Untersuchung

SOHO router exploitability analysis, malware for routers

Roger Andel (rogeraaut@gmail.com), http://sohorouter.wordpress.com

Gefoerdert durch netidee 2008 (http://de.wikipedia.org/wiki/Netidee)

Inhaltsverzeichnis

Vorgehen

Aus einem frei verfuegbaren Datenbestand der national zuordenbaren IP-Adressen wurden die ca 1.600 oesterreichischen IP-Bloecke entnommen. Von den 84 Eintraegen ueber 64k Adressen wurden alle mit mehr als 256k Adressen sowie einige kleinere Bloecke bearbeitet (insgesamt 16 Bloecke). Von den ca 11 Millionen Adressen sind dadurch etwa 3 Millionen Adressen betroffen. Leichte Abweichungen der nationalen Zuordnung im Vergleich mit anderen Quellen sind vernachlaessigbar. Einzelne Bloecke wurden nach Stichprobe als wenig ergiebig identifiziert, so ist beispielsweise ein gesamter Block offenbar nur fuer die Einwahl/Anbindung von mobilen Endgeraeten angelegt. Nachdem diese Zuordnung die Ergebnisse regional nach unten relativiert wurde darauf weiter keine Ruecksicht genommen - ein Gesamtscan, auch weltweit, wuerde diese Bloecke ebenfalls enthalten. Die teilweise von den tatsaechlichen Verhaeltnissen abweichenden Daten der geographischen Zuordnung beeinflussen die Aussage der Ergebnisse nicht und blieben unberuecksichtigt.

Ueber diese IP Adressen wurde ein zweistufiges Verfahren ausgefuehrt. Im ersten Schritt (SCAN) wurden mittels TCP-Scan auf jene Adressen reduziert, welche auf den Ports 80 und 8080 Services anbieten. Von diesen Systemen wurden die Resultate gezogen und nach Basic-Authentication Realms gefiltert. Die erhaltenen Realm-Bezeichnungen wurden gruppiert und fuer die weitere Betrachtung nur die Top 20 Treffer herangezogen. Gaengige Ports, die standardmaessig von einzelnen Routermodellen fuer den Fernwartungszugang verwendet werden, wie 88 oder 1080, wurden vernachlaessigt.

Die durch den ersten Schritt erhaltenen Realms wurden nach Routermodellen unterteilt. Jene Modelle, fuer die vom Hersteller Quellcode fuer die Firmware verfuegbar ist, und deren Firmware auch ueber die Remote-Administrations Anwendung geladen werden kann, wurden in einem zweiten Test (LOGIN) darauf geprueft ob mittels bekannter Standardeinstellungen Zugang gegeben ist.

Die Testserien wurden durchwegs in der Nacht abgesetzt, an den untersuchten Systemen wurden keinerlei Veraenderungen der Software oder von Einstellungen vorgenommen. Abgesehen von standardisierten Antworten der getesteten Geraete unmittelbar nach Anmeldung wurden keinerlei anschlussspezifische Daten entnommen, aufgezeichnet oder ausgewertet. Saemtliche Detailaufzeichnungen sind zu reinen Auswertungszwecken verfuegbar, wurden vollstaendig einer Versionskontrolle unterworfen, und werden nicht veroeffentlicht. Saemtliche Modifikationsprozesse fanden auf Laborgeraeten statt, welche in einem abgetrennten Netzwerk installiert waren. Die fuer die Testserien eingesetzte Software ist oeffentlich zugaenglich, neu erstellte Software ist publiziert und frei.

Die beiden Testvorgaenge fanden verschachtelt und zeitlich versetzt statt, wobei zwei Ergebnisschnitte vorliegen: MSRMT-1, MSRMT-2. Die Kennzahlen aus MSRMT-1 wurden fuer Auswahl zusaetzlicher manueller Erkundungen herangezogen. Zusaetzlich wurden geringfuegige Adressbereiche mit einer speziellen Realm-Suchmaschine sowie mittels Suche nach bestimmten Mustern via Google, Forenspam, Wikispam und Stichproben aus Blacklists herangezogen und die Trefferproportionen mit kleinen Stichproben von LOGIN-Tests verglichen, um einerseits das Kosten-Nutzenverhaeltnis des Scan Aufwandes festzustellen, andererseits um eventuelle Spuren von derzeit in Missbrauch stehenden Routern zu eruieren. Der geringe Anteil der Messergebnisse an den Gesamtzahlen wurde vernachlaessigt.

Messungen und Ergebnisrechnung

Aufgrund der demographischen Aehnlichkeiten von Oesterreich, Deutschland und Schweiz wurden die oesterreichischen Ergebnisse auf schaetzbare Verhaeltnisse im deutschsprachigen Raum extrapoliert. In einer zusaetzlichen Hochrechnung wurden die Resultate auf das gesamte Internet angewandt, wobei die damit erhaeltlichen Dimensionen natuerlich mit Einschraenkungen zu interpretieren sind. Als weiterer Umstand ist vorauszusetzen, dass grosse IP-Adressbloecke nicht notwendigerweise mit hoher Systemdichte korrelieren muessen, diese Einschraenkung aufgrund groesserer leerer Adresssegmente jedoch die Ergebnisse eher nach unten relativiert und deshalb vernachlaessigt wurde.

Das Verhaeltnis D/A/CH nach Adressumfang betraegt in etwa 10/1/2, fuer eine Extrapolation von oesterreichischen Ergebnisse auf den deutschsprachigen Raum wird somit ein Faktor von 13 angesetzt. Dies entspricht auch grob dem Bevoelkerungsverhaeltnis.

		Factor
DE	109,859,561	
AT	11,156,240	
Factor	9.8473644346	10
CH	21,258,470	
AT	11,156,240	
Factor	1.9055228285	2
Factor D/A/CH → AT*13		13

Von den oesterreichischen Adressen wurden insgesamt ca 1/3 untersucht.

Processing AT	
Scanned	3,150,593
Unscanned	8,009,742
Sum	11,160,335
Scanned AT / Unscanned AT : s/u	0.39
Extrapolation Full Scan AT: u/s	2.54
Stretch = Extrapolation * Factor D/A/CH	33.05

Das Verhaeltnis nach IP-Adressraum zwischen AT, D/A/CH und WORLD. Beim weltweiten Adressraum wurden jene Laender abgeschnitten, deren Adressraum geringer als 1 Million ist.

Sum World	3,184,381,797	
Sum > 1m	3,160,249,441	
Factor rel AT		283.27
Factor >1m rel D/A/CH		21.79

Die Messung ergab ca 700 offene Router bei ca 6500 Systemen, fuer die eine Anmeldung erforderlich war. In einzelnen Faellen, bzw bestimmten Routertypen ist mit Standardeinstellungen keine Anmeldung erforderlich. Nachdem dies vor allem sehr alte Modelle betrifft, fuer die auch nur eine eingeschraenkte Verwertbarkeit besteht, wurden diese Systeme nicht weiter betrachtet.

Auf den deutschsprachigen Raum bezogen kann von ca 220.000 Systemen ausgegangen werden, fuer welche eine Anmeldung erforderlich waere, wovon ca 23.000 Router mit Standardeinstellung betrieben werden.

Ipscan-alive ports 80,8080 MSRMNT 2	34579		
Realms (without unprotected systems)	6585		not all realms are routers, but some are even unprotected
Default Account ACK	842		
Default User ACK only	144		(separate DI-524 check)
Default Admin ACK	698		Open Routers Default Admin D/A/CH found
Realms*Stretch	217,633.30		
Admin*Stretch	23,068.80		Open Routers Default Admin D/A/CH expected

Im ersten Messungsschnitt wurde das Verhaeltnis der Gesamtzahlen zu 'low hanging fruit' ermittelt. Es ist erkennbar, dass etwas mehr als die Haelfte der erreichbaren Systeme auf die top 20 Routermodelle entfaellt, wovon wiederum circa 1/3 jene Modelle sehr leicht von aussen modifizierbar sind. In Summe kann davon ausgegangen werden, dass circa 1/5 aller rueckmeldenden Router extrem gefaehrdet sind, uebernommen zu werden. Diese Systeme bieten vor allem keinen oder nur geringen Schutz gegen Brute-Force Attacken, teilweise wuerden solche Versuche nicht in einem Systemlog sichtbar.

Manual analytics MSRMNT 1 (slightly less data)			
complete realms	5,184.00		
Top-20	2,837.00		
Factor	0.5472608025	0.5	½ of router models are mainstream models
Difficult Realms	2,093.00		
Easy Realms	744.00		
Factor	0.3554706163		1/3 of router models with easy to build custom firmware
Weight Top20: Realms/Easy	0.1945351348	0.2	1/5 of open routers are easy to take, modify firmware

Eine Einteilung von erreichten Systemen nach Realm zeigt, dass auf die Top 20 von ca 1100 verschiedenen Rueckmeldungstexten etwa 50% der Einheiten entfallen, und diese als Mainstream-Modelle anzusehen sind. Der folgende Datenblock zeigt die Verteilung und das Verhaeltniss zwischen nachweislich kontrollierbaren Systemen und jenen, fuer die eine Uebernahme mit groesseren Komplikationen verbunden ist. Die Moeglichkeit, eine open-source Firmware aufzubringen, wird dabei ausdruecklich nicht beruecksichtigt.

```
[Liste mit ca 1100 Eintraegen, davon ein grosser Block mit SpeedTouch-MAC
Signatur]
```

		easy	difficult	Top 20
Total Result	5184	744	2093	2837
dreambox	599		599	599
WRT54GL	288		288	288
Thomson	282		282	282
Broadband Router	221		221	221
WGR614v7	188	188		188
NETGEAR WGR614v9	162	162		162
SpeedTouch	153		153	153
Login to the Router Web Configurator	151		151	151
WRT54G	125		125	125
WGR614v6	102	102		102
RP614v4	101	101		101
WGT624	70	70		70
NETGEAR WNDR3700	68	68		68
level_15_access	55		55	55
DI-524	53	53		53
WL-5460AP v2	49		49	49
WPN824v2	47		47	47
WRT54GS	47		47	47
Linksys BEFSR41	40		40	40
DI-804HV	36		36	36

Hochrechnung auf den deutschsprachigen Raum und Gesamtverhaeltnis

Result Expectation D/A/CH			
Realms easy brute-forceable	43,526.66		
Easy Admin	4,613.76	0.1	1/10 of easy routers are open

Result Expectation	
Top Countries > 1m Addresses	
Realms easy brute-forceable	948,452.34
Easy Open Admin	100,534.51

Fazit

Die Untersuchung hat gezeigt, dass im deutssprachigen Raum mit etwa 4.600 Routern zu rechnen ist, welche nicht nur mit Standardeinstellungen in Betrieb sind, sondern auch zusaetzlich ueber den WAN-seitigen Zugang vollstaendig kontrolliert oder modifiziert werden koennen und fuer die eine Firmware leicht herstellbar ist. Weiters sind etwa 44.000 Systeme hochgradig gefaehrdet, nach Ueberwindung des trivialen Sicherungsmechanismus unter Fremdkontrolle zu geraten. Bei Uebertragung des Ergebnisses auf weltweite Verhaeltnisse waere mit etwa 100.000 offenen und ca 1 Mio extrem gefaehrdeten Routern zu rechnen. Mit der zusaetzlichen Schwierigkeit, fuer einzelne Routermodelle eine Firmware zu erzeugen, welche vom Aussehen nicht als speziell erkennbar waere, gelten die dreifachen Zahlen. Bei Nutzung verfuegbarer Routerfunktionen ohne Modifikation der Firmware, beispielsweise zum Scannen des LAN-Segments durch DMZ-Eintraege oder Port-Forwarding, faellt diese Schwierigkeit weg.

Diese Schaetzung verhaelt sich stimmig zu publizierten Daten, welche [psyb0t: 80k-100k] und [vxWorks: 250k / 3.1 Mrd. Addressen] Bedrohungen dokumentieren. Der zusaetzliche Aufwand, Firmware in verschiedenen Sprachen und fuer weitaus mehr Firmware-Releases fertigen zu muessen, darf dabei aber nicht ausser acht gelassen werden.

Gesondert wurde festgestellt, dass von einigen Geraetemodellen Adresslisten erheblichen Ausmasses zu einem im Verhaeltnis zu erzielbaren Verwertungsmoeglichkeiten geringfuegigen Preis online erhaeltlich sind. Einzelne Tests haben gezeigt, dass diese Daten teilweise veraltet sind und eine Datenqualitaet von ca 50% erreichen, was in Anbetracht der Datenmenge allerdings nicht generalisiert wird. Auch sind nicht fuer alle SCAN-Treffer entsprechende Daten erhaeltlich. Dennoch wuerde ein Erwerb eine wesentliche Zeit- und Aufwandsersparnis bedeuten, insofern die wesentlich groessere SCAN-Stufe uebersprungen werden koennte, und selbst mit der Haelfte von verfuegbaren Datensaetzen sehr rasch eine groessere Ausbeute an Treffern erzielbar waere.

[psyb0t] http://www.dronebl.org/blog/8

[vxWorks] http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.html

Entwicklung, technische Innovation, Lagebild

Entwicklung

Attackierbare SOHO-Router sind mehrmals ins Licht der Schlagzeilen gerueckt. Die bestdokumentierten Vorfaelle betrafen [psyb0t], [chuck-norris] als Nachweis der breiten Verletzlichkeit von Serien von Routern derselben Architektur sowie [thomson/bt-home] im Falle von modellspezifischen Fehlern. Aeltere Routermodelle sind nicht gegen jene Angriffe geschuetzt, verfuegen allerdings auch nur ueber eingeschraenkte Moeglichkeiten der Nutzung fuer Malversationszwecke. Nach Reaktionen durch die Routerhersteller hat sich die Situation nunmehr verbessert, es kommt aber immer wieder zur Entdeckung von Sicherheitsluecken. In solchen Faellen ist auf einen Schlag eine grosse Anzahl von Systemen gleicherart bedroht und fuer eine rasche und billige Behebung solcher Schwaechen fehlt die geeignete Infrastruktur. Mit dieser Untersuchung soll erhoben werden, inwiefern man von einer Verbesserung der Gesamtlage ausgehen darf.

Sicherheitsprobleme mit SOHO Routern treten in einem beobachtbar unguenstigen Feld auf:

- Automatisierte Updatemechanismen sind schlecht ausgepraegt, sowie oft abhaengig von Herstellerinfrastruktur, die 'mit der Zeit geht'. Im Regelfall laeuft ein Router still vor sich hin, die Verantwortung fuer die Aktualitaet der Firmware trifft den Kunden. Die Frequenz, in der sich ein Endbenutzer typischen Problemen ausgesetzt sieht, ist gering. Es kommt damit zu keinem Lernerfolg, der vergleichbar waere mit der Handhabe von Sicherheitsmassnahmen auf einem Homecomputer.

- Korrekturen muessten mehrheitlich von technischen Laien vorgenommen werden; diese haben oft keinerlei Problembewusstsein, und sind auch in der Regel von jenen spaerlichen Informationen abgeschnitten, welche im Bedrohungsfall von Relevanz waeren. Um die Moeglichkeiten, sich im Bedarfsfall zu informieren, ist es ebenfalls schlecht bestellt: die Herstellerinformationen betreffen Standardprobleme, Benutzerforen sind oft gerade dann schlecht betreut, wenn eine schwer diagnostizierbare Fehlfunktion eines Produktes vorliegt, und eine Unmenge von Nicht- oder bestenfalls Halbwissen verwaessert die gaengigen Kanaele, ueber welche Rat bezogen werden koennte.

- Die korrekte und sichere Einrichtung von Routern ist lange Zeit schwierig gewesen, Veraenderungen durch die Hersteller haben daran in den letzten Jahren wenig aendern koennen. Die Routermodelle sind zwar heute wesentlich besser geschuetzt, ein allgemeines Problemverstaendnis beim Einsatz darf aber nach wie vor nicht vorausgesetzt werden. Die Usability von Konfigurationswerkzeugen hat sich zwar zum Teil verbessert, der Zwang zu ingenieursmaessigem Vorgehen besteht jedoch nach wie vor und uberfordert damit die meisten.

- Der Status eines Routes ist schlecht sichtbar, viele Modelle sind auch lange nach der Modelleinfuehrung fehlerbehaftet, ein fallweiser Systemausfall wird von vielen Nutzern als Normalitaet betrachtet.

Technische Innovation

Ueber die Probleme der blossen Einrichtung hinaus kommt bei Sicherheitsfragen ein weiterer Umstand hinzu: Sicherheit ist ein Prozess, an dem ausgerechnet das am staerksten gefaehrdete Segment von Internetbenutzern am wenigsten oder ueberhaupt nicht teilnimmt. Die Annahme, dass dies mit dem typischen Verlauf der Marktdurchdringung einer Innovation gekoppelt waere liegt nahe [rogers]. Nutzniesser von Produktverbesserungen sind zwar in der Ueberzahl, der veraenderungsresistente Teil bestimmt aber mit seinem Verhalten die unveraenderliche Gesamteinschaetzung: Die Unsicherheitsaspekte des gesamten Oekosystems werden von jenen nahezu garantiert, welche nicht aus eigenen Stuecken zur Beseitigung dieses Umstandes beitragen wollen oder koennen. Stellt [rogers] einen Anteil von 16% des 'laggards' Segments fest, so deckt sich das in etwa mit den 10% der gegenstaendlichen Untersuchung, abzueglich jener, welche vielleicht aus technischen Gruenden gluecklicherweise gezwungen sein koennten, ihre Systeme zu erneuern. Um an diesem Verhaeltnis etwas zu aendern, darf nicht bei dieser Gruppe angesetzt werden: sie ist nicht in der Lage, die Verantwortung zu uebernehmen. Diese Verantwortung trifft Hersteller und Service Provider gleichermassen, auch wenn zur Zeit vielleicht noch kein deutlich profitorientiertes Ziel ausgemacht werden kann. Auch wenn der relative Anteil von voellig ungeschuetzten Systemen marginal erscheinen sollte, so ist doch das absolute Ausmass der Gefaehrdung bedenklich. Dies gilt darueberhinaus auch besonders deshalb, weil eine Schaedigung potentiell Betroffener selbst in den kleinsten Faellen nur von der Willkuer eines eventuellen Angreifers abhaengt, und im Verhaeltnis zum Aufwand eine unverhaeltnismaessige Groesse erreichen kann.

Lagebild

Die oesterreichische Versorgung der Haushalte mit PC-Computer betrug 2009 ca 70%, staerkste Bundeslaender sind hierbei Wien und Salzburg. Die Versorgung der Haushalte mit Internetanschluessen betrug 2009 ca 70%, staerkste Bundeslaender sind hierbei Wien und Oberoesterreich mit jeweils ueber 70%. Die Versorgung der Haushalte mit Breitbandinternet betrug 2009 ca. 70%, staerkste Bundeslaender sind hierbei Wien und Salzburg mit jeweils ca 60-65%. Insgesamt verfuegen 1.7 Millionen Haushalte ueber Internetzugang. In 41% Prozent der Haushalte wird ueber Internet-Services eingekauft. Von den ca 36.000 oesterreichischen Unternehmen verfuegen etwa 76% ueber einen Breitbandanschluss, welche sich zu mehr oder weniger gleichen Teilen auf DSL-Technik und andere Breitbandanschlussformen verteilen. Staerkstes Segment sind dabei die Dienstleistenden Unternehmen (23.000). Bei den Betriebsgroessen ist die Gruppe mit 10-49 Mitarbeitern am staerksten vertreten [stataus]. Es ist bei dieser Betriebsgroesse davon auszugehen, dass kein eigener Rechenzentrumsbetrieb stattfindet.

Das oesterreichisches Netz umfasst einen IP-Adressraum von ca 11 Millionen Adressen [geoip, andere].

====

[rogers] http://en.wikipedia.org/wiki/Diffusion_of_innovations

[psyb0t] http://en.wikipedia.org/wiki/Psyb0t

[thomson] http://www.gnucitizen.org/blog/default-key-algorithm-in-thomson-and-bt-home-hub-routers/

[chuck-norris] http://seclists.org/fulldisclosure/2010/Feb/387

[stataus] http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_unternehmen_e-commerce/index.html

[geoip] http://www.maxmind.com/app/country

Motivation und Moeglichkeiten

Nach der Ubernahme eines Routers ergeben sich fuer den Angreifer eine Serie von Moeglichkeiten. Diese koennen nach ihrer Skalierbarkeit unterschieden werden, woraus sich ein modulares, mehrstufiges Angriffsszenario zusammenstellen laesst. So kann die geographische Naehe eine Rolle spielen, oder auch die Einheitlichkeit von verwertbarem Datenmaterial. Auch die noetige Vorbereitungszeit fuer einen Angriff aufgrund der Komplexitaet oder des Geheimhaltungsaspekts stellt dabei eine zu beruecksichtigende Groesse dar. Grundsaetzlich kann aber gesagt werden, dass ein verfuegbarer Router das Arsenal an Angriffsvarianten deutlich vergroessert, und die Effektivitaet von ueblicherweise bereits bestehenden und gut entwickelten Schutzsystemen und deren Infrastruktur deutlich vermindern kann. Die dezentrale Natur, die schlechte Sichtbarkeit von Effekten fuer betroffene Systeme und die eingeschraenkte Funktionalitaet beziehungsweise Bedienbarkeit von Routern spielt - einmal ueberwunden - deutlich zugunsten eines Angreifers. Aus der taktisch guenstigen Position der Mitte zwischen zwei Endpunkten koennen Datenstroeme beliebig bearbeitet werden. Aus einer Verteidigungssicht stellen beispielsweise die mangelnden diagnostischen Moeglichkeiten ein Schwierigkeit dar. Ein kontrollierter Router ist vom Angreifer je nach Risikolage seines Vorhabens in Ruhe einrichtbar, die Auswahl fuer eine Wiederherstellung reduziert sich oft auf jene zwischen einem fuer analytische Zwecke ergebnislosen Globalverlust und der Aufzeichnung von Daten, aus welchen sich nur sehr schwer Muster auslesen lassen, mittels derer auf einen Verursacher geschlossen werden koennte.

MITM-Attacken

Ein ubernommener Router ist selbstverstaendlich selbst vom MITM Typ. Bei der typischen verfuegbaren Rechenleistung, der general-purpose Architektur, der ausgezeichneten Netzanbindung und der robusten Arbeitsweise eroeffnen sich zahllose Verianten fuer missbraeuchliche Zwecke. In der Handhabung aehneln Router jenen beim Einsatz von virtuellen Maschinen, in ihrer Leistungsfaehigkeit erinnern die aelteren Geraete an Grossrechnersysteme der 80er Jahre. Neuere Geraete zeigen eine Performance, welche noch vor wenigen Jahren von Desktoprechnern erbracht wurde: Sie sind einerseits nicht so hoch getaktet, andererseits aber auch nicht mit den typischen aufgeblasenen Betriebssystemen belastet. Die Aktualisierung oder Aufbringung neuer Software ist unkompliziert, die Programmierung erfolgt mittlerweile weitgehend standardisiert und aus dem Bereich der Open-Source Firmwareproduktion stehen zahlreiche Halbfertigprodukte bzw. Module zur Verfuegung, welche bereits fuer die Resourceneinschraenkungen von Embedded Systems vorbereitet sind und mit verhaeltnismaessig geringem Aufwand portierbar sind. Im Vergleich zu herkoemmlicher Malware besteht klarerweise zusaetzliche Komplexitaet aufgrund der Plattformeinschraenkungen, andere Aufwaende fallen dafuer zur Zeit noch weg. So ist es derzeit noch nicht noetig, eine Modifikation der Software kunstvoll zu verstecken - auf Routern herrscht von vornherein wenig Transparenz.

Sicherung des Routers

Um eine Entdeckung der Uebernahme zu verhindern wird eine Backdoor Loesung im Authentifizierungscode des Webservers implementiert: Die von den Benutzern administrierten Kennworte waeren davon nicht betroffen, ein Zugang zum Firmware-Update von der Aussenseite kann dadurch gewaehrleistet werden. Zur Sicherung der modifizierten Firmware kann der Auto-Update Mechanismus, welcher in manchen Routermodellen vorhanden ist, zusaetzlich kurz geschlossen werden oder nur mit Kenntnis des eingebrachten Passworts durchfuehrbar sein. Diese Vorkehrungen koennen die Wiederherstellung eines Grundzustandes deutlich erschweren, weil dem typischen

Anwender der Routeradministration eine voellig normale Oberflaeche praesentiert wird, und die administrativen Taetigkeiten zu keinen unerwarteten Reaktionen des Geraets fuehren.

Abgesehen von der Erweiterung des gaengigen Portfolios von Standardangriffen auf Endgeraete sind weitere eigenstaendige Szenarien moeglich.

Es bestehen zwei Moeglichkeiten zur Vorbereitung von MITM-Attacken mittels DNS:

- mittels Eintrag von kontrollierten DNS-Server Adressen in der Verwaltungsoberflaeche

- den Einbau eines fuer solche Zwecke konfektionierten DNS-Servers in der Firmware

Die Abhoerung von Daten

Mit dem Einbau eines Paketfilters in die Firmware wird der gesamte Netzwerkverkehr aus dem LAN-Segment sichtbar. Es bestuende die Moeglichkeit, nach Schluesselwoertern zu filtern, und in Intervallen oder bei Erreichen einer bestimmten Groesse ein Berichtspaket an ein Auswertungssystem zu uebertragen. Zweckmaessige Daten in diesem Zusammenhang waeren Aufrufe von E-Banking Websiten oder der Abruf von E-Mail. Aus dem gewonnenen Datenmaterial koennen E-Mail Accounts oder Kreditkarteninformation extrahiert werden, wenn der Datenverkehr nicht ueber eine gesicherte Verbindung stattgefunden hat. Ebenso koennen Anmeldenamen und Passworte von Teilnehmern gesammelt werden, welche fuer einen Angriff in die Tiefe des LAN Segments hilfreich sind. Der Umstand, dass Benutzer oft dieselben Kennungen fuer verschiedene Systeme verwenden, wuerde dabei ausgenuetzt.

In weiterer Folge eroeffnen sich Moeglichkeiten zur Vorbereitung von Identitaetsdiebstahl mittels individueller Auswertung des beobachtbaren Netzwerkverkehrs. Ueber ein allfaelliges Wireless-Segment wuerde beispielsweise der Datenverkehr mit Mobiltelefonen zugaenglich, deren Datenabgleichsroutinen ueber die Netzstrecke als Informationsquelle erschliessbar.

Zeitdiebstahl und Anonymisierung

Dabei werden den Routern Pakete zur Abarbeitung uebermittelt, z.B. Attacken zur Uebernahme weiterer Router mit Brute-Force Password-Guessing. Die Ruecksendung von Ergebnissen an den Nutzniesser kann dadurch verschleiert werden, indem beispielsweise ein TOR-Service eingerichtet wird, an dessen anonymen Backend eine Webapplikation zur Aufnahme der Ergebnisse laeuft. Die Einrichtung von solchen Backends ist mit uebernommenen oder erfundenen Accounts moeglich, die verfuegbare Rechnerleistung mit typischen Entwickleraccounts bei Google-AppEngine oder Heroku beliebig skalierbar. Die Abholung der gesammelten Daten zur weiteren Verwertung kann ebenfalls vollstaendig anonymisiert mittels Webabfrage erfolgen. Bandbreiten- und Latenzfragen stehen im Hintergrund, da die Datenmengen nach entsprechender Vorverdichtung klein sind.

Proxy

Soferne auf dem Router Shellcode lauffaehig ist kann ein Tunnel etabliert werden, ueber welchen die Herkunft der Datenpakete verschleiert wird. Der Tunnel kann mit netcat oder connect etabliert werden, soferne ssh zur verfuegung steht kann die Datenverbindung verschluesselt erfolgen. Wird auf dem Zielrouter kein direkter Rueckkanal fuer eventuelle Resultate verwendet und anstatt dessen an einen eingerichteten Aggregator versandt, ist eine Entdeckung mit statistischen Mitteln unwahrscheinlich - der Datenverkehr ginge sowohl von seiner Charakteristik als auch Frequenz im herkoemmlichen Netzwerkverkehr unter.

Scanner-Proxy

Am Uebergang zwischen WAN und LAN kann bei offenen Routern die Einstellung der DMZ vorgenommen werden, beziehungsweise kann Port-Forwarding eingerichtet werden. Dadurch wird es moeglich, ein eingeschraenktes Scannen des LAN Segments von aussen durchzufuehren. Die meisten Router zeigen ein Liste der momentan angebundenen Endgeraete im LAN mit den entsprechenden Netzwerkadressen in ihrer Verwaltungsoberflaeche. Die Aufbringung von herkoemmlicher PC-Malware auf gefundene Systeme ist ebenfalls auf diesem Wege moeglich.

Verteilter Datenspeicher im Netz

Einzelne Routermodelle verfuegen ueber die Moeglichkeit, das telnet-service von der LAN-Seite zu oeffnen. Bei Vorhandensein der Firmware-Quelltexte waere eine unmerkliche Modifikation denkbar, die diese Moeglichkeit auch von der WAN-Seite anbietet. Dadurch wuerde sich die potentielle Nutzungsflaeche des Routers deutlich vergroessern, beispielsweise weil tftp von aussen fernsteuerbar nutzbar wuerde - der Router kann somit als temporaerer Datenspeicher eingesetzt werden.

Eine etwas umstaendlichere Variation mit demselben Ergebnis besteht natuerlich durch Einbau einer Befehlsoberflaeche in den routereigenen Webserver, welche allerdings nur dem Angreifer zugaenglich ist.

Fuer den Datenaustausch mit dem Router ist es ohne grossen programmiertechnischen Aufwand auch denkbar, einen trivialen Key-Value Store mit Zugang ueber den Webserver in die Firmware zu integrieren. Bei Sicherung der Daten im Nonvolatile Speicher des Routers wuerde der Datenbestand auch ueber Reboots hinweg verfuegbar.

Im Zusammenspiel mit anderen Routern erhielte man eine verteilte Datenbank - ein 'Feature', welches fuer allfaellige Zwecke eine bedeutende Komplexitaetsreduktion darstellte.

Da die meisten Router uber Moeglichkeiten zur Sicherung und Wiederherstellung der Konfigurationsdaten verfuegen, welche einen Abzug des Nonvolatile Speichers oft in binaerem Datenformat erstellen, kann auf diesem Wege auch eine Sicherung der Daten ueber ein effektives Update der Firmware hinweg angedacht werden. Ebenso eignet sich dieser Weg fuer das Einsammeln von Daten auf mehreren Routern ueber die unauffaellige Standardschnittstelle: ein Web-Request.

Mischformen mit bekannten Szenarien

Bei neueren Modellen koennen ueber USB Massenspeicher verfuegbar sein, welche die Kapazitaet des Routers erheblich vergroessern. Ein Exploit in diesem Bereich fuehrt allerdings in ein Feld hoeherer Sichtbarkeit, da diese Geraete oft als Server im Netzwerk integriert sind und von Endbenutzern wie ein Netzwerklaufwerk wahrnehmbar sind.

Zusaetzliche Moeglichkeiten ergeben sich in geographischer Naehe des Routers. Ist man im Sendebereich eines Access Points, so stellt die Mitnutzung kein Problem dar. Die herkoemmlichen Bedrohungsbilder fuer offene Wireless Router bestehen, ohne dass dies zwangslaeufig wahrnehmbar waere: so ist beispielsweise die Einrichtung einer Wireless-Bridge zu einem Internet-Cafe denkbar, mit welcher der gesamte Datenverkehr aus sicherer Position aufzeichenbar ist. Aufgeklaerte Benutzer kennen diese Bedrohung und sichern sich adequat. Ob diese Sorgfalt von der Mehrheit aber auch in einem Netzwerk geuebt wird, welches als gesichert gilt, ist anzuzweifeln.

Ein Szenario

Alle kontrollierten Router werden fuer eine ungeschminkte DDoS Attacke durch Aufbringen einer geeigneten Firmware vorbereitet. Ein Rollout der Software waere innerhalb eines Tages moeglich. Fuer eine sub-1-Gbps DDoS Attacke sind weniger als 1000 infizierte Router mit einer Bandbreite von 1 Mbps noetig, die Vorbereitung einer solchen Attacke kann ohne aufwaendige CnC Infrastruktur in voelliger Anonymitaet erfolgen, ohne typische DNS Muster von statistischer Signifikanz zu hinterlassen, wenn der Router beispielsweise ueber ein eigenes Kommandointerface im Webserver verfuegt und ueber einen TOR Exitpoint mit Zieladressen versorgt wird.

Hinterlaesst die neue Firmware die Router in einem Zustand, in dem sie weder kontrollierbar noch herkoemmlich ueber das Webinterface updatebar sind, ergibt sich fuer die entsprechenden Internet Provider ein logistisches Problem. Diese Router muessen ausgetauscht oder einzeln auf Grundstellung zurueckgesetzt werden, was mit physikalischem Transport verbunden ist. Die Aufbringung einer sauberen Firmware ueber die ueblicherweise verfuegbaren Wiederherstellungsroutinen mit tftp ist wegen der Erfordernis entsprechender Infrastruktur auf der LAN-Seite des Routers nicht automatisierbar, und auch wenn entsprechendes Know How und Training dazu vorhanden sein sollte mit erheblichem Aufwand verbunden: dieser Prozess ist selbst fuer Fachleute in jedem Einzelfall immer wieder problematisch. Der Imageschaden fuer Routerhersteller und ISPs, vor allem in Anbetracht des betroffenen Personenkreises und seinem Zugang zu technischen Fragen, sowie Kundenreaktionen auf moeglicherweise mehrtaegigen Serviceausfall, sind die Folge.

Technik

Scan

Die abgelaufenen Abfragen gegen die IP-Adressen sind direkt erfolgt, mit 5-10 Abfragen pro Sekunde ist die Netzwerkbelastung minimal - d.h. man kann mit geringer bzw haushaltsueblicher Bandbreite zum Ergebnis gelangen. Die zu testenden Adressen wurden innerhalb ihres Blocks grob verwuerfelt. Netzwerktests, welche guenstigerweise mit wesentlich hoeheren Datenraten abzufuehren sind koennten bereits ueber die aus Stufe 1 'eroberten' Endpunkte geleistet werden. Nur zu Pruefzwecken wurden geringe Teile ueber gesichert anonyme Verbindung abgearbeitet. Die dadurch auftretende Latenz ist weitgehend vernachlaessigbar. Ein weiterfuehrender Scan eines LAN-Segments mittels DMZ-Eintrag wurde mit dem schwaechsten verfuegbaren Routermodell labormaessig geprueft. Es ist davon auszugehen, dass der Erfolg auf alle Router mit dieser Funktionalitaet uebertragbar ist. Ein weiterfuehrender Scan eines LAN-Segments mittels Port-Forwarding wurde mit mehreren Routermodellen mit ebensolchen Ergebnissen geprueft.

Login

Bei einzelnen Routermodellen erfolgt nach Anmeldung zur Administration eine Sperre fuer weitere Adressen. Im Falle eines Angriffs, welcher mittels TOR anonymisiert vorgenommen wuerde, kommt es dadurch nach Wechsel des TOR-Exitpoints zu einer Wartezeit, bis der Prozess fortgesetzt werden koennte. Durch geeignete Automationsschritte, welche leicht herstellbar sind, wuerde die Attacke mit zwischenzeitlichen Abmeldungen nur unwesentlich verzoegert. Vor allem aeltere Routermodelle sehen allerdings keine Abmeldefunktion vor. Die Gesamtmetrik der Messung wuerde sich dadurch allerdings nicht wesentlich verschieben.

Routerspezifische Anmerkungen

Die Firma Netgear stellt fuer die Firmware ihrer Routermodelle den Quelltext zum Download. Das erhaeltliche Paket ist nicht wie dokumentiert verwendbar, jedoch kann mit einem generellen Ueberblick ueber die Werkzeugkonfiguration zur Herstellung von angepasster Firmware eine funktionsfaehige Version erstellt werden. Die erhaeltlichen Quelltexte umfassen im allgemeinen die Vorgaengerversionen der aktuellen Firmware, welche mit den Modellen gegenwaertig ausgeliefertwird. Bei der Herstellung einer Firmware mit den erhaeltlichen Quellen wird allerdings eine Vermengung von vorgefertigten Komponenten mit GPL/open source Komponenten erzeugt. Fuer die vorgefertigten Teile, beispielsweise das System aus Webserver des Routers (httpd) sowie der konkreten Verwaltungsseiten, ist kein Quelltext verfuegbar. Die Anpassung von Firmware-Versionen an die Sprachausstattung erfolgt auf voellig undokumentierte Weise, und traegt insgesamt deutliche Spuren einer gewachsenen, vertrackten Werkzeuginfrastruktur. Ob dahinter lediglich der erreichte Fortschritt an Vereinheitlichung oder eine eventuelle Verschleierungsabsicht steht ist nicht eindeutig beantwortbar - fuer beides sind Argumente denkbar. So ist beispielsweise bei einzelnen Modellen die Moeglichkeit zum Firmware-Update in der WAN-seitigen Administrationsoberflaeche lediglich ausgeblendet, laesst sich jedoch bei gezieltem Aufruf nuetzen. Dies ist ein typischer Fall von 'Security by Obscurity', und es ist davon auszugehen, dass eine deutliche Nachvollziehbarkeit im Quelltext der Firmware vor allem wegen der Imagewirkung beim erwartbar versierten Publikum unerwuenscht gewesen ist.

Bei mindestens einem Modell eines Belkin-Routers wird zum Zweck der Passwort-Verifikation ebenjenes mit an den Webbrowser gesendet und kann im Quelltext der Verwaltungsseite ausgelesen werden. Da dieses Modell in der stattgefundenen Untersuchung nicht aufgefunden wurde, und eine Suche der Signatur mit der spezialisierten Suchmaschine http://shodanhq.com nur eine geringe Anzahl an Treffern ausweist, besteht vermutlich keine Automationswuerdigkeit hinsichtlich der Nutzung dieser Sicherheitsluecke. Bei allen Routern neueren Ursprungs ist erkennbar, dass solcherart Luecken vermieden werden. Die eingegebenen Passworte werden verschluesselt uebertragen, und koennten nur im selben Netzsegment abgehoert werden. In jenen Faellen, in denen md5 zur Anwendung kommt ist es jedoch zwischenzeitlich praktikabel geworden, mit breit verfuegbaren Mitteln eine gezielte Dekodierung zu erreichen. Unter der wesentlich schwierigeren Voraussetzung, den Netzwerkverkehr in beliebigen Netzsegmenten aufzeichnen zu koennen [bgp1], koennte eine automatisierte Entschluesselung auf skalierbare Weise erzielt werden. Obwohl in diesem Fall die Verantwortung eindeutig den Service Provider betraefe, ist auch aus diesem Grund von der Verwendung von Remote-Admin abzusehen.

Die dokumentierte Moeglichkeit bei einigen aelteren Geraeten, als Port-Forward Ziel eine externe WAN-Adresse einzutragen, ist bei Modellen neuerer Bauart generell nicht mehr vorhanden. Es bleibt allerdings anzumerken, dass eine solche Funktion mit entsprechender Firmware dann leicht einzurichten ist, wenn die Pruefung auf gueltige Innenseiten-Adresse lediglich in der Administrationsoberflaeche des Routers durch Einschraenkung der Eingabewerte vorgenommen wird.

====

[.onion] fuer die Identifikation von TOR-traffic ist, so ueberhaupt moeglich, die Kontrolle ueber eine groessere Anzahl von Teilnehmer- oder Endpunkten mindestens erforderlich.

vgl http://oreilly.com/pub/wlg/7333 (2005) und https://www.defcon.org/images/defcon-18/dc-18-presentations/D.Brown/DEFCON-18-Brown-TorCnC.pdf (2010)

[bgp1] http://www.wired.com/threatlevel/2008/08/revealed-the-in/

Anmerkungen

Sicherheitsaspekte

Die Moeglichkeit zur Administration eines Routers aus dem WAN-Segment scheint ueberholt. Die verschiedenen Modelle tragen ihre Signaturen deutlich nach aussen, wofuer es kein gutes Argument gaebe. Zwar ist auch eine voellig gleichgestaltete Anmeldelogik, falls sich Routerhersteller auf eine solche einigen koennten, keine gravierende Verkleinerung der Angriffsflaeche, aber der erforderliche zusaetzliche Verkehrsbedarf zum Zweck einer Modellidentifikation koennte fuer Monitoring-Systeme eine erkennbare Auffaelligkeit darstellen, welche heute schlicht nicht gegeben ist. Die Sinnhaftigkeit von Statusinformation vor einer Anmeldung ist fragwuerdig (dd-wrt, u.a.) Als generelles Muster fuer die Remote-Verwaltung empfiehlt sich fuer Hersteller mindestens die unumgaengliche Nutzung einer gesicherten Verbindung (https), die zwingende Vergabe von Passphrases im Zuge der Inbetriebnahme eines Modells, und die Festlegung von moeglichst defensiven Default-Werten: jede Motivation, die Inbetriebnahme auf moeglichst viele Weisen zu erleichtern, ist abzulehnen. Fuer Laien stellen diese Moeglichkeiten keine nennenswerte Verbesserung ihrer Situation dar, und geschultes Personal kommt auch ohne solche zurecht. Abgesehen von Ueberlegungen hinsichtlich privacy, welche nicht Gegenstand dieser Untersuchung sein sollen, ist es fuer Fernwartungszwecke anzuraten, diese ueber einen gesicherten Tunnel von der LAN Seite des Routers vorzunehmen, und den ueberfluessigen Zugang von Aussen voellig zu unterbinden. Fuer die Nachverfolgbarkeit von administrativen Vorgaengen koennte auch grundsaetzlich eine verschluesselte Ubertragung von Log-Eintraegen an einen Service Provider angedacht werden. Diese Eintraege waeren nur mit Kenntnis des Eigentuemers interpretierbar, und koennten fuer Beweissicherungszwecke herangezogen werden. Ein solcher Mechanismus ist auch von der Schwierigkeit der Unterscheidung von legitimen und illegitimen Netzpaketen nicht betroffen, welche zuerst geloest werden muesste, um die allgemein messbare Schwemme an Testpaketen auszuduennen, in welcher der Einzelangriff zur Zeit unkenntlich bleibt, und zumindest soweit es Endbenutzer anbelangt, vermutlich noch laenger bleiben wird . Letztlich bleibt anzumerken, dass ein bestimmter Teil der Anwender immer als in Sicherheitsfragen insofern unmuendig zu erachten sein wird, dass er zu entsprechenden Massnahmen gezwungen werden muss, und es im Interesse der Gesamtheit ist, diesen wirkungsvoll zu schuetzen. So koennte auf organisatorischem Wege, etwa durch vertragliche Regelung, Sorge getragen werden, dass kein Netzwerkverkehr von aussen initiiert oder aus bekannt verdaechtigen Endpunkten [.onion] an den Router geliefert wuerde. Dies muesste keinerlei Einschraenkung fuer Kunden darstellen, welche bewusst Risiken eingehen koennten, fuer die sie allerdings auch mit Haftungsuebergang belegbar waeren.

Kurioses

In mindestens einem Fall wurde ein Router mit dem LAN-Segment ins WAN geschaltet. Abgesehen von der Unmoeglichkeit, einen solchen Router wirkungsvoll schuetzen zu koennen, zeigt dieses Beispiel aber auch etwas anderes: Die Konfiguration auf diese Weise erfordert besonderes Geschick, und es kann angenommen werden, dass ein 'Spezialist' die Einrichtung vorgenommen hat. In weiterer Folge sind die Kunden im wesentlichen unbetreut, und der Fehler faellt auch nicht auf, solange die Netzversorgung gegeben ist. Mit einem entsprechenden Monitoring duerfte ein solcher Fall ausgeschlossen sein.

In mindestens zwei Faellen wurden Druck- bzw Kopiersysteme gefunden. Diese Systeme sind als Firewall nicht geeignet. In einem Fall handelte es sich um ein System der Marke Ricoh, welche ueber eine Art Haendler-Passwort verfuegt, das in einem Forumbeitrag weitergegeben wurde. Obwohl anzunehmen ist, dass es sich dabei um eine regionale Konvention handelt, dieses Passwort gewohnheitsmaessig nicht weiterzugeben, stellt dieses Verhalten natuerlich eine ernste Bedrohung fuer Endkunden dar.

In mindestens einem Fall war auf einem Router die DMZ mit seiner eigenen Innenadresse eingetragen, woduruch im gegebenen Fall die Firewall (stillschweigend) deaktiviert war.

Download

Sourcecode

Die fuer die Untersuchung hergestellten Softwarekomponenten sind
auf http://github.com/sohorouter verfuegbar. Fuer die Durchfuehrung von SCAN wurde Angry IP Scanner [http://www.angryip.org/w/Home] eingebunden.

Paper

Eine Zusammenfassung der Untersuchung steht
unter http://sohorouter.files.wordpress.com/2010/09/ni34009.pdf zum Download.