Developer tools, technical documentation and coding examples

By wibjorn

Malware signed with the Adobe code signing certificate

Malware signed with the Adobe code signing certificate


msft-mmpc

87,678 Points 4 3 2

First Forums Reply Blog Party Starter Blog Conversation Starter

3 Oct 2012 7:29 PM

- Comments 0
- Likes

Last week, Adobe released an advisory (APSA12-01) announcing the upcoming revocation of an Adobe code signing certificate as it was compromised and used to sign at least two malicious utilities. They identified a compromised build server that required access to the code signing infrastructure and have forensic evidence that links it to the signing of these malicious utilities. They have confirmed that the private key was not compromised and this build server was used to sign the malicious utilities using the standard protocol used for valid Adobe software.

As a member of the Microsoft Active Protections Program (MAPP), the MMPC and other members received information about this compromise and immediately deployed protection for our customers – Win32/Adbposer. One of the primary goals of this attack is to evade antivirus and other security products as most of them have a feature/optimization to trust binaries signed by trusted certificates. The MMPC removed the compromised certificate from our trusted certificate list right away. For your protection please ensure that your virus definition version is greater than 1.137.689.0.

The malicious utilities include a tool used to dump passwords and a malicious ISAPI filter. Following are the details of the samples:

PwDump7.exe
SHA1: c615a284e5f3f41cf829bbb939f2503b39349c8d
Signature timestamp: Thursday, July 26, 2012 8:44:40 PM PDT (GMT -7:00)
Detected as PWS:Win32/Adbposer.A

libeay.dll
SHA1: 934543f9ecc28ebefbd202c8e98833c36831ea75
Signature timestamp: Thursday, July 26, 2012 8:44:13 PM PDT (GMT -7:00)
Detected as PWS:Win32/Adbposer.A.dll

myGeeksmail.dll
SHA1: fecb579abfbc74f7ded61169214349d203a34378
Signature timestamp: Wednesday, July 25, 2012 8:48:59 PM (GMT -7:00)
Detected as Trojan:Win32/Adbposer.B

Adobe has revoked the certificate today for all software code signed after July 10, 2012 and are also in the process of issuing updates signed using a new digital certificate for all affected products.

We have been tracking this issue very closely and the telemetry shows that this issue is not prevalent and is being used in highly targeted attacks only. We will continue to monitor for new malware leveraging this issue.

Tanmay Ganacharya
MMPC

Comments

Explore Certifications

- View streaming technical content about Microsoft products from the experts that build and use it every day.

  Start watching now

Recommended Resources

- **Startups**

  Stronger together: Calling Social Entrepreneurs around the globe with COVID-19 solutions.

- **Students**

  Put professional developer tools and software in the hands of students.

- **Learn events**

  Video content by developers and technical enthusiasts devoted to including you in the conversation.

Interested in the latest announcements and updates to Microsoft Docs? Check out the team blog

---