Volume 2016-334-1

Locky Ransomware (sender creditcontrol@)

Summary
Cautela Labs is aware of a recently discovered Locky ransomware attack. The subject line is **"Please find attached a XLS Invoice 293192 (random numbers)"** with a sender of **"creditcontrol@"** random company name. The email contains a malicious Excel XLS spreadsheet attachment that delivers Locky.

Detailed Information
An email with the subject line **"Please find attached a XLS Invoice 293192 (random numbers)"** pretending to come from **"creditcontrol@"** random company name contains a malicious Excel XLS spreadsheet attachment that delivers the Locky ransomware.

The perpetrators are using email addresses and subject lines designed to scare or entice a user to read the email and open the attachment. A very high proportion of these emails are being targeted toward small and medium size businesses, with the hope of getting a better response than they do from consumers.
These all spoof Ansell Lighting in the body of the email, and the senders or alleged senders are randomly chosen companies, none of which have actually been compromised and are not sending the emails. Their details have just been taken from a long list of companies and inserted into the email.

Ansell Lighting has not been hacked or had their email or other servers compromised. They are not sending the emails to you. They are innocent victims in the same way as every recipient of these emails.

The email looks like the following:

From: creditcontrol@riversideglass.com
Date: Tue 29/11/2016 08:01
Subject: Please find attached a XLS Invoice 293192
Attachment: INVOICE.TAM_293192_20161129_C415186AD.xls
Body content:
Please find attached your Invoice for Goods/Services recently delivered. If you have any questions, then please do not hesitate in contacting us. Karen Lightfoot -Credit Controller, Ansell Lighting, Unit 6B, Stonecross Industrial Park, Yew Tree Way, WA3 3JD. Tel: +44 (0)3624 094 531 Fax: +44 (0)3624 094 531

Affected systems per researchers

- All the alleged senders, companies, names of employees, phone numbers, amounts, reference numbers etc. mentioned in the emails are all innocent and are just picked at random. Some of these companies will exist and some won't.
- Don't try to respond by phone or email, as the person answering the call is not involved in this scam. They have also had their personal or company details spoofed and picked at random from a long list that the perpetrators have collected.

- The perpetrators are choosing companies, government departments and other organizations with subjects that are designed to entice or alarm recipients into blindly opening the attachment or clicking the link in the email.
- At this time, these malicious macros only infect Windows computers.
- They do not affect a Mac, iPhone, iPad, Blackberry, Windows phone or Android phone.
- These macros do not run in Office Online, Open Office, Libre Office, Word Perfect or any other office program that can read Word or Excel files

Corrective Action

- Newer Microsoft Office versions such as Office 2010, 2013, 2016 and Office 365 should be automatically set to higher security to protect you.
- By default protected view is enabled and macros are disabled, UNLESS you or your company have enabled them.
- If protected view mode is turned off and macros are enabled then opening this malicious Excel document will infect you. Simply previewing it in Windows Explorer or your email client might well be enough to infect the system.
- Some versions pretend to have a digital RSA key and say you need to enable editing and Macros to see the content.
- Do NOT enable Macros or editing under any circumstances.

Additional References

https://myonlinesecurity.co.uk/please-find-attached-a-xls-invoice-spoofing-ansell-lighting-delivers-locky/