Aug 2012 W32.Crisis and OSX.Crisis - JAR file Samples - APT

contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html

End of the year presents:
Malicious Java file containing **W32.Crisis and OSX.Crisis**
Related News and Analysis:
Aug 2012
Crisis for Windows Sneaks onto Virtual Machines - Symantec
New Apple Mac Trojan Called OSX/Crisis Discovered - Intego

Download

Download. (Email me if you need the password scheme - see profile for email)

Files

File: adobe.jar
Size: 1124562
MD5: BA170664095B53D97690B5BE208927E2

Containing:

File: mac
Size: 993440
MD5: 6F055150861D8D6E145E9ACA65F92822

File: win
Size: 1043456
MD5: AE8D4770EF02373D7680F160E01E8668

Automatic scans
https://www.virustotal.com/file/53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524/analysis/
SHA256: 53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524
SHA1: 465ca6b7e883a7d145ddf6d59e3ef1c0eec279e5
MD5: ba170664095b53d97690b5be208927e2
File size: 1.1 MB (1124562 bytes)
File name: ba170664095b53d97690b5be208927e2
File type: JAR
Tags: jar
Detection ratio: 36 / 42
Analysis date: 2012-11-23 15:50:50 UTC (1 week, 6 days ago)
Additional information
Antivirus Result Update
Agnitum Trojan.DR.Injector!VcQiekruiLk 20121123
AntiVir Java/Dldr.Trea.CN.1 20121123
Antiy-AVL Trojan/Java.Agent 20121122
Avast Java:Dropper-F [Trj] 20121123
AVG Dropper.Generic6.AOLY 20121123
BitDefender Gen:Variant.Kazy.81085 20121123
CAT-QuickHeal TrojanDropper.Injector.fleh 20121122
ClamAV WIN.Trojan.Crisis 20121123
Commtouch - 20121123
Comodo UnclassifiedMalware 20121123
DrWeb Java.Dropper.15 20121123
Emsisoft Gen:Variant.Kazy.81085 (B) 20121123
eSafe - 20121121
ESET-NOD32 Java/Agent.EU 20121123
F-Prot - 20121123
F-Secure Trojan-Dropper:Java/SelfSign.A 20121123
Fortinet Java/Agent.N!tr 20121123
GData Gen:Variant.Kazy.81085 20121123
Ikarus Trojan-Dropper.Java.Agent 20121123
Jiangmin TrojanDropper.Java.n 20121123
K7AntiVirus - 20121122

Kaspersky Trojan-Dropper.Java.Agent.n 20121123
Kingsoft VIRUS_UNKNOWN 20121119
McAfee Morcut.a 20121123
McAfee-GW-Edition Morcut.a 20121123
Microsoft Trojan:Java/Spoilder.A 20121123
MicroWorld-eScan - 20121123
Norman Spoilder.A 20121123
nProtect MAC.OSX.Trojan.Morcut.A 20121123
Panda Generic Trojan 20121123
PCTools Malware.OSX-Crisis 20121123
Rising Trojan.Win32.Generic.12F274CC 20121123
Sophos Troj/JVDrop-A 20121123
SUPERAntiSpyware - 20121123
Symantec Trojan.Maljava 20121122
TheHacker Trojan/Dropper.Injector.fleh 20121123
TotalDefense Java/Agent.CDT 20121122
TrendMicro JAVA_MORCUT.A 20121123
TrendMicro-HouseCall TROJ_GEN.F47V0724 20121123
VBA32 TrojanPSW.Agent.acnn 20121122
VIPRE Trojan.Win32.Generic!BT 20121123
ViRobot Trojan.S.OSX.Crisis.1124562

https://www.virustotal.com/file/53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524/analysis/
SHA256: 53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524
SHA1: 465ca6b7e883a7d145ddf6d59e3ef1c0eec279e5
MD5: ba170664095b53d97690b5be208927e2
File size: 1.1 MB (1124562 bytes)
File name: ba170664095b53d97690b5be208927e2
File type: JAR
Tags: jar
Detection ratio: 36 / 42
Analysis date: 2012-11-23 15:50:50 UTC (1 week, 6 days ago)
Additional information
Antivirus Result Update
Agnitum Trojan.DR.Injector!VcQiekruiLk 20121123
AntiVir Java/Dldr.Trea.CN.1 20121123
Antiy-AVL Trojan/Java.Agent 20121122
Avast Java:Dropper-F [Trj] 20121123
AVG Dropper.Generic6.AOLY 20121123
BitDefender Gen:Variant.Kazy.81085 20121123
CAT-QuickHeal TrojanDropper.Injector.fleh 20121122

ClamAV WIN.Trojan.Crisis 20121123
Commtouch - 20121123
Comodo UnclassifiedMalware 20121123
DrWeb Java.Dropper.15 20121123
Emsisoft Gen:Variant.Kazy.81085 (B) 20121123
eSafe - 20121121
ESET-NOD32 Java/Agent.EU 20121123
F-Prot - 20121123
F-Secure Trojan-Dropper:Java/SelfSign.A 20121123
Fortinet Java/Agent.N!tr 20121123
GData Gen:Variant.Kazy.81085 20121123
Ikarus Trojan-Dropper.Java.Agent 20121123
Jiangmin TrojanDropper.Java.n 20121123
K7AntiVirus - 20121122
Kaspersky Trojan-Dropper.Java.Agent.n 20121123
Kingsoft VIRUS_UNKNOWN 20121119
McAfee Morcut.a 20121123
McAfee-GW-Edition Morcut.a 20121123
Microsoft Trojan:Java/Spoilder.A 20121123
MicroWorld-eScan - 20121123
Norman Spoilder.A 20121123
nProtect MAC.OSX.Trojan.Morcut.A 20121123
Panda Generic Trojan 20121123
PCTools Malware.OSX-Crisis 20121123
Rising Trojan.Win32.Generic.12F274CC 20121123
Sophos Troj/JVDrop-A 20121123
SUPERAntiSpyware - 20121123
Symantec Trojan.Maljava 20121122
TheHacker Trojan/Dropper.Injector.fleh 20121123
TotalDefense Java/Agent.CDT 20121122
TrendMicro JAVA_MORCUT.A 20121123
TrendMicro-HouseCall TROJ_GEN.F47V0724 20121123
VBA32 TrojanPSW.Agent.acnn 20121122
VIPRE Trojan.Win32.Generic!BT 20121123
ViRobot Trojan.S.OSX.Crisis.1124562

https://www.virustotal.com/file/c93074c0e60d0f9d33056fd6439205610857aa3cf54c1c20a48333b4367268ca/analysis/
SHA256: c93074c0e60d0f9d33056fd6439205610857aa3cf54c1c20a48333b4367268ca
SHA1: 7fa7c4af13ad1bcf12b180a5a9cf24613485608c
MD5: ae8d4770ef02373d7680f160e01e8668
File size: 1019.0 KB (1043456 bytes)

File name: ae8d4770ef02373d7680f160e01e8668
File type: Win32 EXE
Tags: peexe
Detection ratio: 31 / 34
Analysis date: 2012-11-23 15:50:23 UTC (1 week, 6 days ago)
Additional information
Behavioural information
Antivirus Result Update
Agnitum Trojan.DR.Injector!VcQiekruiLk 20121123
AntiVir TR/Drop.Bakefoe.A 20121123
Antiy-AVL Trojan/Win32.Injector.gen 20121122
Avast Win32:Crisis 20121123
BitDefender Gen:Variant.Kazy.81085 20121123
CAT-QuickHeal TrojanDropper.Injector.fleh 20121122
ClamAV WIN.Trojan.Crisis 20121123
Commtouch - 20121123
Comodo TrojWare.Win32.Boychi.a 20121123
Emsisoft Worm.Win32.Boychi.AMN (A) 20121123
ESET-NOD32 Win32/Boychi.A.Gen 20121123
F-Prot - 20121123
Fortinet W32/Swizzor.D!tr 20121123
GData Gen:Variant.Kazy.81085 20121123
Ikarus Worm.Win32.Boychi 20121123
Jiangmin TrojanDropper.Injector.aixs 20121123
K7AntiVirus Trojan 20121122
Kaspersky Trojan-Dropper.Win32.Injector.fleh 20121123
Kingsoft Win32.Troj.Injector.(kcloud) 20121119
McAfee Morcut.a 20121123
McAfee-GW-Edition Morcut.a 20121123
Microsoft Worm:Win32/Boychi.A 20121123
MicroWorld-eScan Gen:Variant.Kazy.81085 20121123
Norman Boychi.A 20121123
nProtect Trojan/W32.Agent.1043456.O 20121123
Panda Suspicious file 20121123
PCTools Malware.Crisis 20121123
Sophos W32/Crisis-A 20121123
SUPERAntiSpyware - 20121123
TheHacker Trojan/Dropper.Injector.fleh 20121123
TotalDefense Win32/Boychi.F 20121122
VBA32 TrojanPSW.Agent.acnn 20121122
VIPRE Trojan.Win32.Generic!BT 20121123
ViRobot Dropper.S.Crisis.1043456 20121123