TIETOKESKUS

Kiristysohjelma tuli taloon

7.3.2017

Samuli Lindström

TIETOKESKUS

Ransomware, cryptolocker, kryptolokkeri

Kiristyshaittaohjelmat ovat jo valitettavan tuttuja kaiken kokoisissa Suomalaisissa organisaatiossa


LUE TÄSTÄ ›› HELSINGIN UUTISET

29.5.2016 - 19.34

Tuttu asia sairaalassa, mutta oudossa paikassa – Yle: Virus HUS:n tietoverkossa – lunnasrahoja vaadittiin

HUS:n tietoverkkoon on hyökätty neljästi ja vaadittu lunnaita.

KUVA

SAVON SANOMAT

Maanantai, 6.3.2017 Nimipäivät: Tc

Savo Kotimaa Talous Ulkomaat Viihde Kulttuuri Urheilu Teemat Pääkirjoitul

Olet lukenut 1/5 maksutonta artikkelia. Katso tilausvaihtoehdot.

Kotimaa Julkaistu 16.02.2017 19:41

Saitko oudon ilmoituksen saapuneesta paketista? Älä klikkaa linkkiä!


mtv Uutiset Sport Viihde Lifestyle TV ja ohjelmat Vic

Digi Etusivu Uusimmat Testit Tuotteet

APPLE

Mac-käyttäjille varoitus: Ensimmäinen kiristyshaittaohjelma löydetty

LIFESTYLE > DIGI | JULKAISTU 20.03.2016 09:30

Haittaohjelma toimii poikkeavalla tavalla: se aktivoituu vasta kolmen päivän kuluttua asennuksesta.

TIETOKESKUS

Mitä sitten?

- Yleisyys
- Haitallisuus
- Vaikuttavuus

TIETOKESKUS

Tarinoita tosielämästä

- Tapaukset on koottu julkisista ja yksityisistä organisaatioista. Kaikilla organisaatioilla on eri virustorjuntaohjelmisto käytössä työasemissa. Sähköpostijärjestelminä toimivat Exchange Online, Exchange 2016 ja Zimbra. Lähtötilanteessa kaikki eivät ole olleet Tietokeskuksen asiakkaita, tapausten jälkeen kaikki ovat Tietokeskuksen palveluasiakkaita.
- Virus pääsi järjestelmiin jokaisessa esitellyssä tapauksessa sähköpostin liitetiedoston kautta. Viestiin oli kirjoitettu uskottava organisaatiota koskettava viesti. Virus aktivoitui, kun pakatun liitetiedoston avasi.
- Vaadittujen lunnaiden suuruus vaihteli 4000€ ja 350 000 € välillä.

TIETOKESKUS

Case 1

- 35 työntekijää, 1 IT henkilö otona
- Haittaohjelma aktivoitui kun liitetiedosto avattiin ”salli makrot”
- Tietoja salattiin useita tunteja. Havaittiin vasta kun toiminnanohjausjärjestelmä lakkasi toimimasta
- Salaamattomia ajantasaisia varmuuskopioita ei ollut saatavilla (käyttäjän tunnuksilla pääsi kiinni myös varmuuskopioihin, jolloin myös ne kryptattiin)

TIETOKESKUS

Case 1

- ”Hello Bad news! Your files are encrypted.”
- Viestissä annettiin ID -tunnus ja sähköpostiosoite, johon pyydettiin olemaan yhteydessä 72h sisällä – muuten ”palauttaminen muuttuu vaikeammaksi”
- Lunnasvaatimus 6 bitcoinia – tapahtumahetkellä noin 4400€
- Tiedostot saatiin palautettua

TIETOKESKUS

Case 2

- 1400 työntekijää 4 täyspäiväistä IT henkilöä
- Kolme vastaanottajaa liitetiedostolle
  - Kaksi siirsi manuaalisesti roskakoriin
  - Yksi henkilö avasi liitteen
- Välittömästi avauksen jälkeen *.zzz tiedostoja alkoi ilmestymään kaikkiin kansioihin joihin käyttäjällä oli pääsy. Kansioissa myös instructions.html tiedosto
- Käyttäjä oli yhteydessä IT tukeen – ohje sammuttaa tietokone

TIETOKESKUS

Case 2

- Varmuuskopiot ajantasalla
- Palauttaminen kesti 6 vrk
  - Tosin iso osa tiedostoista oli käytettävissä kahdessa päivässä
- Varastonhallinnan kuvapankki ei varmistusten piirissä

TIETOKESKUS

Case 3

- 25 henkeä töissä ei IT henkilökuntaa
- Haittaohjelman lähde jäi tunnistamattomaksi
  - Spostin liite?
- Tartunta vain yhdellä käyttäjällä – rajatut pääsyoikeudet
  - Kryptaus kohdistui vain yhteen kansioon

TIETOKESKUS

Case 3

- Levyhälytys valvonnassa
- Kone eristettiin verkosta
- Käyttäjälle varakone
- Saastuneen koneen blankotus
- Palautusaika alle tunti

TIETOKESKUS

Tarinan opetus

- Pelkästään virustorjunta koneessa ei suojaa kiristäjiltä, eikä mikään virustorjunta ole aukoton.
- Varmuuskopiointi on helppoa, palauttaminen ei.
- Käyttäjä (ihminen) on tietoturvan heikoin lenkki.
- Laadi jatkuvuus ja palautussuunnitelma – harjoittele!

TIETOKESKUS

Jos tilanne on päällä

- Etsi saastumisen lähde ja eristä saastuneet koneet verkosta (sammuta ne jos pakko)
- Varmista ettei virus pääse leviämään uudestaan (tiedota!)
- Arvioi onnistumistasi edellisissä (tuleeko salattuja tiedostoja lisää)
- Palauta tiedostot käyttöön varmuuskopioista tai tee jokin seuraavista:
  - Hyväksy että tiedostot ovat mennyttä
  - Selvitä onko kyseisen kryptolokkerin salaukseen tunnettua keinoa purkaa
  - Etsi ohjeet maksua varten, maksa kiristäjille ja toivo että saat tiedostot takaisin
- Pysy rauhallisena ja muista tiedottaa! Tiedotuksen tulee kohdistua oman organisaatiosi lisäksi niihin sidosryhmiin, joihin salaus vaikuttaa.

TIETOKESKUS

Kiitos!