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:
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 policies 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

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:

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://dorttlkolrt.com/images/one.jpg
http://dorttlkolrt.com/images/two.jpg

Files:
rep.jpg (6fae4aed182cb0df0ed705acadee2d6763e33aca0cde8f0e)
one.jpg (c53deb03a46b63337b1c03329109cba08)
two.jpg (7444847a676b926774fed86a0e248585)

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

Associated Domains:

sehpm.com
caisikan-guenilik.com
youngprofessionals.com
aseanian.com
judora-ng.com
ehcc.us
sam73cyber.com
iuliasalaria.org
drdigitalmd.com
baankhon.com
ferienwohnhungen-diana.com
steveloosphoto.com
90.surfband.info
sooimchae.com
highendfile.net
futong8.com
azquasoft.com
ouarazateonline.com
tryea.com
bn369.com
bijouxbx.com
ineshworld.com
filemade.com
shark09.com
bikeviet.com
warmchurch.com
bigtreesset.com
fcserbauinated.com
busanamuslim-online.com
sehpm.com
saikripamusicclass.com
miguepam.com
pandoracharters.com
plushandmore.com
haminalab.com
buildtrue.com
brandbeing.com
pskpc.net
std-check.info
mmlxongbhn.com
eapsegc.com
xn--3-bkca2cpvk2c3c.com
handheldphotos.com
alkhatip.com
ookbooksfree.com
gleegardening.com
leutezentrum.com
trillyo.com
plastemartmaterials.com
hscompany.net
giantuk.com
corporatemonsks.com
newzealand-charm.com
geliyou.com
smilks.com
eturedesigns.com
pianogiae.com
cannobook.net
renohomeimprovementsilc.com
donopolyblocks.com
109tsets.com
carvingstudio935.com
ruanlianje.net
biofieltechnologies.com
bentleysco.com
weapex.com
houseofstarz.com
ovctilcamap.com
spark-leds.com
sapamold.com
www.ubikate.mx
www.ebouw.nl
www.getserved.nl
www.multposting.nl

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.