COMPUTERWOCHE
VOICE OF DIGITAL

Perfide Attacke

Trojanisches Pferd mit DHCP-Server an Bord

Datum: 10.12.2008
Autor(en): Uli Ries

Der Trojaner Trojan.Flush.M installiert auf infizierten PCs einen bösartigen DHCP-Server, der anderen Clients einen vom Angreifer kontrollierten DNS-Eintrag unterschiebt. Somit genügt im Prinzip ein infizierter PC, um ein ganzes Firmennetzwerk mit falschen DNS-Informationen zu verseuchen. Bislang scheint sich der Trojaner allerdings nur langsam zu verbreiten.

Übler Geselle: Ein Trojaner, der einen bösartigen DHCP-Server installiert.

Trojan.Flush.M macht aus jedem infizierten PC einen bösartigen **DHCP-Server**[1], indem der Schädling einen voll funktionstüchtigen Netzwerktreiber (NDISprot) installiert. Um den Treiber verlässlich zu laden, fügt der **Trojaner**[2] noch einen neuen Systemdienst hinzu (ArcNet NDIS Protocol Driver). NDISprot erkennt DHCP-Anfragen anderer **Clients**[3] im Netzwerk erkennen und kann sich selbst als DHCP-Server ausgeben. Gewinnt der gefälschte DHCP-Server das Rennen um die Antwort an den Client gegen den legitimen DHCP-Server des jeweiligen Netzes, verwirft der anfragende Client die langsamere Antwort.

Jeder Client, der seine IP-Daten vom bösartigen DHCP-Server bezieht, bekommt neben den jeweils gültigen Werten für IP-Adresse und Subnetz zwei IP-Adressen von DNS-Server (85.255.112.36 und 85.255.112.41) untergejubelt. Diese DNS-Server stehen unter der Kontrolle der **Cyber-Kriminellen**[4], so dass alle Namensanfragen der – an sich nicht infizierten – Clients prinzipiell mit gefälschten IP-Adressen beantwortet werden können. Somit können die Angreifer jeden beliebigen Aufruf einer Website auf von ihnen bestimmte (**Phishing**[5])-Seiten umleiten.

Bereits ein einziger infizierter PC genügt theoretisch, um alle DNS-Anfragen eines ganzen Unternehmensnetzwerkes zu den Nameservern der Kriminellen zu schicken. In der Praxis wird dies jedoch kaum vorkommen, da der legitime DHCP-Server nicht jedes Rennen gegen die bösartige Komponente verliert. Außerdem hat sich der Trojaner laut **Symantec**[6] bislang kaum verbreitet, so dass die Antiviren-Spezialisten Trojan.Flush.M lediglich als geringe Gefahr einstufen.

Schutz vor dem DHCP-Trojaner sollten die üblichen **Anti-Viren-Programme**[7] bieten, da der Schädling inzwischen in die Signatufiles der Scanner eingeflossen sein sollte. Darüberhinaus können Administratoren die Router und **Firewalls**[8] im Unternehmen so konfigurieren, dass alle von Clients stammenden und ans Internet gerichteten DNS-Anfragen blockiert werden und lediglich der Intranet-DNS-Server mit der Außenwelt kommunizieren darf. Auf diese Weise fällt eine Attacke zudem schnell auf, da die mit gefälschten DNS-Einträgen versorgen Clients keine Namen mehr auflösen können.

Links im Artikel:

[1] **http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol**
[2] **https://www.computerwoche.de/schwerpunkt/t/Trojaner.html**
[3] **https://www.computerwoche.de/schwerpunkt/c/Client.html**
[4] **https://www.computerwoche.de/knowledge_center/security/1878479/**
[5] **https://www.computerwoche.de/knowledge_center/security/1877442/**
[6] **http://http//www.symantec.com/security_response/writeup.jsp?docid=2008-120318-5914-99&tabid=2**
[7] **https://www.computerwoche.de/knowledge_center/security/172251/**
[8] **https://www.computerwoche.de/schwerpunkt/f/Firewall.html**
