

# Teslacrypt Spam Campaign: "Unpaid Issue..." | Malwarebytes Labs

By Malwarebytes Labs

Published: 2016-03-17 · Archived: 2026-04-05 12:51:35 UTC

We have all seen the current upsurge in Ransomware attacks. It has been covered on an international scale, with new variants appearing at a very fast pace, some target Windows, some target Macs and some have cross platform capabilities.

Recently a major healthcare organization fell victim to Ransomware, and surely there are more high profile victims to come. Enterprises face an ever growing threat landscape and the majority of businesses do not report or acknowledge having become a victim of Ransomware. This is due to the possible repercussions, such as loss of customer confidence, degraded reputation and embarrassment, which leads to an inevitable loss of profit and business.

Cyber-criminals are aware of these repercussions and have crafted their attacks to include threats such as releasing specific information related to victims, as we saw with [Chimera Ransomware](#), utilizing a type of cyber-extortion to ensure they achieve their objective of being paid the ransom. Cyber criminals select targets that may give in to their demands, and targeting a major health care organization is more than likely going to generate a paid ransom.

Cyber criminals continue to use exploit kits to infect victims with ransomware but they also use MALSPAM emails to lure possible victims – a key vector into an enterprise environment that lacks the proper security controls, and one with insufficient information security training for end users. Some examples are email messages claiming to be in regards to an overdue bill or invoice, utilizing such terminology in the subject line and given file name, such as invoice.zip or payment\_doc\_298427.zip

The email seen below is an example how the orchestrated attack is carried out (thanks to [Conrad Longmore](#) for the email example):

```
From: Jennie bowles Date: 10 March 2016 at 12:27 Subject: GreenLand Consulting - Unpaid Issue No. 58  
Dear Client! For the third time we are reminding you about your unpaid debt. You used to ask for our  
Respectfully, Jennie bowles Chief Accountant 707 Monroe St FL 58833 928-429-4994
```

The emails usually contain a ZIP file which contains a malicious script/downloader. Upon running this specific malicious script/downloader I was greeted by Teslacrypt ransomware (69.exe) from hellomississmithqq[.]com / [IP](#): 54.212.162.6 (both currently blocked by Malwarebytes Anti-Malware Malicious Website protection).



### **Associated IP addresses with hellomissismithqq[.]com:**

46(dot)108.108.182 54(dot)212.162.6 78(dot)135.108.94 134(dot)19.180.8 202(dot)120.42.190 216(dot)150.77.21  
142(dot)25.97.48 202(dot)120.42.190

### **Other domains that have been identified in this on-going campaign:**

Joecockerhereqq[.]com blizzbauta[.]com yesitisqqq[.]com howareyouqq[.]com thisisitsqq[.]com  
blablaworldqq[.]com fromjamaicaqq[.]com hellomydearqq[.]com witchbehereqq[.]com arendroukysdqq[.]com  
itisverygoodqq[.]com goonwithmazerqq[.]com helloyoungmanqq[.]com invoiceholderqq[.]com  
mafianeedsyouqq[.]com mafiawantsyouqq[.]com soclosebutyetqq[.]com isthereanybodyqq[.]com  
lenovomaybenotqq[.]com lenovowantsyouqq[.]com hellomissismithqq[.]com thisisyourchangeqq[.]com  
www.thisisyourchangeqq[.]com gutentagmeinliebeqq[.]com hellomisterbiznesqq[.]com

Ransomware is not going away, on the contrary it is becoming more and more prevalent with new variants coming out at a fast pace and targeting multiple platforms. It is recommended that users are using anti-malware protection, especially one that has a website protection option. Malwarebytes has an [Anti-Ransomware Beta](#) product that blocks most Ransomware attacks. Furthermore it is recommended that users are ever vigilant and not click on URL links in suspicious emails, and do not open any files contained in these emails. Ensure to keep proper backups as most Ransomware deletes Windows shadow copies.

[Malwarebytes Anti-Malware](#) detects this Teslacrypt sample and its malicious website protection blocks the download domain / Command & Control domains as well.

[Andres](#)

---

Source: <https://blog.malwarebytes.com/threat-analysis/2016/03/teslacrypt-spam-campaign-unpaid-issue/>