Ransomware za vaše Office 365 korisnike

 Da moderne tehnologije nisu imune na stare probleme pokazuje novi maliciozni softver koji napada korisnike Officea 365 koristeći za to – vjerujem da vas ovo ipak neće iznenaditi – makro naredbe!

Prema izvješću [1] tvrtke Avanan riječ je o danas iznimno popularnom *ransomware* tipu malicioznog koda koji se izvršava kao Office makro na računalu korisnika i čini što ransowmare već čini: enkriptira korisničke datoteke AES256 enkripcijom i za ključ traži od žrtve 1.24 Bitcoina.

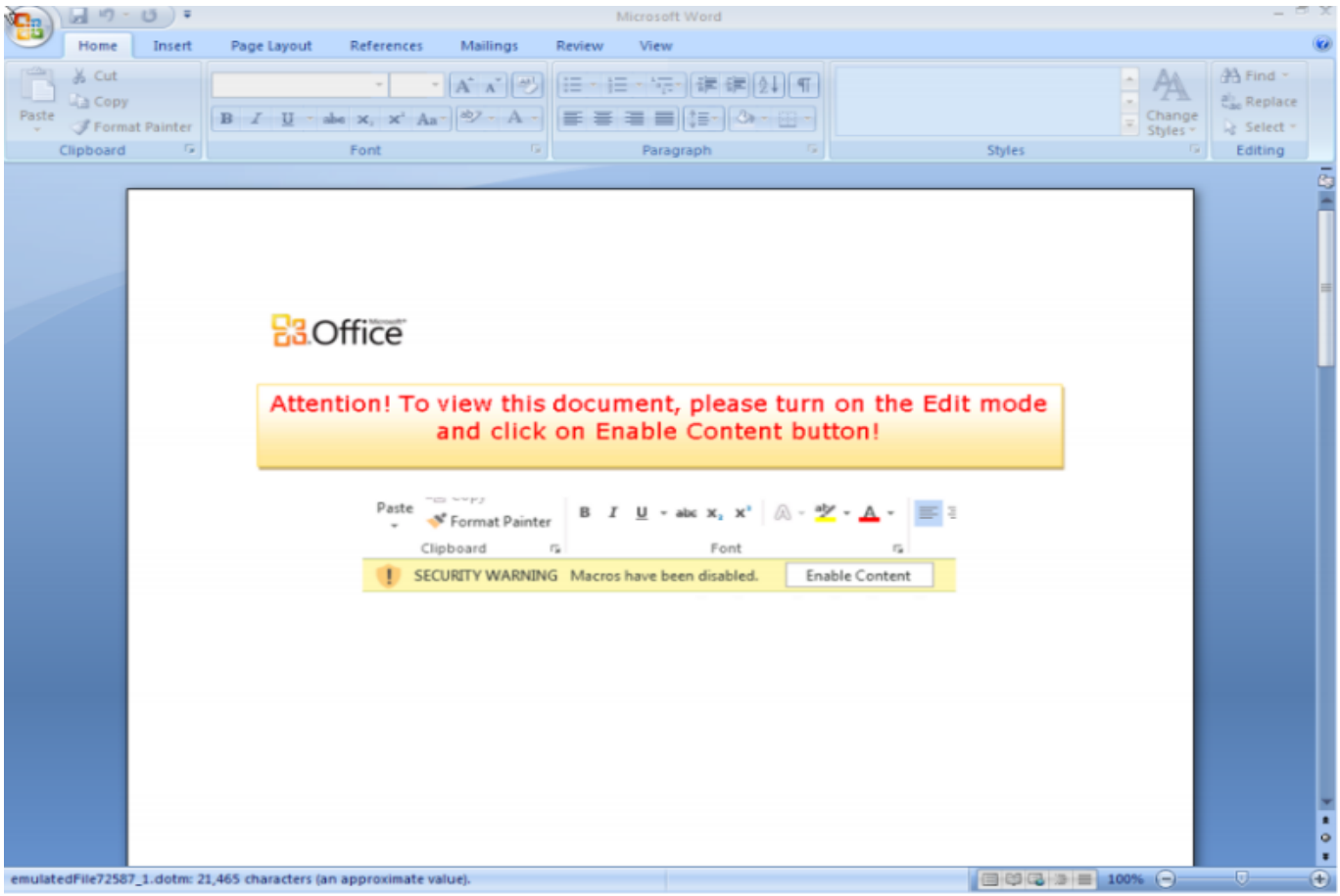
Kako ucjenjivanje ne poluči uvijek rezultate, čini se da su autori Cerbera [2] odlučili žrtvu upozoriti ne samo odgovarajućom porukom na zaslonu, već mu pritom zaraženo računalo i izdeklamira ucjenjivačku poruku, jasno i glasno, kako bi o nesretnom događaju bio obavješten ne samo korisnik, već i njegovi kolege u uredu.

Ovaj je napad svjež, vrlo neugodan, ali srećom relativno ga je lako otkloniti jer ovisi o dva koraka o kojima je moguće (ispravljam se: o kojima je uglavnom moguće) educirati djelatnike i upozoriti ih na sigurnosne opasnosti.

Prvi korak je otvaranje zaraženog privitka e-mail poruke. Educirani djelatnici znat će da je ovo najčešći način prijenosa malicioznog koda, pa (vjerojatno) neće otvarati privitke nepoznatih pošiljatelja.

Ako se ipak dogodi da korisnik otvori zaraženi privitak, morat će još odobriti izvršenje makro naredbe: obzirom da su makro skripte ipak relativno rijetke u svakodnevnom poslovanju i koriste ih tek poneki napredni korisnici, razumno je zabraniti [3] automatsko izvršavanje makro naredbi na nivou organizacije. U tom slučaju, maliciozni će napadač u dokumentu ostaviti veliko upozorenje korisniku da treba omogućiti izvršavanje makro naredbi – što je toliko očito sumnjivo da bi tek najnaivniji korisnik poslušao.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr



Lako je, dakle, osujetiti zle namjere ovog softvera imate li dobro educirane djelatnike i isključeno izvršavanje makro naredbi u Office alatima.

Možda bi nas profesionalce začudilo korištenje tako starog trika kao što su makro naredbe u Office dokumentu, no sam Microsoft je priznao [4] kako napadi makro skriptama iznose 98% svih napada na Office platformu, uključujući i Office 365.

I tu se krije još jedna informacija koju bi bilo vrlo korisno prenijeti korisnicima: zabluda je da korištenje aplikacija u oblaku automatski štiti korisnika i njegovo računalo: u ovom je primjeru više nego očito kako lokalna zaštita - i nadasve edukacija - ne mogu biti zamijenjeni kupnjom usluge u oblaku.

sri, 2016-06-29 19:40 - Radoslav Dejanović**Vijesti:** Sigurnost [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1658

Links
[1] http://www.avanan.com/resources/attack-on-office-365-corporate-users-with-zero-day-ransomware-virus

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

[2] http://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/
[3] https://www.communications.gov.au/what-we-do/internet/stay-smart-online/alert-service/update-your-security-settings-microsoft-office-avoid-new-macro-based-security-attacks%20
[4] http://www.infoworld.com/article/3047267/security/microsoft-adds-macros-lockdown-feature-in-office-2016-in-response-to-increasing-attacks.html
[5] https://sysportal.carnet.hr/taxonomy/term/13

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr