Emotet Tests New Delivery Techniques

April 26, 2022 Axel F

Key Findings

- Proofpoint identified low-volume Emotet activity that drastically differed from typical Emotet threat behaviors.
- The activity occurred while Emotet was on a “spring break,” not conducting its typical high volume threat campaigns. The threat actor has since resumed its typical activity.
- Proofpoint assesses that the threat group distributing Emotet is likely testing new tactics, techniques, and procedures (TTPs) on a small scale before adopting them in broader campaigns or to deploy them in parallel with the broad campaigns.
- The messages contained OneDrive URLs that hosted a zip archive containing XLL files dropping Emotet malware.
- This activity is attributed to TA542.

Overview

Emotet is a prolific botnet and trojan that targets Windows platforms to distribute follow-on malware. It was considered one of the most prolific cybercriminal threats before its disruption by global law enforcement in January 2021.

In November 2021, 10 months after its disappearance from the threat landscape, Proofpoint observed a reemergence of this notorious botnet, and since then, the group associated with Emotet, TA542, has targeted thousands of customers with tens of thousands of messages in multiple geographic regions. In some cases, the message volume reaches over one million per campaign.

However, the new activity observed by Proofpoint is a departure from their typical behaviors and indicates the group is testing new attack techniques on a small scale before adopting them for larger volume campaigns. Alternatively, these new TTPs may indicate that TA542 may now be engaged in more selective and limited attacks in parallel to the typical massive scale email campaigns.

Activity Details

Proofpoint detected a low volume of emails distributing Emotet. The sender emails appeared to be compromised. The emails were not sent by the Emotet spam module. The subjects were simple and contained one word such as "Salary". The email bodies contained only OneDrive URLs and no other content. The OneDrive URLs hosted zip files containing Microsoft Excel Add-in (XLL) files.

The zip archives and XLL files used the same lures as the email subjects, such as “Salary_new.zip.” This particular archive contained four copies of the same XLL file with names such as “Salary_and_bonuses-04.01.2022.xll”. The XLL files, when executed, drop and run Emotet leveraging the Epoch 4 botnet.

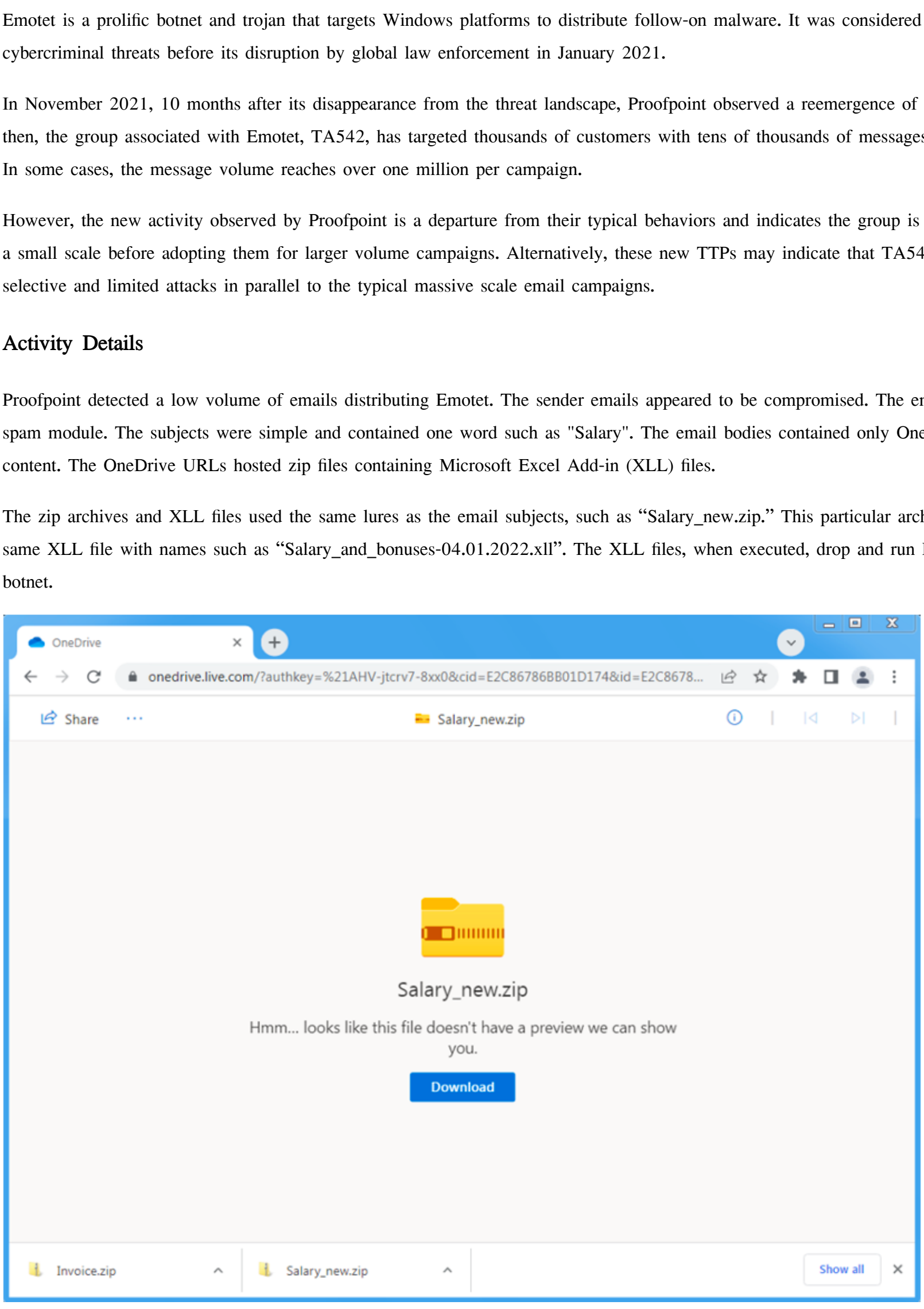

Figure 1: Example OneDrive URL hosting a zip archive

The identified activity differs from previously observed Emotet campaigns in the following ways:

- The low-volume nature of the activity. Typically, Emotet distributes high-volume email campaigns to many customers globally, with some campaigns in recent weeks hitting one million messages total.
- The use of OneDrive URLs. Typically, Emotet delivers Microsoft Office attachments or URLs (hosted on compromised sites) linking to Office files.
- The use of XLL files. Typically, Emotet uses Microsoft Excel or Word documents containing VBA or XL4 macros. XLLs are a type of dynamic link library (DLL) file for Excel and are designed to increase the functionality of the application.

Nevertheless, Proofpoint analysts attribute this activity with high confidence to threat actor TA542 because since 2014 the actor closely controlled the Emotet malware and is not rented it to other actors.

Additional Context

Proofpoint observed the activity at a time when the widespread Emotet campaigns were on pause (a “spring break”) between April 4, 2022, and April 19, 2022. Emotet has since resumed its high-volume campaigns. Proofpoint researchers assess that while on the break, TA542 continued development and testing of new attack vectors, specifically OneDrive URLs and XLL files, in preparation for using them on a wider scale. Alternatively, these new TTPs may indicate that TA542 may now be engaged in more selective and limited scale attacks in parallel to the typical mass scale email campaigns.

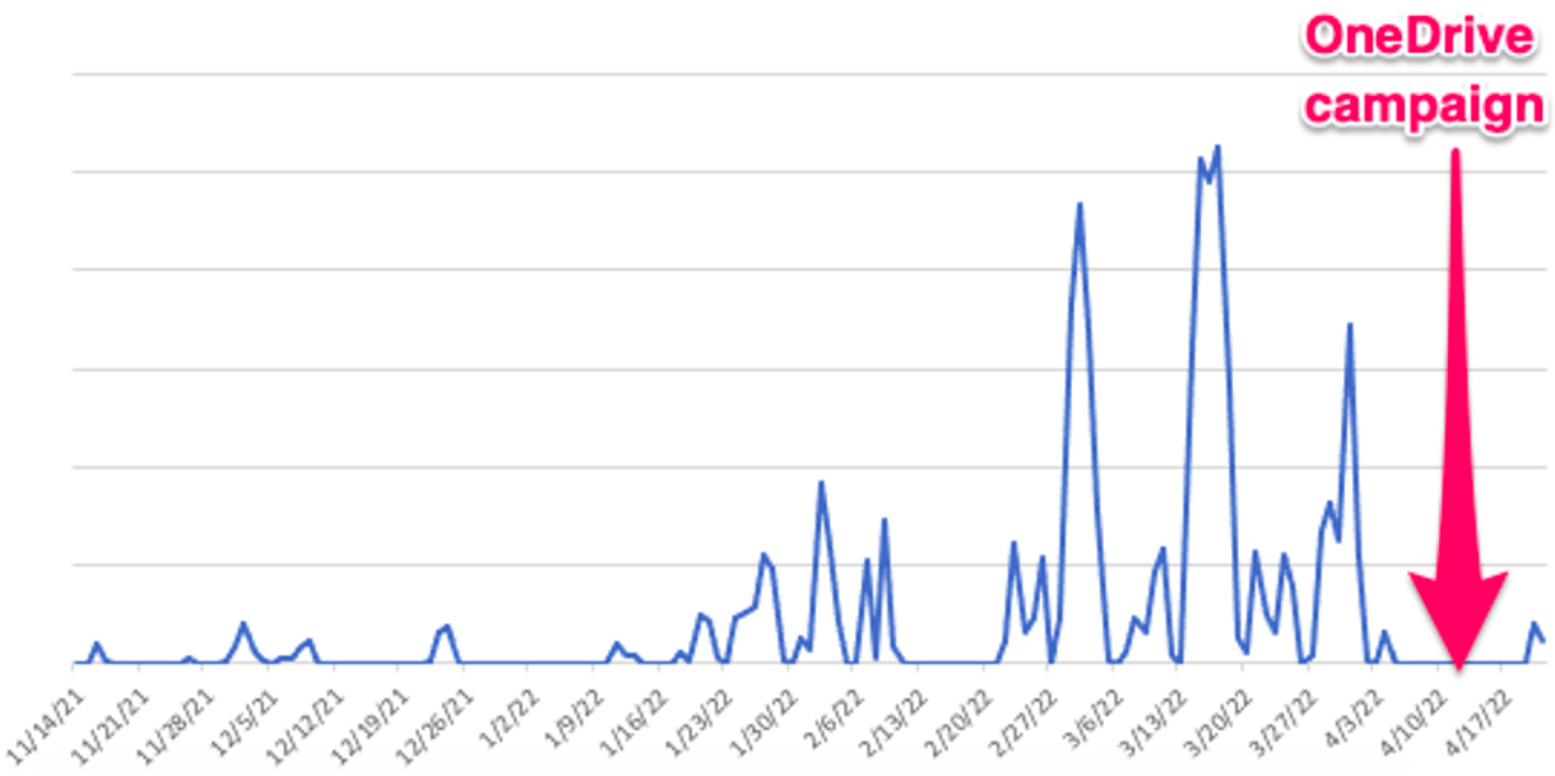

Figure 2: Plot of Emotet email volumes since November 2021

Additionally, it is notable that TA542 is interested in new techniques that do not rely on macro-enabled documents as Microsoft is making it increasingly difficult for threat actors to use macros as an infection vector. In February, Microsoft announced it would begin blocking Visual Basic for Application (VBA) macros obtained from the internet by default in April. This follows Microsoft’s announcement to disable XL4 macros in 2021. Typically, threat actors including TA542 that use macro-enabled attachments rely on social engineering to convince a recipient the content is trustworthy, and enabling macros is necessary to view it.

Indicators of Compromise (IOC)

Indicator		Description
https[:]//1drv[.]ms/u/s!AnTRAbuGZ8jie3V-jtcrv7-8xx0		Example URL leading to zipped XLL
2da9fa07fef0855b4144b70639be4355507612181f9889960253f61eddaa47aa	SHA256	Salary_new.zip
f83e9f85241d02046504d27a22bfc757ea6ff903e56de0a617c8d32d9f1f8411	SHA256	Salary_and_bonuses-01.01.2022.xll
8ee2296a2dc8f15b374e72c21475216e8d20d4e852509beb3cff9e454f4c28d1	SHA256	Emotet Payload ezesqrmrsbhftab.lft

Previous Blog Post