Spam Sent by Necurs Botnet Is Trying & Succeeding in Altering Stock Market Prices

By Catalin Cimpanu

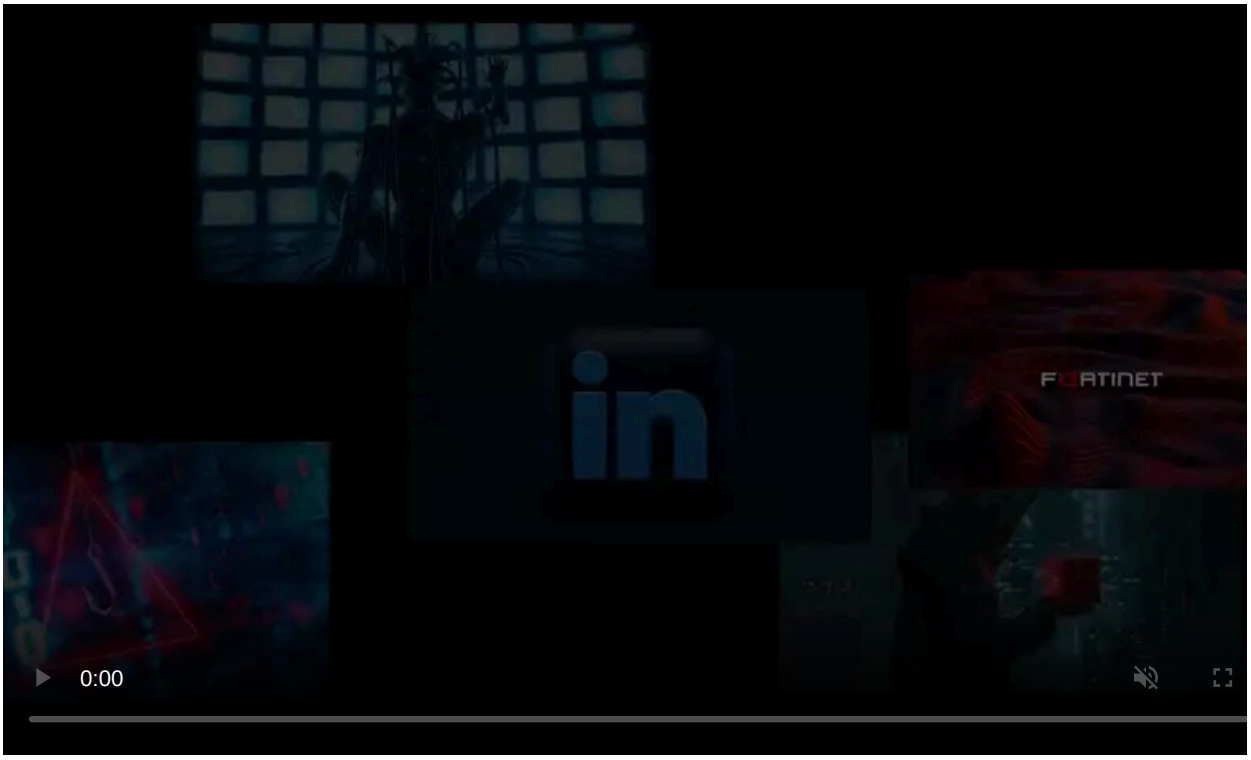
Published: 2017-03-21 · Archived: 2026-04-05 19:19:44 UTC

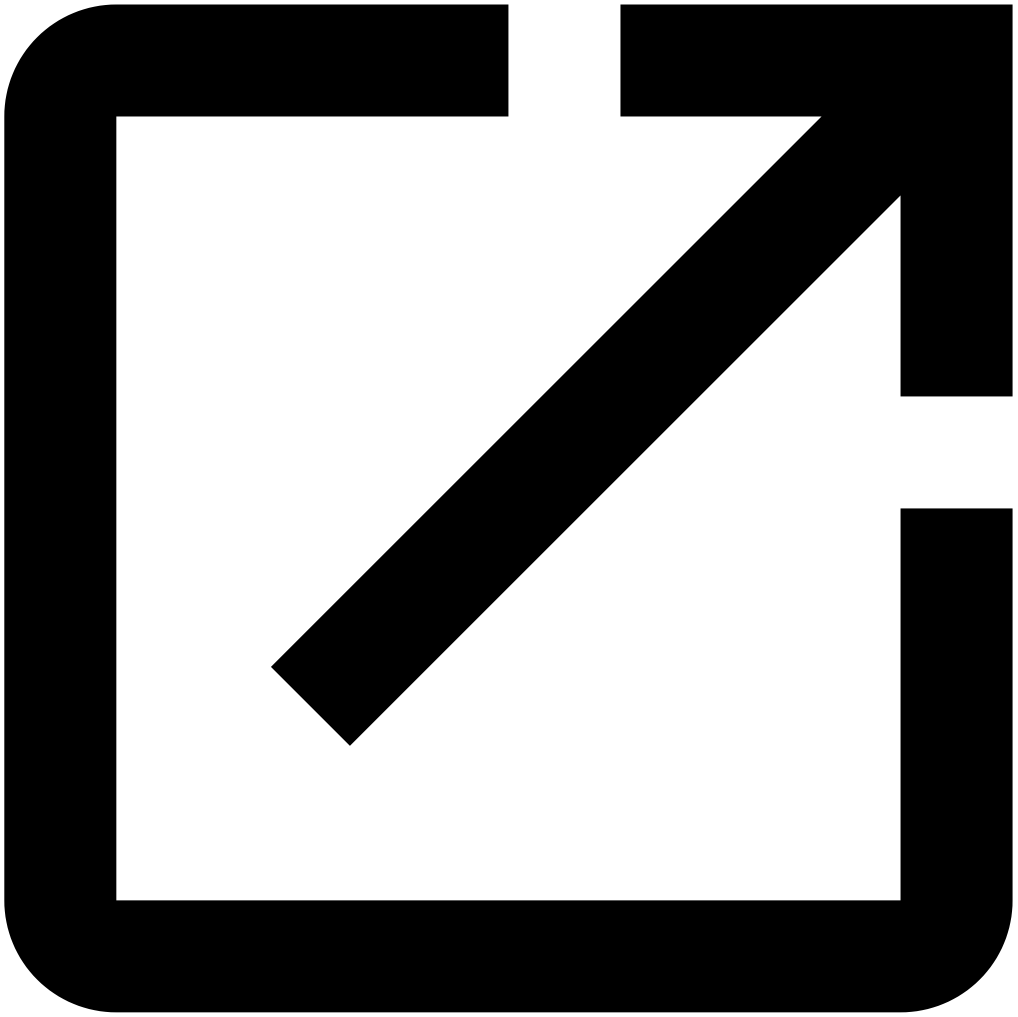
The Necurs botnet is back and active again, but instead of spreading the Locky ransomware or the Dridex banking trojan, its operators are engaged in a spam scheme that tries to boost a company's stock market price artificially.

This particular spam scheme has a special name in the infosec industry, which is "pump&dump." The idea behind pump&dump schemes is to send massive amounts of spam that try to convince users in buying stocks for a particular company.

As users flock to acquire the company's stock, the price surges. When Necurs spam has reached a desired share price value, the Necurs operators, or the people that rented the botnet, sell their stocks at the higher price and earn a profit.

This spam scheme has been around since the 90s, and has mainly targeted so-called "penny stocks," securities for small companies that sell under $5/share, whose prices can be influenced by a few hundreds of new buyers/sellers in a day.


0:00



Necurs pump&dump takes aim at InCapta stock

With a monthly bot population of 5 to 6 million unique bots, Necurs is the perfect spam botnet for these operations, as it can fling tens of thousands of messages per hour without breaking a sweat.

This latest pump&dump spam campaign targeted the stocks of InCapta Inc (INCT), a media holding company.

The spam campaign pushing for InCapta stock started on Monday morning, March 20, and resulted in an immediate share price spike.

Five different observers noted the new Necurs spam campaign, such as Cisco Talos, MalwareTech, MX Lab, My Online Security, and Dynamoo.

Necurs sent out four spam runs

According to MalwareTech, Necurs sent out four different spam waves on Monday (2 spam runs) and Tuesday (2 spam runs), keeping InCapta's stock at a heightened level.

According to Cisco Talos, the spam campaigns sent around tens of thousands of messages per hour, with the second wave being larger than the first.

Just as you'd expect, the spammed message didn't make any sense, trying to trick users into buying InCapta stock because of an impending acquisition by DJI, the world's leader in drone manufacturing.

The spam message incorrectly stated that InCapta had manufactured its own drone. With a little bit of research (Google search), users would have discovered that InCapta is a media company, and would have avoided wasting their money. Below are the first two spam messages sent during the first two waves. The third and fourth spam messages are here and here.

Subject: This stock is about to receive a buy out at 10 times its current market price...

Attachments: None

Body:

Dear Subscriber,

It's been a long time since I sent you my special newsletter containing a hot stock tip.
The reason for that is because I really haven't had many opportunities to present to you.

Incapta Inc (ticker: INCT) is a company that was brought to my attention earlier this morning
by one of my colleagues at an M&A firm in manhattan.

It seems that a buy out from DJI is imminent at $1.37 per share and is set to be announced
next week on Tuesday, March 28.

INCT is a company that 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.

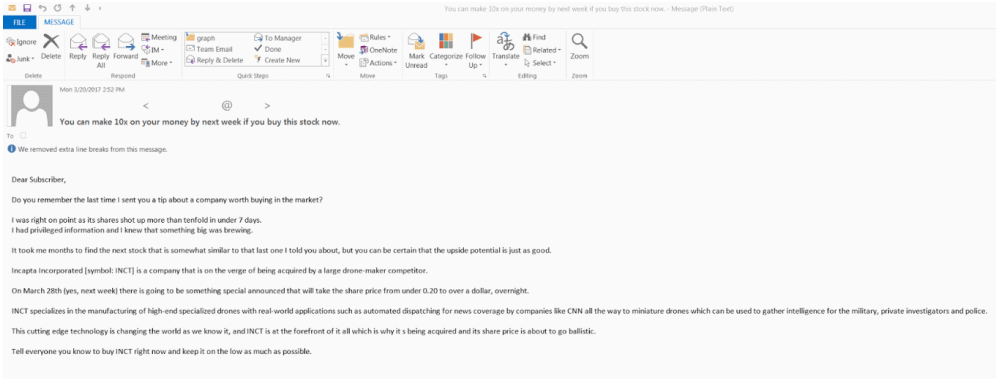
The network of drones operates by connecting to a cloud and complex algorithms efficiently dispatch the drones
within moments of an incident being reported.

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

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.

Tell all your friends about INCT and make sure you buy it as soon as possible today at any price under
20 cents a share to guarantee yourself massive profits.

Necurs pump&dump stock spam for InCapta Inc. (MalwareTech)



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.

Necurs pump&dump stock spam for InCapta Inc. (Cisco Talos)

Necurs returns to life

Prior to yesterday's spam run, the Necurs botnet has been extremely quiet. During 2016, Necurs had focused on delivering spam email with malicious attachments that installed the Locky ransomware or the Dridex banking trojan.

The botnet had gone silent before the winter holidays, as it does every year, but never came back to its previous activity levels, stopping the distribution of Locky altogether. Yesterday's pump&dump campaign was Necurs' biggest campaign this year so far, whose infrastructure was dormant for most of 2017.

Necurs had previously dabbled in pump&dump spam schemes, mostly in 2015 and earlier, before Locky. There were isolated pump&dump spam schemes in 2016, but nothing to eclipse its efforts on spreading Locky and Dridex.

Necurs' Locky infrastructure still dormant

According to Cisco's Talos team, Necurs operators appear to be using a different infrastructure for spreading Locky and another one for pump&dump spam.

As Necurs came back from its winter holiday slumber, Talos researchers say that only the pump&dump infrastructure came back to life, while the one responsible for Locky remains dormant.

"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," the Cisco Talos team explained.

Nonetheless, because ransomware has a wider attack base, compared to the small userbase susceptible to pump&dump schemes, most industry experts expect Necurs to return to spreading Locky or another ransomware family, as it's far more profitable than spreading any other type of spam.

Conrad Longmore, the researcher behind the Dynamoo blog has some advice for people taking their stock market tips from spam messages.

"Pump and dump spam like this is a criminal activity, and typically companies being promoted in this way are in terminal decline (but not always)," Longmore says. "Avoid buying stocks on the recommendation of criminals."

Source: https://www.bleepingcomputer.com/news/security/spam-sent-by-necurs-botnet-is-trying-andamp-succeeding-in-altering-stock-market-prices/