Zeus Panda Banking Trojan Targets Online Holiday Shoppers

proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers

December 14, 2017

Blog
Threat Insight
Zeus Panda Banking Trojan Targets Online Holiday Shoppers

December 14, 2017 Proofpoint Staff

Overview

Banking Trojans work by injecting code into web pages as they are viewed on infected machines, allowing the malware to harvest banking credentials and credit card information as victims interact with legitimate sites. Most often, the injects -- the code that actually performs the man-in-the-browser attacks -- are configured for region-specific banking sites. More recently, we have seen injects for online payment sites, casinos, retailers, and more appearing in banking Trojan campaigns.

Since November -- a period of time that includes Thanksgiving, Black Friday, Cyber Monday and now leading up to Christmas -- we have observed Zeus Panda banking Trojan campaigns that have an increasing focus on non-banking targets with an extensive list of injects clearly designed to capitalize on holiday shopping and activities.

More specifically, these Zeus Panda (aka Panda Banker) campaigns expanded their injects to a variety of online shopping sites for brick and mortar retailers like Zara, specialty online retailers, travel sites, and video streaming sites, among others. The vast majority of these new targets will potentially see higher-than-normal numbers of credit card transactions for the holidays. While Zeus Panda can be configured to steal a variety of information, these injects collected the credit card number, address, phone number, DOB, SSN, and security question-related information such as mother's maiden name.

Analysis

On December 11, a campaign targeted UK business users with a fake resume attachment named "resume.doc" (Figure 1) delivered via email. The subject line "Application submitted from Gumtree Jobs by [First Last Names] for Field Sales Consultant - Status: Emailed" referenced a job application via "Gumtree Jobs", a legitimate jobs and classified advertising platform with users in the UK, Australia, New Zealand, and South Africa. The actor abused the Gumtree brand to lend legitimacy to the campaign but the site itself was not directly abused to send the fraudulent applications.

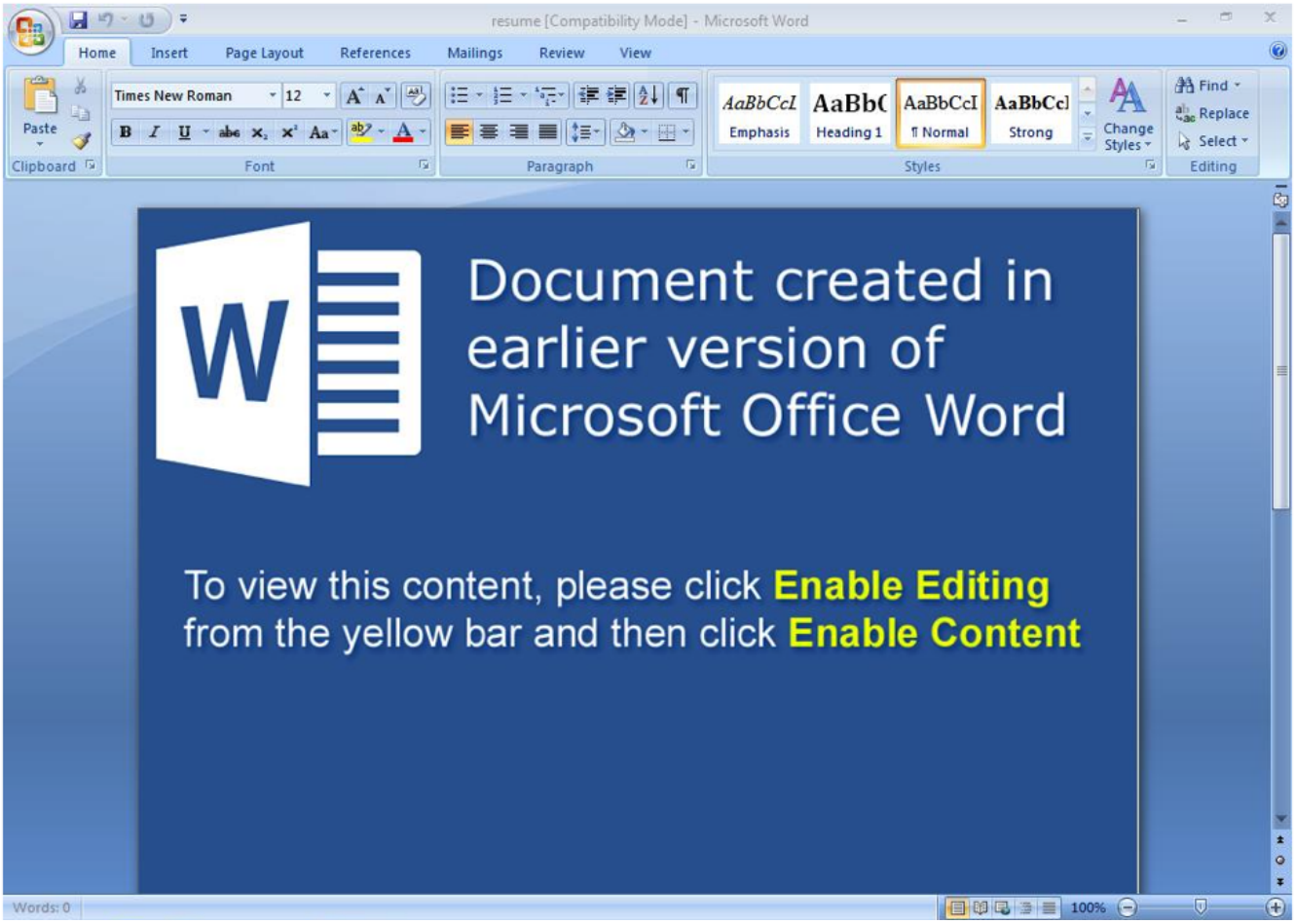

Figure 1: Fake resume document attachment contains macros that, if enabled, launch PowerShell code to download Zeus Panda

However, we first observed this instance of Zeus Panda targeting Canadian companies in November, before the Thanksgiving holiday. For example, on November 13, we observed malicious emails with the subject “Your package is ready to be picked up” containing URLs linking to Microsoft Word documents such as “receipt-package-5a0a062cae04a.doc”. The documents used macros to download Zeus Panda.

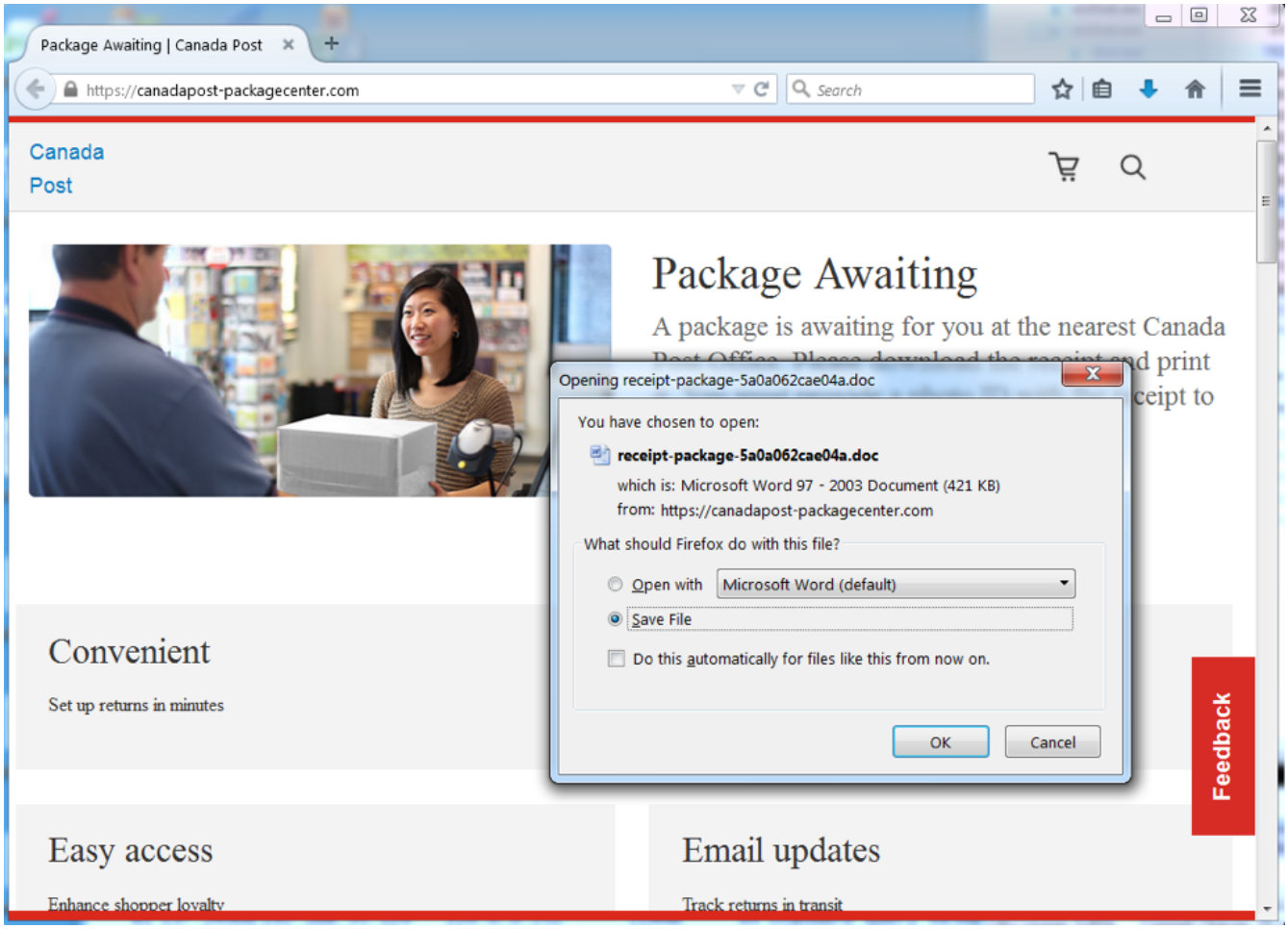

Figure 2: The malicious URLs redirect to another landing page (hxxps://canadapost-packagecenter[.]com/), which in turns starts the document download

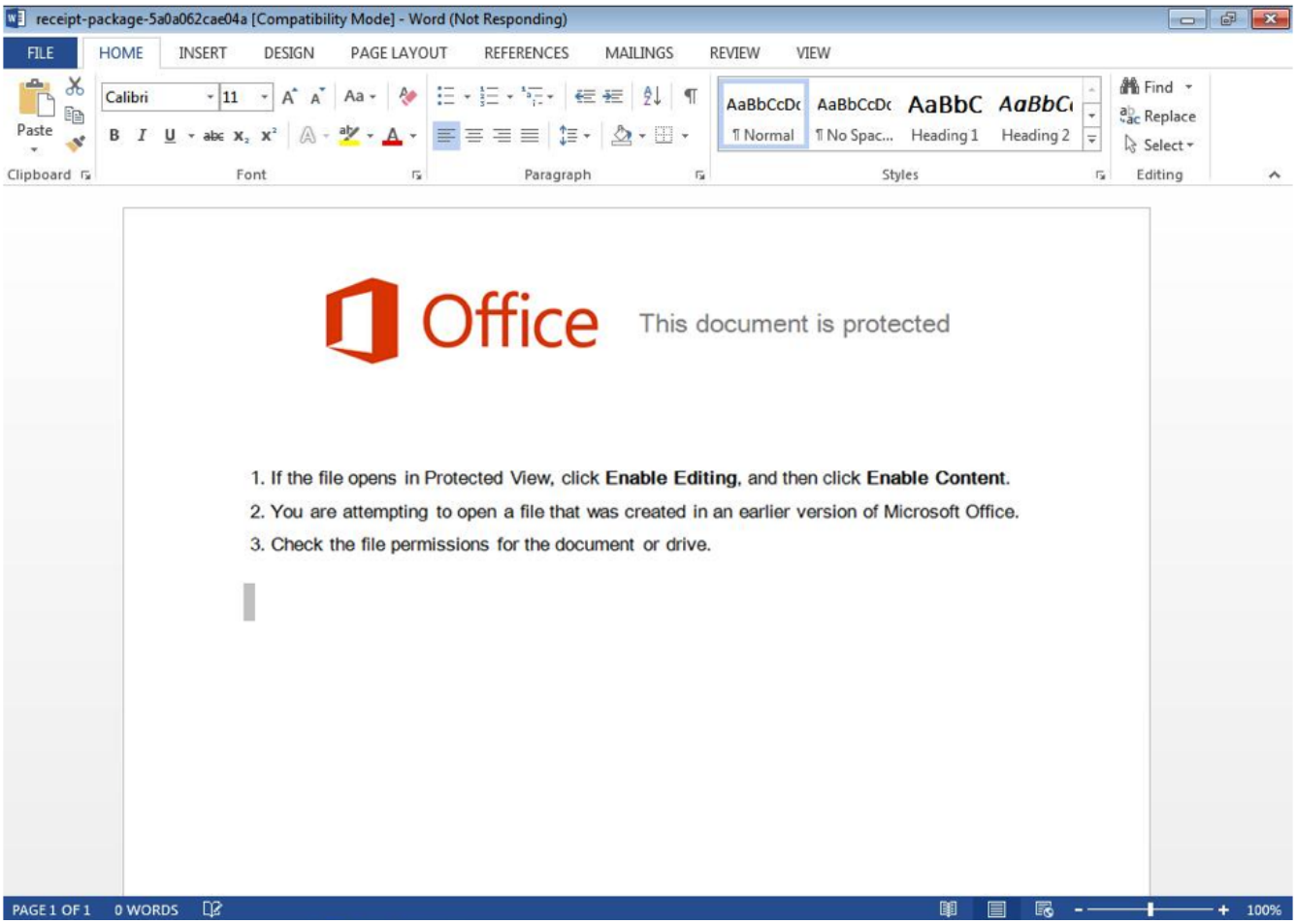

Figure 3: The malicious document receipt-package-5a0a062cae04a.doc contains macros that, if enabled, launched PowerShell code to download Zeus Panda

These instances of Zeus Panda include injects that feature wildcards for increased flexibility and, as noted, target a disproportionate number of non-bank organizations. This campaign provides an example of the ongoing evolution of banking Trojans and their uses, as well as the tendency for threat actors to built campaigns around major events and seasonal trends.

Conclusion

Users infected with banking Trojans like Zeus Panda often do not know they are infected as the malware conducts man-in-the-middle/browser attacks, quietly harvesting credit card numbers or banking credentials as users visit legitimate banking and online shopping sites. While we have reported on previous examples of banking Trojans targeting non-banking services, the timing and specific injects of these recent attacks are clearly focused on online holiday shoppers, travelers, and holiday activities, with far more retail-related and other non-banking injects than we normally associate with a banking Trojan attack. For consumers, keeping endpoint protection up to date is the best defense, although few endpoint antivirus systems can currently detect the malicious nature of this particular document. Organizations can protect users at many levels - the email gateway, the network gateway, and the endpoint. During the holidays, when many users will be traveling or using corporate devices from home, requiring the use of a VPN can ensure that computers are protected and banking Trojan-related traffic can be detected and blocked whether or not a user is physically in the office.

Indicators of Compromise (IOCs)

December 11 campaign

IOC	IOC Type	Description
hxxp://80.82.67[.]217/moo[.]jpg	URL	Document payload
5f7a1b02d5b2904554e65bd01a12f1fa5ff2121eef53f3942c4e9e29c46bdce3	SHA256	Panda
gromnes[.]top	Domain	Panda C&C
aklexim[.]top	Domain	Panda C&C
kichamyn[.]top	Domain	Panda C&C
e13594d83f2a573627e742baf33298b9eeec1ebb8c7955304b8c35559e5f23dc	SHA256	Attachment

November 13 campaign

IOC	IOC Type	Description
hxxp://www.nfk-trading[.]com/analyticsmmrxbctq/redirect/0849e22e843170e1600c1910df8cf9da-id-qblozsmn-to-package-awaiting	URL	Malicious URL in email
hxxps://canadapost-packagecenter[.]com/	URL	Landing page redirection
2514dbf1549b517692e415af85baa6e5eca926cdedb526d2e255b5943501d98b	SHA256	receipt-package-5a0a062cae04a.doc
hxxp://89.248.169[.]136/bigmac.jpg	URL	Document payload
ae92a4a5bc64db6af23219d7fa2d8bce98a5d7eb2eff7193e4f49698e3e5650d	SHA256	Bigmac.jpg (Panda executable)
gromnes[.]top	Domain	Panda C&C

ET and ETPRO Suricata/Snort Signatures

2825353 | ETPRO TROJAN Zeus Panda Banker Malicious SSL Certificate Detected

Subscribe to the Proofpoint Blog