The Register®
Biting the hand that feeds IT

Original URL: http://www.theregister.co.uk/2008/10/03/neosploit_powered_mass_hack_attack/

Hackers exploit Neosploit to booby trap BBC, US postal service

200K login credentials found on crimeware server

By **John Leyden**

Posted in Security, 3rd October 2008 17:24 GMT

Cybercrooks have used the latest version of Neosploit to booby-trap an estimated 80,000 legitimate sites with malicious code.

Victims of the attack include government, Fortune 500, and a weapons manufacturing firm, according to Ian Amit, director of security research at Aladdin Knowledge Systems. Amit said victims of the attack included the US Postal Service, which has since cleaned up its act.

Amit uncovered the assault while researching the newly-released Neosploit 3.1 hacker toolkit. During his research, he discovered login credentials for more than 200,000 servers on a server used by cybercrooks. These credentials included BBC login details fortunately unconnected to the corporation's news or content sites.

Analysis by Amit and his team at Aladdin suggest that at least three gangs were involved in collecting the list and that 80,000 of these sites had been loaded with malicious code by hackers as part of attempt to infect visiting surfers through drive-by download attacks. Organisations in 86 countries are said to be affected. Amit identified the affected orgainsations after examining server logs.

"Out of the 200,000 credentials, nearly 107,000 were validated by the criminal server, and of which, almost 82,000 were used to modify Web related content in order to attack the users of the associated sites," a statement by Aladdin explains.

Amit explained: "After closer investigation of the data gathered during the research, it came to our attention that not only the criminals were able to get their hands on the [government's BBC site, ftp.bbc.co.uk]. If not for the sheer luck that the credentials were not associated with any online material, this incident could have ended up infecting the BBC's website visitors.

"Additionally, reputable universities such as the University of Bradford, a travel agency (easytravelgroup.co.uk), and of course a lot of internet providers and hosting companies were affected," he added. Aladdin is working with CERT and law enforcement agencies worldwide to

inform affected organisations about the compromise to their websites.

Incidents where legitimate websites are compromised with malicious code using tactics such as SQL injection attacks have reached epidemic proportions over recent months. The compromises unearthed by Aladdin join a growing list of assaults and victims. Previous targets have included the government of the City and County of San Francisco, Microsoft acquisition target atmdt.com, BMW in Mexico, Hackney Council, and BusinessWeek.com. Tools such as the The Asprox attack toolkit have featured as part and parcel of these previous attacks. ®

Related stories

Malware authors play Mario on *Daily Mail* website (2 December 2008)
http://www.theregister.co.uk/2008/12/02/daily_mail_malware/

Drive-by download attack mows down thousands of websites (10 November 2008)
http://www.theregister.co.uk/2008/11/10/drive_by_download_mass_attack/

Illegal pharmaceutical ads infiltrate gov, edu sites (again) (4 November 2008)
http://www.theregister.co.uk/2008/11/04/massive_website_hijacking/

SQL injection taints BusinessWeek.com (16 September 2008)
http://www.theregister.co.uk/2008/09/16/businessweek_hacked/

Hijacking huge chunks of the internet - a new How To (27 August 2008)
http://www.theregister.co.uk/2008/08/27/bgp_exploit_revealed/

SQL attacks inject government sites in US, UK (7 August 2008)
http://www.theregister.co.uk/2008/08/07/new_sql_attacks/

Beloved websites riddled with crimeware (30 July 2008)
http://www.theregister.co.uk/2008/07/30/websense_high_profile_website_malware_survey/

Cybercrooks get faster, further and sneakier (29 July 2008)
http://www.theregister.co.uk/2008/07/29/x_force_threat_report/

Drive-by download attacks menace UK.gov (23 July 2008)
http://www.theregister.co.uk/2008/07/23/drive_by_download_asprox_menace/

Tennis sites hit by drive-by download attacks (25 June 2008)
http://www.theregister.co.uk/2008/06/25/sql_injection_attacks/

'Legit' website compromises reach epidemic proportions (5 June 2008)
http://www.channelregister.co.uk/2008/06/05/scansafe_web_malware_survey/

Cybercrooks plant phishing scam on crime reduction website (3 June 2008)
http://www.theregister.co.uk/2008/06/03/home_office_crime_reduction_hack/