Threat summary: Malware Family DNS Changer (Alureon)

MSTI-TS-DNS-Changer

Microsoft

Last update	2017-12-13

Summary

DNS Changer (detected as Alureon) is a family of trojans operating since at least 2006, hijacking the DNS settings of a victim computer to perform click hijacking, or clickjacking,[1] and advertising replacement fraud.

Victims' computers become infected with the malware when they visit certain websites or download codec software (often used to view videos online). Alureon was observed bundled with the rogue security software, Security Essentials 2010.[2]

DNS Changer modifies the host DNS settings and blocks access to Windows Task Manager, Windows Update, and desktop configuration settings. It attempts to disable anti-malware software, redirect search engine results, and present malicious advertisements in lieu of existing website advertisements.

Details

Win32/Alureon,[3] a DNS changer, is the malware behind a large-scale advertising scam that was ultimately used to steal over USD$14,000,000 through legitimate advertising affiliate schemes. Rove Digital, an Estonian company, used a series of dummy corporations in conjunction with the malware to redirect over four million hosts, and 500,000 of these were in the United States.[4]

Clickjacking

When a user browsed from an infected host, and a search result link was clicked, the malware caused the browser to reroute to a different website selected by the malware operator. Each click triggered a payment to the malicious actor, based upon the advertising and referral schemes for which they had enrolled.

The following are examples of specifically tailored clickjacking redirections in the Alureon attack:[5]

- Apple iTunes was hijacked to redirect to a non-Apple website

[1] https://www.microsoft.com/en-us/research/publication/clickjacking-attacks-and-defenses/#

[2] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Rogue:Win32/Fakeinit

[3] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2fAlureon

[4] https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

[5] Ibid.

- Netflix.com was hijacked to redirect to a site called "BudgetMatch"
- The website of the United States Internal Revenue Service was redirected to point to H&R Block's website

Advertising replacement fraud

Using the malware and rogue DNS servers, the adversary replaced legitimate advertisements on websites with advertisements that triggered payments benefiting themselves. The following are examples of Alureon advertising replacement fraud:[6]

- An advertisement on the Wall Street Journal home page was replaced with an advertisement for "Fashion Girl LA"
- On Amazon.com, an advertisement for Windows Internet Explorer 8 was replaced with an advertisement for an email marketing business
- On the ESPN website, an advertisement for "Dr. Pepper Ten" was replaced with an advertisement for a timeshare business

Alureon malware

The Alureon trojan (also known as DNS Changer, TDL4, TDSS and TidServ) contains rootkit functionality, and in a later version, included a banking trojan component. It was primarily served through the DNS Changer malware; hence, both are detected as Win32/Alureon.[7]

The malware is composed of multiple components, including a downloader that fetches additional elements when first executed. Alureon hijacks the print spooler service (spoolsv.exe) to persist, and then updates the master boot record such that a modified bootstrap routine is installed. Next, the malware infects low-level system drivers, such as those responsible for parallel ATA operations (atapi.sys) to implement the rootkit. When Alureon first appeared, the rootkit was known at TDL1. As it was upgraded, different versions were observed, culminating in the last version, TDL4.

Alureon blocks access to Windows Task Manager, Microsoft Update, and desktop configuration settings. The malware attempts to disable antivirus software. It redirects the DNS settings to point to foreign DNS servers under the control of the company "Digital Rove," or one of its subsidiaries.[8] If the infected host is on a network using DHCP to assign IP addresses, the malware can spoof the DHCP replies, thereby providing DNS settings selected by the malware, rather than by the corporate DHCP servers.[9]

The malware reports back on the infected host with system statistics, and in some cases, stolen banking information.

---

[6] https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

[7] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2fAlureon

[8] https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

[9] https://arstechnica.com/tech-policy/2011/11/how-the-most-massive-botnet-scam-ever-made-millions-for-estonian-hackers/

Takedown

On November 8, 2011, the FBI, the Estonian police, and several industry partners performed a takedown operation against the Alureon botnet, which at the time consisted of over four million infected hosts. Over 100 servers in the command and control (C2) networks were seized in an operation named "Operation Ghost Click." The servers were in Chicago and New York, and the Estonian police arrested six individuals at Rove Digital in Estonia, including CEO Vladimir Tsastsin. Rove Digital ran Estdomains, Esthost, Cernel, UkrTelegroup, and numerous other shell corporations. Esthost, an Internet hosting service, lost its ICANN accreditation in 2008 when its founder Vladimir Tsastsin was convicted of credit card fraud in Estonia.

Instead of removing the malicious DNS servers and stranding up to four million infected hosts unable to resolve domains names, the FBI commissioned Internet Systems Consortium (ISC) to replace the malicious DNS servers with legitimate DNS servers so that users' Internet access would not be interrupted. The ISC set up the DNS Changer Working Group (DCWG) with an information page that included tests to see if hosts were infected.[10]

Remediation efforts were accomplished in accordance with the order of a Manhattan federal court judge for a limited period of 120 days during which time the replacement DNS servers would be deployed. This period was later extended to 365 days. Although the replacement DNS servers provided continuity of Internet service to victims, those replacement servers did not remove the malware from the infected computers.

At 12:01 Eastern Daylight Time on Monday July 9, 2012, the DCWG DNS servers stopped responding to DNS queries from infected hosts. This followed the U.S. Department of Justice court order authorizing the clean DNS servers.

On August 10, 2012, the IP address blocks used by the Rove Digital criminal operations had been reallocated by RIPE-NCC and advertised to the Internet.

After the takedown

Infections of Alureon continue to be reported due to the still-active infection vectors. The likely causes are web pages that contain pornographic content and purport to require the installation of the fake video codecs, and the spoofing of DHCP server responses within an infected network.

Furthermore, the concept of changing a victim's DNS server has been adopted by other malware families since it offers a relatively simple approach to monetizing infected machines. This can be achieved using as little as a Visual Basic script delivered to victims through email.

Action on intent

DNS Changer (Alureon) generated revenue through advertisement replacement on victim machines where the malicious actor received fees whenever these advertisements were clicked. The criminal group operated a fake antivirus affiliate scheme which was promoted through the hijacked advertisements. To aid the installation of untrustworthy software, the infected hosts were denied access to security updates and antivirus software. Furthermore, personal information was extracted from the hosts and was sent to a command and control (C2) server.

[10] http://www.dcwg.org/detect/

Detection

Microsoft Antimalware solutions detect and block this threat as Win32/Alureon.[11]

Aliases

- Avira: TR/Dldr.DNSChanger.gen[12]
- Kaspersky: Trojan-Downloader.Win32.Zlob[13]
- McAfee: DNSChanger[14]
- Sophos: Troj/Zlob-AHE[15]
- Symantec: Trojan.Zlob[16]
- Trend Micro: TROJ_DNSCHAN[17]

Activity parameters	Start date: 2006	End date: N/A
Activity group	N/A	
Tags	DNS Changer, Alureon, TDL4, TDL1, Zlob, clickjacking, advertising fraud, Rove Digital, malware, TDSS, TidServ	

[11] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2fAlureon
[12] https://www.avira.com/en/support-threats-summary/tid/3297/threat/TR.Dldr.DNSChanger.Gen
[13] https://securelist.com/monthly-malware-statistics-april-2011/29665/
[14] https://securingtomorrow.mcafee.com/business/an-update-on-dnschanger-and-rogue-dns-servers/
[15] https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Zlob-AHE.aspx
[16] https://www.symantec.com/security_response/writeup.jsp?docid=2005-042316-2917-99
[17] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/troj_dnschan.add