Izsiljevalski virusi

Kdo?

Avtorje je treba iskati v vrstah organiziranega kriminala. Ta hip je skupni svetovni zaslužek z internetnim kriminalom večji kot zaslužek z ilegalnimi drogami. Zadnja kampanja virusa znanega pod imenom CryptoWall je upravljalcem/lastnikom prinesla več kot 300 milijonov dolarjev zaslužka. Sredstva, ki jih imajo na razpolago za razvoj, so skoraj neomejena.

Kako deluje?

Vaba

Po elektronski pošti prejmemo vabo. Zanimiv mail s priponko ali povezavo na neko spletno stran, kjer je skrit manjši košček kode, ki se poveže na okužen strežnik in naloži dejansko škodljivo kodo (virus).

Zagon - instalacija

Program (virus) se instalira, pri tem poskrbi, da onesposobi antivirusne programe in onemogoči dostop do podjetij, ki proizvajajo antivirusne rešitve. Poskrbi tudi za lasten avtomatski zagon ob ponovnem zagonu računalnika.

Klic domov

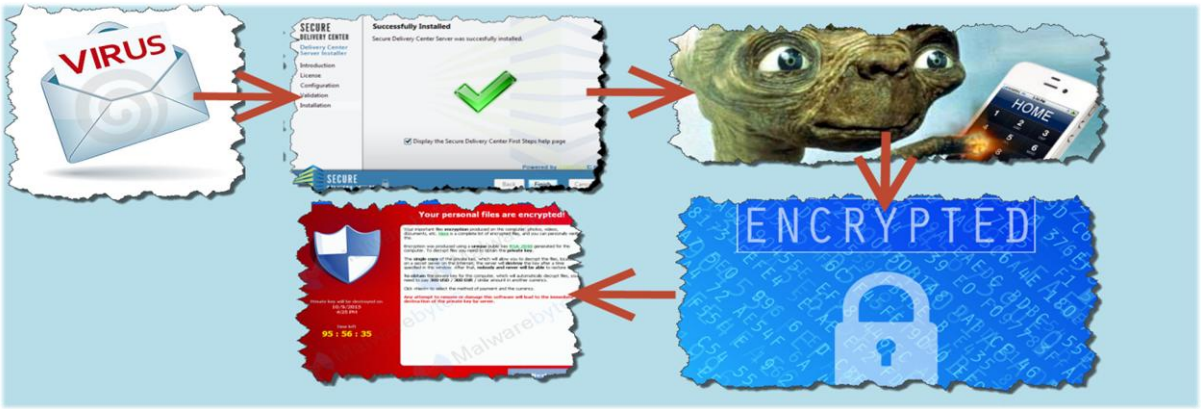
Virus generira enoličen set ključev za kodiranje vaših datotek. Poveže se s tako imenovanim C&C (command and control) strežnikom, kamor posreduje ključe, ki bodo omogočili dekodiranje vaših datotek po plačilu odkupnine. Od tam virus prejme informacije o načinu plačila in računu, kamor plačilo nakažemo.

Kodiranje vaših datotek

Virus nato počaka na trenutek, ko je računalnik manj obremenjen (ni pod nadzorom) in prične kodirati vse datoteke, do katerih ima dostop, vključno z omrežnimi in zunanjimi diski.

Obvestilo

Virus vas obvesti, da so vaši podatki kodirani, dekodiranje pa vas stane med 500€ in 1500€, če plačate takoj, nato se cena dvigne.



Kako se branimo?

NE ODPIRAMO PRIPONK IN NE KLIKAMO POVEZAV V SPOROČILIH

NE ODPIRAMO PRIPONK IN NE KLIKAMO POVEZAV V SPOROČILIH

Smo vedno dovolj nezaupljivi, NOBENA vladna organizacija ali banka vas ne bo pozivala z mailom, da storite nekaj za vas pomembnega.

Tudi če smo sporočilo prejeli od znanega pošiljatelja, smo nezaupljivi. Preverimo, ali je sporočilo napisano v pošiljateljevem stilu, je tema pričakovana? Pošiljateljev računalnik je lahko okužen z vrsto virusa, ki pošilja izsiljevalske viruse.

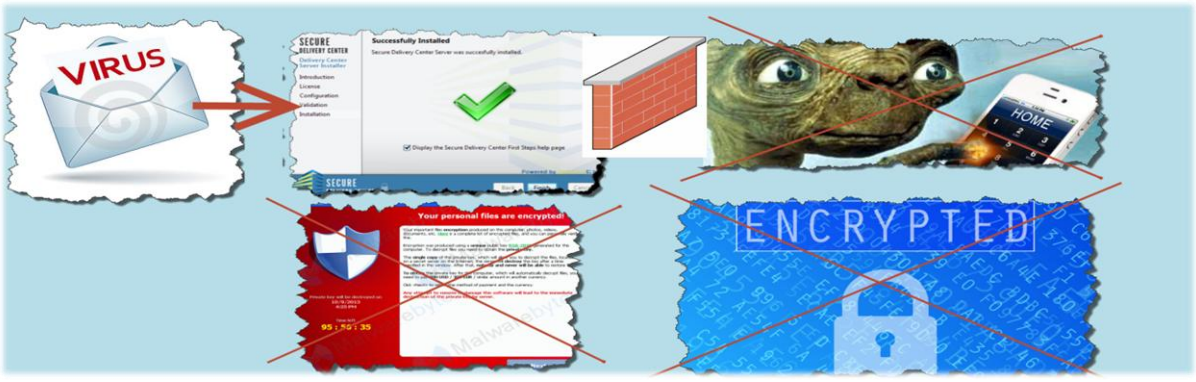
NE ODPIRAMO PRIPONK IN NE KLIKAMO POVEZAV V SPOROČILIH

Kaj storimo, če opazimo okužbo ?

TAKOJ ugasnemo računalnik, potegnemo kabel iz vtičnice, pozabimo lepo obnašanje pri izklopu računalnika. Pokličemo strokovnjaka, ki bo disk pregledal s svojim računalnikom. Nikakor ne poizkušajmo sami z antivirusnim programom odstranjevati virusa.

Kaj lahko stori Multimedia d.o.o. ?

Z uporabo pri nas razvite tehnologije, ki jo sestavljajo usmerjevalnik in nekaj namenskih strežnikov, zaznamo in preprečimo virusov 'Klic domov'. Tako preprečimo komunikacijo s lastnikovim C&C. Tehnologija v nekaj minutah opozori naše strokovnjake o prisotnosti virusa v vašem omrežju. Vsak dan se pojavi na tisoče novih mutacij virusa, ki jih antivirusni programi zaznajo šele po nekaj urah ali dnevih, vendar pa je hkrati aktivnih le nekaj več kot sto C&C strežnikov. Seznami teh strežnikov oziroma njihovi naslovi so javno dostopni, mi pa jih uporabimo za preprečevanje komunikacije virusa s svojim lastnikom. Če virus ne more predati ključa svojemu lastniku, ne prične s kodiranjem datotek, saj v tem primeru ne more pričakovati plačila; tudi informacije o tem, kam je potrebno plačati odkupnino, namreč dobi od svojega C&C strežnika. **VSAKA MINUTA ŠTEJE**. Prej ko odkrijemo okužbo, manj škode bo virus lahko povzročil. Kodiranje je časovno zahtevna operacija, kodiranje vsake datoteke zahteva kar nekaj časa, zato **VSAKA MINUTA ŠTEJE**.



Kako pomagamo, ko se je že zgodilo ...

Multimedia d.o.o. pomaga omejiti škodo, tako da pomaga pri restavriranju podatkov iz varnostnih kopij. Hrani kodirane podatke do morebitnega razbitja izsiljevalske mreže. Takrat namreč organizacije, ki so pomagale pri razbitju kriminalne mreže, ključe za dekodiranje javno objavijo.