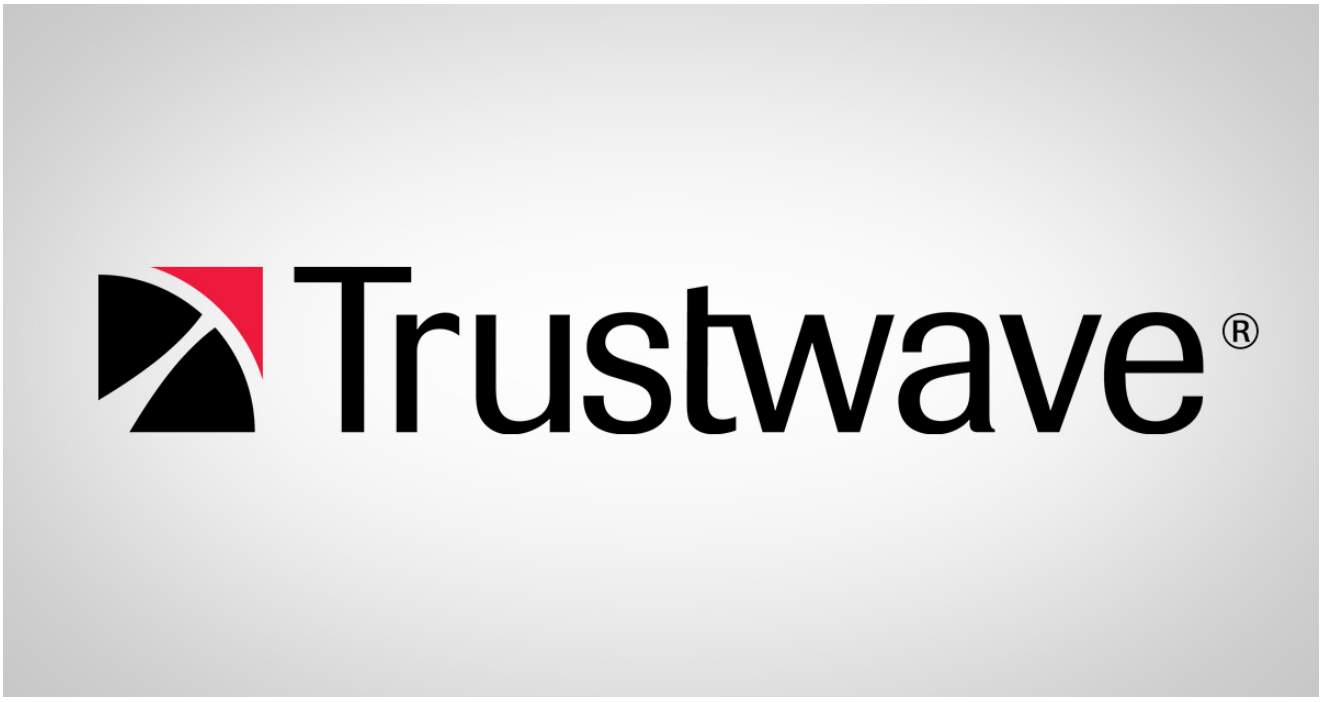
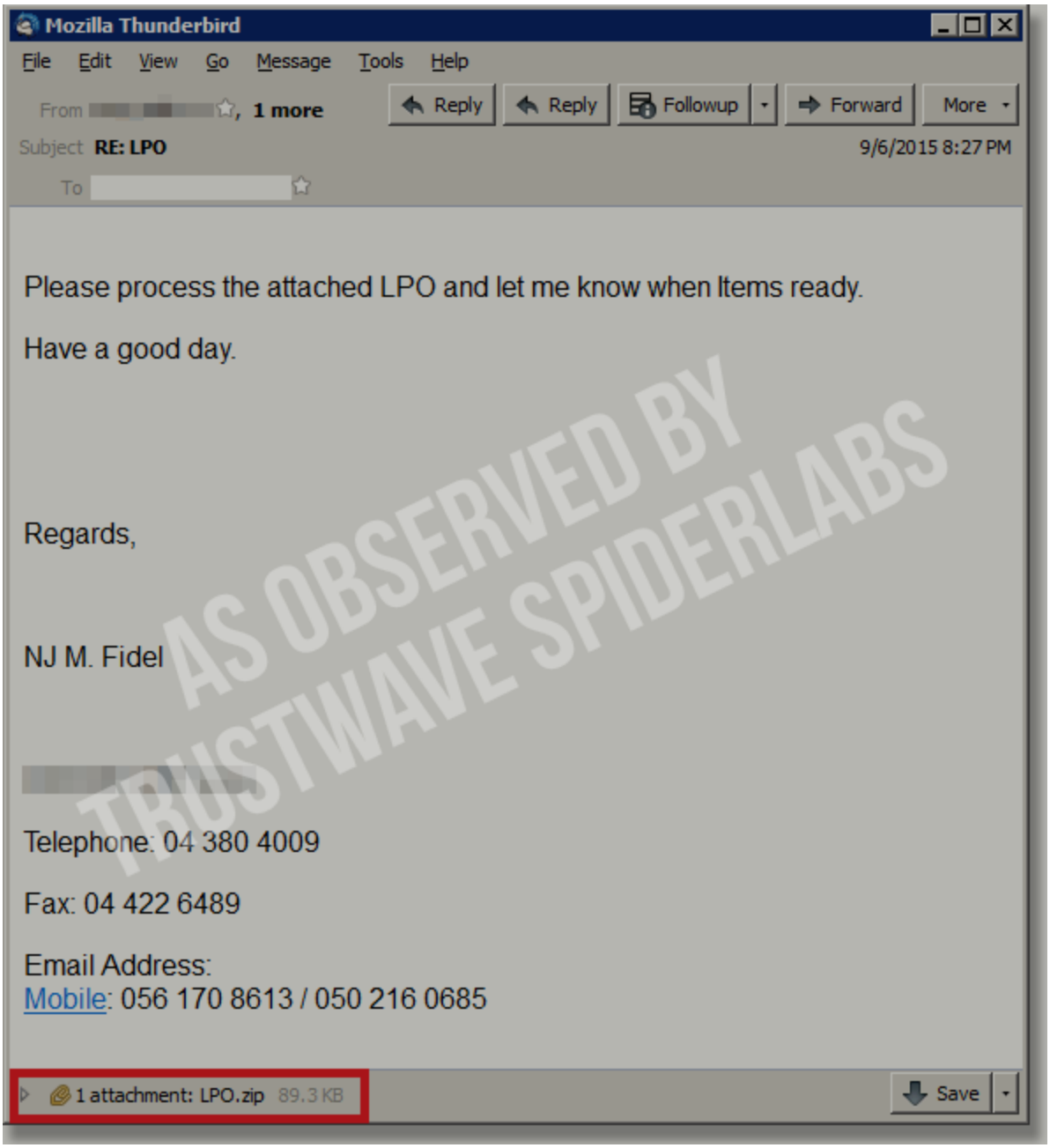
Quaverse RAT: Remote-Access-as-a-Service



****UPDATE as of September 28, 2015 - see the bottom of this post for removal instructions****

Quaverse RAT or QRAT is a fairly new Remote Access Tool (RAT) introduced in May 2015. This RAT is marketed as an undetectable Java RAT. As you might expect from a RAT, the tool is capable of grabbing passwords, key logging and browsing files on the victim's computer. On a regular basis for the past several months, we have observed the inclusion of QRAT in a number of spam campaigns.

Below you'll see an example of one spam message that claimed to be a "limited purchase order" (LPO). Attached to it was a .zip attachment containing an executable .JAR file.

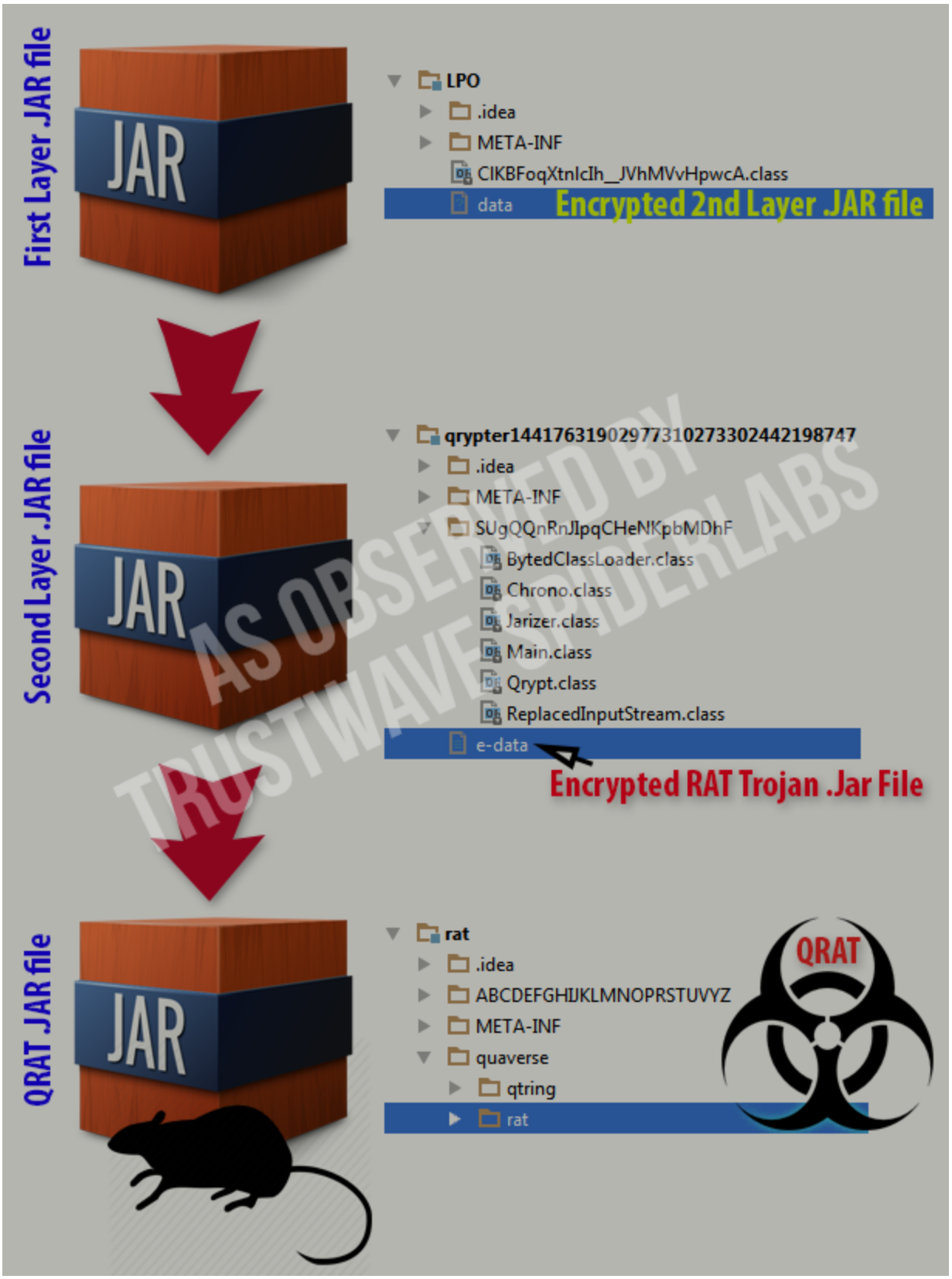


Analysis

QRAT is a Java-based remote access Trojan or RAT that was designed to work only in Windows environments with Java-runtime installed.

```
if(var11.indexOf(Qtring.qtr("qtr%win%qtr")) == -1) {
    JOptionPane.showMessageDialog((Component)null, Qtring.qtr("qtr%Your
    operating system must be Windows to run this application.&qtr"),
    Qtring.qtr("qtr%Operating System Error%qtr"), 0);
}
```

To avoid being detected by antivirus scanners, it uses a "Russian-doll" method with 2 layers of Java encryption. The illustration below shows the levels of encryption used to hide the QRAT server executable.



In the infected system, the configuration files, plugins and Java executables are dropped in the %AppData%\syslogdata folder (e.g., "C:\Documents and Settings\User\Application Data\syslogdata\").

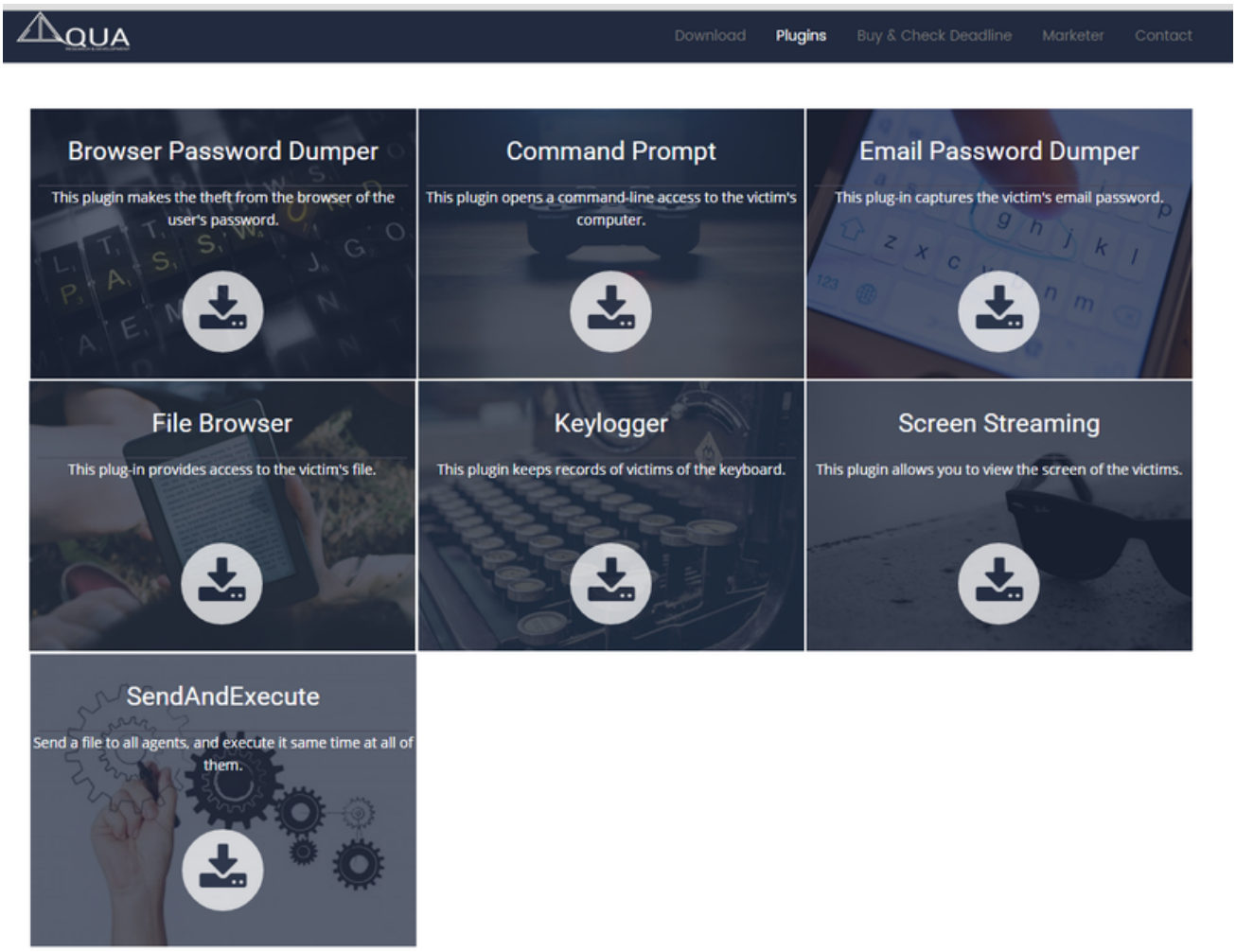
It adds an auto run registry key to keep it persistent in the target's system:

```
addRegisteryKey(Qtring.qtr("qtr%HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\RUN%qtr"),
Qtring.qtr("qtr%QRat-StartUp-Command%qtr"), var13);
```

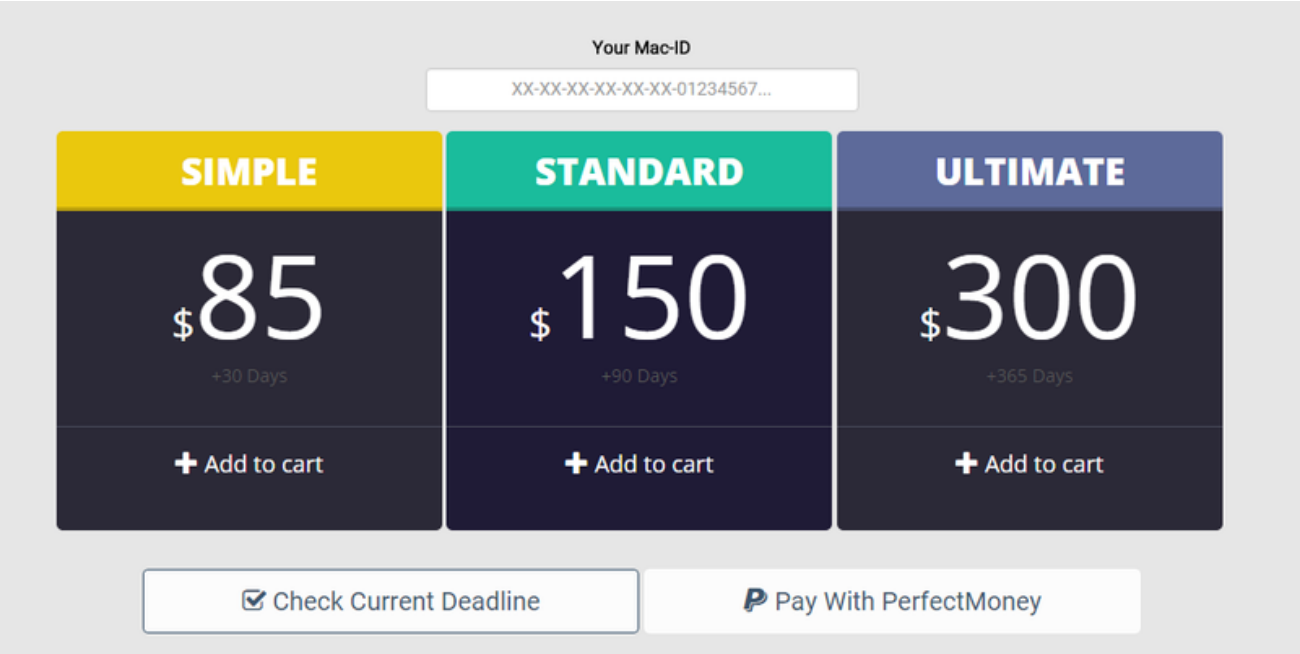
The RAT connects to its host **quaverse.com** at port 1777. It may also connect to the domain name **schelbye.com** that points to the same IP address as quaverse.com. It also uses a list of backup domain names as follows:

- Valtce.co
- Frecarn.co
- Gtfoods.com.ru
- Soqda.com

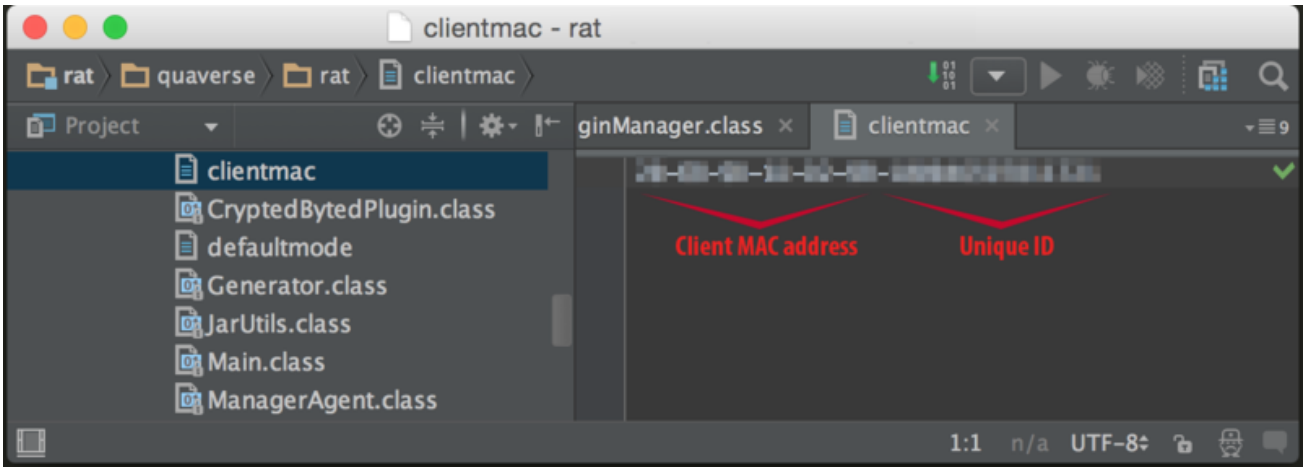
Plugins are also available to extend the functionality of the QRAT agent. These functionalities are not as sophisticated as other RATs we've seen before like DarkComet or AlienSpy, however this is still a very capable RAT that gives the intruder full control of the victim's computer once infected. The plugins are readily available from the slick Quaverse RAT website shown here:



QRAT is sold as a software-as-a-service with prices ranging from $85 for a one month subscription up to $300 for a one year subscription. Purchasing a service subscription requires the purchaser to submit his or her computer's MAC address to be used as a customer identifier.



We've extracted the MAC ID and unique identifier of the intruder from the spam email sample:

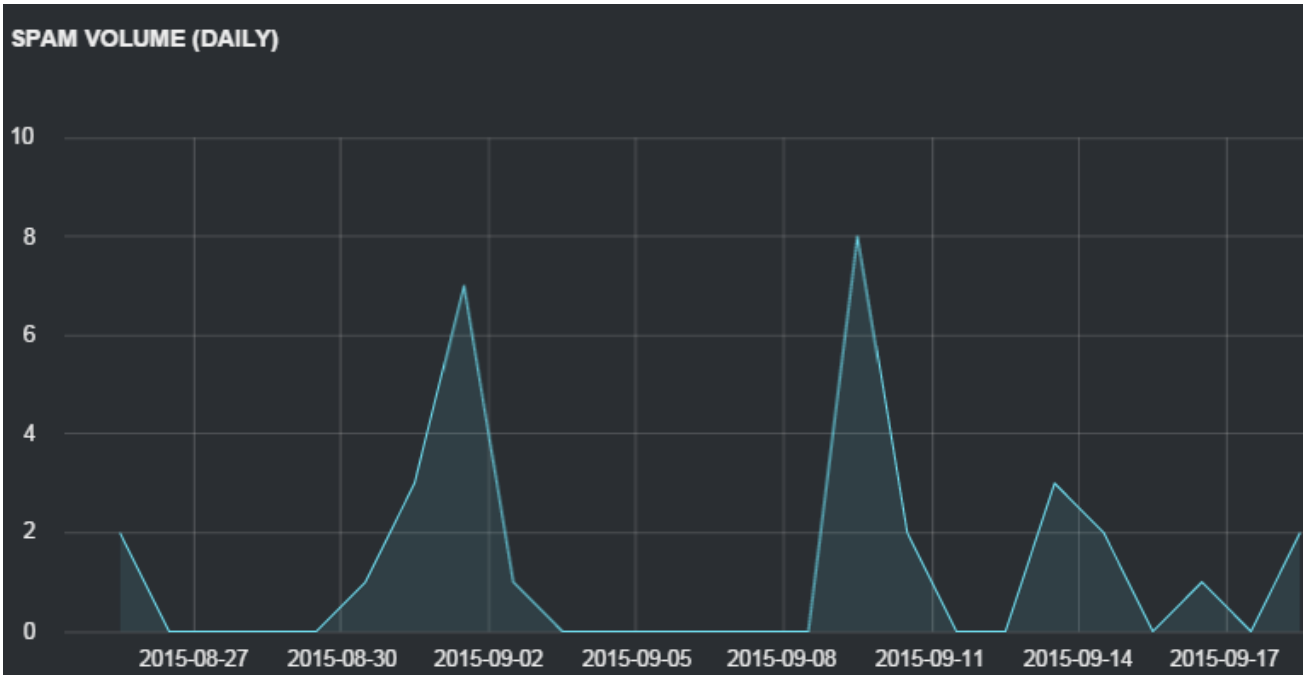


To satisfy our curiosity, we tracked the intruder's MAC address/ID from Quaverse's website and found the RAT server. It seems the intruder bought a one year subscription that will expire on June 20, 2016. Following that logic, the spam campaign started on June 20, 2015.

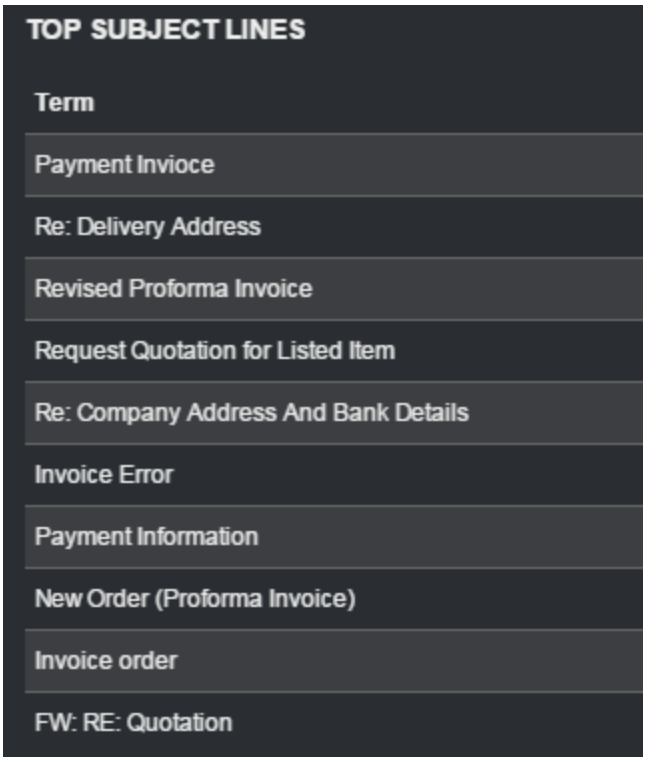
Mac-ID	[redacted]
Expire Date	June 20, 2016, 5:33 am
Crypted Agent	Download Agent.
Crypted Agent with Silent Java Installer	Download Agent with Silent Java Installer.

Conclusion

Remote Access Trojans are some of the more accessible tools that allow intruders to gain complete access to a target system. They are GUI- based and very easy to use, hence their seeming popularity with novice cybercriminals that spread their wares through email. In fact, we're observing an increase in Java-based Remote Access Trojans showing up in our spam-traps over the last couple of months. The chart below shows the volume of related spam volume per day since late August 2015:



The email subject lines usually mention an "Invoice." Here's the top subject lines we've observed:



TOP SUBJECT LINES
Term
Payment Invioce
Re: Delivery Address
Revised Proforma Invoice
Request Quotation for Listed Item
Re: Company Address And Bank Details
Invoice Error
Payment Information
New Order (Proforma Invoice)
Invoice order
FW: RE: Quotation

If you come upon subject lines like those listed or derivatives of them, and you see a .Jar attachment, there is a good chance it includes a malicious Remote Access Trojan. We recommend blocking inbound Java files outright at the email gateway, much like any other executable. The Trustwave Secure Email Gateway blocks such e-mails by default thanks to it including Java Class files in its executables category.

****UPDATE as of September 28, 2015****

Removal Instructions

Listed below are manual removal instructions for QRAT:

Manual Removal Steps:

1. Disconnecting the infected computer from the internet is highly recommended.
2. Identify the malicious Java process. We recommend Sysinternal's Process Explorer tool to search for the malicious process.
    1. Download and run Process Explorer from this page https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
    2. Find the process named "javaw.exe"
    3. Right click on the process then click Properties
    4. In the Javaw.exe process, click the Image tab
    5. Check the command line path if it points to a .Jar file named %appdata%\syslogdata\syslog-Agent.jar (e.g. "C:\Users\UserName\AppData\Roaming\syslogdata\syslog-Agent.jar")
    6. Kill that process

3. Remove QRAT's autorun registry key
    1. Click Start->Run then type "regedit" in the textbox without the quote
    2. In the left pane, locate this registry path: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    3. In the right pane, locate and delete this registry key: "QRat-StartUp-Command" = "C:\Program Files\<Java Bin Path>\javaw.exe" -jar "C:\%Appdata%\syslogdata\syslog-Agent.jar" manageragent" /f
4. Delete the QRAT files and folder
    1. Click Start->Run then type in "**%Appdata%"** the textbox without the quote
    2. Locate the folder named "**syslogdata**"
    3. Delete all the files in the folder and lastly delete the folder itself.
5. Restart computer