


13.exe

Is DLL 

Packer 

Anti Debug 

Anti VM 

Signed 

XOR 

MalFamily: Pony

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	279.00 KB (285696 bytes)
Compile time:	2018-05-14 17:24:37
MD5:	58574b6dc105478f0807ea148349c59f
SHA1:	943170abbf8a69b27e4bc953060a75c8562f2ffe
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-23 13:03:05

URL(s) file hosting

<http://lokipanelhostingpanel.gq/work/worknew/23.exe>

<http://lokipanelhostingpanel.gq/work/worknew/22.exe>

<http://lokipanelhostingpanel.gq/work/worknew/13.exe>

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

Import library

mscoree.dll

12

Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN Fareit/Pony Downloader Checkin 3
- signature: ET TROJAN Pony Downloader HTTP Library MSIE 5 Win98

Harvests information related to installed mail clients

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7d19c9e894f20d4780a31c9a9f17da11
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\IMAP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\32a3dc9c400a4b448b60ab7fe553a392
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\818ecc2f310b344f807e8af5dc013189
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\IMAP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\43e0bb79f0f2d84db98ff4f730d23d24
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows



Messaging Subsystem\Profiles\Outlook\6a50d9bd87f9a8478751861a1591a6c2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\SMTP
Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\POP3
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\SMTP
Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\POP3 Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\IMAP
Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\NNTP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\HTTPMail Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\IMAP
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\SMTP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HTTPMail Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\POP3
Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\POP3 User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\SMTP
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\00471e98b7a362469ed97e3915fd4111

```
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\NNTP
Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HTTPMail
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\IMAP
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\SMTP
Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\IMAP
Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\HTTPMail Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\HTTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000001\NNTP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\Email
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\POP3 Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\POP3
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\HTTP
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\NNTP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\HTTP
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000002\SMTP
Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\NNTP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\POP3
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000003\IMAP
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\NNTP Email Address
```




```
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP
Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP
Server URL
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP
Server URL
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP
Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP
Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP
User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\fb86ed2903a4a11cfb57e524153480001
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail Server
```



```
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP
User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\192e64c97bf3a54488a039619c763627
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\HTTP Server URL
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3
Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\7760e21103136b47946c9c80fa097f15
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\IMAP Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3
Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\POP3 Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP
Server URL
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\NNTP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User
Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail
Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP
Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\SMTP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar
Summary\NNTP Password
```



- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\IMAP Password2

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User Name

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Email Address

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP User Name

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTPMail User Name

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\HTTP User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTPMail User Name

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\HTTPMail User Name

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Port

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\NNTP Server

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 User

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\10b0e4d6eb1de34dabd532a0806a0fec



```
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\POP3 Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\IMAP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\SMTP Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\NNTP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\OMI Account Manager\Accounts
- key: HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts
- key:
HKEY_CURRENT_USER\Identities\{141B4688-D8D4-4AD1-B583-99828374C040}\Software\Microsoft\Internet Account Manager\Accounts
```

Harvests credentials from local FTP client softwares



- file: C:\Program Files (x86)\CuteFTP\sm.dat
- file: C:\Users\Seven01\AppData\Local\CuteFTP\sm.dat
- file: C:\Users\Seven01\AppData\Roaming\CuteFTP\sm.dat
- file: C:\Program Files (x86)\GlobalSCAPE\CuteFTP\sm.dat
- file: C:\Users\Seven01\AppData\Roaming\GlobalSCAPE\CuteFTP\sm.dat
- file: C:\ProgramData\CuteFTP\sm.dat
- file: C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat
- file: C:\Users\Seven01\AppData\Local\GlobalSCAPE\CuteFTP\sm.dat
- file: C:\Users\Seven01\AppData\Local\FlashFXP\4\Sites.dat
- file: C:\ProgramData\FlashFXP\3\Sites.dat
- file: C:\Users\Seven01\AppData\Roaming\FlashFXP\4\Sites.dat
- file: C:\ProgramData\FlashFXP\4\Sites.dat
- file: C:\Users\Seven01\AppData\Roaming\FlashFXP\3\Sites.dat
- file: C:\Users\Seven01\AppData\Local\FlashFXP\3\Sites.dat
- file: C:\Users\Seven01\AppData\Local\FlashFXP\3\Quick.dat
- file: C:\Users\Seven01\AppData\Roaming\FlashFXP\4\Quick.dat
- file: C:\ProgramData\FlashFXP\4\Quick.dat
- file: C:\Users\Seven01\AppData\Roaming\FlashFXP\3\Quick.dat
- file: C:\Users\Seven01\AppData\Local\FlashFXP\4\Quick.dat
- file: C:\ProgramData\FlashFXP\3\Quick.dat
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\sitemanager.xml
- file: C:\Users\Seven01\AppData\Local\FileZilla\sitemanager.xml
- file: C:\ProgramData\FileZilla\sitemanager.xml
- file: C:\Users\Seven01\AppData\Roaming\FileZilla\recentservers.xml
- file: C:\Users\Seven01\AppData\Local\FileZilla\recentservers.xml
- file: C:\ProgramData\FileZilla\recentservers.xml
- file: C:\ProgramData\VanDyke\Config\Sessions*.*
- file: C:\Users\Seven01\AppData\Roaming\VanDyke\Config\Sessions*.*
- file: C:\Users\Seven01\AppData\Local\VanDyke\Config\Sessions*.*
- file: C:\ProgramData\FTP Explorer*.*
- file: C:\Users\Seven01\AppData\Local\FTP Explorer*.*
- file: C:\Users\Seven01\AppData\Roaming\FTP Explorer*.*
- file: C:\Users\Seven01\AppData\Local\SmartFTP*.*
- file: C:\Users\Seven01\AppData\Roaming\SmartFTP*.*
- file: C:\ProgramData\SmartFTP*.*
- file: C:\Users\Seven01\AppData\Local\TurboFTP*.*
- file: C:\ProgramData\TurboFTP*.*
- file: C:\Users\Seven01\AppData\Roaming\TurboFTP*.*
- file: C:\ProgramData\FTPRush*.*
- file: C:\Users\Seven01\AppData\Local\FTPRush*.*
- file: C:\Users\Seven01\AppData\Roaming\FTPRush*.*
- file: C:\Users\Seven01\AppData\Roaming\LeapWare\LeapFTP*.*
- file: C:\Users\Seven01\AppData\Local\LeapWare\LeapFTP*.*
- file: C:\ProgramData\LeapWare\LeapFTP*.*
- file: C:\Users\Seven01\AppData\Local\FTPGetter*.*
- file: C:\ProgramData\FTPGetter*.*
- file: C:\Users\Seven01\AppData\Roaming\FTPGetter*.*
- file: C:\Users\Seven01\AppData\Local\Estsoft\ALFTP*.*
- file: C:\ProgramData\Estsoft\ALFTP*.*
- file: C:\Users\Seven01\AppData\Roaming\Estsoft\ALFTP*.*
- file: C:\Program Files (x86)\Common Files\Ipswitch\WS_FTP*.*
- key: HKEY_CURRENT_USER\Software\Far Manager\Plugins\FTP\Hosts
- key: HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts
- key: HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts
- key: HKEY_CURRENT_USER\Software\Far\SavedDialogHistory\FTPHost
- key: HKEY_CURRENT_USER\Software\Far2\SavedDialogHistory\FTPHost
- key: HKEY_CURRENT_USER\Software\Far Manager\SavedDialogHistory\FTPHost
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
- key: HKEY_CURRENT_USER\Software\GlobalSCAPE\CuteFTP 7 Home\QCToolbar



- key: HKEY_LOCAL_MACHINE\Software\Ghisler\Windows Commander
- key: HKEY_CURRENT_USER\Software\Ghisler\Windows Commander
- key: HKEY_CURRENT_USER\Software\Ghisler\Total Commander
- key: HKEY_LOCAL_MACHINE\Software\Ghisler\Total Commander
- key: HKEY_CURRENT_USER\Software\BPFTP\Bullet Proof FTP\Options
- key: HKEY_CURRENT_USER\Software\BPFTP\Bullet Proof FTP\Main
- key: HKEY_CURRENT_USER\Software\FileZilla
- key: HKEY_LOCAL_MACHINE\Software\FileZilla
- key: HKEY_CURRENT_USER\Software\FileZilla Client
- key: HKEY_LOCAL_MACHINE\Software\FileZilla Client
- key: HKEY_CURRENT_USER\Software\TurboFTP
- key: HKEY_LOCAL_MACHINE\Software\TurboFTP
- key: HKEY_CURRENT_USER\Software\Sota\FFFTP\Options
- key: HKEY_CURRENT_USER\Software\Sota\FFFTP
- key: HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites
- key: HKEY_CURRENT_USER\Software\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224
- key: HKEY_CURRENT_USER\Software\FTP Explorer\Profiles
- key: HKEY_LOCAL_MACHINE\Software\FTPClient\Sites
- key: HKEY_CURRENT_USER\Software\FTPClient\Sites
- key: HKEY_CURRENT_USER\Software\LinaxFTP\Site Manager
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Robo-FTP 3.7\Scripts
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Robo-FTP 3.7\FTPServers
- key: HKEY_CURRENT_USER\SOFTWARE\Robo-FTP 3.7\FTPServers
- key: HKEY_CURRENT_USER\SOFTWARE\Robo-FTP 3.7\Scripts
- key: HKEY_CURRENT_USER\Software\MAS-Soft\FTPInfo\Setup
- key: HKEY_LOCAL_MACHINE\Software\SoftX.org\FTPClient\Sites
- key: HKEY_CURRENT_USER\Software\SoftX.org\FTPClient\Sites
- key: HKEY_CURRENT_USER\Software\BulletProof Software\BulletProof FTP Client\Main
- key: HKEY_CURRENT_USER\Software\BulletProof Software\BulletProof FTP Client\Options

Collects information about installed applications

- Program: Python 2.7.10
- Program: Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
- Program: Microsoft Visual C++ 2005 Redistributable
- Program: Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.7523
- Program: Adobe Shockwave Player 12.2
- Program: Microsoft Visual C++ 2012 Redistributable - 11.0.61030
- Program: Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
- Program: Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005
- Program: Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030
- Program: Adobe Reader XI
- Program: Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23506
- Program: Microsoft Visual C++ 2015 Redistributable - 14.0.23506
- Program: Java 8 Update 74
- Program: Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030
- Program: Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23506
- Program: Microsoft Visual C++ 2013 Redistributable - 12.0.30501
- Program: Adobe Flash Player 20 ActiveX
- Program: Python 2.7 Pillow-2.9.0
- Program: Adobe Flash Player 20 NPAPI
- Program: Java 6 Update 22

Exhibits behavior characteristic of Pony malware

- C2: <http://mepsb-com.me/solisoft/coreserver/shit.exe>

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.48, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00045200, virtual_size: 0x000451f4

Performs some HTTP requests

- url: <http://mepsb-com.me/solisoft/coreserver/shit.exe>

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- http_version_old: HTTP traffic uses version 1.0
- suspicious_request: <http://mepsb-com.me/solisoft/coreserver/shit.exe>

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\7305000.exe

A process created a hidden window

- Process: MSBuild.exe -> C:\Users\Seven01\AppData\Local\Temp\7306437.bat

Possible date expiration check, exits too soon after checking local time

- process: MSBuild.exe, PID 2724

Creates RWX memory

1 HTTP Request(s) detected

<http://mepsb-com.me/solisoft/coreserver/shit.exe>

Hostname: mepsb-com.me

IP Address:

Port: 80

Count: 1