

Medre.A - AutoCAD worm samples

Archived: 2026-04-05 20:14:14 UTC



Medre.A is an AutoCAD worm, written in AutoLISP and is a very unusual piece of malware. It was

ESET reported Peru and neighboring countries as the target but I noticed that one of the samples' (MD5 25c7e10bb537b4265f6144f2cd7f6d95) original name is 未命名1 (Unnamed 1), so I wonder if some targets/sources were Chinese speaking.

P.S. The samples were donated by an anonymous but the original source is someone from Malwarebytes forum and I want to thank him/her (sorry don't know the name) for sharing. I hope they do not mind me posting them here.

File information

File: 2dda8e76f8488e8cd44dd25167e91642a0b27e245848be96ef0bea2797feb40eMD5:
ea04c29bc814af6d96157c1113b3806dSize: 22105

File: 7c489147ce4238ba0f9f992a7dbe7afc9e1b2ef9afd4d25e3b182d69e90e18c9MD5:
916744d1e7064a5522092f310a7c4ab0Size: 22052

File: 79baf616d2701cc26ef328cd9c13682db317932aa47efb8eb079d8af4a49e0a3

MD5: 7b563740f41e495a68b70cbb22980b20

Size: 12334

File: b886a58c6be03d75bf0a84ea3dc18c46aa98f6a9a5905f37661a23fd48d10232MD5:
25c7e10bb537b4265f6144f2cd7f6d95Size: 22602

File: e8e1148f7497aa546e46a45f35704ed6d9f9cb8d83d04a825aaa5ae6335d979MD5:
73dd85951ea154fbb40c26cd259ee0b7Size: 12334



Download



Automatic scans

SHA256: 7c489147ce4238ba0f9f992a7dbe7afc9e1b2ef9afd4d25e3b182d69e90e18c9

SHA1: 023e6c7730445db2b4c777b5d9b612e902dc7f72

MD5: 916744d1e7064a5522092f310a7c4ab0

File size: 21.5 KB (22052 bytes)

File name: 7c489147ce4238ba0f9f992a7dbe7afc9e1b2ef9afd4d25e3b182d69e90e18c9

File type: unknown

Detection ratio: 8 / 42

Analysis date: 2012-06-23 08:40:10 UTC (1 day, 17 hours ago)

Antivirus Result Update

Avast ALS:Merde-A [Wrm] 20120623

BitDefender Trojan.ACAD.H 20120623

Comodo UnclassifiedMalware 20120623

DrWeb - 20120623

Emsisoft - 20120623

F-Secure Trojan.ACAD.H 20120623

GData Trojan.ACAD.H 20120623

McAfee-GW-Edition Heuristic.LooksLike.Win32.Suspicious.H 20120623

NOD32 ACAD/Medre.A 20120622

Norman Bursted.F 20120622

nProtect - 20120623

SUPERAntiSpyware - 20120623

TrendMicro-HouseCall - 20120622

Additional information

ssdeep

384:HwvP/eyqn0QVgxccQ5YBvuOUIEERnVvdeQRv2J:6uOUgF4

TrID

Unknown!

First seen by VirusTotal

2012-06-21 19:08:34 UTC (3 days, 6 hours ago)

Last seen by VirusTotal

2012-06-23 08:40:10 UTC (1 day, 17 hours ago)

File names (max. 25)

1340366575.fc9e1b2ef9afd4d25e3b182d69e90e18c9

muestraACAD.txt

7c489147ce4238ba0f9f992a7dbe7afc9e1b2ef9afd4d25e3b182d69e90e18c9

file-4134327_

SHA256: 2dda8e76f8488e8cd44dd25167e91642a0b27e245848be96ef0bea2797feb40e

SHA1: ffadbc944a2976982e1daf0b715478e6062c9488

MD5: ea04c29bc814af6d96157c1113b3806d

File size: 21.6 KB (22105 bytes)

File name: account.exe

File type: unknown

Detection ratio: 10 / 42

Analysis date: 2012-06-23 20:28:06 UTC (1 day, 5 hours ago)

01

Avast ALS:Merde-A [Wrm] 20120623

BitDefender Trojan.ACAD.H 20120623

Comodo UnclassifiedMalware 20120623

Emsisoft Trojan.Acad!IK 20120623

F-Secure Trojan.ACAD.H 20120623

GData Trojan.ACAD.H 20120623

Ikarus Trojan.Acad 20120623

McAfee-GW-Edition Heuristic.LooksLike.Win32.Suspicious.H 20120623

Microsoft - 20120623

NOD32 ACAD/Medre.A 20120622

Norman Bursted.F 20120622

nProtect - 20120623

SUPERAntiSpyware - 20120623

TrendMicro-HouseCall - 20120623

384:HwvP/eyqn0QVgxccL5YBvuOIOFIIdZKyGNERNVvdeQ6v2J:buObFI6ZKRwY4

TrID

Unknown!

First seen by VirusTotal

2012-06-21 17:21:19 UTC (3 days, 8 hours ago)

Last seen by VirusTotal

2012-06-23 20:28:06 UTC (1 day, 5 hours ago)

File names (max. 25)

dsfg.txt

account.exe

2dda8e76f8488e8cd44dd25167e91642a0b27e245848be96ef0bea2797feb40e.exe

file-4134326_

2dda8e76f8488e8cd44dd25167e91642a0b27e245848be96ef0bea2797feb40e

1340366574.42a0b27e245848be96ef0bea2797feb40e

SHA256: 79baf616d2701cc26ef328cd9c13682db317932aa47efb8eb079d8af4a49e0a3

SHA1: 43ea33bedadc9bfc92c570b316b78b6fd9787f09

MD5: 7b563740f41e495a68b70cbb22980b20

File size: 12.0 KB (12334 bytes)

File name: acad.fas

File type: unknown

Detection ratio: 26 / 42

Analysis date: 2012-06-23 19:47:19 UTC (1 day, 5 hours ago)

AhnLab-V3 - 20120623

AntiVir ACAD/Bursted.A.3 20120623

Avast Other:Malware-gen [Trj] 20120623

AVG ACAD/Bursted.G 20120623

BitDefender Trojan.Acad.Bursted.W 20120623

ClamAV Worm.ACAD-1 20120623

Comodo UnclassifiedMalware 20120623

Emsisoft Email-Worm.Acad!IK 20120623

F-Secure Trojan.Acad.Bursted.W 20120623

Fortinet ACM/Medre.A@mm 20120623

GData Trojan.Acad.Bursted.W 20120623

Ikarus Email-Worm.Acad 20120623

Kaspersky Email-Worm.Acad.Medre.a 20120623

McAfee ALS/Bursted 20120623

McAfee-GW-Edition ALS/Bursted 20120623

Microsoft Worm:ALisp/Blemfox.A 20120623

NOD32 ACAD/Medre.A 20120622

Norman Bursted.E 20120622

nProtect Trojan.Acad.Bursted.W 20120623

Panda ACAD/Medre.A.worm 20120623

PCTools ALS.Bursted.B 20120623

Sophos AL/Bursted-AP 20120623

SUPERAntiSpyware - 20120623

Symantec ALS.Bursted.B 20120623

TrendMicro ACM_BURSTD.LEX 20120623

TrendMicro-HouseCall ACM_BURSTD.LEX 20120623

VBA32 - 20120622

VIPRE - 20120623

ViRobot I-Worm.Acad.A.Medre.12334 20120623

VirusBuster Worm.Acad.Medre.A 20120623

192:9FHRKCzYIvLCUglLBvFodl+gysUbfV01T5cjjhGkfHji:9/hdKJFobyxAYjLji

TrID

AutoCAD Fast-load AutoLISP (FAS4) (100.0%)

First seen by VirusTotal

2011-10-24 21:23:59 UTC (8 months ago)

Last seen by VirusTotal

2012-06-23 19:47:19 UTC (1 day, 5 hours ago)

File names (max. 25)

79baf616d2701cc26ef328cd9c13682db317932aa47efb8eb079d8af4a49e0a3

acad.fas

file-3312805_fas

20120104203533acad.fas

acad-fas.txt

cad.fas

SHA256: b886a58c6be03d75bf0a84ea3dc18c46aa98f6a9a5905f37661a23fd48d10232

SHA1: f46c445f912c6d1224e22f9e6a76020d594888b9

MD5: 25c7e10bb537b4265f6144f2cd7f6d95

File size: 22.1 KB (22602 bytes)

File name: b886a58c6be03d75bf0a84ea3dc18c46aa98f6a9a5905f37661a23fd48d10232

File type: unknown

Detection ratio: 8 / 42

Analysis date: 2012-06-23 08:41:41 UTC (1 day, 17 hours ago)

Avast ALS:Merde-A [Wrm] 20120623

BitDefender Trojan.ACAD.H 20120623

Comodo UnclassifiedMalware 20120623

Emsisoft - 20120623

F-Secure Trojan.ACAD.H 20120623

GData Trojan.ACAD.H 20120623

McAfee - 20120623

McAfee-GW-Edition Heuristic.LooksLike.Win32.Suspicious.H 20120623

Microsoft - 20120623

NOD32 ACAD/Medre.A 20120622

Norman Bursted.F 20120622

nProtect - 20120623

SUPERAntiSpyware - 20120623

TrendMicro-HouseCall - 20120622

384:HwvP/eyqn0QVgxccE5YBvuOeIbERnVvdeQ5v2J:iuOeFd4

TrID

Unknown!

First seen by VirusTotal

2012-06-21 17:23:36 UTC (3 days, 8 hours ago)

Last seen by VirusTotal

2012-06-23 08:41:41 UTC (1 day, 17 hours ago)

File names (max. 25)

b886a58c6be03d75bf0a84ea3dc18c46aa98f6a9a5905f37661a23fd48d10232

file-4134329_

1340366577.46aa98f6a9a5905f37661a23fd48d10232

未命名1

SHA256: e8e1148f7497aa546e46a45f35704ed6d9f9cb8d83d04a825aaa5ae6335d979b

SHA1: 44561e474bda129379d87750f49fd57a5d378f91

MD5: 73dd85951ea154fbb40c26cd259ee0b7

File size: 12.0 KB (12334 bytes)

File name: e8e1148f7497aa546e46a45f35704ed6d9f9cb8d83d04a825aaa5ae6335d979b

File type: unknown

Detection ratio: 17 / 42

Analysis date: 2012-06-23 08:42:46 UTC (1 day, 17 hours ago)

01

Antiy-AVL Trojan/win32.agent 20120623

Avast Other:Malware-gen [Trj] 20120623

BitDefender Trojan.Acad.Bursted.W 20120623

Comodo UnclassifiedMalware 20120623

Emsisoft Worm.ALisp!IK 20120623

F-Secure Trojan.Acad.Bursted.W 20120623

Fortinet ACM/Medre.A@mm 20120623

GData Trojan.Acad.Bursted.W 20120623

Ikarus Worm.ALisp 20120623

Kaspersky Email-Worm.Acad.Medre.a 20120623

McAfee - 20120623

McAfee-GW-Edition - 20120623

Microsoft Worm:ALisp/Blemfox.gen!A 20120623

NOD32 ACAD/Medre.A 20120622

Norman Bursted.G 20120622

nProtect - 20120623

Panda ACAD/Medre.A.worm 20120622

PCTools ALS.Bursted.B 20120623

SUPERAntiSpyware - 20120623

Symantec ALS.Bursted.B 20120623

TrendMicro-HouseCall - 20120622

ViRobot I-Worm.Acad.A.Medre.12334.A 20120623

Additional information

ssdeep

192:9FHRKCzYIvLCUgLLBvFodl+gysUbfV01T5cjhhGkcHji:9/hdKJFobyxAYj4ji

TrID

AutoCAD Fast-load AutoLISP (FAS4) (100.0%)

First seen by VirusTotal

2012-06-12 04:10:49 UTC (1 week, 5 days ago)

Last seen by VirusTotal

2012-06-23 08:42:46 UTC (1 day, 17 hours ago)

File names (max. 25)

file-4134332_

pisurith

e8e1148f7497aa546e46a45f35704ed6d9f9cb8d83d04a825aaa5ae6335d979b

1340366586.d6d9f9cb8d83d04a825aaa5ae6335d979b

Source: <http://contagiodump.blogspot.com/2012/06/medrea-autocad-worm-samples.html>