

Avea Jet Mobil Modem – Adware Uyarısı

written by Mert SARICA | 2 September 2010

Adware, İngilizce açılımı ile advertising-supported software yani reklam destekli yazılım, yüklenildiği bilgisayara yüklenme işleminden sonra program kullanımdayken otomatik olarak çalışan, gösteren ve indirme yapan bir yazılım paketidir. Adware'lerin bazı tipleri spyware statüsündedir ve kişisel bilgilere gizlice ulaşılmasında kullanılırlar. (Vikipedi)

Bir arkadaşım Avea Jet Mobil Modem kurulumu yapmaya çalıştığında Kaspersky antivirüs yazılımı tarafından kurulumun Adware nedeniyle engellendiğinden bahsetmişti. Dün dizüstü bilgisayarını getirerek incelememi rica etti. Vaktim kısıtlı olduğu için sadece modem kurulum dosyasını alarak sanal makina içine kurulumu gerçekleştirdim. Ardından kurulan tüm dosyaları zipleyerek virustotal sitesine yüklediğimde 39 antivirüsten 11 tanesi, zip dosyası içinde Adware tespit etti. Dosyaları tam olarak tespit edebilmek içinse kurulum yapılan klasörü uyarı veren antivirüs yazılımlarından rastgele bir tanesi ile taradığımda 4 adet dosya için Adware (BIDevManager.dll, BIRas.dll, BIUSBSound.dll, CMCOMService.dll) uyarısı aldım.

False positive diyebilmek için 11 farklı antivirüs yazılımı tarafından üretilen uyarı biraz yüksek bir rakam olduğu için Netsec grubuna bir e-posta göndererek bu sorun ile karşılaşan kimse olup olmadığını sorduğumda Avea'dan bir yetkili benimle iletişime geçerek konuyu en kısa sürede inceleyeceklerini iletti.

MF627 model Avea Jet mobil modem kullananlarınız var ise ve böyle bir uyarı ile daha önce karşılaştıysanız ve halen karşılaşmaya devam ediyorsanız paylaşımda bulunmanızı tavsiye ederim. Bu sayede yetkililer bunun genel bir sorun olduğu veya olmadığı kanısına kolaylıkla vararak (adware veya yanlış alarm) mobil modem uygulaması üzerinde yer alan güncelleme özelliğinden faydalanarak bu dosyaların güncellenmesi ve/veya antivirüs yazılımları tarafından uyarı üretilmemesi konularında girişimde bulunabilirler.

Konu ile ilgili olarak tarafıma geri dönüş yapılması durumunda sizleri tekrar bilgilendiriyor olacağım.

Mobil modem model: MF627

Ekran görüntüleri:

VirusTotal - Free Online Vir... x Bilgisayardan İnternet yerli... x

http://www.virustotal.com/file-scan/report.html?id=abc1d2b30cf112394bd8c51f61f27644ccde5031b3268a22f0aa3ed0b5663ad8-1283361102

Hack 4 Career. Infor...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: Avea.zip
Submission date: 2010-09-01 17:11:42 (UTC)
Current status: finished
Result: 11 /39 (28.2%)

VT Community
not reviewed
Safety score: -

Compact Print results

Antivirus	Version	Last Update	Result
AntiVir	8.2.4.46	2010.09.01	-
Antiy-AVL	2.0.9.7	2010.09.01	AdWare/Win32.Agent.gen
Authenticum	5.2.0.5	2010.09.01	-
Avast	4.8.1351.0	2010.09.01	-
Avast5	5.0.594.0	2010.09.01	-
AVG	9.0.0.851	2010.09.01	-
BitDefender	7.2	2010.09.01	-
CAT-QuickHeal	11.00	2010.09.01	AdWare.Agent.rdg (Not a Virus)
ClamAV	0.96.2.0-git	2010.09.01	-
Comodo	5936	2010.09.01	-
DrWeb	5.0.2.03300	2010.09.01	Adware.Siggen.8058
Emnisoft	5.0.0.37	2010.09.01	Riskware.AdWare.Win32.Agent!IK
eSafe	7.0.17.0	2010.09.01	-
eTrust-Vet	36.1.7830	2010.09.01	-
F-Prot	4.6.1.107	2010.09.01	-
F-Secure	9.0.15370.0	2010.09.01	-
Fortinet	4.1.143.0	2010.09.01	Adware/Agent
GData	21	2010.09.01	-
Ikarus	T3.1.1.88.0	2010.09.01	not-a-virus:AdWare.Win32.Agent
Jiangmin	13.0.900	2010.08.30	Adware/Agent.cnc
K7AntiVirus	9.62.2406	2010.08.31	-
Kaspersky	7.0.0.125	2010.09.01	not-a-virus:AdWare.Win32.Agent.rdg
McAfee	5.400.0.1158	2010.09.01	Artemis!9BB18F926ED
Microsoft	1.6103	2010.09.01	-
NOD32	5416	2010.09.01	-

Emsisoft ANTI-MALWARE

Help

Clean Computer

Menu

Processes scanned: 0	Traces scanned: 0	Objects detected: 4
Files scanned: 238	Cookies scanned: 0	

Scanning: C:\Program Files\Avea Jet Mobil Modem\UIPlugin\UIPhoneBook.dll

Diagnosis	Details
☐ Riskware.AdWare.Win32.Agent!IK	4 files - low risk
☐ File: C:\Program Files\Avea Jet Mobil Modem\Component\BIDevManager.dll	
☐ File: C:\Program Files\Avea Jet Mobil Modem\Component\BIRas.dll	
☐ File: C:\Program Files\Avea Jet Mobil Modem\Component\BIUSBSound.dll	
☐ File: C:\Program Files\Avea Jet Mobil Modem\Component\CMCOMService.dll	

Scanning files 92 %

Pause Stop

Actions on scan end

Scan running

At the left top you can see the number of Processes, Files, Spyware Traces and Cookies as well as the number of already detected objects.

You can get more information about a detected Malware by clicking its name in the result list while the scan is running. A browser window will be opened with the online description of that Malware.