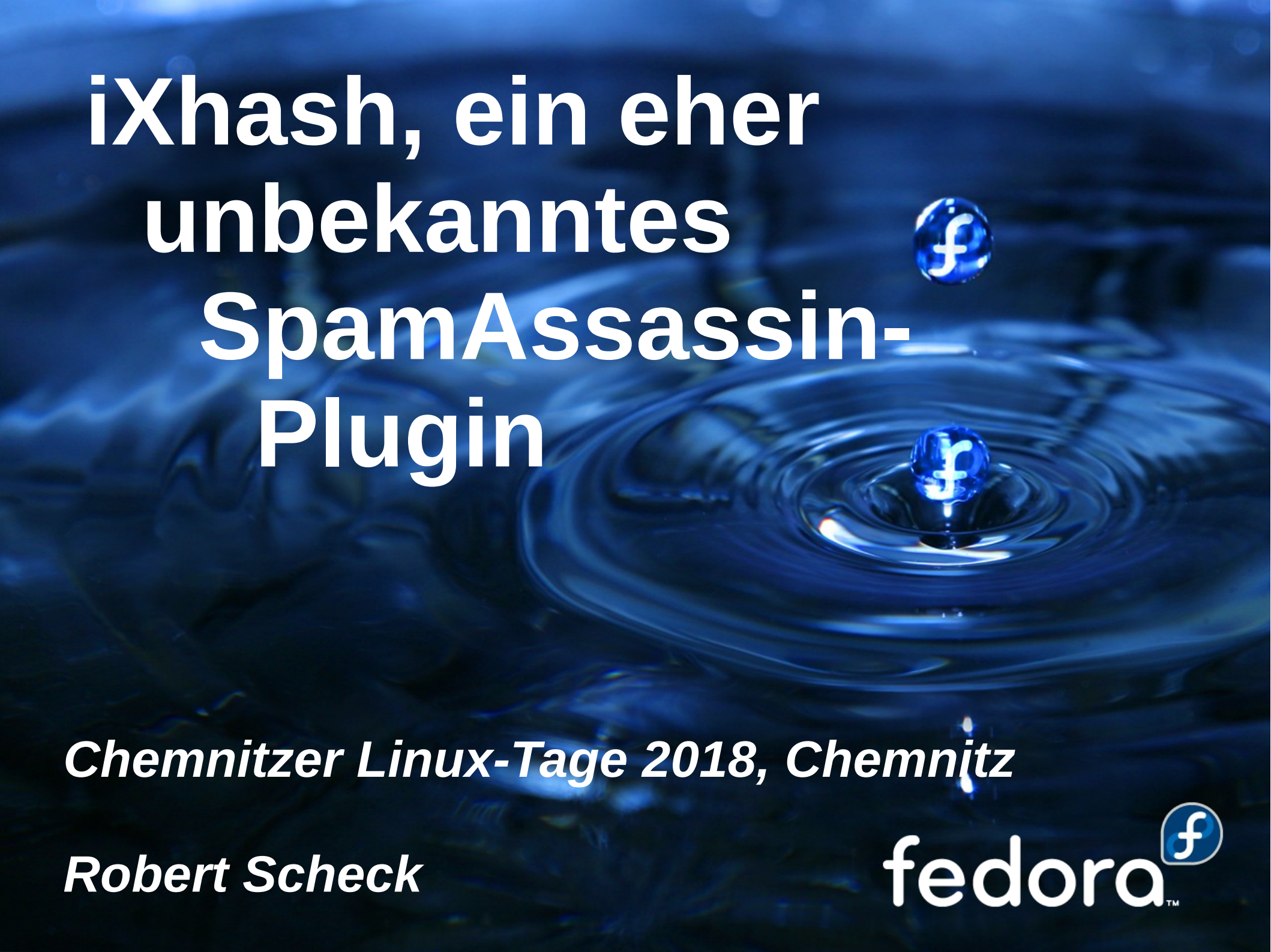

iXhash, ein eher unbekanntes SpamAssassin-Plugin

Chemnitzer Linux-Tage 2018, Chemnitz

Robert Scheck

fedora™

Robert Scheck

- Fedora Package Maintainer (etwa 120 Pakete)
- Fedora Provenpackager und Packager Sponsor
- Fedora Ambassador und Ambassador Mentor
- Open Source Contributor und Software-Entwickler

- Mail: robert@fedoraproject.org
- Web: https://fedoraproject.org/wiki/RobertScheck

SpamAssassin

- Verbreitetes Filterprogramm für Spam
- 2001: Erstes Release, Version 3.4.1 von 2015
- Einsatz auf Benutzerebene oder im Mailserver
- Vergibt nach bestimmten Regeln Punkte zur Einschätzung der Spam-Wahrscheinlichkeit
- Entwickelt in Perl
- Kombinierbar mit Prüfsummen-basierten Filtern

NiX Spam

- Bewährter Spamfilter der iX-Redaktion (Heise)
- Zwei DNS-Blacklists
  - „ix.dnsbl.manitu.net“ für IP-Adressen
  - Fuzzy Checksum für Body von E-Mails

- Mehr dazu: http://www.nixspam.org/

NiX Spam und Procmail

- Procmail-Skript von Bert Ungerer (Heise)
- 2003 vorgestellt als „nixspam.procmailrc“
- Nachfolger des NiX-Spam-Filterskripts noch heute dort im Einsatz
- Fuzzy Checksum für Body von E-Mails
- Prüfsummen als Datei und per DNS verfügbar

- Mehr dazu: http://www.nixspam.org/

iXhash

- SpamAssassin-Plugin
- Entwickelt von Dirk Bonengel
- 2007: Erste Version, Version 1.5.5 von 2009
- Keine direkte Verbindung zu iX bzw. Heise
  - Gleiche Algorithmen zur Prüfsummenermittlung

- Projektseite: http://www.ixhash.net/

iXhash2

- Plugin für SpamAssassin >= 3.2.0
- Fork von iXhash durch Henrik Krohns im Jahr 2012
- „Inoffizielle verbesserte Version von iXhash“
  - Asynchrone DNS-Abfragen
  - Performance-Optimierungen
- Vollständig kompatibel zu iXhash 1.5.5

- Download: http://mailfud.org/iXhash2/

Skript zur Demonstration…

```
#!/usr/bin/perl

use strict;
use lib '/usr/share/perl5/Mail/SpamAssassin/Plugin';
use iXhash2;

# Read e-mail from STDIN and split into header and body
my ($header, $body) = split(/\n\n/, join("", <STDIN>), 2);

print "Hash via method #1: ",
  Mail::SpamAssassin::Plugin::iXhash2::compute1sthash($body), "\n";

print "Hash via method #2: ",
  Mail::SpamAssassin::Plugin::iXhash2::compute2ndhash($body), "\n";

print "Hash via method #3: ",
  Mail::SpamAssassin::Plugin::iXhash2::compute3rdhash($body), "\n";
```

…und Action!

- Alle Prüfsummen aus Testmail generieren

```
$ cat /usr/share/doc/spamassassin-iXhash2/iXhash2.eml | demo.pl
Hash via method #1: cbdc00eaaf002aad4448b75f47a9784f
Hash via method #2: 464d43b6999bdbdf6071b8b1d3f9a525
Hash via method #3: b02ad35492c64f721e97e9a2f63b700c
$
```

- Prüfsumme bei DNS-Blacklist abfragen

```
$ host 464d43b6999bdbdf6071b8b1d3f9a525.generic.ixhash.net
464d43b6999bdbdf6071b8b1d3f9a525.generic.ixhash.net has ↵
address 127.0.0.2
$
```

Mehrere Prüfsummen?

- Logik zur Ermittlung der Prüfsummen ist vermutlich nicht der „Heilige Gral“ der Anti-Spam-Welt
- Methode #1 setzt 20 Zeichen und 2 Zeilen voraus
- Methode #2 erwartet mindestens 3 Zeichen aus `[<>()|@*'!?,]` oder die Zeichenfolge `:/`
- Methode #3 greift ab 8 Nichtleerzeichen und wenn keine Prüfsumme aus Methoden #1 oder #2
- Algorithmen selbst bitte im Perl-Code nachlesen

Aktive DNS-Blacklisten

- ix.dnsbl.manitu.net
  - Zone wird auf Basis von NiX Spam befüllt
  - Spamtraps kommen wohl auch zum Einsatz
- generic.ixhash.net
  - Zone von Dirk Bonengel gepflegt

Vorteile

- Gute Erkennung bei deutschsprachigem Spam
  - Danke, liebe iX-Redaktion!
  - Erkennungsrate abhängig von eigenem Spam
- SpamAssassin benutzt sowieso jeder – oder?
- DNS funktioniert in abgeschotteten Umgebungen
  - Pyzor: Port 24441 (UDP & TCP) ausgehend
  - Razor2: Port 2703 (TCP) ausgehend

Lohnt sich der Einsatz?

- Nur Versuch macht klug!
- Letzte 4 Wochen meines Mailservers: 15427 Mails
  - 9732 abgewiesene Spam-Mails insgesamt
  - Davon 73 Mails durch SpamAssassin
  - Davon 43 Mails nur durch iXhash
  - Aber: 29 Spam-Mails durch *alle* Filter gefallen
- Nicht jeder bekommt die gleiche Art von Spam
- Feedback an mich erwünscht!

Installation

- Fedora, Red Hat Enterprise Linux und CentOS
  - `yum install spamassassin-iXhash2`
- Andere Linux-Distributionen
  - http://mailfud.org/iXhash2/iXhash2-2.05.tar.gz herunterladen, entpacken und Anleitung folgen

Mögliche Zukunft

- Weitere DNS-Blacklists von anderen Nutzern?
- Import von iXhash2 in Versionskontrollsystem?
- Spezielle DNS-Antwort zur Signalisierung von Problemen seitens der DNS-Blacklist an Admin?
- Webbasiertes Formular zum Melden von Spam?
- …

- Weitere Ideen, Gedanken und Anregungen sind willkommen

Fragen?

fedora™

Vielen Dank!