglednik kako bi sačekao da korisnik pokrene bančinu on-line aplikaciju i zatim prisluškivao ili čak u ime korisnika zadavao financijske transakcije; pri tome korisnik ne mora biti svjestan te zle rabote jer mu je preglednik pod kontrolom malicioznog koda lako može zatajiti. Drugi primjer kojeg autori navode je mogućnost krađe korisnikovih lozinki spremljenih u napadnutom pregledniku i njihovo slanje, u *plaintext* formatu, napadačevom poslužitelju - koristeći isti taj preglednik.

Slično kao i DirtyCOW napad za Linux, ovaj napad zahtjeva izvršavanje lokalnog koda na računalu, pa ga je (zasad) nemoguće izvesti s udaljenog mjesta; naravno, obzirom da se velika većina sigurnosnih incidenata ionako događa kad korisnik pokrene nešto što nije trebao, ne smijemo ovaj propust smatrati teorijskom prijetnjom - osim ako vaša računala zaista nemaju niti jednog korisnika.

Slično kao i DirtyCOW, i AtomicBombing je zapravo vrlo stara stvar jer Windowsi već dugo vremena koriste atomske tablice; no, za razliku od Linuxova propusta koji je namjerno ignoriran (tj. proglašen više teorijskom nego praktičnom prijetnjom u vrijeme otkrića, pa smjerno zaboravljen), atomske tablice su dio funkcionalnosti operacijskog sustava i njihov problem je arhitekturalne naravi: dizajn nije uzeo u obzir ovakve akrobacije s kodom, tim više što je DEP zaštita vrlo efikasna u sprečavanju mnogih *owerflow* napada. No, stvari su se promjenile pojavom ROP programiranja kao protumjere i atomske tablice ponovo su postale zanimljiv vektor napada.

Microsoft još nije izdao zakrpu za ovaj problem; ona će svakako doći, vjerojatno u vidu odgovarajućih izmjena u samom operacijskom sustavu, a kako je riječ o fundamentalnoj funkcionalnosti sustava bit će zanimljivo vidjeti na koji će se način Microsoft otkloniti ovaj propust, a da pritom ne potrga nešto važno. U međuvremenu, ne preostaje nam ništa drugo već da pazimo kako mi ili naši korisnici ne bi pokreneli kakav zločest program: zasad nas baš ništa neće upozoriti na ovu malicioznu aktivnost.

Stoga je vrlo važno napomenuti ovo: trenutno je jedini način zadržavanja sigurnosti računala onemogućavanje skidanja i pokretanja aplikacija s Interneta. I tako sve do sigurnosne nadogradnje koja će riješiti ovaj problem. Sigurnosni utorče, kad ćeš više doći?!?!

sri, 2016-11-02 09:40 - Radoslav Dejanović**Vijesti:** Windows [9]
Kategorije: Sigurnost [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1698

Links
[1] http://blog.ensilo.com/atombombing-a-code-injection-that-bypasses-current-security-solutions
[2] https://msdn.microsoft.com/en-us/library/windows/desktop/ms649053(v=vs.85).aspx
[3] https://msdn.microsoft.com/en-us/library/windows/desktop/ms681951(v=vs.85).aspx
[4] https://breakingmalware.com/injection-techniques/atombombing-brand-new-code-injection-for-windows/

[5] https://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
[6] https://en.wikipedia.org/wiki/Return-oriented_programming
[7] https://en.wikipedia.org/wiki/User_Account_Control
[8] https://en.wikipedia.org/wiki/Man-in-the-browser
[9] https://sysportal.carnet.hr/taxonomy/term/12
[10] https://sysportal.carnet.hr/taxonomy/term/30