National Cybersecurity and Communications Integration Center

17 October 2014

Suspicious "Invoic" Email Sent to Government Personnel

Summary

On 15 October 2014, a phishing email was dispersed to a wide variety of government employees. NCCIC has also received a number of reports indicating that members within the Education Sector and Financial Sector; International, State, Local, and Tribal organizations have also received similar email messages. The email suggested that the recipient had an unpaid debt and the attachment was an invoice showing the debt information. The subject line reads "UNPAID INVOIC" and the content simply instructs recipients to open the attachment which is a PDF file that is believed to be malicious. Rather than installing malware files from the PDF file itself, it appears to use embedded JavaScript within the file to redirect victims to a malicious website where additional malware can be installed.[1,2,3]

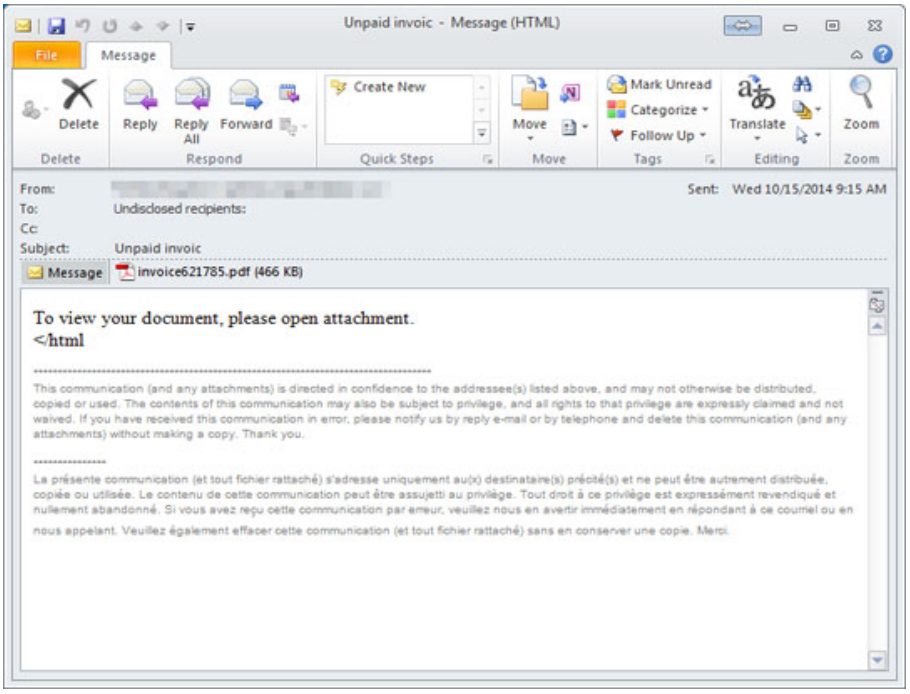

Figure 1: Screen shot of one of the phishing messages.

The following technical indicators were found through initial analysis findings:

- File: invoice621785.pdf
- Size: 476741
- MD5: 536445d39de9f19947aa493c1ee57751

It should be noted that the PDF file's naming convention has been observed with different numerical values following the word "invoice" and invoice is spelled correctly in some of the email messages and incorrectly in others, but the campaign is likely the same.

Analysis conducted on the MD5 Hash in VirusTotal yields that only 29 of 54 possible security vendors are detecting it[4] right now and there is a possibility that the campaign could eventually lead to machines becoming compromised with the Dyre/Dyreza banking malware.[5,6] Dyreza is similar to many other types of banking malware in that it exploits vulnerability within the infected machine's system, gives malicious actors remote access onto the infected machine, and intercepts sensitive login information (e.g. usernames and passwords).[7,8] Most of the major security vendors (F-Secure, AVG, BitDefender, McAfee, Kaspersky, Symantec, and so on) are detecting the malware[9]; however, there is a possibility that this campaign could be using a newer variant of the Dyre/Dyreza banking malware.[10]

Vendor Naming Convention of Detected Malware:[11]

- AVG – Exploit_c.ABHT
- F-Secure – Exploit.PDF.CVE-2013-2729.A
- Kaspersky – Exploit.PDF.Agent.c
- McAfee – Exploit-CVE2013-2729
- Microsoft – Exploit:JS/Pdfjsc.BC
- Symantec – Trojan.Pidief
- TrendMicro – TROJ_PIDIEF.YYJU

Possible Malicious IP addresses:[12]

- 63.167.150.122
- 64.50.186.140
- 65.55.169.133
- 65.55.169.124
- 74.114.188.69
- 159.220.28.56
- 157.56.110.117
- 157.56.110.130
- 157.56.110.148
- 216.22.15.81

The following email addresses were observed sending similar phishing messages:[13]

- Tharvey[@]vista-dental.com
- Jerry.Beets[@]pilottravelcenters.com
- Alena.Karatkevich[@]ppnc.org
- Jed[@]countertrade.com
- Charlieg[@]glendinningprods.com
- aris.tzounakos[@]aon.ca
- Pthorpe[@]samuel.com
- jacky.williams[@]thomsonreuters.com

Initial findings suggest that the campaign aims to exploit vulnerabilities CVE-2013-2729[14] and CVE-2010-0188[15]; both of which exploit vulnerability within Adobe Reader and Acrobat. Each of these vulnerabilities are old and Adobe has issued patches and software updates that do address these vulnerabilities.[16,17] A good suggestion for those who received this message would be to verify the version of Adobe and Acrobat they are using and if outdated, implementing the updates is recommended.

This is a good example of how malicious cyber actors often reuse old tactics and techniques. This is also a good example of how important it is to follow best practices[18] and install updates and patches for software applications as they become available. Users that have the most updated versions of both Adobe and Acrobat likely would not be vulnerable to this attack as it does not seem to function with updated versions, but those who received the message should still be cautious.

Victims who may have opened the attachment or who may have questions should direct concerns to their respective Security Special Operations Center (SOC). If one did open the attachment, it is recommended that they turn off the computer and contact their respective organization's IT department to report the potential issue.[19,20]

Who Can I Share This With?

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Contact Information:

Any questions regarding this advisory can be directed to DHS NCCIC and to be added to the normal distribution for similar products, please send requests to NCCIC@hq.dhs.gov or (888) 282-0870.

References

[1] Trusted Third Party Analysis
[2] Old Adobe Vulnerability Used in Dyreza Attack, accessed 17 October 2014, http://www.viruss.eu/malware/old-adobe-vulnerability-used-in-dyreza-attack-targets-bitcoin-sites-2/
[3] Adobe Vulnerability Leads to Dyreza Attack, accessed 17 October 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/old-adobe-vulnerability-used-in-dyreza-attack-targets-bitcoin-sites/
[4] VirusTotal Detection Ratio, accessed 16 October 2014, https://www.virustotal.com/en/file/6b6fdc4b116802728ec763ac7b25472046465dd0cf58146b3755e7efcb83f135/analysis/
[5] New Banking Malware Dyreza, accessed 16 October 2014, http://www.pcworld.com/article/2364360/new-powerful-banking-malware-called-dyreza-emerges.html
[6] VirusTotal Analysis, accessed 16 October 2014, https://www.virustotal.com/en/file/6b6fdc4b116802728ec763ac7b25472046465dd0cf58146b3755e7efcb83f135/analysis/
[7] New Banking Malware Dyreza, accessed 16 October 2014, http://www.pcworld.com/article/2364360/new-powerful-banking-malware-called-dyreza-emerges.html
[8] VirusTotal Analysis, accessed 16 October 2014, https://www.virustotal.com/en/file/6b6fdc4b116802728ec763ac7b25472046465dd0cf58146b3755e7efcb83f135/analysis/
[9] VirusTotal Detection Ratio, accessed 16 October 2014, https://www.virustotal.com/en/file/6b6fdc4b116802728ec763ac7b25472046465dd0cf58146b3755e7efcb83f135/analysis/
[10] Trusted Third Party Analysis
[11] VirusTotal Summary for Listed MD5 Hash, accessed 17 October 2014, https://www.virustotal.com/en/file/6b6fdc4b116802728ec763ac7b25472046465dd0cf58146b3755e7efcb83f135/analysis/
[12] Trusted Third Party Analysis
[13] Trusted Third Party Analysis
[14] Mitre Summary of CVE-2013-2729, accessed 16 October 2014, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2729
[15] Mitre Summary of CVE-2010-0188, accessed 16 October 2014, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188
[16] Adobe Security Updates Addressing CVE-2013-2729, accessed 16 October 2014, http://www.adobe.com/support/security/bulletins/apsb13-15.html
[17] Adobe Security Updates Addressing CVE-2010-0188, accessed 16 October 2014, http://www.adobe.com/support/security/bulletins/apsb10-07.html
[18] Symantec Patch Management Best Practices, accessed 16 October 2014, http://www.symantec.com/business/support/index?page=content&id=HOWTO3124
[19] Old Adobe Vulnerability Used in Dyreza Attack, accessed 17 October 2014, http://www.viruss.eu/malware/old-adobe-vulnerability-used-in-dyreza-attack-targets-bitcoin-sites-2/
[20] Adobe Vulnerability Leads to Dyreza Attack, accessed 17 October 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/old-adobe-vulnerability-used-in-dyreza-attack-targets-bitcoin-sites/