NCSC Security Advisory **18 March 2015**

CryptoWall Ransomware Campaign Impacting New Zealand Organisations

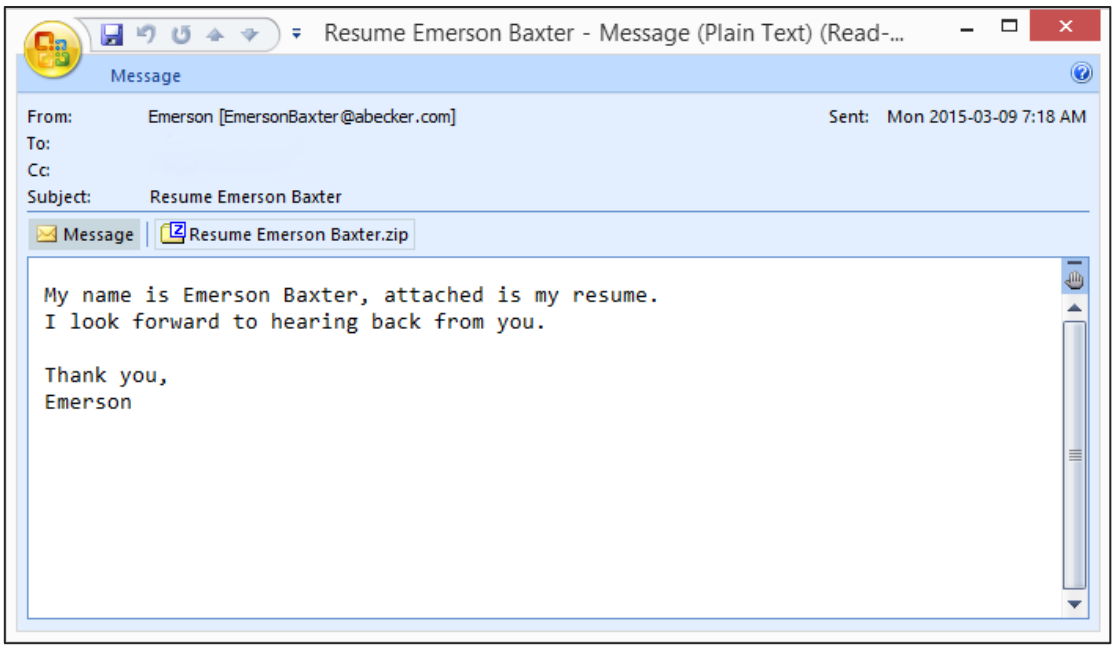
Outline

The NCSC is aware of a CryptoWall ransomware campaign currently impacting New Zealand organisations. CryptoWall is malicious software that encrypts files on an infected computer including any files accessible on network drives. The victim is then required to pay a ransom to have the files decrypted and access restored.

Cryptowall is being distributed through email campaigns that entice recipients into opening a malicious attachment, by such methods as claiming the attachment is a bill, a special offer or a delivery notice.

The current campaign is using a “Resume” theme with a zip file attachment containing a malicious JavaScript file.

An example of the current campaign is attached below:



P O Box 12-209, Wellington, New Zealand | incidents@ncsc.govt.nz | Phone: +64 4 498 7654 | Fax: +64 4 498 7655

Specific Recommendations

The NCSC recommends specific mitigations to protect against this threat:

- Advise employees not to open unsolicited email attachments or follow unsolicited web links in emails.
- Conduct routine backups of important files, keeping backups stored offline.
- Ensure computer systems are running antivirus software with the latest signatures.
- Consider implementing application whitelisting or, at least, software restriction polices to prevent the malicious software executing successfully. For more information on how to configure Software Restriction Policies, please see these articles from Microsoft:
    - http://support.microsoft.com/kb/310791
    - http://technet.microsoft.com/en-us/library/hh994606.aspx

General Recommendations

To protect against this and other cyber security threats NCSC recommends implementing the Australian Signals Directorate's Top four mitigation strategies; application whitelisting, patching systems, restricting administrative privileges, and create a defence in depth system. For more information see:

- www.asd.gov.au/publications/protect/top_4_mitigations.htm

P O Box 12-209, Wellington, New Zealand | incidents@ncsc.govt.nz | Phone: +64 4 498 7654 | Fax: +64 4 498 7655

Technical Analysis:

The NCSC has performed initial analysis on several copies of the CryptoWall email and malicious files. The following may be useful to aid in detection:

Email subjects:

Resume <name>

Email Attachments:

Resume <name>.zip
Resume <name>.js

URL's:

http://grandviewconsulting.net/images/rep.jpg
http://dorttlokolrt.com/images/one.jpg
http://dorttlokolrt.com/images/two.jpg

Files:

rep.jpg (6fae4aed182cb0df0ed705acadee2fde)
one.jpg (c53deb03a46b6333bc1c03294f9cbb08)
two.jpg (7444847a676b926774fed86a0e248585)

File Paths:

%Temp%
C:\<random>\<random>.exe
C:\Users\<User>\AppData\Roaming\<random>.exe

Associated Domains:

sehpam.com
caliskan-guvenlik.com
youngprofreshional.com
aseanian.com
judora-ng.com
ehcc.us
sam73cyber.com
iuliasalaria.org
drdigitalmd.com
baankhon.com
ferienwohnungen-diana.com
steveloosphoto.com
90.surfband.info
sooimchae.com
highendtile.net
futong8.com
azquasoft.com
ouarzazateonline.com
tryea.com
bn369.com
bijouxbjx.com
ineshworld.com
filemade.com
shark09.com
bikeviet.com
warmchurch.com
bigtreeasset.com
fcserbiaunited.com
busanamuslim-online.com
sehpam.com
saikripamusicclass.com
miguelations.com
pandoracharters.com
plushandmore.com
haminalab.com
buildtrue.com
brandbeing.com
pskpc.net
std-check.info
mhxlongbinh.com
eapsegypt.com
xn---3-6kca2cpvkm2c3c.com
handheldphotos.com
alkhatip.com
cookbooksfree.com
gleegardening.com
leutezentrum.com
trillyo.com
plastemartmaterials.com
hscompany.net
giantuk.com
corporatemonks.com
newzealand-charm.com
geiliyou.com
smiliks.com
eturedesigns.com
pianogiare.com
cannabook.net
renohomeimprovementsllc.com
donopolyblocks.com
109tset.com
carvingstudio935.com
ruanlianjie.net
biofiltechnologies.com
bentleysco.com
weapex.com
houseofstarz.com
ocvitcamap.com
spark-leds.com
sapacmold.com
www.ubikate.mx
www.ebouw.nl
www.getserved.nl
www.multiposting.nl