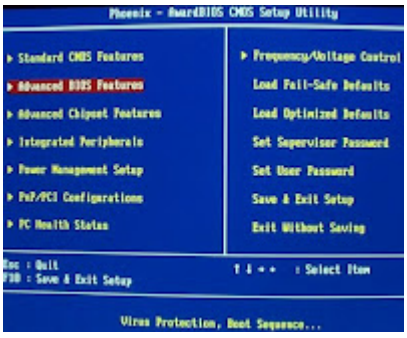
Mebromi BIOS rootkit affecting Award BIOS (aka "BMW" virus)

Mebromi BIOS rootkit affecting Award BIOS (aka "BMW" virus)



On September 13, 2011, Marco Giuliani from Webroot posted a detailed analysis of Mebromi - BIOS rootkit affecting Chinese computers with AWARD BIOS, which was earlier discovered by **Qihoo 360. As noted by** *cfans* from **bbs.kafan.cn and** *kerne1_madman* from hi.baidu.com/kerne1_madman, **the infection starts with a binary with MD5** 1AA4C64363B68622C9426CE96C4186F2 **that downloads the actual dropper MD5 BB5511A6586BA04335712E6C65E83671. While looking for the samples, I found one domain referenced on CleanMX on** 2011-08-31 **that was used for distribution of the downloader with binary called** qvodffs.exe MD5 1AA4C64363B68622C9426CE96C4186F2 hxxp://av.88ss.info/qvodffs.exe. In other cases it was called 123.exe (noted by Prevx -seen on Aug 29, 2011)

Exploit information and analysis links

- 360发布“BMW病毒”技术分析报告 - 360.cn
- http://bbs.kafan.cn
- “BMW”我终于逮到你了！ http://hi.baidu.com/kerne1_madman
- Mebromi: the first BIOS rootkit in the wild - Webroot.com
- Malware burrows deep into computer BIOS to escape AV http://www.theregister.co.uk
- BIOS Threat is Showing up Again! Symantec.com
- http://threatexpert.com/report.aspx?md5=b3106dbfb3ab114755af311883f33697
- http://www.threatexpert.com/report.aspx?md5=1aa4c64363b68622c9426ce96c4186f2

General File Information

Downloader: 123.exe
MD5: 1AA4C64363B68622C9426CE96C4186F2

File Type: exe

Infection Vector: Malicious link

Dropper: b.exe
MD5: BB5511A6586BA04335712E6C65E83671

File Type: exe

Infection Vector: downloaded by other malicious binaries

Download

Automated Scans

123

Submission date:
2011-09-18 11:41:03 (UTC)
Result:
38 /44 (86.4%)
http://www.virustotal.com/file-scan/report.html?id=7936deb5e6a236e8dce91352d0617e3db3bbe0fbaeba5fb08bbeac7590338c4d-1316346063

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.09.17.00	2011.09.17	Dropper/Rootkit.89600
AntiVir	7.11.14.223	2011.09.16	EXP/Shellcode.bak.2
Antiy-AVL	2.0.3.7	2011.09.18	Backdoor/Win32.Agent.gen
Avast5	5.0.677.0	2011.09.18	Win32:Qmgr-C [Trj]
AVG	10.0.0.1190	2011.09.18	Small.CSX
BitDefender	7.2	2011.09.18	Trojan.Generic.KDV.360525
CAT-QuickHeal	11.00	2011.09.18	Backdoor.Agent.bote
ClamAV	0.97.0.0	2011.09.18	Trojan.Agent-124036
Commtouch	5.3.2.6	2011.09.17	W32/Agent.JH.gen!Eldorado
Comodo	10156	2011.09.18	TrojWare.Win32.Trojan.Agent.Gen
DrWeb	5.0.2.03300	2011.09.18	BackDoor.Siggen.34341
Emsisoft	5.1.0.11	2011.09.18	Trojan-Dropper.Agent!IK
eSafe	7.0.17.0	2011.09.15	Win32.Agent
eTrust-Vet	36.1.8566	2011.09.17	Win32/Agent.BIU
F-Prot	4.6.2.117	2011.09.17	W32/Agent.JH.gen!Eldorado
F-Secure	9.0.16440.0	2011.09.18	Backdoor:W32/Agent.DQJS
Fortinet	4.3.370.0	2011.09.18	W32/Agent.BOTE!tr.bdr
GData	22	2011.09.18	Trojan.Generic.KDV.360525

Ikarus T3.1.1.107.0 2011.09.18 Trojan-Dropper.Agent
Jiangmin 13.0.900 2011.09.17 Backdoor/Agent.dfpb
K7AntiVirus 9.113.5150 2011.09.17 Riskware
Kaspersky 9.0.0.837 2011.09.18 Backdoor.Win32.Agent.bote
McAfee 5.400.0.1158 2011.09.18 Artemis!1AA4C64363B6
McAfee-GW-Edition 2010.1D 2011.09.17 Artemis!1AA4C64363B6
Microsoft 1.7604 2011.09.18 Exploit:Win32/ShellCode.gen!B
NOD32 6472 2011.09.18 Win32/Wapomi.AO
Norman 6.07.11 2011.09.17 W32/Suspicious_Gen2.PORRF
nProtect 2011-09-18.01 2011.09.18 Backdoor/W32.Agent.89600.AA
Panda 10.0.3.5 2011.09.18 Trj/CI.A
PCTools 8.0.0.5 2011.09.18 Malware.Wapomi
Prevx 3.0 2011.09.18 High Risk Cloaked Malware
Rising 23.75.04.02 2011.09.16 Trojan.Win32.Generic.128D4656
Symantec 20111.2.0.82 2011.09.18 W32.Wapomi!gen1
TheHacker 6.7.0.1.298 2011.09.17 Backdoor/Agent.bote
VBA32 3.12.16.4 2011.09.16 Backdoor.Agent.bote
VIPRE 10510 2011.09.18 Trojan.Win32.Generic!BT
ViRobot 2011.9.17.4674 2011.09.18 Backdoor.Win32.S.Agent.89600.I
MD5 : 1aa4c64363b68622c9426ce96c4186f2

smona13163373465369908093 7
2011-09-18 09:21:19 (UTC)
Result:38 /44 (86.4%)
http://www.virustotal.com/file-scan/report.html?id=8802ad7f2d267b754afef8fd81fe8e5f0ecc13e7f69b82e89e980922d94291ba-1316337679
AhnLab-V3 2011.09.17.00 2011.09.17 Win-Trojan/Mybios.130048
AntiVir 7.11.14.223 2011.09.16 TR/Dropper.Gen
Antiy-AVL 2.0.3.7 2011.09.18 Trojan/Win32.Mybios.gen
Avast5 5.0.677.0 2011.09.17 Win32:SuspBehav-C [Heur]
AVG 10.0.0.1190 2011.09.17 Dropper.Generic4.SZO
BitDefender 7.2 2011.09.18 Trojan.Generic.KDV.328903
ByteHero 1.0.0.1 2011.09.13 Trojan.Win32.Heur.Gen
CAT-QuickHeal 11.00 2011.09.16 Rootkit.Mybios.a
ClamAV 0.97.0.0 2011.09.18 Trojan.MyBios
Comodo 10153 2011.09.18 Heur.Suspicious
DrWeb 5.0.2.03300 2011.09.18 Trojan.Bioskit.1
Emsisoft 5.1.0.11 2011.09.18 Rootkit.Win32.Mybios!IK
eSafe 7.0.17.0 2011.09.15 Win32.TRDropper
eTrust-Vet 36.1.8566 2011.09.17 Win32/Rootkit.KM
F-Prot 4.6.2.117 2011.09.17 -
F-Secure 9.0.16440.0 2011.09.18 Trojan:W32/MyBios.A
Fortinet 4.3.370.0 2011.09.18 W32/Mybios.A!tr.rkit

GData 22 2011.09.18 Trojan.Generic.KDV.328903
Ikarus T3.1.1.107.0 2011.09.18 Rootkit.Win32.Mybios
Jiangmin 13.0.900 2011.09.17 Rootkit.Mybios.b
K7AntiVirus 9.113.5150 2011.09.17 Trojan
Kaspersky 9.0.0.837 2011.09.18 Rootkit.Win32.Mybios.a
McAfee 5.400.0.1158 2011.09.18 Boiskit.a
McAfee-GW-Edition 2010.1D 2011.09.17 Heuristic.LooksLike.Heuristic.BehavesLike.Win32.Trojan.B
Microsoft 1.7604 2011.09.18 TrojanDropper:Win32/Wador.A
NOD32 6472 2011.09.18 Win32/TrojanDropper.RootDrop.AB
Norman 6.07.11 2011.09.17 W32/Mebromi.A
nProtect 2011-09-18.01 2011.09.18 Trojan/W32.Agent.130048.IS
Panda 10.0.3.5 2011.09.18 Trj/CI.A
PCTools 8.0.0.5 2011.09.18 Trojan.Mebromi
Rising 23.75.04.02 2011.09.16 Trojan.Win32.Generic.1294136C
Symantec 20111.2.0.82 2011.09.18 Trojan.Mebromi
TheHacker 6.7.0.1.298 2011.09.17 Trojan/Mybios.a
TrendMicro 9.500.0.1008 2011.09.18 TROJ_MYBIOS.AB
TrendMicro-HouseCall 9.500.0.1008 2011.09.18 TROJ_MYBIOS.AB
VBA32 3.12.16.4 2011.09.16 Rootkit.Mybios.a
ViRobot 2011.9.17.4674 2011.09.18 Spyware.Mybios.RootKit.130048
VirusBuster 14.0.218.0 2011.09.17 Trojan.DR.RootDrop!QdYd6vAKrQU
MD5 : bb5511a6586ba04335712e6c65e83671

Source: http://contagiodump.blogspot.com/2011/09/mebromi-bios-rootkit-affecting-award.html