

Ajankohtaiset kyberuhat terveydenhuollossa

Esitelmän sisältö

- Tällä hetkellä pinnalla olevat kyberuhkat
- Onko terveydenhuollon järjestelmät rakennettu kestävämmän kyberhyökkäyksiä?
- Kiristyshaittaohjelmat
- Terveystuoltoalan kyberuhkia -raportin uudistaminen

Tällä hetkellä pinnalla olevia kyberuhkia

Suomessa jatkuvasti näkyvää

1. Laskutushuijaukset (CEO-fraud)
2. Kiristyshaittaohjelmat
3. Palvelunestohyökkäykset (ja niillä uhkailu)
4. Arkaluontoisen tiedon varastaminen (kohdistetut hyökkäykset)
5. Haittaohjelmien jakelualustat (EK) jylläävät HAVARO-havainnoissa
6. Palvelimen tai muun laitteen käyttäminen väliresurssina (esim. murrettu Wordpress-sivusto)
7. Tietojenkalastelu (luottokorttitiedot, käyttäjätunnukset ja salasanat)

Maailmalla näkyy, mutta ei (vielä) Suomessa

- Pankkihaittaohjelma asiakkaan tietokoneessa (ei aktiivisesti kohdistettu Suomeen)
- Suuret tietomurtojen avulla tehdyt petokset (esim. SWIFT)
- Massiiviset palvelunestohyökkäykset (>> 100 gbps)
- Kohdistetut hyökkäykset teollisuusjärjestelmiä (ICS) vastaan, esim. sähkönjakelun sabotaasi



Terveydenhuollon tietojärjestelmät

Olemmeko varautuneet hyökkäykseen? Oikeasti?

#OpSafePharma 3.0: tietomurtoja Italian terveydenhuoltoon

- Hakkerit tyytymättömiä terveydenhuollon hoitosuositukseen ja rahankäyttöön.
- Neljään terveydenhuollon organisaatioon tietomurto elokuussa 2016; niistä kahdesta vuodettiin tietoja nettiin, kaikkien sivuja töhrittiin.
- Hyökkäysvektorina yhteisen sisällönhallintajärjestelmän haavoittuvuus



The screenshot shows the RiskBased Security website. The header includes the logo and navigation links: ABOUT RBS, NEWS, PRODUCTS, SERVICES. The main navigation bar contains: Home, Security Intelligence, Industry Solutions, Compliance, Cyber Liability. The article title is "Anonymous Italy Targets Web Agency Engitel; Several Organizations Compromised". The date is APRIL 10, 2016 BY RBS. The article text discusses a systemic risk with cloud providers and hosting solutions, mentioning a hosting provider breach and a specific incident where Anonymous Italy leaked data affecting over 40 sites belonging to an Italian web agency called Engitel. The article also mentions that the breach was originally posted on an Anonymouse news blog with the actual data being posted to the file sharing site MEGA. The leak was posted in six parts which includes a total of 321MB of compressed data, and when extracted totals 553MB made up of 2,859 files over 124 folders. At the bottom, there are two links: www.aboutjob.it.customers.html and www.hrweb.it.rar, both with a small icon of a document with a red 'X'.

Palvelunestohyökkäykset Kanta-palveluun

- Useita hyökkäyksiä 12.10. alkaen
- Kohteina myös tunnistuspalvelut:
 - » yrityksille suunnattu Katso (omistajat TEM ja Verohallinto)
 - » kansalaisille suunnattu Vetuma (omistaja Valtori)
- Seurauksia: apteekista ei saa ostettua reseptilääkkeitä

Tietoa Kelasta / Ajankohtaista

14.10.2016

Tunnistuspalveluissa palvelunestohyökkäys

Kelan käyttämässä tunnistuspalveluissa on ollut tällä viikolla käyttökatoja palvelunestohyökkäyksen takia.

Ensimmäinen palvelunestohyökkäys alkoi keskiviikkona 12. lokakuuta iltapäivällä. Hyökkäys kohdistui Vetuma- ja Katso-tunnistuspalveluihin sekä Kelan Kanta-palveluihin.

Palvelunestohyökkäys aiheutti käyttökatoja palveluihin lähinnä ilta- ja yöaikaan. Häiriö esti tunnistautumisen ja siten Kelan verkkoasioinnin ja Omakanta-palvelun käytön osalla asiakkaita.

Häiriöitä Katso- ja Vetuma-tunnistuspalveluissa on ilmennyt myös tänään perjantaina.

Pahoittelemme asiakkaillemme aiheutunutta haittaa.

Miksi joku hyökkäisi terveydenhuollon tietojärjestelmään?

- "Koska se on mahdollista"
- Maineen hankkiminen mustahattujen piireissä
- Kohteen maineen pilaaminen
- Kosto organisaatiolle tai yksittäiselle henkilölle
- Painostaminen toiminnan muuttamiseksi
- Rahan kiristäminen
- Henkilötietojen varastaminen ja myynti
- Käyttö muun hyökkäyksen välikappaleena
- Tietojen väärentäminen kovien lääkkeiden saamiseksi
- ...

Hyökkäysvektoreita

- **Fyysinen:** Kävellään sisään sairaalaan ja pannaan verkkopistoke seinään tai hyödynnetään langatonta lähiverkkoa.
- **Työasemat:** Lähetetään etähallinnan antava haittaohjelma sähköpostilla sairaalan työntekijälle. Murrettua työntekijän tietokonetta käytetään jalansijana lateraalileviämisessä.
- **Työntekijät:** Huijataan työntekijältä käyttäjätunnus ja salasana ja toimitaan sitten työntekijän identiteetillä.
- **Infrastruktuuri:** Skannataan avoimia palveluita ja pyritään hyödyntämään niiden haavoittuvuuksia jalansijan saamiseksi.

Kyberturvallinen järjestelmä

- Suunnittelu
- Toteutus
- **Testaus hyökkääjien silmin**
- Tuotantoon vienti
- Ylläpito ja korjaukset
- Käytöstä poisto

NIS-direktiivin tilanne

- NIS-direktiivin osalta Liikenne- ja viestintäministeriö on käynnistänyt terveydenhuoltoalaa koskevan työryhmän, jossa ovat mukana STM ja Valvira.
 - » 1) tietoturvan vähimmäistaso
 - » 2) poikkeamista ilmoittaminen
 - » 3) keskeisten yritysten/toimijoiden määrittely
- Direktiivi koskee seuraavia sektoreita:
 - » 1) Energia, 2) Liikenne, 3) Pankkiala, 4) Finanssimarkkinoiden infrastruktuurit, 5) Terveydenhuoltoala (mukaan lukien sairaalat ja yksityisklinikat), 6) Juomaveden toimittaminen ja jakelu, 7) Digitaalinen infrastruktuuri
- Direktiivi tuli voimaan elokuussa 2016. EU:n jäsenvaltioiden on saatettava säännökset osaksi kansallista lainsäädäntöä 9. toukokuuta 2018 mennessä.



BadBlock is on the block!

This machine was infected with ransomware BadBlock. Many of your files are encrypted using RSA algorithm, and the key to decrypt this files is with us on our server.

-What this means?

It means that to decrypt and recover your files, you will need to pay a ransom, in bitcoins. The actual ransom for your machine is 2 bitcoins (USD ~900.00).

If you are not interested in pay this ransom, you can easily format this machine, or even remove BadBlock (it's not that hard), but all your files will become unrecoverable!

-How do I pay?

You simply buy bitcoins, and transfer them to this account: [REDACTED]
The amount is 2 bitcoins, like we talked earlier... You can use [this link](#) or [this link](#) to help you out on how to buy the bitcoins.

-What happens after the payment?

BadBlock still running on your computer right now, and waiting to detect one payment of 2 BTC on the address mentioned above. Once we receive the payment, we will start to decrypt all the encrypted files. The process to detect the payment can take up to 2 hours, and only after this it will start decrypting your files. So after payment, leave this machine powered.

For this reason we strongly recommend you to not try to remove BadBlock, and disable your anti-virus for a while, until you pay and the payment gets processed, to BadBlock start decrypting. If your anti-virus gets updated and remove BadBlock automatically, even if you pay the ransom, it will not be able to recover your files!

How do I know that you will really decrypt my files after payment?

Medbitin havainnot

- Vuosina 2015 ja 2016 useita tartuntoja tiedostoja salaavista kiristyshaittaohjelmista
- Toistaiseksi ei todella merkittäviä vaikutuksia tuotantoon
 - » Yksittäisiin järjestelmiin/toimintoihin on tullut käyttökatkoja
 - » Hukattu työaika
- Kiristyshaittaohjelmat ovat toistaiseksi melko yksinkertaisia.

Medbitin tyypillinen vaste tartuntaan

- Havainnointi: havainto käyttäjältä tai virustorjunnasta
- Eristäminen: saastunut käyttäjätunnus ja konetili suljetaan
- Palautuminen: salakirjoitetut kohteet paikannetaan ja palautetaan varmuuskopioista
- Tutkinta: tunnistaako virustorjunta; jos ei, niin miksi?
- Hallinnolliset toimenpiteet: tiedottamista, tilastointia, rikosilmoitus

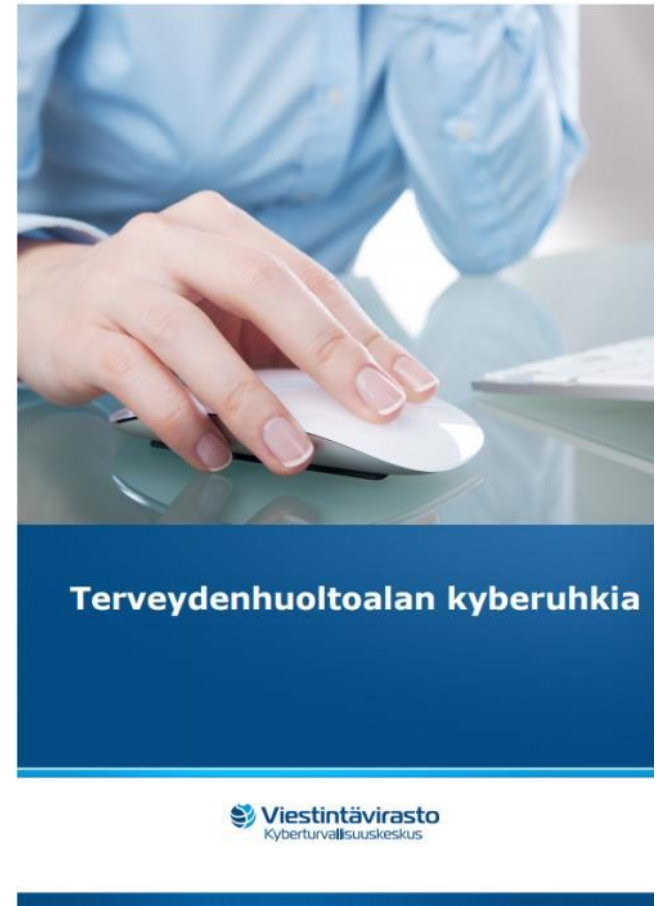
Medbitin kehitystoimet

- Uusi sisäinen ohjeistus erityisesti kiristyshaittaohjelmatartuntojen selvittämiseksi
- Tietoturvapoikkeamaprosessin parantaminen
- Käyttövaltuushallinto ja verkkolevyjen käyttöoikeudet
- Varmuuskopiointi- ja palautusrutiinien parantaminen
- IPS:n käyttöönotto internetliikenteessä
 - » Yhdessä virustorjunnan kanssa toistaiseksi täydellinen tartuntojen torjunta.
- Tiedottaminen käyttäjille
- Tulevaisuudessa: suorituksenaikainen haittaohjelmien käyttäytymisen analysointi, eri lokilähteiden automaattinen analysointi, ohjelmistojen valkolistaus, operoinnin resurssit

Terveysthuollon kyberuhkia -raportin uudistaminen

Terveysthuoltoalan kyberuhkia -raportti

- Katsaus organisaatioiden johdolle ja kyberturvallisuudesta vastaaville henkilöille
- Julkaistiin vuodenvaihteessa 2015-2016
- Raportti tullaan päivittämään loppuvuonna. Kehitysehdotukset ja syötteet ovat tervetulleita!



Viestintäviraston Kyberturvallisuuskeskus



Tietoturvapalvelut huoltovarmuuskriittisille yrityksille

- Tietoturvaloukkausten ilmoituspiste ja tilannekuva
 - » Neuvonta, opastus
 - » Vahinkojen rajoittaminen
 - » Luottamuksellinen käsittely
 - » Yleinen ja toimialakohtainen tilannekuva
- Tietoturvaloukkausten havainnointi (HAVARO)
 - » Haitallisen ja/tai normaalista poikkeavan liikenteen havainnointi
 - » Asiakkaiden varoittaminen
 - » Raportointi
- Yhteistyöverkostot
 - » Luottamuksellinen tietoturva-asioiden tiedonvaihto
 - » Kaksi tasoa: 1) Toimialakohtainen sähköpostijakelu 2) Tiedonvaihtoryhmät
- Haavoittuvuuskoordinaointi
 - » Yhteistyö haavoittuvuuden tai vakavan ohjelmistovirheen löytäjän ja ohjelmistovalmistajien kanssa
 - » Tieto haavoittuvuudesta loppukäyttäjille
- Järjestelmäturvallisuus
 - » Turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvät turvallisuusasiat
 - » Salaustuotteiden ja tietojärjestelmien hyväksyntä
 - » Kansallisen ja kansainvälisten turvaluokitellun tietoaineiston käsittelyn ohjeistus



Viestintävirasto

Kyberturvallisuuskeskus

cert@viestintavirasto.fi

www.kyberturvallisuuskeskus.fi

www.viestintavirasto.fi
