el.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:	559.50 KB (572928 bytes)
Compile time:	1975-01-31 01:34:17
MD5:	0903293a028b830ac6a2a470bd9402b7
SHA1:	e98c8a0706abce792be4083efb3ace56c057a1db
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-11-05 14:30:06

URL(s) file hosting

http://greatmobiles.co.uk/wp-ftp/el.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-11-05 04:06:44	21/68	

Import library

mscoree.dll

13 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN Fareit/Pony Downloader Checkin 2

- signature: ET TROJAN Likely Zbot Generic Post to gate.php Dotted-Quad
- signature: ET TROJAN Trojan Generic - POST To gate.php with no referer

Anomalous binary characteristics

- anomaly: Timestamp on binary predates the release date of the OS version it requires by at least a year

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\00000001\SMTP Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\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\00000002\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\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\00000003\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\00000002\IMAP Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\SMTP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\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\00000003\IMAP User Name
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\POP3 Server
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\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\00000001\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\00000001\NNTP Email Address
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\SMTP Port
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\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\00000001\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\00000002\POP3 User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\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\00000002\NNTP Password2
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\HTTP User
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\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\00000003\POP3 Password
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\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\0a0d020000000000c000000000000046
- 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\f86ed2903a4a11cfb57e524153480001
- 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\8503020000000000c000000000000046
- 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 9\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\LinasFTP\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

Attempts to access Bitcoin/ALTCoin wallets

- file: C:\Users\Seven01\AppData\Roaming\Bitcoin*.*
- file: C:\Users\Seven01\AppData\Local\Bitcoin*.*
- file: C:\ProgramData\Bitcoin*.*
- file: C:\ProgramData\Electrum*.*
- file: C:\Users\Seven01\AppData\Local\Electrum*.*
- file: C:\Users\Seven01\AppData\Roaming\Electrum*.*
- file: C:\Users\Seven01\AppData\Roaming\MultiBit*.*
- file: C:\ProgramData\MultiBit*.*
- file: C:\Users\Seven01\AppData\Local\MultiBit*.*
- file: C:\Users\Seven01\AppData\Local\Litecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Litecoin*.*
- file: C:\ProgramData\Litecoin*.*
- file: C:\Users\Seven01\AppData\Local\Namecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Namecoin*.*
- file: C:\ProgramData\Namecoin*.*
- file: C:\ProgramData\Terracoin*.*
- file: C:\Users\Seven01\AppData\Local\Terracoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Terracoin*.*
- file: C:\Users\Seven01\AppData\Roaming\PPCoin*.*
- file: C:\Users\Seven01\AppData\Local\PPCoin*.*
- file: C:\ProgramData\PPCoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Primecoin*.*
- file: C:\Users\Seven01\AppData\Local\Primecoin*.*
- file: C:\ProgramData\Primecoin*.*
- file: C:\ProgramData\Feathercoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Feathercoin*.*
- file: C:\Users\Seven01\AppData\Local\Feathercoin*.*
- file: C:\ProgramData\NovaCoin*.*
- file: C:\Users\Seven01\AppData\Roaming\NovaCoin*.*
- file: C:\Users\Seven01\AppData\Local\NovaCoin*.*

- file: C:\Users\Seven01\AppData\Local\Freicoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Freicoin*.*
- file: C:\ProgramData\Freicoin*.*
- file: C:\Users\Seven01\AppData\Local\Devcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Devcoin*.*
- file: C:\ProgramData\Devcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Franko*.*
- file: C:\Users\Seven01\AppData\Local\Franko*.*
- file: C:\ProgramData\Franko*.*
- file: C:\Users\Seven01\AppData\Local\ProtoShares*.*
- file: C:\Users\Seven01\AppData\Roaming\ProtoShares*.*
- file: C:\ProgramData\ProtoShares*.*
- file: C:\Users\Seven01\AppData\Roaming\Megacoin*.*
- file: C:\Users\Seven01\AppData\Local\Megacoin*.*
- file: C:\ProgramData\Megacoin*.*
- file: C:\ProgramData\Quarkcoin*.*
- file: C:\Users\Seven01\AppData\Local\Quarkcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Quarkcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Worldcoin*.*
- file: C:\Users\Seven01\AppData\Local\Worldcoin*.*
- file: C:\ProgramData\Worldcoin*.*
- file: C:\Users\Seven01\AppData\Local\Infinitecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Infinitecoin*.*
- file: C:\ProgramData\Infinitecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Ixcoin*.*
- file: C:\Users\Seven01\AppData\Local\Ixcoin*.*
- file: C:\ProgramData\Ixcoin*.*
- file: C:\ProgramData\Anoncoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Anoncoin*.*
- file: C:\Users\Seven01\AppData\Local\Anoncoin*.*
- file: C:\ProgramData\BBQcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\BBQcoin*.*
- file: C:\Users\Seven01\AppData\Local\BBQcoin*.*
- file: C:\ProgramData\Digitalcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Digitalcoin*.*
- file: C:\Users\Seven01\AppData\Local\Digitalcoin*.*
- file: C:\ProgramData\Mincoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Mincoin*.*
- file: C:\Users\Seven01\AppData\Local\Mincoin*.*
- file: C:\Users\Seven01\AppData\Local\GoldCoin (GLD)*.*
- file: C:\ProgramData\GoldCoin (GLD)*.*
- file: C:\Users\Seven01\AppData\Roaming\GoldCoin (GLD)*.*
- file: C:\Users\Seven01\AppData\Roaming\Yacoin*.*
- file: C:\Users\Seven01\AppData\Local\Yacoin*.*
- file: C:\ProgramData\Yacoin*.*
- file: C:\ProgramData\Zetacoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Zetacoin*.*
- file: C:\Users\Seven01\AppData\Local\Zetacoin*.*
- file: C:\Users\Seven01\AppData\Local\Fastcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Fastcoin*.*
- file: C:\ProgramData\Fastcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\I0coin*.*
- file: C:\Users\Seven01\AppData\Local\I0coin*.*
- file: C:\ProgramData\I0coin*.*
- file: C:\Users\Seven01\AppData\Roaming\Tagcoin*.*
- file: C:\ProgramData\Tagcoin*.*
- file: C:\Users\Seven01\AppData\Local\Tagcoin*.*
- file: C:\ProgramData\Bytecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Bytecoin*.*
- file: C:\Users\Seven01\AppData\Local\Bytecoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Florincoin*.*
- file: C:\Users\Seven01\AppData\Local\Florincoin*.*
- file: C:\ProgramData\Florincoin*.*

- file: C:\Users\Seven01\AppData\Roaming\Phoenixcoin*.*
- file: C:\Users\Seven01\AppData\Local\Phoenixcoin*.*
- file: C:\ProgramData\Phoenixcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Luckycoin*.*
- file: C:\Users\Seven01\AppData\Local\Luckycoin*.*
- file: C:\ProgramData\Luckycoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Craftcoin*.*
- file: C:\ProgramData\Craftcoin*.*
- file: C:\Users\Seven01\AppData\Local\Craftcoin*.*
- file: C:\Users\Seven01\AppData\Roaming\Junkcoin*.*
- file: C:\Users\Seven01\AppData\Local\Junkcoin*.*
- file: C:\ProgramData\Junkcoin*.*

Contacts C&C server HTTP check-in (Banking Trojan)

- url: http://141.105.64.137/el/gate.php

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://141.105.64.137/el/gate.php

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.21, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0008b200, virtual_size: 0x0008b054

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
- url: http://141.105.64.137/el/gate.php

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

- post_no_referer: HTTP traffic contains a POST request with no referer header
- http_version_old: HTTP traffic uses version 1.0
- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://141.105.64.137/el/gate.php

Dynamic (imported) function loading detected

- DynamicLoader: CRYPTBASE.dll/SystemFunction036

- DynamicLoader: uxtheme.dll/ThemeInitApiHook
- DynamicLoader: USER32.dll/IsProcessDPIAware
- DynamicLoader: ole32.dll/StgOpenStorage
- DynamicLoader: CRYPT32.dll/CryptUnprotectData
- DynamicLoader: CRYPT32.dll/CertOpenSystemStoreA
- DynamicLoader: CRYPT32.dll/CertEnumCertificatesInStore
- DynamicLoader: CRYPT32.dll/CertCloseStore
- DynamicLoader: CRYPT32.dll/CryptAcquireCertificatePrivateKey
- DynamicLoader: ADVAPI32.dll/AllocateAndInitializeSid
- DynamicLoader: ADVAPI32.dll/CheckTokenMembership
- DynamicLoader: ADVAPI32.dll/FreeSid
- DynamicLoader: ADVAPI32.dll/CredEnumerateA
- DynamicLoader: ADVAPI32.dll/CredFree
- DynamicLoader: ADVAPI32.dll/CryptGetUserKey
- DynamicLoader: ADVAPI32.dll/CryptExportKey
- DynamicLoader: ADVAPI32.dll/CryptDestroyKey
- DynamicLoader: ADVAPI32.dll/CryptReleaseContext
- DynamicLoader: ADVAPI32.dll/RevertToSelf
- DynamicLoader: ADVAPI32.dll/OpenProcessToken
- DynamicLoader: ADVAPI32.dll/ImpersonateLoggedOnUser
- DynamicLoader: ADVAPI32.dll/GetTokenInformation
- DynamicLoader: ADVAPI32.dll/ConvertSidToStringSidA
- DynamicLoader: ADVAPI32.dll/LogonUserA
- DynamicLoader: ADVAPI32.dll/LookupPrivilegeValueA
- DynamicLoader: ADVAPI32.dll/AdjustTokenPrivileges
- DynamicLoader: ADVAPI32.dll/CreateProcessAsUserA
- DynamicLoader: shell32.dll/SHGetFolderPathA
- DynamicLoader: netapi32.dll/NetApiBufferFree
- DynamicLoader: netapi32.dll/NetUserEnum
- DynamicLoader: kernel32.dll/WTSGetActiveConsoleSessionId
- DynamicLoader: kernel32.dll/ProcessIdToSessionId
- DynamicLoader: msi.dll/MsiGetComponentPathA
- DynamicLoader: pstorec.dll/PStoreCreateInstance
- DynamicLoader: userenv.dll/CreateEnvironmentBlock
- DynamicLoader: userenv.dll/DestroyEnvironmentBlock
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/IsWow64Process
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: MLANG.dll/
- DynamicLoader: wininet.dll/FindFirstUrlCacheEntryA
- DynamicLoader: kernel32.dll/SetFileInformationByHandle
- DynamicLoader: shell32.dll/SHGetFolderPathW
- DynamicLoader: urlmon.dll/CreateUri
- DynamicLoader: kernel32.dll/InitializeSRWLock
- DynamicLoader: kernel32.dll/AcquireSRWLockExclusive
- DynamicLoader: kernel32.dll/AcquireSRWLockShared
- DynamicLoader: kernel32.dll/ReleaseSRWLockExclusive
- DynamicLoader: kernel32.dll/ReleaseSRWLockShared
- DynamicLoader: kernel32.dll/InitializeSRWLock
- DynamicLoader: kernel32.dll/AcquireSRWLockExclusive
- DynamicLoader: kernel32.dll/AcquireSRWLockShared
- DynamicLoader: kernel32.dll/ReleaseSRWLockExclusive
- DynamicLoader: kernel32.dll/ReleaseSRWLockShared
- DynamicLoader: wininet.dll/FindNextUrlCacheEntryA
- DynamicLoader: wininet.dll/FindCloseUrlCache
- DynamicLoader: userenv.dll/GetUserProfileDirectoryW
- DynamicLoader: sechost.dll/ConvertSidToStringSidW
- DynamicLoader: kernel32.dll/GetNativeSystemInfo

SetUnhandledExceptionFilter detected (possible anti-debug)

2 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 205.185.216.10
Port: 80
Count: 1

http://141.105.64.137/el/gate.php
Hostname: 141.105.64.137
IP Address:
Port: 80
Count: 1

1 Host(s) detected

IP Address	Hostname	Reverse DNS
141.105.64.137		

1 Countr(y|ies) detected

Hosts	Country
1	Russian Federation