heinlein

Willkommen

Linux höchstpersönlich.

heinlein

24.05.2023 / Carsten Rosenberg, Manu Zurmühl

Spamhaus DQS und mehr

heinlein

Wer wir sind

Carsten Rosenberg
Linux-Consultant

Manu Zurmühl
Linux Consultant

Geschichte der Realtime Blocklists

- erste IP Datenbanken ab 1997
  - Vixie's Mail Abuse Prevention System (MAPS)
  - teilweise als BGP Feed oder Listen als FTP/Rsync Download
- DNSBL ab 1998
- erste Domain Blocklist (URI DNSBLs) 2004 - Surbl.org
- weitere Arten von Daten erst in den letzten Jahren
  - E-Mail Adressen
  - File Hashes etc.
  - sehr junge (neuregistrierte) Domains

RBL - Realtime Blacklists

- ggf. auch *Domain Name System Blacklist* oder *Domain Name System-based Blackhole List*
- immer öfter jetzt auch Blocklist genannt
- Idee: Prüfung der Source IP einer eingehenden E-Mail ob diese wegen Spam etc. bei einem Blocklist-Anbieter gelistet wurden
- DNS basierte Abfrage von IP Adressen
- entstanden in den 90er aus Spammer IP-Listen, die vorher via FTP o.ä. übertragen wurden
- diese wurden aber irgendwann zu groß oder änderten sich zu schnell

RBL - Realtime Blacklists

- Nutzung des DNS Systems um von der eingebauten Lastverteilung und Segmentierung profitieren zu können
- dafür musste die abzufragende IP Adresse sinnvoll in das DNS Prinzip eingebaut werden
- Implementierung: IPs werden als Sub-Sub-Sub-Sub-Domains dargestellt und kann via A Record oder TXT Record abgerufen werden
- IP Adressen werden an ihren Okteten umgedreht um eine bessere Segmentierung zu ermöglichen

RBL - Beispiel

Beispiel IP 188.37.4.25

```
# dig 25.4.37.188.zen.spamhaus.org
...

;; ANSWER SECTION:
25.4.37.188.zen.spamhaus.org. 300 IN   A   127.0.0.3
25.4.37.188.zen.spamhaus.org. 300 IN   A   127.0.0.11
25.4.37.188.zen.spamhaus.org. 300 IN   A   127.0.0.4
```

RBL - Realtime Blacklists

- Antworten sind bei A Record Queries als Localhost Adressen dargestellt
  - Sehr viele Return-Codes kodierbar
  - Antwort kann im Fehlerfall kaum schaden verursachen
- Mit unterschiedlichen Return Codes können Kategorien einer Blocklist dargestellt werden

RBL - Realtime Blacklists

- Achtung: nicht jeder Return Code zeigt einen Spammer
  - Spamhaus PBL listet z.B. End-User IP Adressen wie DSL-Anschlüsse oder LTE Netze
  - der Return Code einer Blocklist muss mit der eigenen Policy abgestimmt werden
- Achtung #2: Sofern möglich immer direkt auf die Return Codes matchen
  - https://www.golem.de/news/spamfilter-e-mail-zustellungsfehler-durch-abgelaufene-spamcop-domain-2101-153801.html
- Spamhaus hat seit einiger Zeit explizite Fehler Return Codes

127.255.255.252 → Typing error in DNSBL name
127.255.255.254 → Anonymous query through public resolver
127.255.255.255 → Excessive number of queries

RBL - Realtime Blacklists

- Schlechtes Beispiel:

```
smtpd_recipient_restrictions =
  ...
  reject_rbl_client zen.spamhaus.org
```

- Besseres Beispiel:

```
smtpd_recipient_restrictions =
  ...
  reject_rbl_client zen.spamhaus.org=127.0.0.[2..11]
```

- Wir empfehlen aber zusammen mit dem Rspamd keine RBLs mehr in Postfix zu nutzen ;)

URIBL / URI DNSBLs

- Uniform Resource Identifier BlockList
- weitere Namen: URI DNSBL, RHSBL
- gleiches Prinzip wie bei RBL
- ABER - es werden Domains abgefragt und keine IP-Adressen
- Domains werden nicht verdreht, da ihr Aufbau bereits eine Segmentierung erlaubt (example.com)

```
# dig stormibeverie.com.dbl.spamhaus.org
...
;; ANSWER SECTION:
stormibeverie.com.dbl.spamhaus.org. 300  IN A  127.0.1.2
```

Weitere Blocklists-Arten (Non-Postfix)

- Neuartige Blocklisten erlauben auch die Abfrage potenziell jeglicher Werte (gehashed)
  - E-Mail-Adressen
  - komplette URLs
  - Crypto-Wallets
  - Attachment-Hashes

The Spamhaus Project SLU

- Non-Profit Organisation
- Betreiber der offenen und freien RBLs hinter spamhaus.org
- Fair Use Policy
  - *non-commercial use* für kleine und mittlere Organisationen
  - Abfrage darf nicht von einem öffentlichen Resolver (z.B. euer ISP) kommen
  - es dürfen nicht zu viele Abfragen erfolgen (kein genaues Limit - 300k Requests?)

Spamhaus Technology Limited

- Kommerzielle Firma hinter den Spamhaus Subskriptionen
- bietet neben den freien RBLs weiter Datenbanken und Dienste an.

Spamhaus Data Feed und Data Query Service

- Data Feed - Rsync Transfer der Spamhaus RBL Daten
  - Nicht alle RBLs sind erhältlich
- Data Query Service - erweiterte DNS RBL Datenbanken

Freie und kommerzielle RBL Angebote

- spamhaus.org: DROP, EDROP, SBL, CSS, XBL, PBL, DBL
- Spamhaus DQS Extras: AuthBL, ZRD, HBL

Weitere kommerzielle Angebote

- Border Gateway Protocol (BGP) Firewall
- DNS Firewall
- Passive DNS API
- Spamhaus Intelligence API
- Domain Reputation Data available via API
- abuse.ch Data Sets (soon)

Spamhaus DQS Detail - ZEN

- Klassische IP RBL
- enthält die Kategorien SBL, CSS, XBL, PBL
- Kodierung via DNS Answer

127.0.0.2 → SBL - Direct UBE sources, spam operations & spam services
127.0.0.3 → CSS - Direct snowshoe spam sources detected via automation
127.0.0.4-7 → XBL - CBL (3rd party exploits such as proxies, trojans, etc.)
127.0.0.10-11 → PBL - End-user Non-MTA IP addresses set by ISP outbound mail policy

Spamhaus DQS Detail - AuthBL

- Liste mit IP Adressen von Brute-Force Bot-Net Servern
- Kann genutzt werden um den authentifizierten Versand von diesen IPs zu unterbinden
- Teilweise auch in der XBL enthalten

127.0.0.20 → AuthBL listed

Spamhaus DQS Detail - DBL

- Abfrage von Domains und (neu) Subdomains
  - e.g: bad-spammerdomain.new
  - e.g: hacked-wordpress.blogspot.com

127.0.1.2 | spam domain
127.0.1.4 | phish domain
127.0.1.5 | malware domain
127.0.1.6 | botnet C&C domain
127.0.1.102 | abused legit spam
127.0.1.103 | abused spammed redirector domain
127.0.1.104 | abused legit phish
127.0.1.105 | abused legit malware
127.0.1.106 | abused legit botnet C&C

Spamhaus DQS Detail - ZRD

- in den letzten 0-24h Stunden registrierte Domains
- Spammer registrieren teilweise immer neue Domains um Domain Blocklisten zu umgehen

127.0.2.2 → 0-2 hours ago
127.0.2.3 → 2-3 hours ago
127.0.2.4 → 3-4 hours ago
...

Spamhaus DQS Detail - HBL

- Effektives Matching von Reply-To Adressen, Bitcoin Erpresser-Mails und Malware Hashes
- Nur in der bezahlten Spamhaus DQS Variante enthalten

- Cryptowallets (Bitcoin, Etherium etc.)
- Malware Hashes
- Email addresses

Spamhaus BGP Firewall

- Erweiterung der DROP, EDROP und ASN Listen von Spamhaus
- Listet dedizierte und kompormitierte Botnet Controller IPs
- Wird auf Routern verwendet um den Traffic zu diesen IPs umzuleiten und damit effektiv zu verhindern

Spamhaus DNS Firewall

- RPZ Zonen oder Managed Service von Spamhaus um die DNs Auflösung bekannter Spam und Phishing Domains zu unterbinden
- Wirkt damit auch nach der Annahme einer Mail

Passive DNS API

- Rest-API um Anfragen DNS Abfragen an weltweite DNS Recursor auswerten zu können
- Nützlich für Threat-Analysen
- Zusammenhänge von IP-Netzwerken und Domains
- Markenschutz?

Spamhaus Intelligence API

- Rest-API für erweiterte Informationen über IP Adressen und Domains
- Während Blocklisten wie ZEN oder DBL nur die Listung und eine Kategorie zurückliefern, stellt SIA auch historische Informationen und Relationen zu IPs und Domains zur Verfügung
- Spamhaus nennt das eXBL, eSBL, eDBL


```
{
    "ipaddress": "179.108.187.53",
    "dataset": "XBL",
    "listed": 1663178006,
    "seen": 1663178004,
    "valid_until": 1663782804,
    "rule": "07e001d2",
    "heuristic": "SPAMBOT",
    "botname": "gamut",
    "dstip": "164.90.197.3",
    "dstport": 25,
    "protocol": "TCP",
    "srcip": "179.108.187.53",
    "srcport": 26023,
    "helo": "[179.108.187.53]",
    "subject": "Payment from your account."
    "asn": "263271",
    "cc": "BR",
    "lat": -22.9201,
    "lon": -43.0811,
  },
```

Spamhaus DQS und Rspamd

- Neben den typischen Abfragen wie der Remote IP können wir beliebige IP oder Domain Daten gegen Spamhaus prüfen
- Außerdem: E-Mail Adressen, Attachment Hashes, Crypto-Adressen
- Und: aufgelöste Domains eben wieder gegen die ZEN Liste

- Beispiel DBL:
  - Second Level Domain + Subdomain
  - DKIM Domain
  - Domains von E-Mail Adressen im Body
  - HELO Hostname
  - Reserve DNS Name (PTR)
  - Reply-To Domain
  - URLs aus dem E-Mail Body
  - URLs aus *Content* (PDF, ICS, ICA)

```
  spamhaus_dbl {
    symbol = "SH_DBL_UNKNOWN";
    rbl = "_your_code_.dbl.dq.spamhaus.,com";
    no_ip = true;
    emails_domainonly = true;
    disable_monitoring = true;
    content_urls = true;

    selector = "urls:get_host";
    checks = ['from', 'dkim', 'emails', 'helo', 'rdns', 'replyto', 'urls'];

    returncodes = {
      SH_DBL_SPAM = "127.0.1.2";
      SH_DBL_PHISH = "127.0.1.4";
      SH_DBL_MALWARE = "127.0.1.5";
      SH_DBL_BOTNET = "127.0.1.6";
      SH_DBL_ABUSE = "127.0.1.102";
      SH_DBL_ABUSE_REDIR = "127.0.1.103";
      SH_DBL_ABUSE_PHISH = "127.0.1.104";
      SH_DBL_ABUSE_MALWARE = "127.0.1.105";
      SH_DBL_ABUSE_BOTNET = "127.0.1.106";
    }
  }
```

heinlein

Fragen und Diskussionen

Linux höchstpersönlich.

Die Heinlein-Gruppe: Gemeinsam für digitale Souveränität

Heinlein Support

- Akademie: Für die oberen 10% des Wissens – unsere Linux-Schulungen für IT-Experten.
- Consulting: Security- und Strategieberatung, Projektumsetzung und umfassender Support für IT-Administratoren
- Services: SLA-Verträge, Hosting und Lizenzen als Unterstützung & Absicherung Ihrer kritischen IT-Infrastruktur

Weitere Marken

- mailbox.org: E-Mail, Online-Office, Cloud-Speicher und Videokonferenzen nach neuesten Sicherheitsstandards und mit grüner Energie.
- OpenTalk: Videocalls, wie sie sein sollten – mit unserer sicheren, benutzerfreundlichen und skalierbaren Videokonferenz für Behörden, Provider, Unternehmen und Schulen.

CompetenceCall

Das Backup für Ihre Server-Administration.

Nutzen Sie unsere SLA-Verträge und sichern Sie sich den 24/7-Support unserer Linux-Consultans.

- Kontimuierliche Absicherung mit garantierten Reaktionszeiten und festen SLAs
- Rückendeckung im Notfall: mindestens LPIC-2 zertifizierte Profis mit jahrelanger, täglicher' Admin-Erfahrung
- Projektunterstützung: maßgeschneiderte Lösungen, die Flexibilität, Sicherheit, Administrierbarkeit und Hochverfügbarkeit vereinen
- Services: Performanceanalyse, Serverhärtung, Netzwerkanalyse, Konfigurationshilfe, Datenrestaurierung

Werde Teil des Teams

- Du bist neugierig, voller Tatendrang und überzeugt von Linux, Open Source und sicherer, freier Kommunikation?

- Wir freuen uns über Unterstützung im Team:
  www.heinlein-support.de/jobs

Bleiben wir im Kontakt

Carsten Rosenberg

Tel. +49 30 40 50 51-46
c.rosenberg@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de

Bleiben wir im Kontakt

Manu Zurmühl

Tel. +49 30 40 50 51-51
m.zurmuehl@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de