TA505 shifts with the times | Proofpoint US

By June 08, 2018 Proofpoint Staff

Published: 2018-06-08 · Archived: 2026-04-05 20:07:39 UTC

Overview

In September 2017, Proofpoint researchers detailed the history and ongoing activities of an actor we track as TA505. Throughout 2016 and 2017, TA505 was among the most prolific financially motivated actors we follow, regularly distributing massive malicious spam campaigns bearing diverse payloads ranging from Jaff ransomware to The Trick banking Trojan. TA505 was behind many of the Dridex campaigns that plagued organizations in 2015 and introduced Locky ransomware in 2016, bringing unprecedented scale to malicious spam distribution. Since we wrote our original TA505 profile, the actor has continued to explore the use of new malicious attachments and new payloads. In 2018, though, the scale and regularity of their campaigns decreased, while the diversity of payloads has increased. Given the importance of this actor in the email threat landscape we wanted to revisit our profile and update it with the latest activity from TA505.

For additional historical information on TA505, read our Actor Profile.

Activity since September 2017

Locky - September/October

By the fourth quarter of 2017, TA505 was still sending very high-volume campaigns primarily distributing Locky ransomware. As in the preceding months, TA505 pivoted through various attachment types to deliver the malicious payload. For the last half of September and the first half of October, the group primarily used VBScript files compressed in 7-Zip archives to distribute Locky Affiliate ID 3 (Affid=3). 7-Zip files are not natively supported in Microsoft Windows and require the installation of 7-Zip software; recipients also needed to execute the VBScript after installing 7-Zip and decompressing the attachments. While this combination of files is somewhat unusual for attachment campaigns and requires more user interaction than many, most researchers expect that TA505 was using new vectors to bypass protections put in place by organizations saturated with Locky-bearing messages over the previous year.

Geo-targeted Locky and The Trick - October

On October 10, TA505 introduced their first geo-targeted campaign dropping either Locky or The Trick banking Trojan. In this campaign, HTML files were attached to emails inquiring about the status of an invoice. When users opened the HTML attachments to view the fake invoice, embedded JavaScript downloaded The Trick banking Trojan with gtag "mac1" if the victim appeared to reside in the UK, Australia, Luxembourg, Ireland, or Belgium. All other victims received Locky (Affid=3 with file extension “.ykcol”).

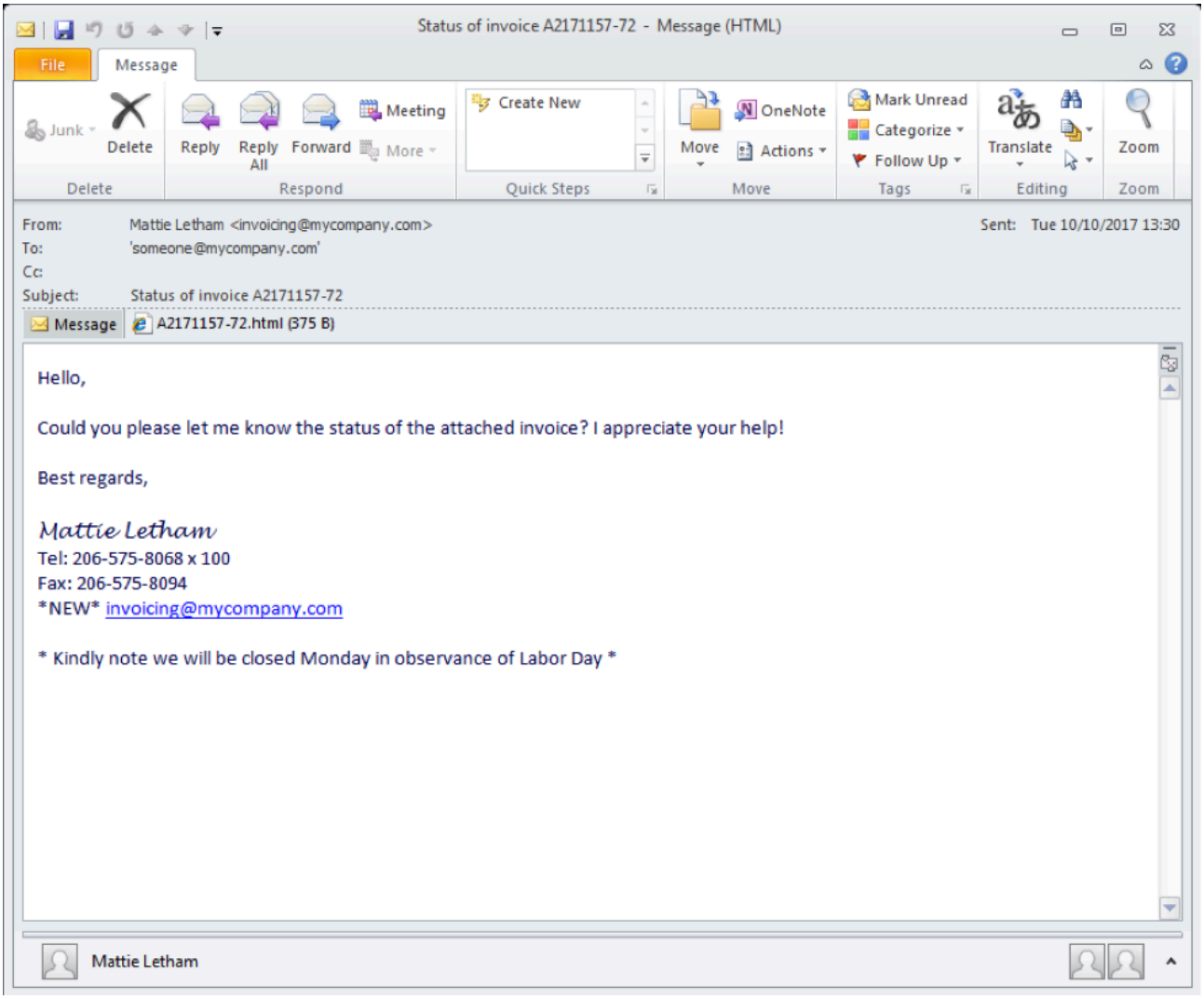

Figure 1: Lure email with .html attachment, October 10, 2017

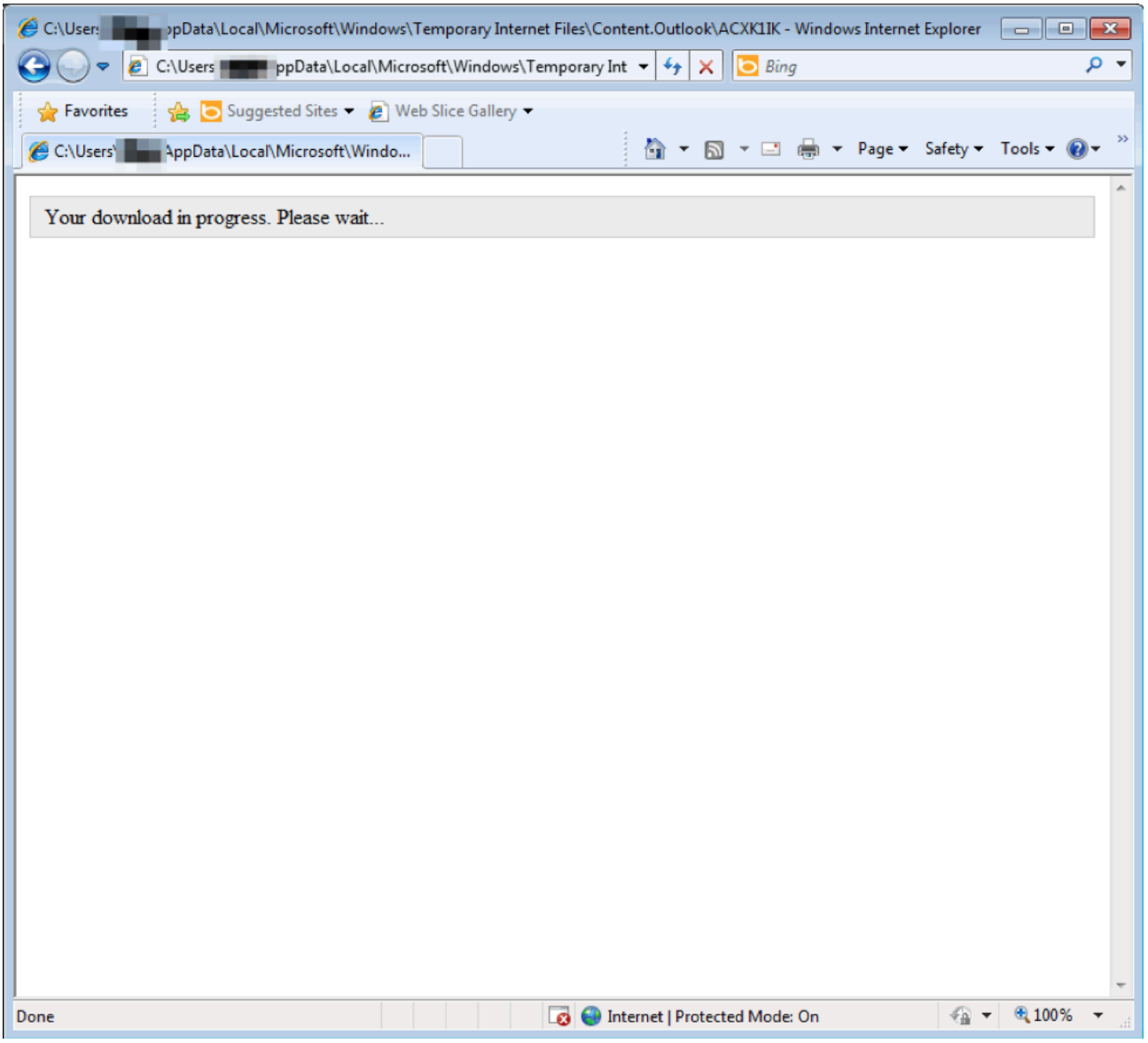

Figure 2: .html attachment with JavaScript that downloads the final payload, October 10, 2017

TA505 sent several similar campaigns in mid-October with VBScript compressed in 7-Zip files that also downloaded either Locky or The Trick. By late October, the actor switched to Microsoft Word attachments that abused Dynamic Data Exchange (DDE) to download either Locky or Locky and The Trick in several more geo-targeted campaigns. This was the first time that we observed TA505 abusing DDE, a legitimate feature in Microsoft Office that became a regular part of multiple threat actors' toolkits in Q4 2017. Recipients of these emails, which also used simple lures with attached fake invoices, needed to open the Microsoft Word attachments and click through a security dialog (Figure 3) to download the malware.

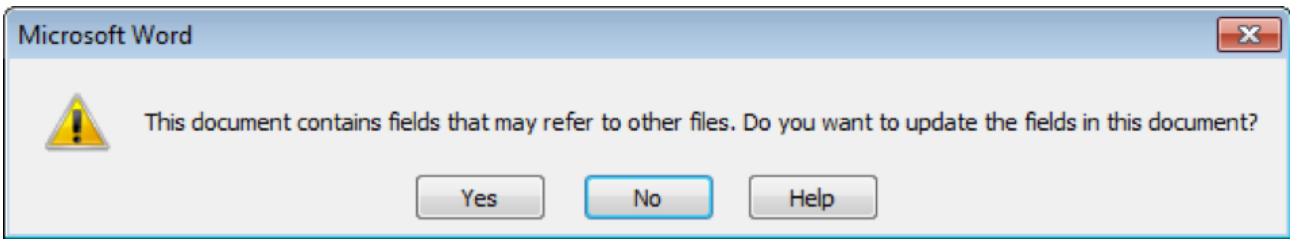

Figure 3: DDE confirmation associated with late-October campaigns

Embedded .lnk and .vbs - November

On October 31, TA505 sent two campaigns, both using .lnk files embedded in Microsoft Word documents. As shown in Figure 4, recipients must open the attached Word document, enable editing, and then execute the .lnk file by double clicking an image in the document. They must further confirm that they want to open the .lnk file (Figure 5), which, in turn, downloads an intermediate downloader. This downloader then downloads either Locky or The Trick depending on location. Despite the number of steps involved, TA505 relies on light social engineering in the email and lure as well as end user conditioning to proceed through the scheme and infect their PC with malware.

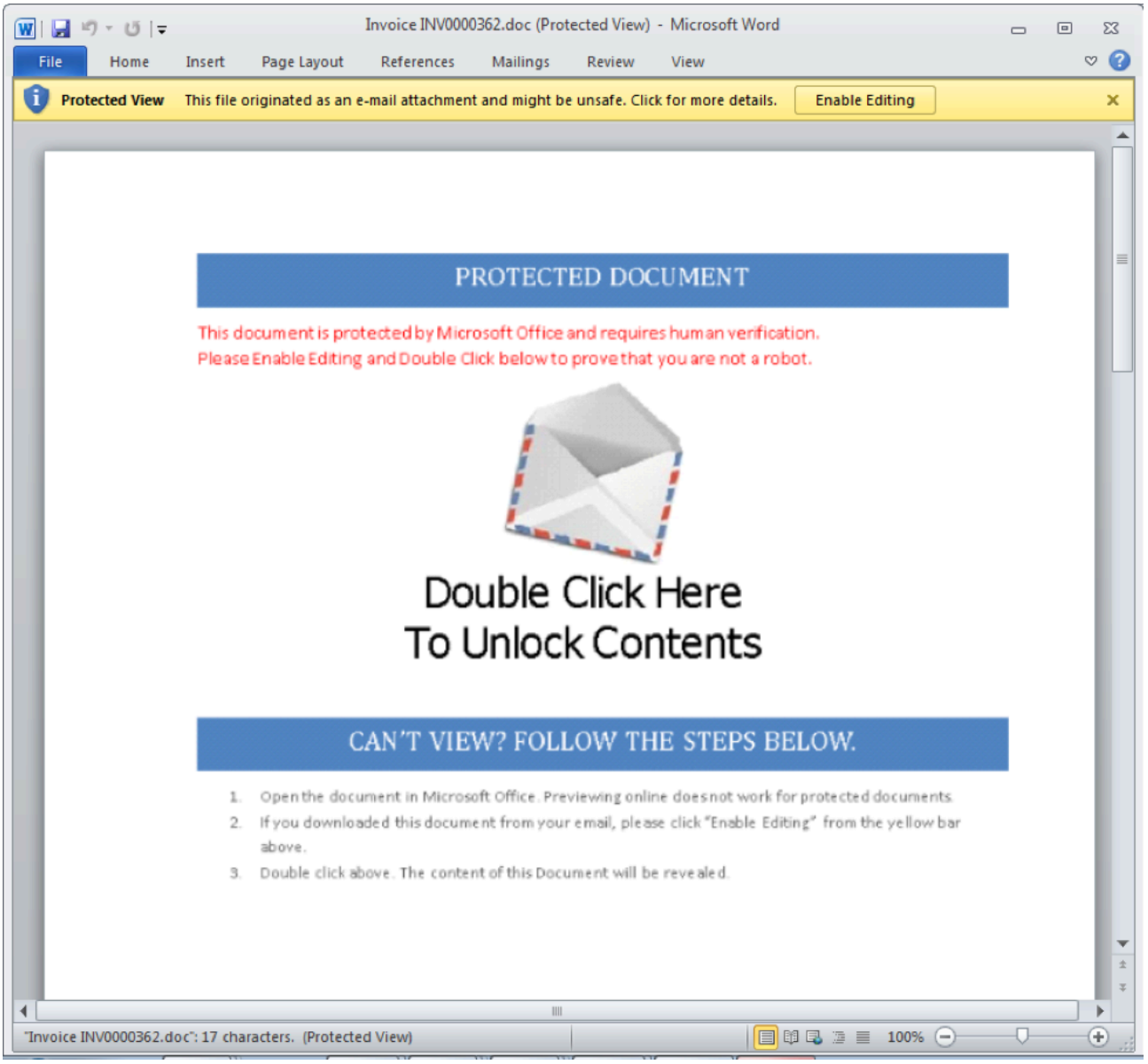

Figure 4: Microsoft Word document with embedded malicious .lnk file, October 31, 2017

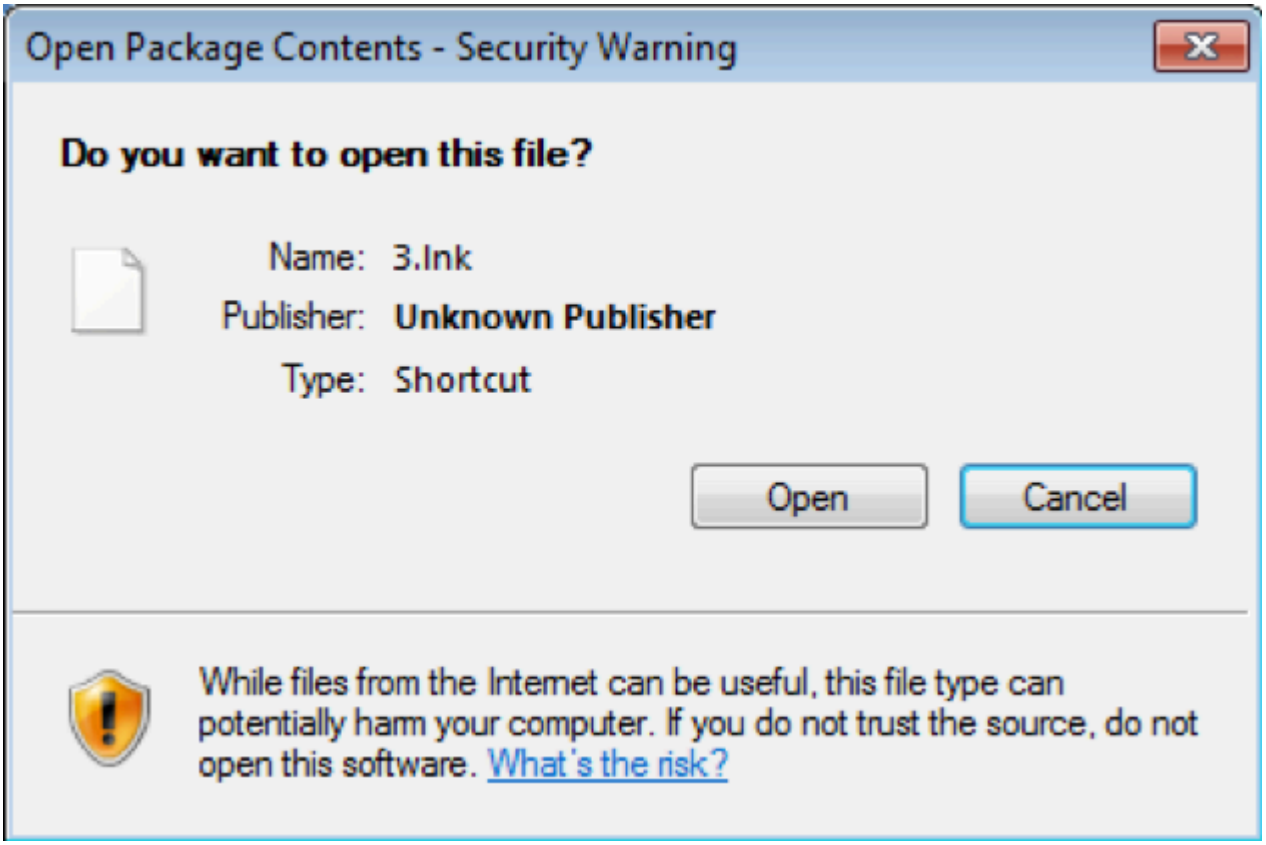

Figure 5: Security dialog for embedded .lnk file

Through November 9, TA505 distributed several such campaigns, sometimes two per day, largely distributing Locky. Activity for the rest of November was light, featuring only five more campaigns using embedded Visual Basic scripts in Word documents or VB Script in 7-Zip attachments to distribute The Trick, Dridex, Scarab ransomware, and GlobeImposter ransomware.

GlobeImposter - December

December saw yet another shift in payloads for TA505. Of the 34 campaigns the group sent in a month that was extremely active even by TA505 standards, 24 were distributing GlobeImposter ransomware. Like The Trick banking Trojan, GlobeImposter was a relatively low-profile, regionally focused malware strain that became a global threat when TA505 began distributing it in massive campaigns. The majority of these campaigns used malicious VBScript or JavaScript compressed in 7-Zip attachments.

The remaining ten campaigns in December distributed a range of malware including The Trick, the DreamSmasher reconnaissance tool, and Dridex.

Shifting to low-volume campaigns - January/February 2018

TA505 has typically taken some time to resume full operations after the Russian Orthodox holidays. The group is also heavily reliant on the Necurs botnet for its massive campaigns and its operators of the botnet appear to have lost control of the botnet for much of January and February. However, in previous years, Necurs disruptions resulted in complete silence from TA505. This year, the group remained active, though campaign frequency and volume were a tiny fraction of their peaks in 2017 during this period.

Rather, TA505 appeared to once again be exploring new payloads and vectors. We observed the actor send two large pharmaceutical spam campaigns via BlackTDS in February, a highly unusual move for a group focused on malicious attachments since at least 2014. We have also observed smaller campaigns distributing GandCrab ransomware, DreamSmasher, Dridex, and Quant Loader.

The slow return of Necurs-powered large campaigns - March 2018 to present

Beginning in March, TA505 launched several large campaigns, again utilizing the Necurs sending infrastructure, albeit much less frequently than in 2017. Campaigns in March and April largely delivered the FlawedAmmyy remote access Trojan (RAT), often via the intermediate Quant Loader malware. Attachments in these campaigns were frequently Zip archives containing ".url" files which, if opened and allowed by the user, downloaded Javascript via the SMB protocol. The Javascript then downloaded Quant Loader, which, in turn downloaded the FlawedAmmyy RAT. RATs are generally used in targeted attacks, begging the question how a threat actor distributing large-scale malicious spam might use such a tool.

We observed a handful of TA505 campaigns delivering FlawedAmmyy in late April and May, with the most recent occurring on June 7. While the frequency of these campaigns remains off from their normal cadence and message volumes still have not returned to 2017 levels, the trend of shifting vectors and experimentation with new techniques continues. The last two campaigns we observed from TA505 made use of .iqy attachments -- Microsoft Excel Web Query files are used to pull external data into Excel and, in these cases, the functionality was abused to download FlawedAmmyy.

Conclusion

Over the past four years, TA505 has introduced both Dridex and Locky to the threat landscape in relentless, massive email campaigns. The group also turned smaller targeted or regionally-focused malware like The Trick, GlobeImposter, and FlawedAmmyy into global phenomena. TA505 regularly changes vectors, shifts payloads, and experiments with new techniques, all apparently to bypass defenses and deliver payloads from bankers to RATs, often at a scale unmatched by other high-profile actors.

Their recent foray into large-scale distribution of RATs and intermediate loaders bears further observation as, unlike with Locky or GlobeImposter infections, victims may not realize they are infected until the group triggers additional malware installations or steals valuable data. The group’s willingness to explore new vectors, payloads, sending infrastructure, and other malicious services like BlackTDS, even when they do not have access to the Necurs spam cannon, exemplifies the adaptability of modern threat actors.
