adwizz.exe

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

MalFamily: Filerepmalware **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	65.50 KB (67072 bytes)
Compile time:	2017-09-15 08:05:28
MD5:	8606b485b012595d85cd21edaad99808
SHA1:	72e5edfeaa5f39bba60b840a8b41581964668c22
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-11-30 13:16:22

URL(s) file hosting

http://hitechnovation.com/Extra/Downloads/adwizz.exe
http://hitechnovation.com/Downloads/DList.txt
http://hitechnovation.com/thankyou.txt

Antivirus Report

Report date	Detection Ratio	Permalink
2017-11-30 11:01:55	4/67	

Import library

mscoree.dll

3 Behaviors detected by system signatures

Creates RWX memory

Performs some HTTP requests

- url: http://img.banggood.com/deals/affiliate_member_banner/e58478453181d060df81288ac201245231.jpg
- url: http://img.banggood.com/deals/affiliate_member_banner/a1b7f6c7d739aa48d5dfaacf54df399465.jpg
- url: http://img.banggood.com/deals/affiliate_member_banner/c8bfde373852a0ec6e7e532fd157a12f69.jpg
- url: http://img.banggood.com/deals/affiliate_member_banner/00b682284a10bdccd33c429ec31f4bec51.jpg

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

- IP: 192.168.56.1:80

4 HTTP Request(s) detected

http://img.banggood.com/deals/affiliate_member_banner/e58478453181d060df81288ac201245231.jpg

Hostname: img.banggood.com
IP Address: 2.20.157.210
Port: 80
Count: 1

http://img.banggood.com/deals/affiliate_member_banner/a1b7f6c7d739aa48d5dfaacf54df399465.jpg

Hostname: img.banggood.com
IP Address: 2.20.157.210
Port: 80
Count: 1

http://img.banggood.com/deals/affiliate_member_banner/c8bfde373852a0ec6e7e532fd157a12f69.jpg

Hostname: img.banggood.com
IP Address: 2.20.157.210
Port: 80
Count: 1

http://img.banggood.com/deals/affiliate_member_banner/00b682284a10bdccd33c429ec31f4bec51.jpg
Hostname: img.banggood.com
IP Address: 2.20.157.210
Port: 80
Count: 1