Empirische Untersuchung von IP-Blacklists

Christian Dietrich, Christian Rossow

Institut für Internet-Sicherheit
FH Gelsenkirchen
Neidenburger Straße 43
45877 Gelsenkirchen
dietrich@internet-sicherheit.de
rossow@internet-sicherheit.de

Abstract: Diese Arbeit präsentiert empirische Untersuchungsmethoden und Untersuchungsergebnisse von IP-Blacklists. IP-Blacklisting ist ein wichtiges Antispam-Verfahren. Die beiden Analysemethoden Inhalts- und Verhaltensanalyse wurden entwickelt und hier dargestellt. Die Inhaltsanalyse wurde auf 11 Listen, die Verhaltensanalyse auf 2 Listen angewendet. Die Ergebnisse zeigen den Umfang einer Liste, den Grad der Überschneidung zwischen 2 Listen, die regionale Ausrichtung und die Hitrate einer Liste sowie die Verteilung der gelisteten IP-Adressen nach Aktivitätszeiträumen.

1 Die Rolle von IP-Blacklisting

Schwarze Listen finden in vielen verschiedenen Bereichen Anwendung, wie etwa bei der Kreditwürdigkeit, dem Luftfahrtschutz oder im Fall von Robinsonlisten zum Schutz vor unerwünschter Werbung. Als Antispam-Mechanismus eignet sich insbesondere das sog. IP-Blacklisting. Als IP-Blacklisting bezeichnet man im Kontext der Spamabwehr das Verfahren, IP-Adressen in einer Liste zu sammeln und jeglichen E-Mail-Verkehr, der von diesen IP-Adressen eingeliefert wird, zu unterbinden.

IP-Blacklisting stellt in der Regel die erste Filterstufe von E-Mail-Servern dar. Mit Hilfe von Blacklisting filtern insbesondere große E-Mail Service Provider bereits bis zu 95% aller eingehenden Verbindungen an Mailsystemen. Bei der Auswahl, welche Blacklists zur Spamabwehr auf einem Mailsystem eingesetzt werden, verlassen sich viele IT-Entscheider auf Hörensagen oder auf ihr Gefühl. Bisher gibt es sowohl im deutschsprachigen wie auch im internationalen Raum nur eine geringe Anzahl an wissenschaftlichen Veröffentlichungen und Forschungsergebnissen zu IP-Blacklisting. Diese Umstände sind die Hauptmotivation für unsere empirische Analyse von Blacklists.

2 Analyseverfahren

Für diese Untersuchung wurden 2 Analyseverfahren entwickelt und angewendet. Zum einen ist dies die sog. Inhaltsanalyse und zum anderen die sog. Verhaltensanalyse.

Untersuchungsgegenstand der Inhaltsanalyse ist der vollständige Datenbestand einer Blacklist zu einem Zeitpunkt. Ziel der Inhaltsanalyse ist, Überschneidungen zwischen verschiedenen Blacklists oder weiteren qualifizierenden Listen zu eruieren und die Veränderung über der Zeit zu beobachten.

Im Juli 2007 wurden hierzu 9 Blacklists, eine Whitelist sowie eine sog. Bogon-Liste der Inhaltsanalyse unterzogen. Im Januar 2008 wurde erneut der Inhalt von 11 Blacklists, einer Whitelist sowie einer Bogon-Liste untersucht.

Neben der Analyse des Inhalts einer Blacklists, also der gelisteten IP-Adressen, ist das Abfrageverhalten von Interesse. Hierbei wird das Verhalten der abfragenden Hosts untersucht. Auf diese Weise kann man beispielsweise den Anteil des Inhalts einer Blacklist bestimmen, der überhaupt abgefragt wird. Darüber hinaus kann die Menge an positiven Antworten, also Treffern auf der Blacklist, in Verhältnis gesetzt werden zur gesamten Menge an Anfragen. Ferner können Entwicklungen aufgezeigt werden, wie beispielsweise der Spam-Trend oder die Veränderung der Nutzerzahl einer Blacklist. Des Weiteren können Anomalien untersucht werden.

Untersuchungsgegenstände der Verhaltensanalyse sind somit in erster Linie die Menge an abgefragten IP-Adressen einer Blacklist sowie die Menge an abfragenden IP-Adressen. In einem Zeitraum von 7 Monaten wurde das Abfrageverhalten der beiden IP-Blacklists NiX Spam und Blackholes untersucht.

3 Ergebnisse

3.1 Inhaltsanalyse

Die Inhaltsanalyse zeigt u.a. den Umfang von Blacklists. Hierbei ist insbesondere der insgesamt abgedeckte IP-Adressbereich – die sog. covered range, gemessen in Anzahl an einzelnen IP-Adressen interessant. Darüber hinaus kann der Anteil der gelisteten Adressen an der theoretischen Gesamtanzahl von IP-Adressen gemessen werden. Das theoretische Maximum der Anzahl an IPv4-Adressen liegt bei rund 4,2 Milliarden. Für die Praxis ist allerdings der Anteil der gelisteten Adressen an der praktisch nutzbaren Menge an IP-Adressen aussagekräftiger. Hierbei wird anstelle der theoretischen 4,2 Mrd. die Anzahl an advertised IP-Adressen zugrunde gelegt (Spalte: % of advert.). Die folgende Tabelle zeigt den Umfang einiger ausgewählter Blacklists.

Tab. 1: Umfang von ausgewählten Blacklists.

Name	covered range	# of entries	% of IPv4	% of advertised
pbl.spamhaus.org	400.370.466	804.462	9,3200%	22,60%
xbl.spamhaus.org	4.994.959	4.994.959	0,1163%	0,28%
NiX Spam	343.388	343.388	0,0080%	0,02%

Darüber hinaus wurde eine Vergleichstabelle angefertigt. Die Vergleichsmatrix zeigt den Anteil, der sich in zwei zu vergleichenden Blacklists überschneidet. Abbildung 1 zeigt den Anteil der Menge an IP-Adressen der Blacklist A (Zeile), der von der Blacklist B (Spalte) abgedeckt wird. Werte werden mit ansteigender Überschneidung dunkler eingefärbt, kleine Überschneidungen bleiben ungefärbt.

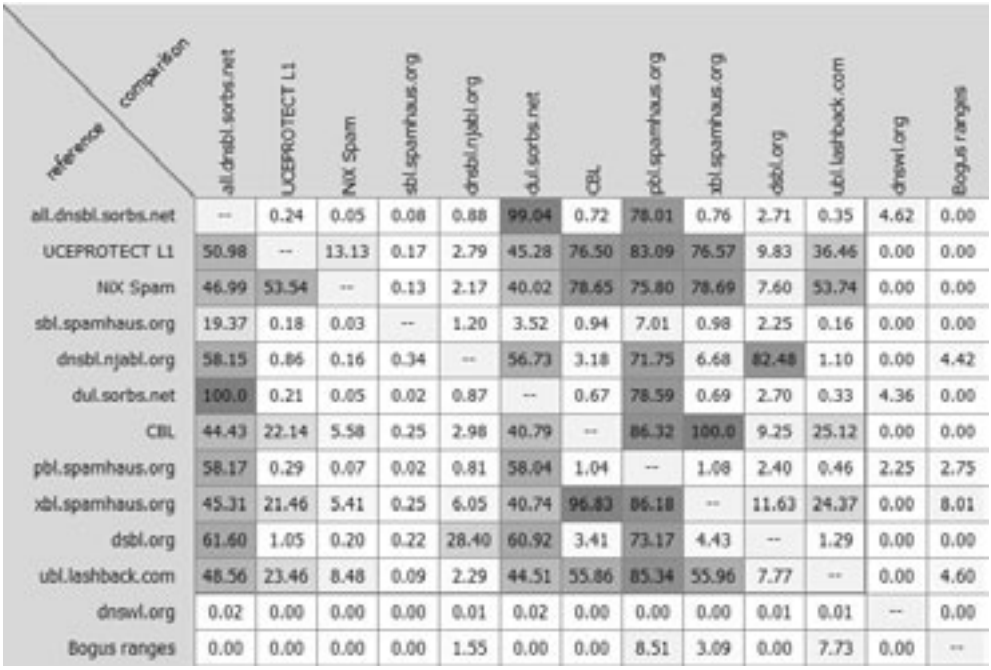
Die dunklen Bereiche in Abbildung 1 zeigen deutlich die Beziehungen der Blacklists mit einer hohen Überschneidung, wie beispielsweise die Blacklists von Spamhaus. Es ist offensichtlich, dass die XBL (xbl.spamhaus.org) die CBL komplett umfasst. Darüber hinaus ist ein Großteil der CBL (ca. 86%) in der PBL enthalten. Weitere Erkenntnisse insbesondere zur Überschneidung von Black- und Whitelists sowie Black- und Bogon-Lists enthält die Langfassung dieses Artikels.

Zwei Blacklisten mit geringen Überschneidungen zu vereinen ist wesentlich effektiver als Blacklisten zu kombinieren, die eine hohe Anzahl von gemeinsamen Listungen aufweisen. So macht es beispielsweise wenig Sinn, Spamhaus' XBL mit der CBL zu kombinieren, da letztere voll in der XBL enthalten ist. Andererseits kann die NiX Spam Liste gut in Kombination mit der Blackliste dsbl.org eingesetzt werden, da bei diesen Blacklisten kaum Überschneidungen untereinander bestehen.

3.2 Verhaltensanalyse

Im Rahmen der Verhaltensanalyse wurde zunächst die Gesamtzahl an Zugriffen pro Tag sowie die Anzahl an positiven Antworten pro Tag gemessen. Zu Beginn lag die Zahl der Requests pro Tag bei rund 5,5 Mio. Anfragen. Am Ende des Messzeitraums wurden täglich etwa 9,5 Mio. Anfragen an den messenden DNS-Server der NiX Spam Blacklist gestellt.

Zwei weitere wichtige Kennwerte des Verhaltens einer Blacklist sind zum einen die Menge an anfragenden IP-Adressen sowie zum anderen die Menge an abgefragten IP-Adressen. Betrachtet man die Menge an anfragenden IP-Adressen ergibt sich in etwa ein Bild der Nutzer einer Blacklist. Im Falle der NiX Spam sind dies pro Tag etwa 10.000 verschiedene Adressen und damit mindestens 10.000 Nutzer der Blacklist.



reference \ comparison	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	sbl.spamhaus.org	dnsbl.njabl.org	dul.sorbs.net	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dsbl.org	ubl.lashback.com	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	--	0.24	0.05	0.08	0.88	99.04	0.72	78.01	0.76	2.71	0.35	4.62	0.00
UCEPROTECT L1	50.98	--	13.13	0.17	2.79	45.28	76.50	83.09	76.57	9.83	36.46	0.00	0.00
NiX Spam	46.99	53.54	--	0.13	2.17	40.02	78.65	75.80	78.69	7.60	53.74	0.00	0.00
sbl.spamhaus.org	19.37	0.18	0.03	--	1.20	3.52	0.94	7.01	0.98	2.25	0.16	0.00	0.00
dnsbl.njabl.org	58.15	0.86	0.16	0.34	--	56.73	3.18	71.75	6.68	82.48	1.10	0.00	4.42
dul.sorbs.net	100.0	0.21	0.05	0.02	0.87	--	0.67	78.59	0.69	2.70	0.33	4.36	0.00
CBL	44.43	22.14	5.58	0.25	2.98	40.79	--	86.32	100.0	9.25	25.12	0.00	0.00
pbl.spamhaus.org	58.17	0.29	0.07	0.02	0.81	58.04	1.04	--	1.08	2.40	0.46	2.25	2.75
xbl.spamhaus.org	45.31	21.46	5.41	0.25	6.05	40.74	96.83	86.18	--	11.63	24.37	0.00	8.01
dsbl.org	61.60	1.05	0.20	0.22	28.40	60.92	3.41	73.17	4.43	--	1.29	0.00	0.00
ubl.lashback.com	48.56	23.46	8.48	0.09	2.29	44.51	55.86	85.34	55.96	7.77	--	0.00	4.60
dnswl.org	0.02	0.00	0.00	0.00	0.01	0.02	0.00	0.00	0.00	0.01	0.01	--	0.00
Bogus ranges	0.00	0.00	0.00	0.00	1.55	0.00	0.00	8.51	3.09	0.00	7.73	0.00	--

Abbildung 1: Vergleichsmatrix von IP-Blacklists. Januar 2008.

Am Heiligabend, den 24. Dezember 2007 wurden beispielsweise über den gesamten Tag hinweg bei der NiX-Spam-Blacklist 1.158.148 verschiedene IP-Adressen abgefragt. Hiervon standen 112.980 verschiedene IP-Adressen (entspricht 9,8%) auf der Blacklist. Die Liste hatte am 24. Dezember 2007 einen Umfang von rund 300.000 IP-Adressen. Dies bedeutet, dass ungefähr 37,6% der gelisteten IP-Adressen an einem Tag abgefragt wurden. Für die Blackholes lässt sich ebenfalls die Menge an abgefragten IP-Adressen ermitteln. Diese liegt pro Tag im Durchschnitt bei rund 1 Mio. verschiedenen IP-Adressen. Am 24.Dezember 2007 beispielsweise standen hiervon etwa 320.000 verschiedene IP-Adressen auf der Liste. Dies entspricht rund 32% und liegt damit deutlich höher als bei der NiX Spam (dort waren es 9,8%).

3.3 Hitrate

Ein wichtiger Indikator für die Qualität einer Blacklist ist die Hitrate bzw. Trefferquote. Die Hitrate der NiX Spam hat sich über den gesamten Messzeitraum hinweg fast verdoppelt und lag zuletzt bei deutlich über 40%. Demgegenüber lässt sich bei der Blackholes feststellen, dass die Hitrate während des gesamten Messzeitraums im Durchschnitt sinkt. Sie liegt schließlich bei rund 30%.

Eine hohe Hitrate bedeutet in erster Linie, dass viele abgefragte Adressen auch tatsächlich auf der Liste stehen. Dies ist allerdings nur in dem Fall gut, wenn zugleich der Anteil der fehlerhaft gelisteten IP-Adressen, die sog. False Positive Rate, sehr gering ist. Für die Bewertung der Qualität einer Blacklist muss daher neben der Trefferquote immer auch die False Positive Rate berücksichtigt werden.

3.4 Regionale Ausrichtung einer Blacklist

Für die NiX Spam Blacklist fällt zum Beispiel auf, dass mit Abstand die meisten Anfragen – nämlich etwa zwei Drittel – aus Deutschland kommen. Etwa ein Drittel aller Anfragen aus Deutschland wird positiv beantwortet. Nach Deutschland sind die USA das Land, das die häufigsten Anfragen erzeugt. Für Nutzer aus den USA liegt die Hitrate der NiX Spam bei lediglich rund 15%. Nutzer aus Schweden erzeugten zwar nur rund 3 Mio. Anfragen, allerdings ist die Hitrate mit rund 49% positiver Antworten außerordentlich hoch.

Bei der Blackholes zeigt sich ein anderes Bild. Auffällig ist hier, dass mit rund 36% der Großteil der Anfragen aus den USA gestellt wird. Darüber hinaus liegen die Nutzerzahlen der übrigen Länder näher beieinander als bei der NiX Spam. Dies lässt auf einen weiter gestreuten Nutzerkreis der Blackholes im Vergleich zur NiX Spam schließen. Im Mittel liegt die Hitrate bei 30%. Für Nutzer aus den USA ist die Hitrate mit 36% am höchsten. Nutzer aus der Ukraine haben innerhalb der Top10 die geringste Hitrate von 26%.

3.5 Verteilung nach Aktivitätszeiträumen

Mit einer Statistik über die Verteilung der Zeiträume, in denen IP-Adressen abgefragt wurden, kann man zeigen, dass bei der NiX Spam nur rund 8% der abgefragten IP-Adressen überhaupt über einen Zeitraum von mehr als 3 Tagen abgefragt werden. Anders ausgedrückt: 92% aller abgefragten IP-Adressen werden lediglich in einem Zeitraum von maximal 3 Tagen abgefragt. Noch deutlicher ist die Statistik über 24 Stunden: 3 von 4 abgefragten IP-Adressen werden nur in einem Zeitfenster von einem Tag abgefragt.

Fazit und Ausblick

Die Ergebnisse zeigen wichtige Kenndaten wie Umfang von IP-Blacklists und Überschneidungen untereinander. Die kurzen Aktivitätszeiten einzelner IP-Adressen von meist weniger als einem Tag beweisen, dass Blacklisten schnell auf die Kurzlebigkeit von Spammern reagieren müssen und es sich nur selten bewährt, Einträge permanent zu speichern. Auf der anderen Seite lässt die regionale Analyse Schwachstellen entdecken – wie etwa geringe Trefferquoten für Nutzer aus bestimmten Ländern. In der Anwendung kann so mit Hilfe der Ergebnisse die Spamabwehr mit IP-Blacklisting optimiert werden.