Anonymisierungsdienst von Cyberkriminellen missbraucht

Tor-Netzwerk wird zur Steuerung gekaperter Rechner eingesetzt.

(ddp direct) Der Wunsch, keine digitalen Fingerabdrücke im Internet zu hinterlassen, ist vor allem für Onlinekriminelle von existenzieller Bedeutung. Nach Analysen der G Data SecurityLabs ist es Malware-Autoren gelungen, das weltweit umspannende Tor-Netzwerk für ihre Zwecke einzusetzen. Bei den Angreifern handelt es sich um Botnetz-Betreiber (Botmaster), die den Anonymisierungsdienst zur Verschleierung der Kommunikation zwischen den Steuerungsservern (C&C-Server) und den infizierten Computern missbrauchen. Durch diese neue Taktik wird es nach Einschätzung von G Data zukünftig deutlich schwerer sein, C&C-Server zu lokalisieren und unschädlich zu machen.

Wie nutzen die Täter das Tor-Netzwerk?

Die Steuerung der gekaperten Rechner (Zombies) erfolgte bisher über eine direkte Verbindung zu einem Command & Control Server (C& C-Server) oder durch eine P2P-Kommunikationsstruktur. Die C&C-Server sind mit Schaltzentralen zu vergleichen, mit denen die Betreiber ihre Befehle an die Zombies versenden. Hierüber ist es möglich, beispielsweise DDoS-Angriffe oder den millionenfachen Versand von Spam-Mails zu initiieren und zu koordinieren. Die direkte Verbindung oder der Einsatz von P2P-Strukturen birgt für die Botmaster jedoch eine große Gefahr: Ermittlungsbehörden ist es immer wieder gelungen, die Standorte der C&C-Server ausfindig zu machen und diese auszuschalten. Durch den Einsatz des Tor-Netzwerkes, wird dies zukünftig aber deutlich schwerer werden.

Was ist das Tor-Netzwerk?

Tor ist ein weltweit von vielen Anwendern genutztes Netzwerk, um im Internet anonym zu surfen und so keine Spuren zu hinterlassen. Bei diesem Dienst handelt es sich nicht um einen illegalen Service. So wurde das Tor-Netzwerk u.a. von politischen Aktivisten des Arabischen Frühlings eingesetzt, um sich einem möglichen Zugriff durch die damaligen Sicherheitsbehörden zu entziehen und Webservice-Blockaden durch Regierungen zu entziehen. Die Funktionsweise von Tor ist denkbar einfach: Potentielle Anwender geben ihren Rechner als sog. Tunnel (Tor Relay) frei und werden dadurch zu einem von vielen Weiterleitungspunkte für die unterschiedliche Services des Tor-Netzwerkes.Wird beispielsweise auf dem eigenen Computer eine Internetseite im Tor-Browser aufgerufen, so geschieht die Anfrage an den Webserver nicht auf dem direkten Wege, sondern über einer der unzähligen anderen Weiterleitungspunkte des Netzwerkes. Dadurch ist es kaum möglich, die ursprüngliche IP-Adresse des Nutzers herauszubekommen.

Was ist ein Botnetz?

Als Botnetz wird ein Verbund miteinander vernetzter, infizierter Rechner bezeichnet, wobei diese Rechner unter der Kontrolle eines sogenannten Botmasters stehen. Dies passiert gemeinhin ohne das Wissen und die Zustimmung der Besitzer der einzelnen Rechner, die durch den Botmaster ferngesteuert werden können. Die infizierten Rechner bezeichnet man als Zombies.

Der Botmaster kann die unter seiner Kontrolle stehenden, gekaperten Opferrechner für eine Vielzahl unterschiedlicher Zwecke missbrauchen. Da er auf die einzelnen Rechner zugreifen kann, als säße er selbst physikalisch vor dem jeweiligen System, ist sowohl der Zugriff auf die auf den jeweiligen Systemen gespeicherten Daten als auch die unbemerkte Verwendung der Netzwerkverbindung der Rechner möglich. Botnetze werden unter anderem dafür benutzt, gezielte Überlastangriffe auf Webserver zu starten (DoS- und DDoS-Attacken) und um Spam zu versenden.

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/duj5p4

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.de/it-hightech/anonymisierungsdienst-von-cyberkriminellen-missbraucht-14157

=== Onlinekriminelle missbrauchen das Tor-Netzwerk zur Steuerung von Zombie-Rechnern. (Bild) ===

Onlinekriminelle missbrauchen das Tor-Netzwerk zur Steuerung der Zombie-Rechner.

Shortlink:
http://shortpr.com/hgeqte

Permanentlink:
http://www.themenportal.de/bilder/onlinekriminelle-missbrauchen-das-tor-netzwerk-zur-steuerung-von-zombie-rechnern

=== So machen sich die Täter die Anonymisierung des Tor-Netzwerkers zur Steuerung gekaperter Rechner zunutze. (Infografik) ===

So machen sich die Täter die Anonymisierung des Tor-Netzwerkers zur Steuerung gekaperter Rechner zunutze.

Shortlink:
http://shortpr.com/paspld

Permanentlink:
http://www.themenportal.
de/infografiken/so-machen-sich-die-taeter-die-anonymisierung-des-tor-netzwerkers-zur-steuerung-gekaperter-rechner-zunutze

=== Die Kommunikation zwischen C&C-Server und den Zombie Computern erfolgte bisher (u.a.) auf direktem Weg. (Infografik) ===

Die Kommunikation zwischen C&C-Server und den Zombie Computern erfolgte bisher (u.a.) auf direktem Weg.

Shortlink:
http://shortpr.com/ctx9m0

Permanentlink:
http://www.themenportal.
de/infografiken/die-kommunikation-zwischen-c-c-server-und-den-zombie-computern-erfolgte-bisher-u-a-auf-direktem-weg

Pressekontakt

G Data Software AG

Herr Thorsten Urbanski
Königsallee b 178
44799 Bochum

presse@gdata.de

Firmenkontakt

G Data Software AG

Herr Thorsten Urbanski
Königsallee b 178
44799 Bochum

gdata.de
presse@gdata.de

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Anlage: Bild