Bulletproof-Hoster im Visier - IT-Services für Kriminelle

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Bulletproof-Hoster stellen für Cyber-Verbrecher die nötige IT-Infrastruktur zur Verfügung - und das scheinbar legal.

Sie treten als ganz normale Internet-Service-Provider (ISPs) auf und bieten ihren Kunden die üblichen Dienste an wie Bandbreite, Verfügbarkeit, Sicherheitsfunktionen und Spam-Filter. Quasi unter dem Ladentisch verkaufen Bulletproof-Hoster aber die einschlägigen Angebote: Anonymisierungsservices, versteckte Server und qualitäts–geprüfte Schadsoftware werden zusammen mit einer gesicherten Kommunikation bereitgestellt. Kriminelle sichern sich so verschlüsselten E-Mail-Verkehr, geschlossene Nutzergruppen und Mobiltelefone für den einmaligen Gebrauch. Damit sind sie in der Lage, illegale Services aller Art im Web auszubringen. Die Server dieser Anbieter stehen oft in Osteuropa, speziell Estland, aber auch Asien oder das sonnige Kalifornien sind potenzielle Standorte.

Das Ende von McColo

Auf der diesjährigen IT-Defense in Köln widmete sich Oberstleutnant Volker Kozok, Referent beim Bundesministerium der Verteidigung, dem Bulletproof-Hosting. Die kriminellen Aktivitäten von McColo dienten ihm dabei als Beispiel.

Der US-Anbieter, der seine Dienste am 11. November 2008 einstellen musste, gehört zu den bekannteren Fällen. Um ihm das Handwerk zu legen, war eine dreijährige konzertierte Aktion verschiedener amerikanischer Behörden notwendig. Federal Trade Commission (FTC), FBI, Nasa, State Department und andere waren mit dem Fall beschäftigt. Das zeigt, wie schwierig es ist, dieser Art der Kriminalität beizukommen. Die Internet-Straftaten allein hätten für die Schließung nicht einmal ausgereicht. In den USA muss ein Service-Provider laut einer FBI-Definition mindestens 90 Prozent seiner Aktivitäten mit Bulletproof-Hosting bestreiten, damit man deshalb gegen ihn vorgehen kann. Bei McColo gab letztlich ein Verstoß gegen das Wirtschaftsrecht den Ausschlag.

Kurze Euphorie

Das Ende von McColo war zunächst ein Warnschuss für die Cyber-Mafia. Das weltweite Spam-Aufkommen ging um ein Drittel zurück. Manche Quellen sprechen sogar von bis zu zwei Dritteln. Bei den Behörden keimte Hoffnung auf. Wenn es gelänge, weitere Hoster dichtzumachen, könnte man vielleicht den gesamten Spam aus der Welt verbannen. Doch die Euphorie währte nur kurz. 3FN trat in die Fussstapfen von McColo, und laut Symantecs Spam-Report war im April 2009 das Spam-Aufkommen wieder so hoch wie vor der Schließung McColos.

McColo stellte mehrere Botnets zur Verfügung und duldete Schadsoftware auf seinen Systemen, um den digitalen Müll in Umlauf zu bringen. Dabei werden infizierte Rechner zu einem automatisierten Netz aus Zombie-Rechnern zusammengeschaltet. McColo hat schließlich sechs von dreizehn der erfolgreichsten Botnets gehostet: Conficker, Asprox, Srizibi, Torpig, Avalanche und Ghostnet.

Bulletproof-Hoster haben eine offizielle Anschrift, doch in der Regel findet man dort nur eine Briefkastenfirma. Bei McColo stießen die Ermittler beispielsweise auf nette Geschäfte und einen Friseurladen. Nichts deutete auf einen ISP hin. Der Server-Raum konnte dann aber doch ausfindig gemacht werden. Die Ausstattung war sehr professionell und keinesfalls

schäbig. Klimatisierung und Einbruchmeldeanlagen erweckten den Eindruck eines ISP am Puls der Zeit. Allerdings fanden die Ermittler Blade-Server vor, die mit Inhalten der übelsten Sorte bestückt waren: Malware, Botnetze, Kinderpornografie, manipulierte Sicherheitssoftware und Spam-Server für gefälschte Medikamente.

Gefälschte Sicherheitssoftware
Arglose Anwender fangen sich Schadcode ein, indem sie zum Beispiel auf gehackte Web-Seiten zugreifen. Dort poppt in der Regel eine Warnmeldung auf, dass der Computer gefährdet sei. Prompt bekommt man eine Software angeboten, die das Problem lösen könne. "Jene Software funktioniert tatsächlich und macht 99 Prozent der Malware unschädlich, nur die nicht, die vom Angreifer benutzt wird", so Kozok. Installiert man die Sicherheitssoftware, speist der Angreifer schädlichen Code ein, und man wird beispielsweise Teil eines Botnets. Außerdem können auf diesem Weg Passwörter und Kreditkartennummern abgegriffen werden. Pikanterweise kostet die Software oft auch noch Geld, weil das für den Nutzer vertrauenswürdiger wirkt.

Botnets
Bulletproof-Hoster bieten ihren Kunden verschiedene Botnet-Services an. Dabei steuert der Bot-Controller über einen Server eine Armada von Zombie-Rechnern. Diese versenden Spam oder fahren DDoS-Attacken (Distributed Denial of Service), ohne dass der Benutzer des infizierten Rechners etwas bemerkt. Angreifer können ein Botnetz mieten und nach ihren Wünschen konfigurieren lassen. Die Netzgröße variiert dabei nach der Anzahl der PCs, nach der Art der Schadprogramme (Trojaner, Spam) und nach den Sicherheitsstandards der Opfer (Flux-/Doubleflux-Netze, Proxys, Privacy Protection). In der Praxis läuft das folgendermaßen: Wünscht ein Kunde 10.000 Rechner, werden 30.000 angeboten, um mögliche Downtimes auszugleichen. "Preislich bewegt sich der Rahmen um 1500 Dollar für eine Stunde Botnet zur Miete", sagt Kozok. Bei DoS/DDoS-Angriffen ist in der Regel nur eine zeitlich begrenzte Nutzung vorgesehen. Schließlich soll die Attacke beendet sein, bevor sich Ermittlungsbehörden einschalten oder die Medien davon Wind bekommen.

Kinderpornografie
Reguläre Internet-Dienstanbieter sind per Gesetz dazu verpflichtet, keine kinderpornografischen Inhalte zuzulassen. Oft wissen sie aber gar nicht, dass sie Kinderpornografie hosten. Das riesige Datenaufkommen und die Tricks der Kriminellen machen es schwer, derartige Inhalte zu lokalisieren. Diese sind in der Regel nur über eine genaue URL-Eingabe abrufbar. Gefasst werden Täter nur, wenn so eine URL auffliegt. Dann lassen sich sämtliche Zugriffe zurückverfolgen. Bulletproof-Hoster scheren sich nicht darum, was ihre Kunden hosten. Die Nutzungs–bedingungen sind so formuliert, dass es möglich ist, Spam oder Kinder–pornografie zu verteilen, Phishing-Attacken zu lancieren oder Cyber-Verbrechen zu begehen. Dazu kommen Mechanismen, die verhindern, dass Ermittlungsbehörden zugreifen können. Server für Bulletproof-Hosting sind über den ganzen Erdball verteilt. Bis dato gibt es international noch keine einheitlichen gesetzlichen Regeln, was den Umgang mit kinderpornografischen Inhalten anbelangt.

Pharmazie - gefälschte Medikamente
Ein weiteres blühendes Geschäftsfeld der Internet-Kriminalität betrifft Pharmazeutika. Auch hier hatte McColo Web-Services für illegale Anbieter im Angebot. Diese verkauften Viagra und gefälschte Medikamente. Wer auf ein Viagra-Angebot via Spam-Mail hereinfiel, bekam bald Post aus Indien. Die Tabletten kamen ohne Beipackzettel in Folie eingehüllt. Mit etwas Glück enthielten sie nur unschädliche Substanzen aus wirkungs–

losen Pulvern. Im Fall von gefälschten Medikamenten wiegt der Fall schwerer, denn diese können Leben und Gesundheit gefährden, wenn die versprochene Wirkung ausbleibt.

Herausforderungen und Maßnahmen

Spam, Phishing und Geldwäsche - die Liste der von Bulletproof-Hostern angebotenen Services ist lang. Die Service-Provider der "dunklen Seite" schaffen es, ihre Dienste ganz legal unter das Volk zu bringen. Fragt man sich, wie sich ein derartiges Geschäftsmodell durchsetzen konnte, ist die Antwort simpel. Organisierte Kriminalität verspricht hohe Gewinn–spannen. Diese werden von Bulletproof-Hostern postwendend in eine "sichere" IT-Infrastruktur gesteckt. Damit können sie ihren kriminellen Kunden eine Technik zur Verfügung stellen, die sich von derjenigen normaler ISPs nicht unterscheidet, außer dass sie wesentlich mehr Sicherheits-Features für Kunden bietet. Wird ein Bulletproof-Hoster geschlossen, tritt der nächste in seine Fußstapfen. Das Spam-Volumen übersteigt immer noch bei weitem das aller regulären E-Mails.

Echte Sicherheit im Internet kann nicht von Unternehmen garantiert werden, meint Kozok: "Sie ist als nationale beziehungsweise internationale Aufgabe zu begreifen. Industrie, Universitäten und Ermittlungsbehörden müssen zusammenarbeiten - auch länder–übergreifend", fordert der Sicherheitsexperte. "Wir müssen die Strukturen der organisierten Kriminalität kennen. Dann können wir ihrer Ausbreitung entgegenwirken und die Bedrohungen für unsere IT-Strukturen bewerten."

computerwoche.de 22.03.10