Inhalt

Bereits im November des Jahres 2011 wurden die Betreiber des bisher wahrscheinlich größten Botnetzes dingfest gemacht und angeklagt. In einem Zeitraum von fast 4 Jahren wurden wahrscheinlich über 100 Millionen Rechner in mehr als 100 Ländern infiziert. Angeblich sind in Deutschland aktuell circa 33.000 Computer pro Tag von diesem DNS-Betrug betroffen.

[*Anm.: aus meiner Sicht sagt dies nichts über die tatsächliche Zahl befallener Rechner aus, da jeder Rechner bei einer Verbindung zum Internet unzählige Anfragen an den DNS Server stellt. Ich schätze, dass es sich um 5-10 Tausend Rechner handelt; höchstens*]

Obwohl das **Botnetz** stillgelegt ist gibt es jetzt ein Nachbeben. Befallenen Rechnern droht der **Totalausschluß vom Internet**.

Hintergründe *

Die Betreiber des Botnetzes hatten diverse Firmen gegründet, die Kunden garantierte Werbeeinblendungen versprachen. Diese Werbung wurde statt der originalen Werbung dann in die Seiten prominenter WEB-Seiten eingeblendet. Das spülte dann ca. 14 Millionen US Dollar in die Kassen der Betrüger.

Die Technik
Das Internet kennt keine WEB-Adressen wie www.ArchiCrypt.de oder www.passwort-zentrale.de. Das Internet arbeitet ausschließlich mit so genannten IP-Adressen. Wenn Sie jetzt in Ihren Browser www.ArchiCrypt.com eintragen, dann muss Ihr Computer irgendwo nachfragen, wie die aktuelle IP-Adresse der Seite lautet. Und genau hier betreten die DNS-Server die Showbühne. Sie sind für Namensauflösungen verantwortlich, liefern also bei einer Anfrage nach www.ArchiCrypt.de zum Beispiel die IP Adresse 88.172.90.12. Mit dieser IP Adresse arbeitet Ihr Computer dann weiter.

> Ein DNS-Server ist also so etwas wie eine Adressauskunft.

Der Betrug
DNS-Changer änderte die Netzwerkeinstellungen befallener Rechner. Ein anderer DNS-Server wird in Ihrem Rechner eingetragen, so dass alle Adressanfragen bei dem **präparierten DNS-Server** landen. Wenn man jetzt zum Beispiel die Adresse www.microsoft.com eingibt, landet man nicht dort, sondern auf einer Seite der Botnetzbetreiber. Eine manipulierte Seite mit Werbeeinblendungen der Betrüger wird angezeigt.

Der Schädling hat zudem noch weitere Finessen.

Er arbeitet auch als s.g. DHCP-Server. Andere Rechner im Netzwerk beziehen dann hier die eigene IP Adresse, die Netzmaske des Gateway und eben auch den DNS-Server (*ist dann ebenfalls der präparierte*) über den Adressen aufgelöst werden.

Der Schädling versucht auch, mittels einer Passwortliste, die Einträge im Router zu ändern. Auch schützt er sich selbst, indem es Antivirenprogramme daran hindert, ihre Virensignaturen auf den neusten Stand zu bringen.

Warum erst jetzt die Reaktion *

Das FBI hat nach der Festnahme der Betreiber die „bösen“ DNS-Server vom Netz genommen. Und, laut Angaben des FBI, die Server schnell durch eigene Server ersetzt, damit befallene Rechner weiterhin ins Internet können. Diese Server sollen jetzt abgeschaltet werden.

[*Anm.: Ich möchte hier keine Verschwörungstheorie ins Leben rufen, finde das aber zu selbstlos vom FBI. Warum zunächst Erste Hilfe leisten, indem man eigene Server ins Netz stellt und dann nach einem knappen viertel Jahr die Server vom Netz nehmen. Das einzige, was hier als Begründung im positiven Sinne in Frage kommt, wäre, dass man Zeit gewinnen wollte. Oft ist es jedoch so, dass man sich solche Schädlinge beim Besuch übler Seiten im Internet zuzieht. Da bietet es sich für das FBI doch an, sich einmal anzusehen, wer da welche Adressanfragen stellt. Schließlich erfolgt die Anfrage nach der IP-Adresse* ***nicht anonym****. Nein, die IP-Adresse des anfragenden Rechners wird mitgesandt. Ein Schelm, wer böses dabei denkt …*]

Wenn diese Server vom Netz gehen, dann kommt es dazu, dass befallene Rechner einen Eintrag in den Netzwerkeinstellungen haben (*DNS-Server*), der nicht mehr existiert. Das heißt im Klartext, dass Namen (Adressen wie www.spiegel.de) nicht

mehr aufgelöst werden können. Es erscheinen dann Meldungen wie: „Diese Seite kann nicht angezeigt werden.“

Abhilfe *

Abhilfe gibt es schon lange. Am 11. September 2011 stellte das FBI ein PDF Dokument zur Verfügung, in dem wirklich gut beschrieben ist, wie man eine Infektion feststellt.

Das Dokument finden Sie hier:
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

Medienwirksam haben jetzt das BSI, BKA und Telekom eine Seite ins Netz gestellt, mit der Sie sehr einfach einen Befall Ihres Rechners prüfen können. Besuchen Sie einfach die Seite www.dns-ok.de und Ihnen wird angezeigt, ob Ihr Rechner befallen ist.

Auf der Seite https://www.botfrei.de/decleaner.html finden Sie ein Werkzeug zum Beseitigen des Schadprogramms. Wenn man die Hinweise liest, scheint der Eingriff durch den Cleaner nicht ganz ungefährlich zu sein. Zudem deuten die Hinweise auch darauf hin, dass aktuelle Virenscanner den Schädling schon lange kennen. Wenn Sie allerdings auf www.dns-ok.de eine Warnmeldung erhalten, dann geht es wohl nicht anders…