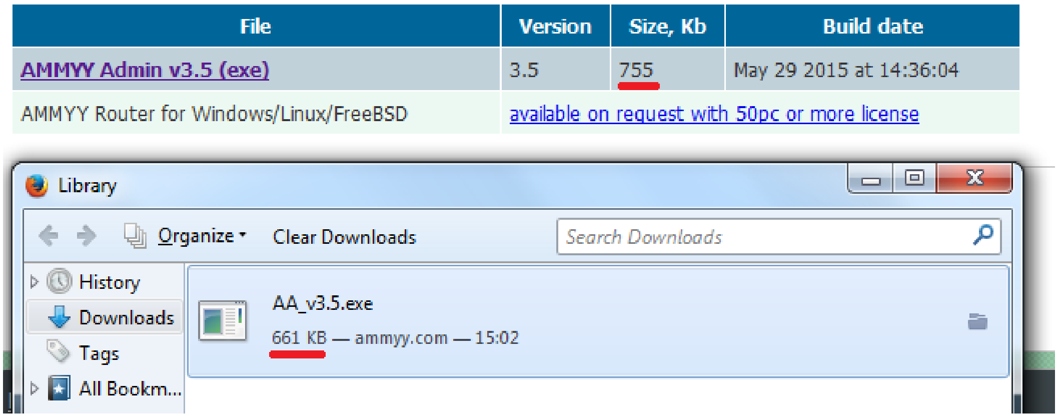
Technical Analysis

We downloaded the Ammyy Admin from the official site and observed that the size of the file mentioned on the site was different than that of the file which was actually being downloaded.

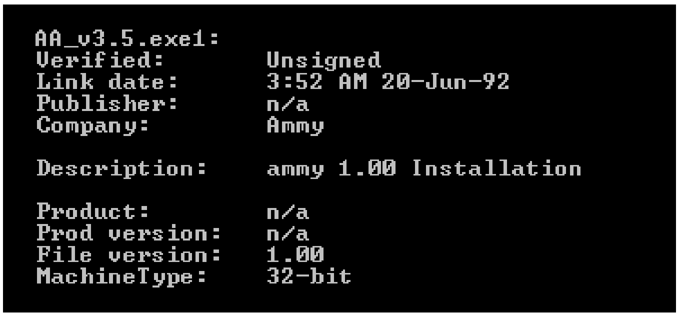


File	Version	Size, Kb	Build date
AMMYY Admin v3.5 (exe)	3.5	755	May 29 2015 at 14:36:04
AMMYY Router for Windows/Linux/FreeBSD	available on request with 50pc or more license		

AA_v3.5.exe
661 KB — ammyy.com — 15:02

Fig.2 The change in size of the file downloaded and of that mentioned on the site

Once the file was downloaded, we found that the file was not digitally signed and the version information was different than that of the original application which had a valid digital certificate.

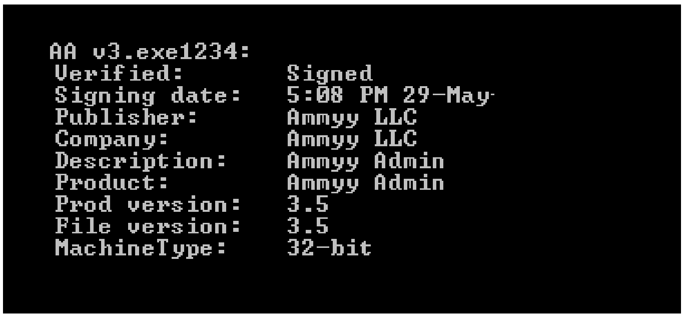


```
AA_v3.5.exe1:
Verified:       Unsigned
Link date:      3:52 AM 20-Jun-92
Publisher:      n/a
Company:        Ammy

Description:    ammy 1.00 Installation

Product:        n/a
Prod version:   n/a
File version:   1.00
MachineType:    32-bit
```

Fig.3 Version info of the malicious installer downloaded from the site

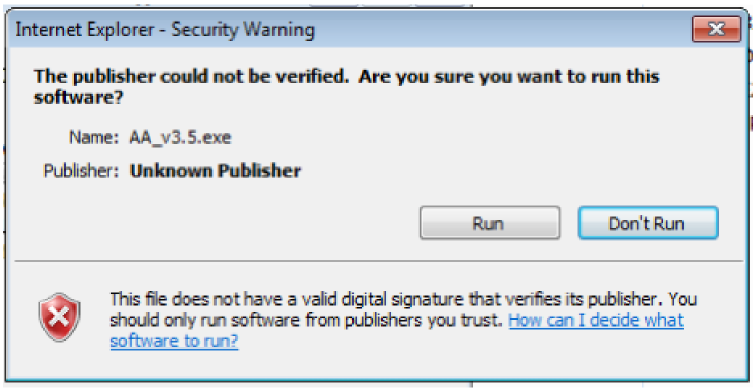


```
AA v3.exe1234:
 Verified:       Signed
 Signing date:   5:08 PM 29-May
 Publisher:      Ammyy LLC
 Company:        Ammyy LLC
 Description:    Ammyy Admin
 Product:        Ammyy Admin
 Prod version:   3.5
 File version:   3.5
 MachineType:    32-bit
```

Fig.4 Version info of the genuine Ammyy Admin application

© 2016 Quick Heal Technologies Limited

On running the downloaded installer (malicious), the original Ammyy Admin application window opens up as any ordinary software would. This gives the user no reason for suspicion. Whereas, the installer drops and executes the Cerber3 Ransomware payload in the background, which then silently starts encrypting the user's files.



Internet Explorer - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: AA_v3.5.exe

Publisher: **Unknown Publisher**

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Fig.5 Internet Explorer prompting about the file's legitimacy before executing it

Dropped files upon execution:

%temp%\AA_v3.exe	[Original Ammyy Admin executable]
%temp%\encrypted.exe	[Cerber3 ransomware payload]

During our analysis on 12th September 2016, we observed that the malware changed the name of the Cerber payload from **encrypted.exe** to **in.exe**. We have also observed that the malware gets distributed at any given time on a day. And when this is not the case, the legitimate application is available for download.

Cerber3 Ransomware appends '.cerber3' extension to all the encrypted files and also deletes volume shadow copies to avoid any chance of data recovery. Besides being propagated through the Ammyy Admin website, Cerber3 Ransomware is also known to spread through spam emails hidden in attachments, links and other exploits.

© 2016 Quick Heal Technologies Limited