TA505 targets the US retail industry with personalized attachments | Proofpoint US

By December 06, 2018 Proofpoint Staff

Published: 2018-12-06 · Archived: 2026-04-05 18:20:47 UTC

Overview

Since November 15, 2018, Proofpoint began observing email campaigns from a specific actor targeting large retail chains, restaurant chains and grocery chains, as well as other organizations in the food and beverage industries. These email campaigns attempted to deliver various malware families, including Remote Manipulator System (RMS) and FlawedAmmyy, among others.

We also observed personalization of attachments in one such campaign. These attachments included the targeted company's logo in the body of the attachment to make messages more believable.

We attributed these campaigns to TA505, the actor behind the largest Dridex and Locky ransomware campaigns of the last two years and more recently associated with distribution of remote access Trojans (RATs) and downloaders. This change in tactics -- the use of personalized attachments in moderately large campaigns combined with retail industry targeting -- arrives just in time for the holiday shopping season.

Campaign Details

On December 3, 2018, we observed a TA505 campaign targeting almost exclusively retail, grocery, and restaurant chains. This campaign distributed tens of thousands of messages.

More interestingly, each intended target received a personalized attachment, a technique that TA505 has not previously used. The email (Figure 1) purported to be sent from a Ricoh printer and contain a scanned document. The bogus scan was actually a malicious Microsoft Word attachment (Figure 2). The document attached was unique to the targeted company, and even contained the targeted company's logo in the document lure (blurred in the figure with a black box).

The document contains macros that, if enabled, downloaded and executed an MSI file. The execution leads to the installation of Remote Manipulator System (RMS) with a settings file that contains a custom command and control (C&C) address.

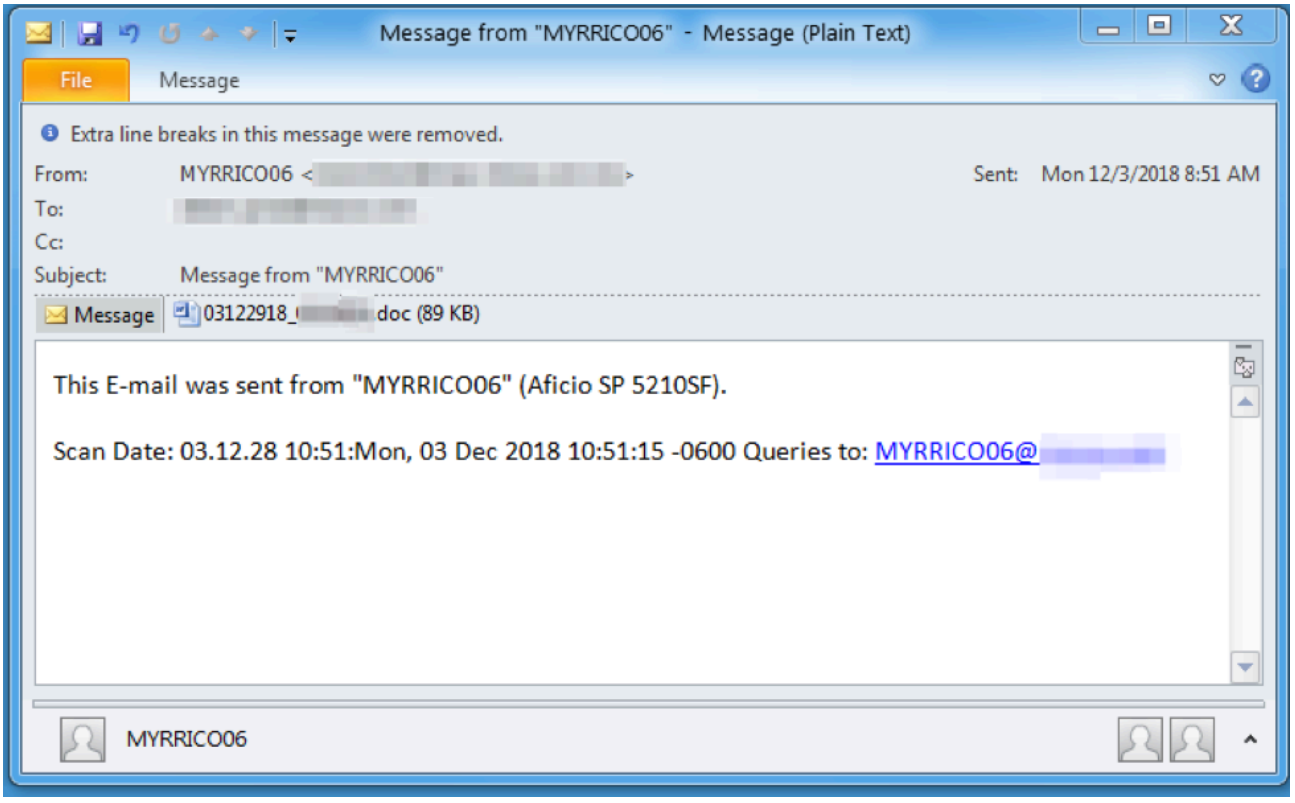

Figure 1: Email used in attempts to deliver malicious document on December 3

The lure shown in Figure 2 continues the social engineering introduced in the email, enticing recipients to enable macros so that they can view the contents of the fake scanned document.

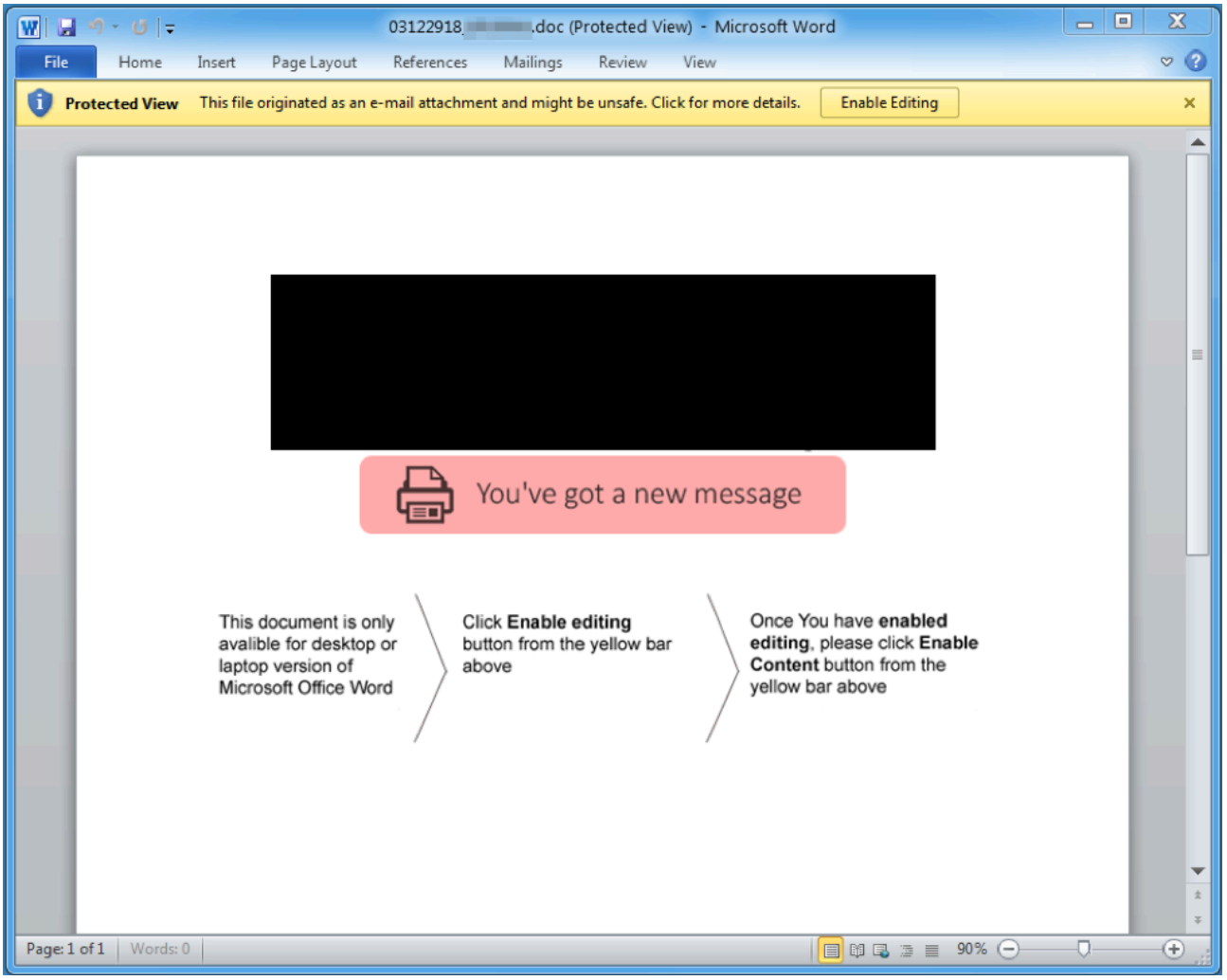

Figure 2: Attached document with the logo blacked out and social engineering to trick recipients into enabling macros

Conclusion

TA505 has helped shape the threat landscape for years, largely because of the massive volumes associated with their campaigns through the end of 2017. When this group changes tactics, it tends to correspond to broader shifts and, throughout the year, we have seen both TA505 and a number of other actors focus on downloaders, RATs, information stealers, and banking Trojans, often in smaller, more targeted campaigns. Threat actors follow the money and, with dropping cryptocurrency values, the return on investment in better targeting, improved social engineering, and management of persistent infections now seems to be greater than that for large “smash and grab” ransomware campaigns.

Given the ongoing holiday shopping season, the clear US retail and grocery targeting associated with these campaigns, and the nature of the malware they are distributing -- RATs and backdoors -- TA505 appears poised to take advantage of increased activity in this sector through the end of the year.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
hxxp://local365office[.]com/content	URL	Document payload
9206f08916ab6f9708d81a6cf2f916e2f606fd048a6b2355a39db97e258d0883	SHA256	RMS MSI dropper
06c637ac62cab511c5c42e142855ba0447a1c8ac8ee4b0f1f8b00faa5310fe9f	SHA256	Self-extracting RAR containing RMS
609b0a416f9b16a6df9b967dc32cd739402af31566e019a8fb8abdf3cb573e30	SHA256	RMS RAT
89.144.25[.]32:5655	IP:Port	RMS RAT C&C
0F 2B 44 E3 98 BA 76 C5 F5 77 79 C4 15 48 60 7B	Certificate Serial	Serial number of the code signing certificate
DIGITAL DR	String	Subject name of the code signing certificate

ET and ETPRO Suricata/Snort Signatures

2812668 ETPRO POLICY Remote Utilities Access Tool Activity

Subscribe to the Proofpoint Blog
