Zlob trojan

By Contributors to Wikimedia projects

Published: 2007-08-05 · Archived: 2026-04-05 21:14:55 UTC

From Wikipedia, the free encyclopedia

Zlob	
Malware details	
Technical name	• TrojanDownloader:Win32/Zlob (Microsoft) • Trojan.Zlob (Symantec) • Trojan.Zlob.[Letter] (Symantec) • Trojan-Downloader:W32/Zlob (F-Secure) • Win32.Trojandownloader.Zlob (F-Secure) • Trojan-Downloader.Win32.Zlob (F-Secure) • TROJ_ZLOB.[Letter] (Trend Micro) • Trojan-Downloader.Win32.Zlob.[letter] (Kaspersky) • Downloader.Win32.Zlob.[Letter] (Kaspersky) • TR/Dldr.Zlob.Gen (Avira) • TR/Drop.Zlob.[Letter] (Avira)
Type	Malware
Subtype	Spyware

The **Zlob Trojan**, identified by some antiviruses as **Trojan.Zlob**, is a Trojan horse which masquerades as a required video codec in the form of ActiveX. It was first detected in late 2005, but only started gaining attention in mid-2006.[1]

Once installed, it displays popup ads which appear similar to real Microsoft Windows warning popups, informing the user that their computer is infected with spyware. Clicking these popups triggers the download of a fake anti-spyware program (such as Virus Heat and MS Antivirus (Antivirus 2009)) in which the Trojan horse is hidden.[1]

The Trojan has also been linked to downloading atnvrsinstall.exe which uses the Windows Security shield icon to look as if it is an anti-virus installation file from Microsoft. Having this file run can wreak havoc on computers and networks. One typical symptom is random computer shutdowns or reboots with random comments.[*further explanation needed*] This is caused by the programs using Task Scheduler to run a file called "zlberfker.exe."

Project Honeypot Spam Domains List (PHSDL)[2] tracks and catalogs spam domains. Some of the domains on the list are redirects to porn sites and various video watching sites that show a number of online videos. Playing videos on these sites activates a request to download an ActiveX codec which is malware. It prevents the user from closing the browser in the usual manner. Other variants of Zlob Trojan installation come in the form of a Java cab file masquerading as a computer scan.[3]

There is evidence that the Zlob Trojan might be a tool of the Russian Business Network[4] or at least of Russian origin.[5]

RSPlug, DNSChanger, and other variants

[edit]

The group that created Zlob has also created a Mac Trojan with similar behaviors (named RSPlug).[6] Some variants of the Zlob family, like the so-called "DNSChanger", add rogue DNS name servers to the registry of Windows-based computers[7] and attempt to hack into any detected router to change the DNS settings, potentially re-routing traffic from legitimate web sites to other suspicious web sites.[8] DNSChanger in particular gained significant attention when the U.S. FBI announced it had shut down the source of the malware in late November 2011.[9] However, as there were millions of infected computers which would lose access to the Internet if the malware group's servers were shut down, the FBI opted to convert the servers into legitimate DNS servers. Due to cost concerns, however, these servers were set to shut down on the morning of 9 July 2012, which could cause thousands of still-infected computers to lose Internet access.[10] This server shutdown did occur as planned, although the expected issues with infected computers did not materialize. By the date of the shutdown, there were many free of charge programs available that removed the Zlob malware effectively and without requiring great technical knowledge. The malware did however remain in the wild and as at 2015 could still be found on unprotected computers. The malware was also self-replicating, something the FBI did not fully understand, and the servers that were shut down may have only been one of the initial sources of the malware. Current antivirus programs are very effective at detecting and removing Zlob and its time in the wild appears to be coming to an end.[*citation needed*][*needs update*]

- Search-daily Hijacker
- Trojan.Win32.DNSChanger

1. ^ Jump up to: **a** **b** *"The ZLOB Show: Trojan Poses as Fake Video Codec, Loads More Threats"*. *Trend Micro. Retrieved 26 November 2007.*
2. ^ Project Honeypot Spam Domains List
3. ^ PHSDL Zlob Trojan Forum Spam Hijacking Attempt Documentation
4. ^ *"RBN – Fake Codecs"*.
5. ^ *"TCP – Проект Киберкультуры | Zlob Team"*.
6. ^ *Tung, Liam (8 November 2007). "Multiplying Mac Trojan not epidemic yet". CNET News. Retrieved 26 November 2007.*
7. ^ *Podrezov, Alexey (7 November 2005). "F-Secure Virus Descriptions: DNSChanger". F-Secure Corporation. Retrieved 26 November 2007.*

8. ^ *Vincentas (9 July 2013). "Zlob Trojan in SpyWareLoop.com". Spyware Loop. Retrieved 28 July 2013.*
9. ^ *"International Cyber Ring That Infected Millions of Computers Dismantled". U.S. FBI. 9 November 2011. Retrieved 6 June 2012.*
10. ^ *Kerr, Dara (5 June 2012). "Facebook warns users of the end of the Internet via DNSChanger". CNET. Retrieved 6 June 2012.*

- List of ActiveX Zlob Trojan fake codecs and other misleading Zlob-installers
- Listing of 113 fake codec domains
- Flash's Security Blog, a blog listing fake codecs and rogue security software.
- S!Ri.URZ, SmitfraudFix.
- Zlob/VideoAccess/Trojan.Win32.DNSChanger – malekal.com (fr)

Anti Zlob Malware Forums

- Geeks to Go Forum
- SWI Forum Archived 4 December 2008 at the Wayback Machine
- TSG Forum Archived 4 December 2007 at the Wayback Machine
- dns-ok.gov.au An Australian Government website, which has the diagnostic ability to determine if your computer is infected by DNSChanger.
