zero-install.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✗ | Anti VM ✗ | Signed ✓ | XOR ✓

MalScore: 49.5

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	3599.55 KB (3685936 bytes)
Compile time:	2016-10-20 23:52:38
MD5:	2d040f75dfb93fb91fa86dc9acd21c57
SHA1:	be3ec2036aee454a3fdd596521449ff20f4ad7ae
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2016-10-26 09:03:02

URL(s) file hosting

http://0install.de/files/zero-install.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-08-24 00:11:12	0/65	

Import library

mscoree.dll

6 Behaviors detected by system signatures

Creates RWX memory

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: http://www.usertrust.com1
- ioc: http://crl.usertrust.com/UTN-USERFirst-Object.crl0

Reads data out of its own binary image

- self_read: process: zero-install.exe, pid: 2456, offset: 0x00000000, length: 0x00001000
- self_read: process: zero-install.exe, pid: 2456, offset: 0x00000080, length: 0x00000200

Performs some HTTP requests

- url: http://repository.certum.pl/ctnca.cer
- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
- url: http://0install.de/feeds/ZeroInstall.xml

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:80

Presents an Authenticode digital signature

- md5_fingerprint: 52a33c86b7eeff58b5b85563f30cbb4a
- sha1_fingerprint: d2162b9a39238bb51d8488c046e506997481d57d
- cn: Open Source Developer, Bastian Eicher/emailAddress=info@0install.de
- sn: 129763274282511330507202919722346505897

4 HTTP Request(s) detected

http://repository.certum.pl/ctnca.cer
Hostname: repository.certum.pl
IP Address: 23.111.11.204
Port: 80
Count: 4

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 2.228.46.112
Port: 80
Count: 5

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 2.228.46.112
Port: 80
Count: 3

http://0install.de/feeds/ZeroInstall.xml
Hostname: 0install.de
IP Address: 37.120.161.26
Port: 80
Count: 1