KANKAANPÄÄ

Kiristysohjelma tuli taloon…

Jukka Ehto
Tietohallintopäällikkö, DI
+358 44 5772274
jukka.ehto@kankaanpaa.fi

KANKAANPÄÄ

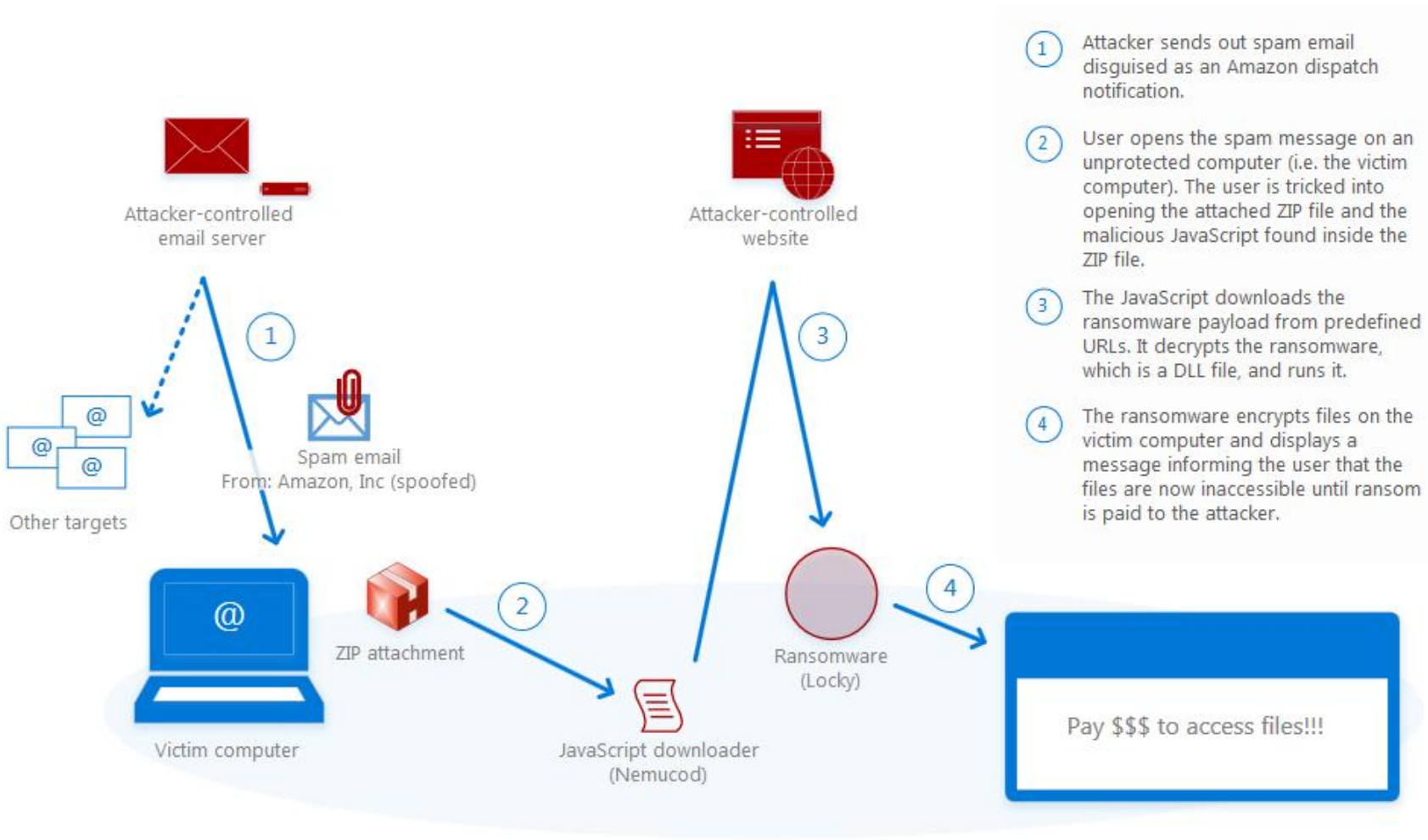
Tietoturvallisuuteen panostettu:

- Tietoturvapolitiikka
- Käyttösäännöt
- Auditointia
- Koulutusta
- Tiedotusta
- Tekniikkaa
  - Palomuuri
  - Sisällönsuodatus
  - IDS (tunkeutumisen havaitsemisjärjestelmä)
  - Virus- ja haittaohjelmatorjunta työasemilla ja palvelimilla


Perjantai 25.11.2016 klo 8:40


Locky!

KANKAANPÄÄ



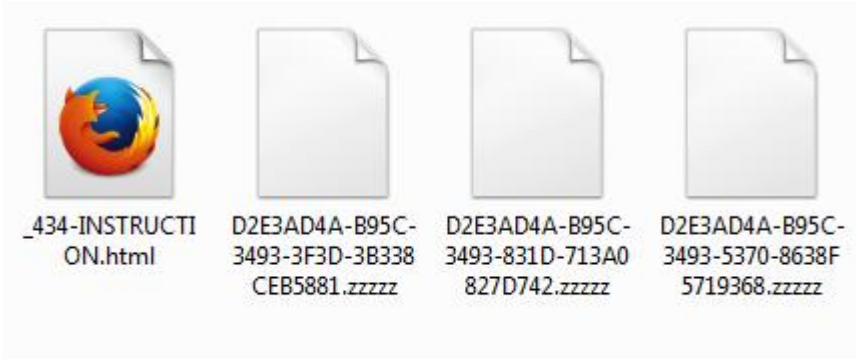
1. Attacker sends out spam email disguised as an Amazon dispatch notification.
2. User opens the spam message on an unprotected computer (i.e. the victim computer). The user is tricked into opening the attached ZIP file and the malicious JavaScript found inside the ZIP file.
3. The JavaScript downloads the ransomware payload from predefined URLs. It decrypts the ransomware, which is a DLL file, and runs it.
4. The ransomware encrypts files on the victim computer and displays a message informing the user that the files are now inaccessible until ransom is paid to the attacker.

KANKAANPÄÄ

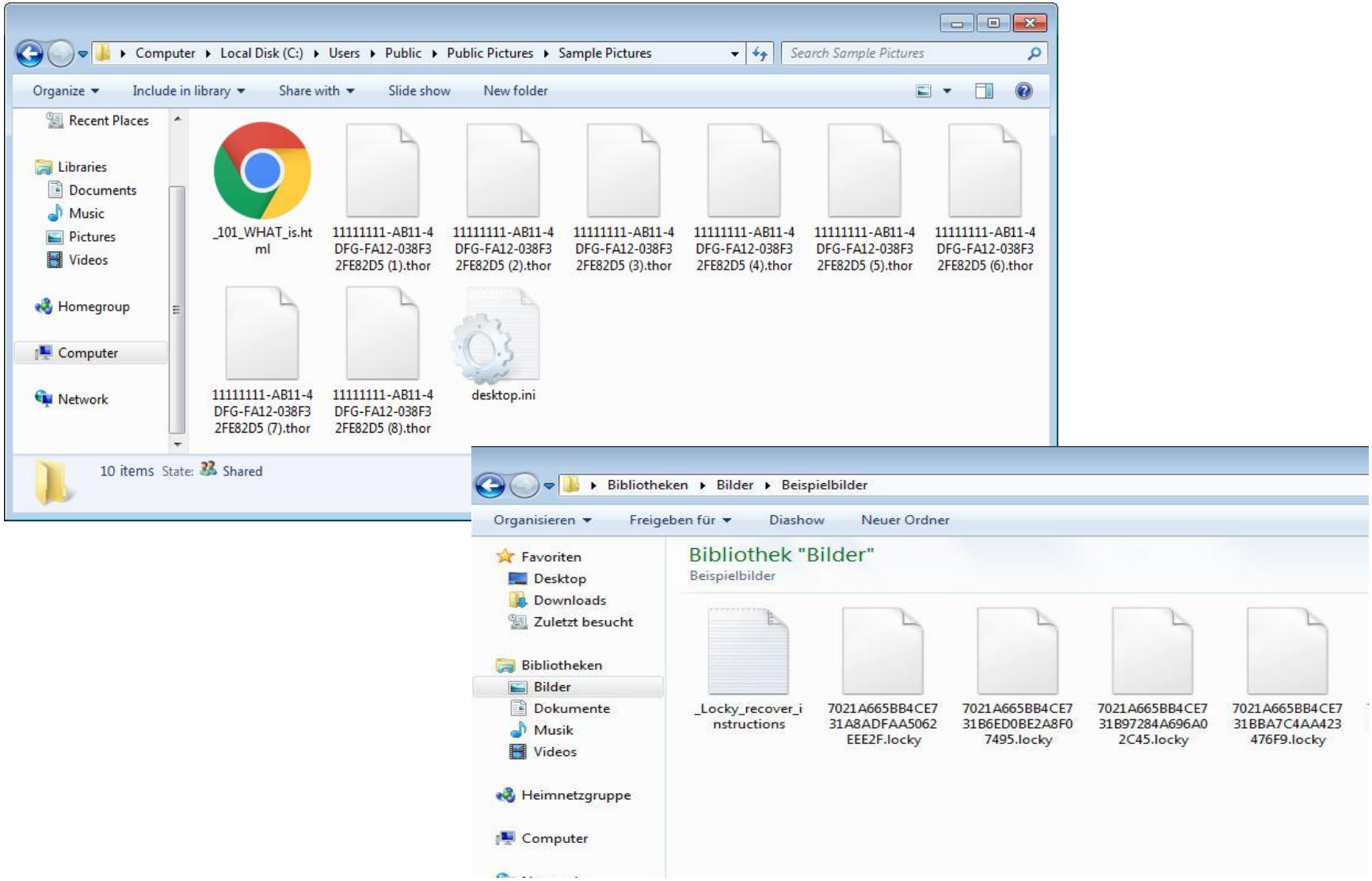

[SPAM] Bestellung 30155 - Message (HTML)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Other Actions
Actions
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
From:
To:
Cc:
Subject: [SPAM] Bestellung 30155
Message
Bestellung Bestellung 30155.zip.zip
Sehr geehrte Damen und Herren,
anbei erhalten Sie unsere Bestellung. Diese ist maschinell erstellt und ist daher ohne Unterschrift gültig.

Dear ladies and gentlemen,
enclosed you receive our order. This order has been created automatically and is valid without signature.
Mit freundlichen Grüßen / Best regards

KANKAANPÄÄ


_434-INSTRUCTION.html
D2E3AD4A-B95C-3493-3F3D-3B338CEB5881.zzzzz
D2E3AD4A-B95C-3493-831D-713A0827D742.zzzzz
D2E3AD4A-B95C-3493-5370-8638F5719368.zzzzz

KANKAANPÄÄ


Computer ▸ Local Disk (C:) ▸ Users ▸ Public ▸ Public Pictures ▸ Sample Pictures
Search Sample Pictures
Organize
Include in library
Share with
Slide show
New folder
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
_101_WHAT_is.html
11111111-AB11-4DFG-FA12-038F32FE82D5 (1).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (2).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (3).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (4).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (5).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (6).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (7).thor
11111111-AB11-4DFG-FA12-038F32FE82D5 (8).thor
desktop.ini
10 items State: Shared
Bibliotheken ▸ Bilder ▸ Beispielbilder
Organisieren
Freigeben für
Diashow
Neuer Ordner
Favoriten
Desktop
Downloads
Zuletzt besucht
Bibliotheken
Bilder
Dokumente
Musik
Videos
Heimnetzgruppe
Computer
Bibliothek "Bilder"
Beispielbilder
_Locky_recover_instructions
7021A665BB4CE731A8ADFAA5062EEE2F.locky
7021A665BB4CE731B6ED0BE2A8F07495.locky
7021A665BB4CE731B97284A696A02C45.locky
7021A665BB4CE731BBA7C4AA423476F9.locky

KANKAANPÄÄ

=__=+ $|*-*=_
||*.**

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: mwddgguaa5rj7b54.onion/D2E3AD4AB95C3493
4. Follow the instructions on the site.

!!! Your personal identification ID: D2E3AD4AB95C3493 !!!
=|+|$|+. =-

KANKAANPÄÄ

Kuinka voi ostaa Locky Decryptor™?

1 Voi suorittaa maksun bitcoinien avulla, jotka saa eri tavoilla.

2 On rekisteröitävä bitcoin-lompakko:

Yksinkertaisin online-lompakko tai lompakon luomisen muita tapoja.

3 Huolimatta siitä, että bitcoinien hankinta ei ole helppoa, joka päivä se tulee helpommaksi.

Suosituksemme:

localbitcoins.com (WU)	Bitcoinien osto Western Unionin kautta.
coincafe.com	Nopeata ja yksinkertaista palvelua varten. Maksutavat: Western Union, Bank of America, käteisten osto FedExin, Moneygramin kautta, rahan siirto. New-Yorkissa: bitcoinien pankkiautomaatti, henkilökohtaisesti.
localbitcoins.com	Palvelusta löytyy ihmisiä, joilla on valmiutta myydä teille bitcoinia suoraan.
cex.io	Bitcoinien osto VISA/MASTERCARD-kortilla tai tilisiirrolla.
btcdirect.eu	Euroopan paras sivusto.
bitquick.co	Bitcoinien osto käteisellä.
howtobuybitcoins.info	Kansainvälinen alue koskien bitcoinien vaihtoa.
cashintocoins.com	Bitcoinit käteisellä.
coinjar.com	CoinJar-sivustolta saa ostaa bitcoinit suoraan.
anxpro.com	
bittylicious.com	

4 Lähetä 4.00 bitcoinit osoitteeseen:

1JN6BUx1ARqGq984eYYgeER6NtPauH1MB7

Huomautus: tapahtuman vahvistamiseksi maksu käsitellään alle 30 minuuttia tai pidemmän ajan, ole rauhallinen...

Pvm	Bitcoinien summa	Tapahtuman ID	Vahvistus
not found			

5 Päivitä sivu ja lataa dekoodausohjelma.

Bitcoinin yhden vahvistuksen jälkeen lähtee sivulle, josta saa ladata dekoodausohjelma.

KANKAANPÄÄ

Yhteenveto Locky -tapauksesta

- Locky ehti toimia 46 min.
- kryptasi yli 50000 tiedostoa
- lunnaita ei maksettu

KANKAANPÄÄ

Kaikki paitsi varmuuskopiointi on turhaa…