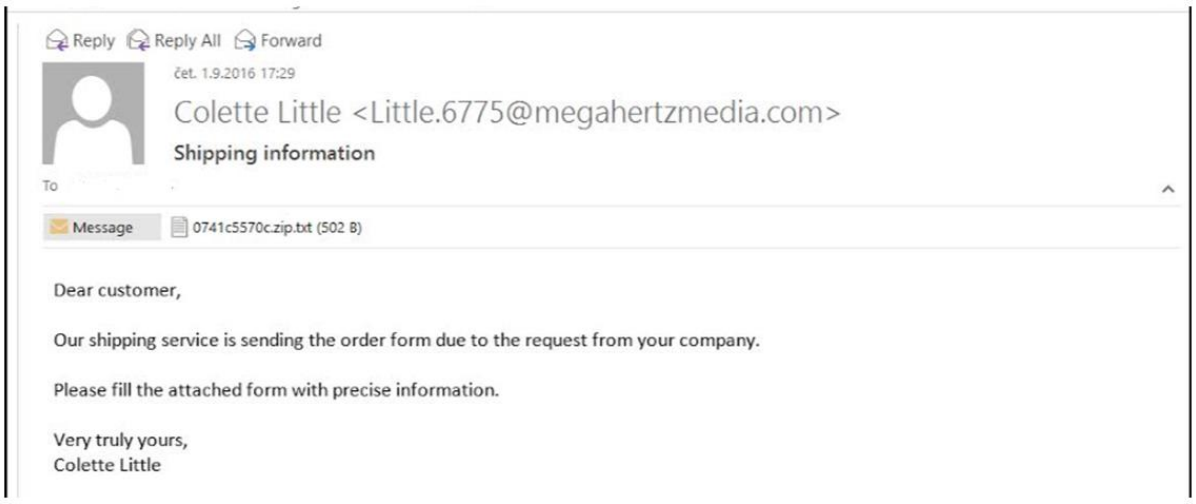
Kako prepoznati zlonamerna sporočila

V zadjem času se tudi v Sloveniji s svetlobno hitrostjo širijo različice Ransomware računalniških virusov , ki kriptirajo datoteke na vašem računalniku, kar posledično pomeni, da ostanemo brez vseh dokumentov, glasbe, slik, ter ostalih datotek.. Kljub temu, da je bilo o njem že vilko povedanega, ne mine dan, ko nebi bilo novih okužb. Virus se največkrat širi preko elektronske pošte v zip priponkah, wordovih dokumetih ali excelovih dokumentih. Vsakič, ko v poštni nabiralnik prejmete priponko od osebe, ki jo ne poznate, ali od znane osebe vendar priponke ne pričakujete, bodite pozorni. V zip datotekah so navadno majhne datoteke tako imenovanega formata java ali vbs skript, ki ob kliku zažene izvajanje virusa. Pri wordovih in excellovih datotekah pa velja posebna previdnost če od vas zahtevajo zagon Makrojev. Ko odprete dokument in imate privzete nastavitve programa, da se makroji ne zaženejo avtomatsko, še niste okuženi. Škodljivi dokumenti so narejeni tako, da je vsebina wordovega ali excelovega dokumenta popolnoma neberljiva ali pa se slike ne prikažejo. Ob zagonu makrojev se praviloma vsebina pravilno prikaže, vendar ste s tem zagnali virus. Antivirusni sistemi, ki so naloženi na vašem računalniku velikokrat tega ne bodo zaznali. Virus deluje tako, da se ob zagonu poveže na oddaljen strežnik, preko katerega prenese škodljivo datoteko na vaš računalnik in jo zažene. Ta začne kriptirati datoteke. Ko kriptira vse se pojavi obvestilo, da so datoteke kriptirane ter navodila za plačilo odkupnine v digitalni valuti bitcoin. Prve različice so zahtevale okoli 1 bitcoin, pri novejši različici virusa pa zahtevajo že 3 bitcoine kar znaša približno 1500€. Po plačilu naj nam bi spletni kriminalci posredovali unikatni ključ, s katerim bi lahko dešifrirali dokumente in tako pridobili podatke nazaj.

Konkreten primer

Poglejmo si konkreten primer, kako lahko ugotovimo ali gre za legitimno sporočilo ali za sporočilo z zlonamerno vsebino. V elektronski predal smo prejeli naslednje sporočilo:



Poglejmo si lastnosti sporočila:

1. Sporočilo prihaja iz domene megahertzmedia.com

2. Elektronski predal na domeni je Little.6755
3. Ime pošiljatelja je Colette Little
4. Sporočilo od vas zahteva, da izpolnite vsebino v priponki

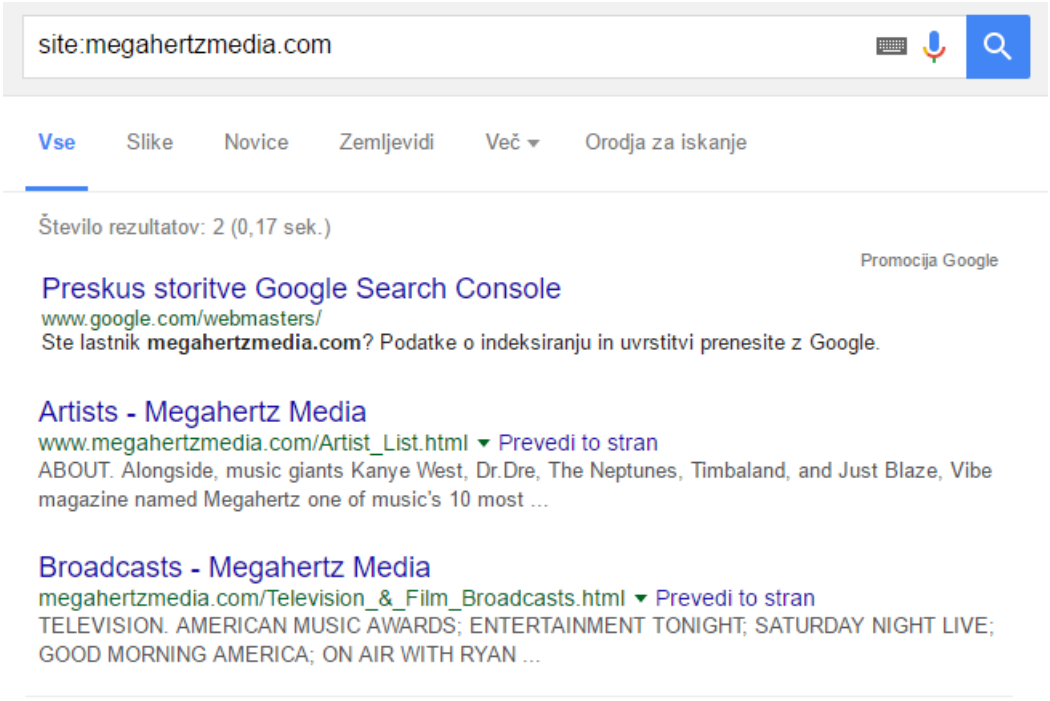
Iz zgoraj naštetega lahko povzamemo, da **neznan** pošiljatel od vas zahteva **klik** na priponko. **V tem trenutku so izpolnjeni vsi pogoji za rdeč alarm in premislek o tem ali bomo na priponko kliknili ali ne**.

Kako prepoznati lažno domeno

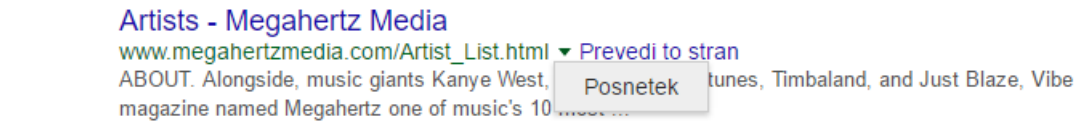
Vse akcije, ki jih bomo izvajali, so namenjene temu, da preverimo pristnost domene pošiljatelja, v našem primeru spletne strani »megahertzmedia.com« . V prvem koraku priporočam, da v spletnem iskalniku Google vpišemo slednjo iskalno poizvedbo:

- **Site:megahertzmedia.com**

S parametrom »site« Googlu povemo, naj nam prikaže samo rezultate iz podane domene.



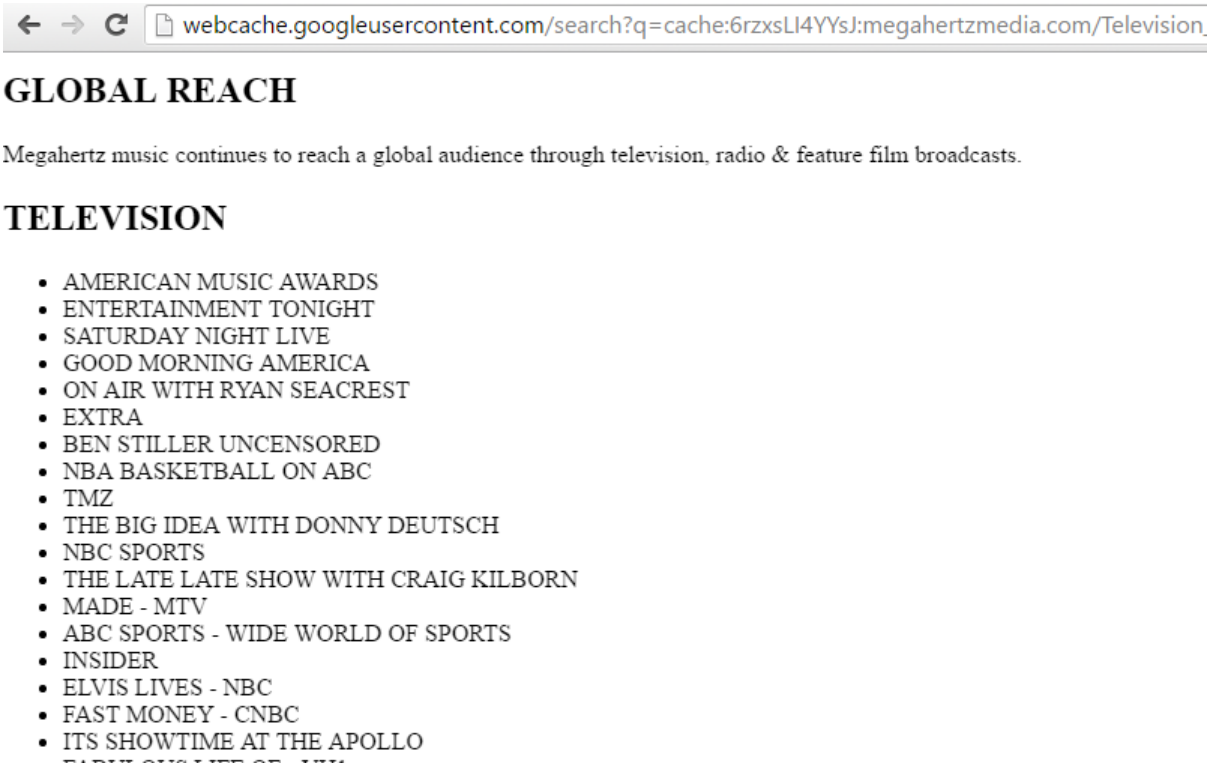
Prikažeta se nam dva zadetka. V veliko primerih lahko že iz opisa v Googlu presodimo ali je vsebina kakorkoli povezana z nami ali ne. V kolikor še vedno ne uspemo presodit kaj se skriva za spletno stranjo, nam Gogle v veliko primerih ponuja posnetek spletne strani. Dobimo ga tako, da kliknemo na zeleno puščico na zadetku in nato »Posnetek«.



Ne klikajte na neznane povezave v elektronski pošti

Po vsej verjetnosti se je kdo med branjem vprašal zakaj iščemo posnetke spletnih strani in ne preprosto kliknemo na povezavo in tako vidimo kaj se skriva na spletni strani. Klikanje po neznanih in potencialno sumljivih spletnih straneh je lahko nevarno, saj se lahko okužimo z mimohodom. Več na to temo pa v naslednjih člankih.

V našem primeru iz posnetka spletne strani pridobimo spodnjo vsebino:

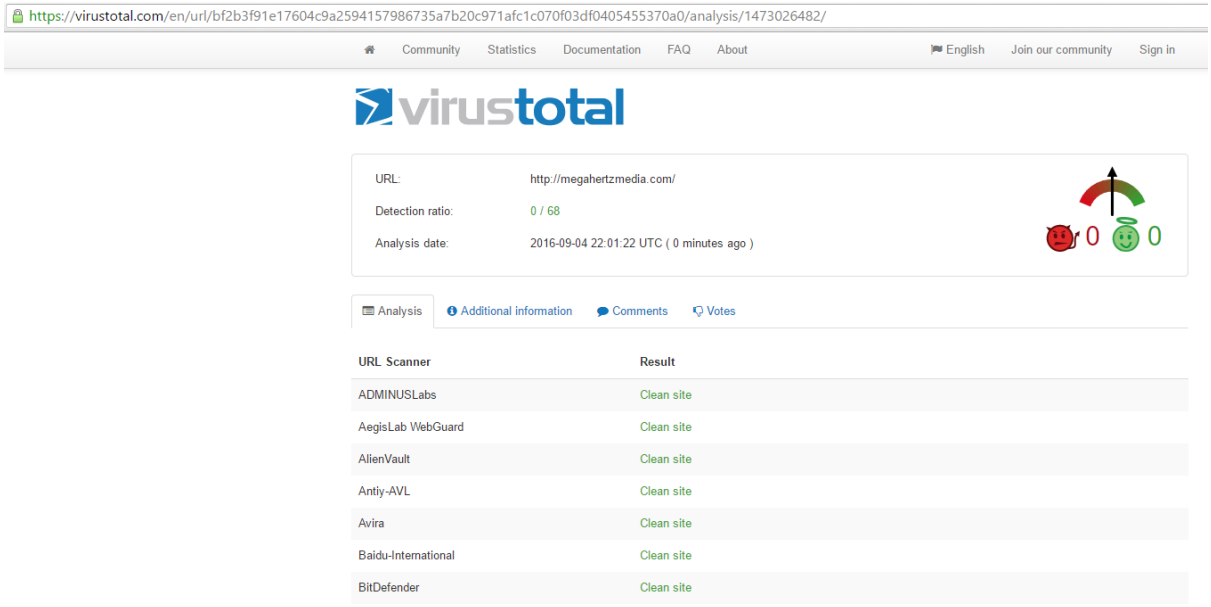


Iz vsebine lahko vsak prejemnik sporočila približno sklepa ali je vsebina sporočila kakorkoli povezana s spletno stranjo in posledično z nami, ali gre za nelegitimno sporočilo.

Kako preveriti, ali se na spletni strani nahaja virus

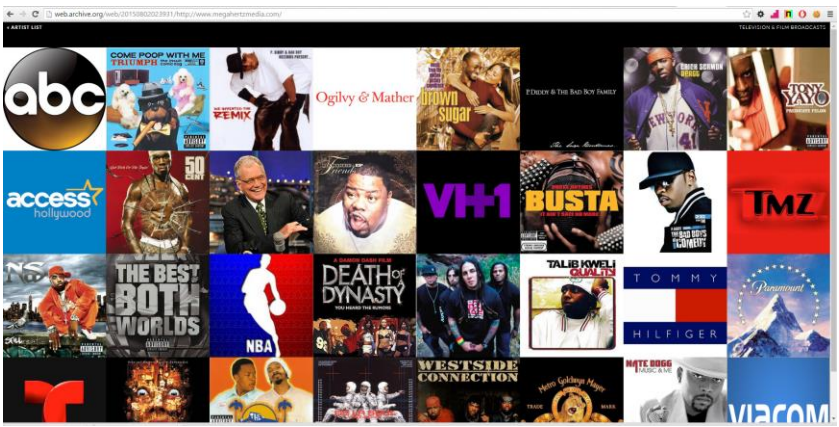
Če vas kljub vsemu še vedno zanima kaj se skriva na spletni strani, vam priporočam spletno stran www.virustotal.com . Gre za spletno stran, preko katere lahko z 68-imi antivirusnimi programi pregledamo spletno stran oziroma datoteko. Vsak izmed antivirusnih programov bo dal svoj odgovor ali je zaznal na strani zlonamerno aktivnost ali ne.

V našem primeru je vseh 68 antivirusnih programov odgovorilo, da je spletna stran brez virusev in jo je načeloma varno obiskati. **Vendar pozor, to nikakor ne pomeni, da je brez virusov tudi sporočilo, ki smo ga prejeli v elektronski predal.**



S tem testom smo dokazali le to, da je stran brez virusov in jo lahko obiščemo v spletnem brskalniku. V našem primeru ob obisku strani ugotovimo, da je prazna, in na njej ni vsebine.

Iz tega lahko ponovno sklepamo, da je elektronska pošta vprašljiva in nam potrdi sum, da jo ne odpiramo. Če se je kdaj nahajalo kaj na spletni starni in kaj, imamo možnost vpogleda v spletni arhiv (Way back machine). Gre za storitev, kjer se shranjujejo kopije spletnih strani. Iz te storitve (web.archive.org) lahko končno uotovimo kako je izgledala spletna stran:



Velikokrat je pri raziskovanju spletnih strani zanimiv tudi podatek kdo ima domeno v lasti. Iz spletnih zapisov »whois« Pridobimo informacijo, da je domena registrirana pri registrarju Godaddy, ki je eno izmed največjih ameriških podjetjij za nakup spletnih domen. Podatki organizacije pa so : Domains by proxy, kar pomeni, da je domena registrirana kot anonimna. Lastnik domene je plačal približno 5$, da so v spodnji tabeli podatki ki jih je zapolnilo podjetje godaddy in ne pravilni podatki lastnika domene.

Showing results for: MEGAHERTZMEDIA.COM

Original Query: megahertzmedia.com

Contact Information

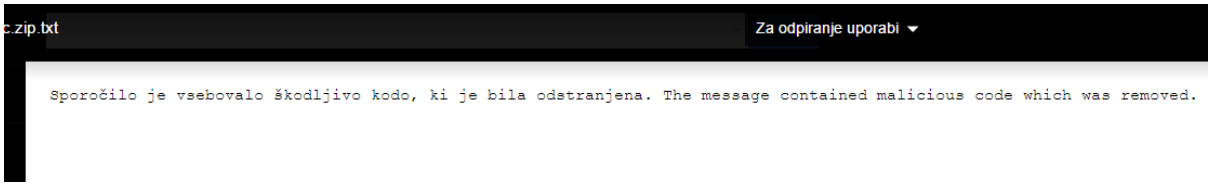
Registrant Contact	Admin Contact	Tech Contact
Name: Registration Private	Name: Registration Private	Name: Registration Private
Organization: Domains By Proxy, LLC	Organization: Domains By Proxy, LLC	Organization: Domains By Proxy, LLC
Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US	Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US	Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US
Phone: +1.4806242599	Phone: +1.4806242599	Phone: +1.4806242599
Ext:	Ext:	Ext:
Fax: +1.4806242598	Fax: +1.4806242598	Fax: +1.4806242598
Fax Ext:	Fax Ext:	Fax Ext:
Email:MEGAHERTZMEDIA.COM @domainsbyproxy.com	Email:MEGAHERTZMEDIA.COM @domainsbyproxy.com	Email:MEGAHERTZMEDIA.COM @domainsbyproxy.com

To je še en indic, kipostavlja pod vprašaj legitimnost sporočila, ki smo ga prejeli v elektronski predal.

- Spletna stran je prazna, na njej ni vsebine
- Vsebina, ki je bila na spletni strani ni nikakor povezana z nami in/ali sporočilom ki smo ga prejeli
- Iz vsebine na spletni strani ni mogoče pridobiti nikakršnih podatkov podjetja, kontaktne številke, naslova, kontaktne osebe,...
- Domena je registrirana kot anonimna

Vojna na spletu

Med spletnimi kriminalci in organizacijami, ki skrbijo za varnost na internetu vlada nenehna vojna. Tako kot v fizičnem svetu, tudi za virtualni svet velja, da so spletni kriminalci vedno korak v prednosti. Zato tudi prihaja do tega, da se takšna vsebina pojavi v vašem elektronskem predalu kljub temu, da imamo postavljene filtre neželene pošte, požarne pregrade in antivirusni program . V veliko primerih opažam, da sporočilo, ki vsebuje zlonamerno vsebino ne obstane veliko časa neopaženo. Najkasneje v roku parih dneh takšnega sporočila ni mogoče več posredovati naprej ali prenesti vsebine na lokalni računalnik, saj sistem zazna zlonamerno priponko in jo avtomatsko odstrani. Tudi v našem primeru se je v roku 24-ih ur povajilo sledeče sporočilo:



V kolikor do tega trenutka nismo verjeli ali gre za zlonamerno pošto ali ne, lahko verjamemo programom, ki ugotovijo to namesto nas.

Zaključek

Na konkretnem primeru smo prikazali kako ugotoviti ali gre za legitimno sporočilo ali za sporočilo z zlonamerno vsebino. Ponovno bi rad poudaril nekaj osnovnih pravil za varno spletno komuniciranje:

- Neklikajte priponk, ki jih preko elektronske pošte prejmete od neznanih pošiljateljev
- Ne klikajte na povezave ki jih preko elektronske pošte prejmete od neznanih pošiljateljev
- Uporabljajte antivirusni program ter požarni zid
- Imejte vedno posodobljen operacijski sistem, brskalnike, vtičnike ter ostalo programsko opremo
- Ne odgovarjajte na takšna sporočila, saj s tem spletnim napadlcem le sporočite, da je vaš elektronski predal aktiven in posledično lahko pričakujete še več neželene pošte
- Ko se prepričate, da sporočilo vsebuje zlonamerne priponke je najbolje da jih izbrišete. Strah je v tem primeru odveč, v kolikor na priponke ali povezave ne klikate, se ne okužite.

Prikazali smo samo en primer ugotavljanja legitimnosti elektronske pošte. Takšnih primerov je na tisoče oziroma milijone, in vsak je omejen samo s človeško domišljijo

Avtor: Boštjan Špehonja,
Specialist informacijske varnosti
(https://www.linkedin.com/in/bostjanspehonja)