Izsiljevalski kriptovirusi na obhodu

Izgubili smo vse datoteke!

..Kriptovirusi vam z zaklenitvijo vseh datotek lahko povzročijo številne težave. Okužbo se težko prepreči, se jo pa da prekiniti in s tem preprečiti škodo. Najboljša preventiva je požarni zid nove generacije..

Laična razlaga napada s kriptovirusom

Gre za proces v dveh fazah. Najprej se vaša naprava okuži s kratko kodo, ki se zažene in s spleta prenese glavno zlonamerno kodo, ki potem s krmilnega strežnika prenese javni ključ in nato uporabnikove datoteke zaklene. Za pridobitev zasebnega ključa, ki bi bil zmožen odkleniti datoteke, izsiljevalci zahtevajo odkupnino (od 300 do 2.500 evrov), ki mora biti plačana v 72 urah, drugače grozijo z uničenjem edinstvenega zasebnega ključa.

Tehnične podrobnosti o okužbi

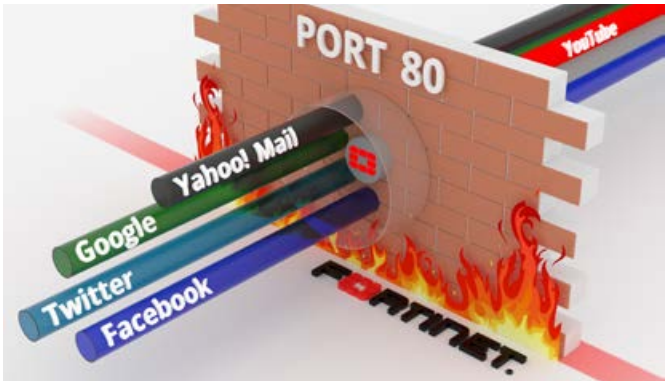
V prvi fazi se uporabnikov računalnik ali mobilna naprava okuži s kratko programsko kodo, ki se imenuje »bootloader«. To se najpogosteje zgodi z odprtjem priponke v e-pošti ali pa na zlonamerni spletni strani. Ta del je skoraj nemogoče popolnoma preprečiti. Preprečimo sicer 99 odstotkov ali celo več poskusov, vsake toliko časa pa ena modifikacija uide protivirusnim (antivirus, antispam) sistemom in se znajde v poštnem nabiralniku uporabnika.

V drugi fazi procesa se »bootloader« zažene in s kontrolnega strežnika prenese dejanski virus. Teh virusov je bistveno manj kot »bootloaderjev«, poglavitno pa je, da se morajo od nekje prenesti. Običajno zlikovci za to uporabljajo novo registrirane domene. Ko se to zgodi, virus začne komunicirati s svojim kontrolnim strežnikom C&C, ki mu sporoči različne podatke o našem računalniku, C&C strežnik pa mu preda javni ključ, s katerim bo zaklenil vaše podatke. Kodira večino najpogostejših datotek.

Čeprav samo okužbo težko preprečimo, lahko veliko naredimo s prekinitvijo druge faze napada.

Kako se lotiti boja s kriptovirusi?

1. Investirajte v požarni zid nove generacije. Če se že spoznate na to področje, potem veste, da med največje štejejo Fortinet, Palo Alto in Checkpoint. Če izberete FortiGate, lahko v njem nastavite ustrezne filtre in protivirusno politiko:
   a. Filter spletnih vsebin (web content filter): Prepovedali boste lahko dostop do varnostno problematičnih strani, kot so »phishing« in »malicious web«. Pametno je prepovedati tudi kategorijo Unrated, s čimer boste zelo dobro omejili potencial za napade. Alternativno lahko za to kategorijo določite, da spletni brskalnik pokaže le opozorilo. To je verjetno dovolj, saj virusna koda tega opozorila zaenkrat ne zna dekodirati in bo tako ustavljen prenos glavne zlonamerne kode.
   b. Protivirusna politika: za ustrezno preprečevanje virusnih okužb moramo nujno skenirati tudi protokol HTTPS. Tehnično je to izvedljivo, ima pa to pri nas pravne omejitve.
2. Kupite ali najemite primeren protivirusni filter za e-pošto: Tak filter ne bo prestregel čisto vsega (zato potrebujete požarni zid nove generacije), bo pa precej omejil izpostavljenost.
3. Vzpostavite primerne sisteme varnostnih kopij: ti morajo biti nujno izvedeni tako, da datoteke v varnostnih kopijah niso dosegljive na mreži.



Poleg »web filter« funkcije naprave FortiGate omogočajo tudi druge napredne možnosti. Slika prikazuje filtriranje aplikacij, ki sicer vse delajo prek »porta« 80, pa vendar lahko nekatere spustimo skozi, druge pa zavrnemo. Mogoče je tudi bolj gradualno kontrolirati protokole znotraj aplikacij, pri Skypu lahko denimo preprečimo le pošiljanje datotek.

Kaj lahko storite takoj?

Nikar ne čakajte na katastrofo. Napadalci znajo obiti protivirusno opremo tako, da zlonamerne kode skrijejo v različne tipe datotek in kompresij. Dejansko izpostavljenost vašega omrežja lahko preverite z brezplačnimi testi (na primer http://metal.fortiguard.com). (P. R.)