Necurs Diversifies Its Portfolio

By Edmund Brumaghin

Published: 2017-03-20 · Archived: 2026-04-05 13:44:40 UTC

Monday, March 20, 2017 17:18

The post was authored by Sean Baird, Edmund Brumaghin and Earl Carter, with contributions from Jaeson Schultz.

Executive Summary

The Necurs botnet is the largest spam botnet in the world. Over the past year it has been used primarily for the distribution of Locky ransomware and Dridex. Earlier this year, we wrote about how the Necurs botnet went offline and seemingly disappeared, taking most of the high volume Locky malspam with it. Talos recently identified a significant increase in the amount of spam emails originating from the Necurs botnet, indicating that it may have come back to life, but rather than distributing malware in the form of malicious attachments, it appears to have shifted back to penny stock pump-and-dump messages. This is not the first time that Necurs has been used to send high volume pump-and-dump emails. In analyzing previous telemetry data associated with these campaigns, we identified a similar campaign on December 20, 2016 shortly before the Necurs botnet went offline for an extended period. This strategic divergence from the distribution of malware may be indicative of a change in the way that attackers are attempting to economically leverage this botnet.

Detailed Information

On March 20, 2017 we observed a marked increase in the amount of spam messages that appear to be originating from the Necurs botnet. Interestingly, these messages don't appear to follow the same theme that we have grown accustomed to seeing from Necurs, which has been one of the primary distribution mechanisms for the Locky

ransomware family and the Dridex banking trojan. Email campaigns associated with Locky and Dridex generally pose as transaction notifications, and purport to contain shipping notifications, ACH transaction notifications, etc. In this particular campaign, the emails do not contain any hyperlinks to malicious servers or any malicious attachments and are simply claiming to be stock market alerts about a specific stock ticker ($INCT) that the messages claim is about to go higher.

The message was structured to entice the user into thinking that this was too good of an opportunity to pass up -- a classic get rich quick scheme. First, the email begins with a simple introduction:

"It's been a long time since I sent you my special newsletter containing a hot stock tip."

It then claims that InCapta Inc ($INCT) is going to be bought out at $1.37 per share by DJI (a drone company) based on information purportedly obtained from colleagues at an M&A firm in Manhattan. The email explains that DJI is moving forward with the buyout because InCapta has:

"revolutionized the drone industry by creating the first independent drones that can be dispatched to areas of interest such as crime scenes, car chases, wild fires, etc."

Furthermore:

"The network of drones operates by connecting to a cloud and complex algorithms efficiently dispatch the drones within moments of an incident being reported."

"This way the media outlet that owns the drones can be the first to the scene and get exclusive, live-streamed."

To add urgency, they mention that the buyout is supposed to be announced on March 28, and recommend setting a buying limit by recommending purchasing before the stock reaches 20 cents a share to guarantee "massive returns." The email adds further urgency by claiming that DJI is going to pay 1000% more than the current value because:

"This has the potential to literally change the world of news broadcasting as we know it and DJI (the most prominent drone-maker in the world) sees the potential of this technology which is why they are willing to pay $1.37 a share to acquire it. A premium of over 1,000% over Friday's closing price."

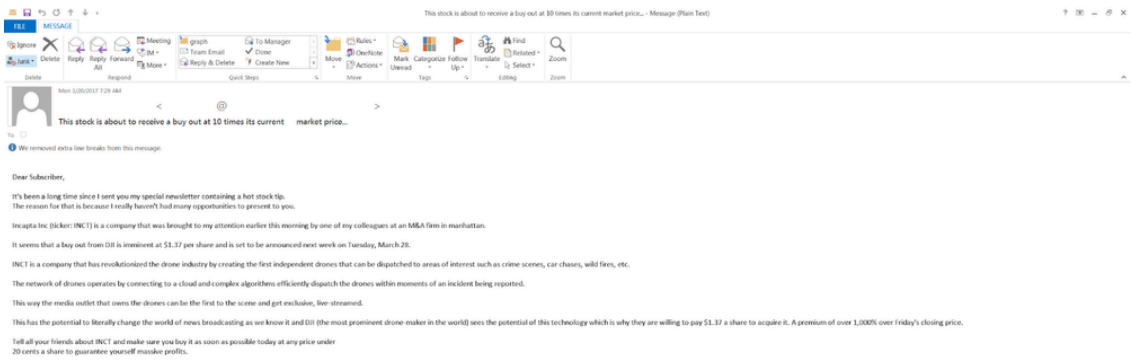


Figure 1: Sample Message

As is normal when dealing with email campaigns, these messages were sent in relatively high volumes, with tens of thousands seen just over the course of the morning on March 20. In analyzing our email telemetry, we can clearly see a change in the volume of emails being seen versus when Necurs was offline. While the volume of messages was high, the spam campaign itself did not appear to last long at all, with the majority of messages sent over the course of only a couple of hours.

The stock ticker in question appears to be associated with InCapta Inc., a mobile application development company. The stock has seen a significant increase in the volume of shares being traded. While analyzing this particular spam campaign, we observed that the volume of shares being traded reached over 1 million shares (the total later in the day was over 4.5 million shares), which is exponentially higher than the average volume of shares traded.

Figure 2: Google Finance for $INCT

Shortly after analyzing this initial campaign, we observed a second higher volume spam campaign within our SpamCop telemetry.

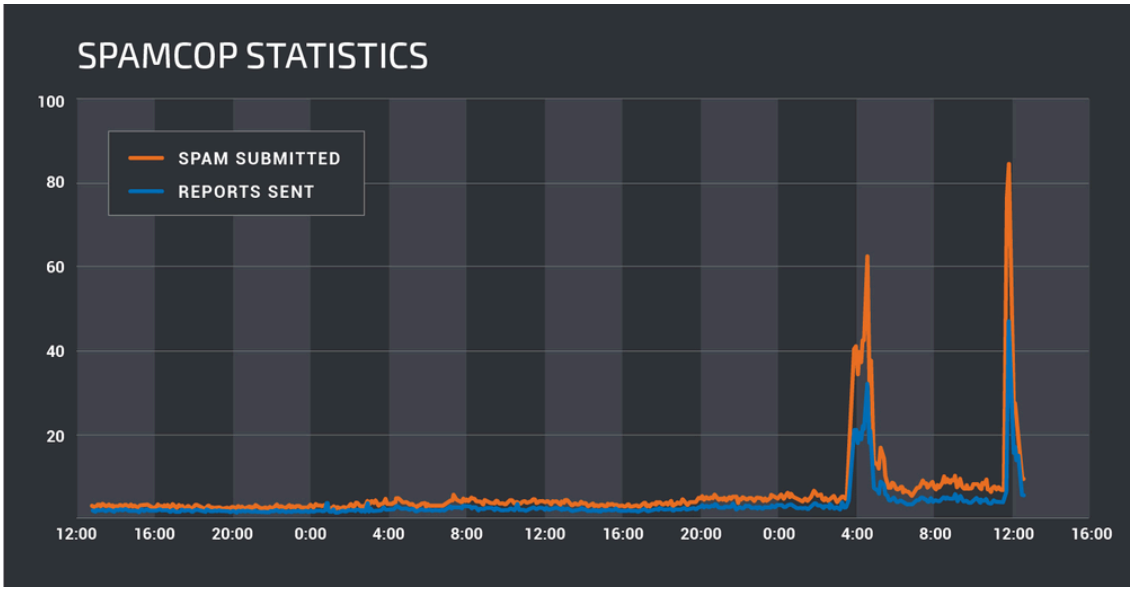
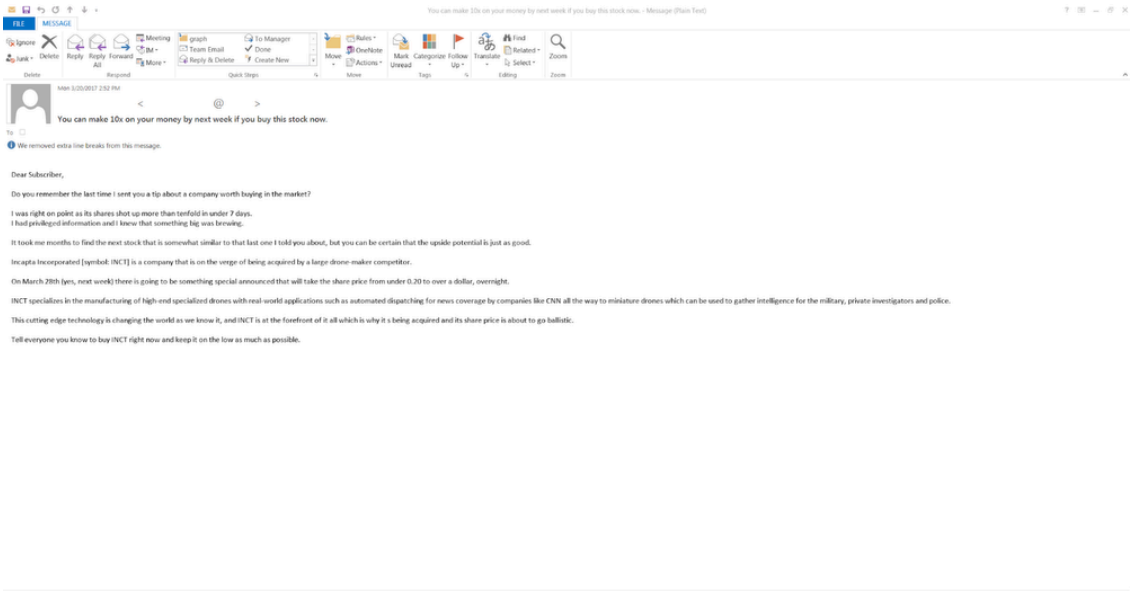


Figure 3: SpamCop Statistics

Interestingly enough, the stock price also increased around the time this second wave of spam emails was being sent. This second email campaign was very similar to the first but contained a slightly different subject and message body:



You can make 10x on your money by next week if you buy this stock now.

We removed extra line breaks from this message.

Dear Subscriber,

Do you remember the last time I sent you a tip about a company worth buying in the market?

I was right on point as its shares shot up more than tenfold in under 7 days.
I had privileged information and I knew that something big was brewing.

It took me months to find the next stock that is somewhat similar to that last one I told you about, but you can be certain that the upside potential is just as good.

Incapta Incorporated [symbol: INCT] is a company that is on the verge of being acquired by a large drone-maker competitor.

On March 28th (yes, next week) there is going to be something special announced that will take the share price from under 0.20 to over a dollar, overnight.

INCT specializes in the manufacturing of high-end specialized drones with real-world applications such as automated dispatching for news coverage by companies like CNN all the way to miniature drones which can be used to gather intelligence for the military, private investigators and police.

This cutting edge technology is changing the world as we know it, and INCT is at the forefront of it all which is why it s being acquired and its share price is about to go ballistic.

Tell everyone you know to buy INCT right now and keep it on the low as much as possible.

Figure 4: Second Sample Message

Historical Necurs Campaigns

On September 21, 2016, Talos published a blog post outlining the "Rising Tides of Spam" which detailed the increase of spam emails sent by Necurs in the summer of 2016. These emails often carried Dridex or Locky malware variants, delivering millions of messages per day to inboxes around the globe.

In late December, 2016, however, this email flow suddenly stopped, and email volume reduced to less than half of the flow typical of Necurs infrastructure. During this downtime, our spam block lists have been averaging 50K addresses. The addresses being blocked spiked to over 150K during these new campaigns. This spike is reflected in the email volume from March 20, 2017, discussed earlier and displayed in the graph below.

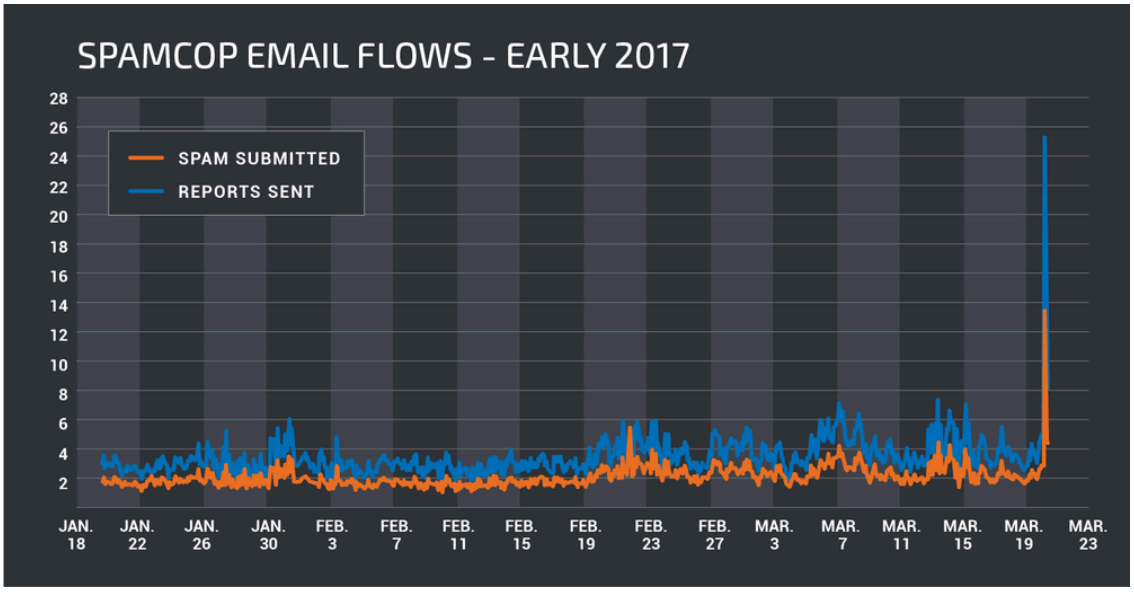


Figure 5: SpamCop Email Flows - Early 2017

But does Necurs have a history of sending pump-and-dump spam? Prior to the arrests in early 2016 which led to a quiet period of low botnet activity, Necurs had often sent different pump-and-dump stock scams. Just before this

most recent downtime began, we saw a moderate amount of pump-and-dump scam email volume coming through our data sources on December 20, 2016. These scam messages urged recipients to buy $SWRM and had email subjects similar to the following:

- "Read Now if you want a stock that will more than double by Christmas."
- "This stock will quadruple before Christmas. Time to buy now!" This December 20 campaign shares headers and attributes similar to the March 20 campaign, indicating that the December 20 campaign was also facilitated by the Necurs botnet. One such attributes is the X-PHP-Originating-Script header found in emails from the pump-and-dump campaigns.
- X-PHP-Originating-Script: 1001:Sendmail.php This header does not exist in the emails sent during the massive 2016 malware campaigns that were distributing Locky and Dridex however, revealing behind-the-scenes differences between Necurs' services and infrastructure. On the other hand, both of these campaign types share common recipients, hinting at the fact that Necurs operators may use a shared database of email addresses even when clients request different services.

Conclusion

Necurs is a good example of how over time attackers may change their methodologies as well as the strategies they use to monetize systems under their control. Botnets like Necurs represent one vector that Talos continues to monitor for activity and changes in attack techniques. As threats continue to change and evolve, Talos will continue to monitor the evolving threat landscape to ensure that our customers remain protected against any new threats.

Talos will continue to monitor the Necurs botnet for signs that it has once again been activated, for whatever purposes it may be used.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	N/A
CWS	N/A
Email Security	✔
Network Security	N/A
Threat Grid	N/A
Umbrella	N/A
WSA	N/A

Email Security can block malicious emails sent by threat actors as part of their campaign.
