**Carlo Schäfer**

# Die Rolle von Spam im Cybercrime

*Weltweit werden jeden Tag durchschnittlich mehr als 28 Milliarden Spam- und Phishing-Nachrichten (Wood et al., 2015, S. 12) versandt, das entsprach im September 2015 einem Anteil von 52,2 Prozent aller E-Mail-Nachrichten (Nahorney, 2015, S. 17). Davon wiederum haben etwa 76 Prozent ihren Ursprung in Botnetzen (Wood et al., 2014, S. 14). Vieles im Cybercrime beginnt mit einer einfachen E-Mail: Spam- und Phishing-Nachrichten sind ein zentrales Einfallstor für Computerkriminalität – und Botnetze die geeigneten Werkzeuge zu ihrer Verbreitung. Was also kann, was muss getan werden?*



Die Versender von Spam- und Phishing-Nachrichten verwenden unter anderem kompromittierte E-Mail-Accounts (also E-Mail-Konten, deren Zugangsdaten Unberechtigten bekannt geworden sind), um ihre unerwünschten Nachrichten massenhaft über fremde *Simple Mail Transfer Protocol* (SMTP)-Server (Klensin, 2008) zu ihren Bestimmungsorten zu verteilen. Erst dadurch wird es möglich, einen niedrigen Schwarzmarktpreis für die Versendung zu realisieren. Dieser liegt zwischen 70 und 150 (US-) Dollar (Wood et al., 2015, S. 17) für eine Spamkampagne, die an eine Million verifizierter, also auf Existenz und Erreichbarkeit geprüfter, E-Mail-Adressen gerichtet ist.

Die „Service-Leistung" besteht dabei nur in der Auslieferung von Spam an die gebuchten E-Mail-Adressen. Möchte der Auftraggeber die E-Mail-Adressen selbst kennen, um sie erneut oder für andere Zwecke zu benutzen, ist dies teurer; dennoch bezahlt man für 1.000 (zum Beispiel durch das Auslesen von kompromittierten E-Mail-Konten) gestohlene E-Mail-Adressen auch nur bis zu 10 Dollar (Wood et al., 2015, S. 17). Diese Preise zeigen, dass der eigentliche Versandvorgang fast keine Kosten verursacht. Und ein derart geringer Preis wiederum erhöht natürlich für die Auftraggeber den Anreiz zur massiven Verbreitung unerwünschter Nachrichten.

Es wird geschätzt, dass Computerkriminalität im Jahre 2014 weltweit einen volkswirtschaftlichen Gesamtschaden von circa 400 Milliarden Dollar verursacht hat (die Angaben schwanken zwischen 375 Milliarden und 575 Milliarden Dollar) – dies übersteigt die gesamte Wirtschaftsleistung mancher Staaten. Auf die USA, China und Deutschland – drei der vier größten Wirtschaftsnationen – entfielen davon zusammengerechnet etwa 200 Milliarden Dollar. Dabei sind 160 Milliarden Dollar Schaden allein durch den Diebstahl von weltweit 800 Millionen persönlicher Datensätze, wie zum Beispiel gestohlener Kreditkarteninformationen, entstanden (CSIS, 2014, S. 2 f.).

## Botnetze

Wegen der hohen Verbreitung sind Botnetze eines der größten Risiken für die Internetsicherheit. Die Gefahr von Botnetzen geht von ihrer großen Anzahl an kontrollierten Bots aus. Erst damit wird es möglich, Computer mit einer *Distributed Denial of Service* (DDoS)-Attacke anzugreifen oder eben eine große Anzahl an unerwünschten E-Mails zu versenden (Ianelli & Hackworth, 2005, S. 7). Die Anzahl bekannter Bots ist im Jahr 2014 zwar auf 1,9 Millionen gesunken, im Vergleich zu 2,3 Millionen im Jahr 2013 bzw. 3,4 Millionen im Jahr 2012. In großen Aktionen haben das FBI, das *European Cybercrime Centre* (EC3) von Europol und andere Regierungsbehörden mit Technologie-Unternehmen zusammengearbeitet, um Botnetze ausfindig zu machen und anschließend zu deaktivieren (Wood et al., 2015, S. 97). Dadurch sollte der entstandenen Gefahr Einhalt geboten werden.

### Spam und Botnetze in Symbiose

- Spam führt zur Verteilung von Bots
- Bots werden zum Versand von Spam verwendet
- Wie kann man mittels Spam Bots verteilen?
  - Ausführbare Datei im Anhang
  - Drive-by-Download bei verwundbarem Browser
  - Client-side Exploit bei verwundbarer Anwendung (z. B. Adobe Reader)
- Heute Stand der Technik: Template-based Spamming
- Neue Verbreitungswege: Twitter

*Felix Freiling, 2015*

Im August 2015 stellte dennoch fast jede zweitausendste E-Mail einen Phishing-Versuch dar, und durchschnittlich eine von 250 Nachrichten war mit Malware (Viren, Würmer, Trojaner) versehen. Täglich kamen 1,5 Millionen neue Malware-Varianten hinzu (Nahorney, 2015, S. 8–11). Die Urheber derart verseuchter Nachrichten bezwecken damit, die eigene Malware weiter zu verbreiten, um das Botnetz zu vergrößern, sowie Daten auszuspionieren. Einmal auf einem Gerät eingeschleust, kann die Malware – etwa über Keylogger, die jede Tastatureingabe protokollieren – Online-Banking-Passworte, Kreditkartennummern, Zugangsdaten für E-Mail-Accounts oder ähnliches auslesen, die dann weitergenutzt oder wiederum auf dem Schwarzmarkt verkauft werden.

## Spamming

Massive Spam-Verteilung ist deutlich anspruchsvoller als ein reiner DDoS-Angriff. Für DDoS-Attacken braucht man nur einen Internetzugang, um darüber zum Beispiel *Domain Name System* (DNS)-Abfragen oder Aufrufe von Internetseiten zu tätigen, und kommt somit mit Bordmitteln des Betriebssystems aus.

Um Spam- und Phishing-Nachrichten im großen Stile zu versenden, werden dagegen ein offener *SMTP-Relay-Server* oder eben gültige Zugangsdaten für einen bestehenden SMTP-Server benötigt. Die Verbreitung unerwünschter Nachrichten wird zusätzlich dadurch erschwert, dass aktuelle Anti-Spam-Engines fast keine Nachrichten von dynamischen IP-Adressen annehmen (wie sie Bots vorwiegend besitzen), die mittels *DNS-based*

*Blackhole List* (DNSBL) – einer Art Schwarzen Liste zur Spam-Bekämpfung – propagiert werden (The Spamhaus Project, 2015).

Offene SMTP-Server sind glücklicherweise eher selten und werden gleichfalls in DNSBL geführt, womit sie an Relevanz verlieren. Im Gegensatz dazu sind Zugriffe mit validen Zugangsdaten zu einem SMTP-Server vor DNSBL geschützt, da E-Mail-Provider ihren Kunden die Möglichkeit geben möchten, E-Mail von jedem Internetzugang aus versenden zu können.

### Phishing

Durch Phishing-Nachrichten selbst bzw. auf Internetseiten, die in den E-Mails verlinkt sind, wird versucht, an die verschiedensten Zugangsdaten von Nutzern zu gelangen – und damit Identitätsdiebstahl zu begehen. Ziele sind unter anderem Bankkonten, Konten von Bezahlsystemen wie PayPal, Zugänge zu Versandhäusern sowie Online-Auktionshäusern – oder eben auch E-Mail-Zugänge, die zur weiteren Verbreitung solcher Nachrichten missbraucht werden. Im Jahre 2013 begannen 95 Prozent (Verizon, 2015, S. 12) aller im öffentlichen Sektor erkannten Cyberspionage-Vorfälle mit einer Phishing-Nachricht – und trotz großer Bemühungen war es bisher nur möglich, diesen Anteil auf 66 Prozent im ersten Halbjahr 2015 zu senken. Dabei deuten Daten von *Verizon Enterprise Solutions* darauf hin, dass aktuell immer noch 23 Prozent aller Empfänger von Phishing-Nachrichten diese öffnen und 11 Prozent auf Anhänge klicken (Verizon, 2015, S. 12).

Aus diesen Daten lässt sich ableiten, dass fast alles Unglück mit einer E-Mail beginnt. Spam- und Phishing-Nachrichten bilden ein zentrales Einfallstor für Computerkriminalität. Darum ist ja der Markt der Anti-Spam-Engines so gut vertreten. Dass diese Produkte außerdem recht gute Erkennungsraten besitzen, um die Mailboxen der Anwender vor solchen unerwünschten Nachrichten zu schützen, gibt Anlass zur Hoffnung. Aber durch dieses Vorgehen werden nur die Symptome, leider jedoch nicht die Ursachen bzw. Quellen der Spam- und Phishing-Nachrichten bekämpft.

Die Verursacher sind eher selten und nur mit großem Aufwand ausfindig zu machen und entziehen sich selbst dann häufig einer Bestrafung. Wohingegen die Quellen schnell gefunden sind: es sind vorwiegend die unzähligen Bots. Diese Bots sind aber meist nur der Ort der Erzeugung unerwünschter Nachrichten. Für die eigentliche Versendung missbrauchen die Bots jedoch häufig andere Rechner, insbesondere auch solche, zu deren E-Mail-Systemen sie sich unberechtigt Zugang verschaffen können. Auf diese Weise kann der Spammer auch seine Identität verbergen, da die Empfänger der – gefälschten – Nachrichten nur die IP-Adressen der missbrauchten E-Mail-Systeme sehen, aber nicht die der Bots.

**Phishing und Pharming**

- Definition nach Arbeitsgruppe *Identitätsschutz im Internet* (a-i3)
- „Verfahren, bei denen ein Täter mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten zu erlangen versucht."
- Pharming: Phishing via DNS-Manipulation
  - Manipulation des lokalen DNS-Resolvers
  - Modifikation der lokalen HOSTS-Datei
  - DNS cache poisoning/pollution bei verwundbaren DNS-Servern
- Besonders tückisch, da üblicherweise DNS vertraut wird

*Felix Freiling, 2015*

### Die übliche Vorgehensweise

Ein Ziel effektiver Spam-Bekämpfung müsste es sein, kompromittierte Accounts zu erkennen, da erst diese es ermöglichen, den SMTP-Server zu missbrauchen. Durch Deaktivierung oder Blockierung dieser Accounts würde der Spam- und Phishing-Versand sofort und unmittelbar an der Quelle reduziert. E-Mail-Provider müssten nicht mehr befürchten, dass ihre eigenen Server auf verschiedenen DNSBL landen; letzteres bedeutet ja regelmäßig, dass sie von der Außenwelt faktisch abgeschnitten sind oder der reguläre ausgehende E-Mail-Verkehr maßgeblich beeinträchtigt ist.

Wenn der Fokus auf eine schnelle Erkennung von kompromittierten Accounts gelegt wird, kann die Integrität weiterer Systeme gewahrt werden, wie zum Beispiel die des Mailboxservers, der das eigentliche Konto mit allen E-Mails vorhält. Auf diesem Server befinden sich valide E-Mail-Adressen – von denen jede einzelne E-Mail mindestens je eine als Absender bzw. Empfänger enthält –, die auf dem Schwarzmarkt sehr begehrt sind. Und unglücklicherweise sind die Zugangsdaten für den Mailboxserver meistens mit denen für den SMTP-Server identisch. Die Folgen eines missbrauchten Kontos haben auch Auswirkungen auf die komplette E-Mail-Infrastruktur des E-Mail-Providers, da alle anderen Kunden in Mitleidenschaft gezogen werden, wenn die Server durch die vom Spammer erzeugten Nachrichten überlastet sind oder andere E-Mail-Provider die Annahme von Nachrichten verzögern oder sogar ablehnen.

**Carlo Schäfer**

**Carlo Schäfer** ist Diplom-Informatiker und arbeitet an der Friedrich-Schiller-Universität Jena im Bereich E-Mail und IT-Sicherheit. Zuvor war er mehrjährig Projektleiter für Spam-Abwehr im Thüringer Landesrechenzentrum.

Meistens wird die Erkennung kompromittierter SMTP-Accounts vernachlässigt. In den wenigsten Umgebungen werden ausgehende Nachrichten durch Spamfilter analysiert, da nicht klar ist, was man anschließend mit diesen Nachrichten anfängt. Zustellen möchte man den Spam nicht; aber den Absender kann oder will man gegebenenfalls auch nicht informieren, da die vorgebliche Absenderadresse gefälscht sein könnte. Vom Gesetzgeber her ist es auch nicht gestattet, E-Mails einfach zu löschen (Heckmann, 2014, Kap. 8, Rn. 207). Somit sind der Aufwand und die entstehenden Probleme der Spamkontrolle von ausgehenden Nachrichten nicht wirklich zu rechtfertigen.

Am weitläufigsten ist daher die Limitierung der Anzahl an E-Mails (in einem definierten Zeitintervall) je IP-Adresse oder besser sogar je Konto. Dadurch werden aber wiederum nur die Symptome des Spam-Versands behandelt, die Konten jedoch bleiben dagegen meistens unangetastet oder werden erst durch manuelle Kontrolle von Mitarbeitern des E-Mail-Providers gesperrt. In den wenigsten Umgebungen werden die Server rund um die Uhr von Administratoren überwacht, was zur Folge hat, dass außerhalb der Regelarbeitszeit tagsüber sowie an Wochenenden, Feiertagen oder in der Urlaubszeit diese SMTP-Server ihrem Schicksal überlassen werden. In dieser Zeit werden weitere Spam- und Phishing-Nachrichten zu Tausenden erzeugt – bis ein Mitarbeiter diesem Vorgang schließlich doch Einhalt gebietet.

### Wirkungsvolle Abhilfe

Eine schnelle Erkennung und Reaktion ist nötig, um Anomalien von missbrauchten Konten festzustellen. Dadurch wird direkt der Ursprung von Spam- und Phishing-Nachrichten bekämpft, und die Auswirkungen auf die eigene E-Mail-Infrastruktur werden auf ein Minimum reduziert.

Neue Methoden und Ansätze, welche diese Anforderung umsetzten, sind bereits veröffentlicht. Diese erkennen wesentlich schneller und zuverlässiger einen Kontenmissbrauch, als dies aktuell verbreitete Methoden ermöglichen. Dabei wird nicht der E-Mail-Inhalt analysiert; allein das Kontenverhalten verrät, ob verschiedene Bots (Schäfer, 2014) oder andere Personen (Schäfer, 2015) das Konto missbrauchen. In manchen Umgebungen ist es aus datenschutzrechtlichen Gründen nicht gestattet oder technisch auch gar nicht möglich (z. B. bei Anwendung von E-Mail-Verschlüsselung), auf den Inhalt von E-Mails zuzugreifen, sodass eine inhaltsbasierte Spam-Erkennung ohnehin nicht realisierbar wäre. Durch die angesprochene Anomalie-Erkennung ist es nun tatsächlich möglich, innerhalb von Sekunden zu reagieren und die Anzahl der Spam- und Phishing-Nachrichten auf einen Bruchteil zu reduzieren.

Die letzte Herausforderung ist nun, diese Ansätze zur Bekämpfung der lokal erzeugten Spam- und Phishing-Nachrichten so schnell wie möglich in breite Anwendung zu bringen, so dass der Computerkriminalität ein Teil der (finanziellen) Handlungsgrundlage entzogen wird. Vor einer finanziellen Belastung, etwa als Folge von kostenaufwändigen Plausibilisierungen und technischen Anforderungen, sollte man sich nicht scheuen, da diese durch die gewonnene Sicherheit zeitnah refinanziert wird.

## Referenzen


CSIS (2014). Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies, June 2014. URL: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Heckmann, D. (Hrsg.) (2014). juris PraxisKommentar Internetrecht. Telemediengesetz, E-Commerce, E-Government. 4. Aufl. Saarbrücken: juris.

Ianelli, N. & Hackworth, A. (2005). Botnets as a vehicle for online crime. Bd. 1. CERT Coordination Center. URL: https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51249.pdf

Klensin, J. (2008). Simple Mail Transfer Protocol. Network Working Group, October 2008. URL: https://tools.ietf.org/html/rfc5321 (Stand: 05.01.2016)

Nahorney, B. (2015). Symantec Intelligence Report September 2015. Symantec Corporation. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2015.en-us.pdf

Schäfer, C. (2014). Detection of Compromised E-Mail Accounts used by a Spam Botnet with Country Counting and Theoretical Geographical Travelling Speed Extracted from Metadata. In Proc. 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Nov. 2014, S. 329–334. URL: http://dx.doi.org/10.1109/ISSREW.2014.32

Schäfer, C. (2015). Detection of Compromised E-Mail Accounts used for Spamming in Correlation with Mail User Agent Access Activities Extracted from Metadata. In Proc. 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), May 2015. URL: http://dx.doi.org/10.1109/CISDA.2015.7208641

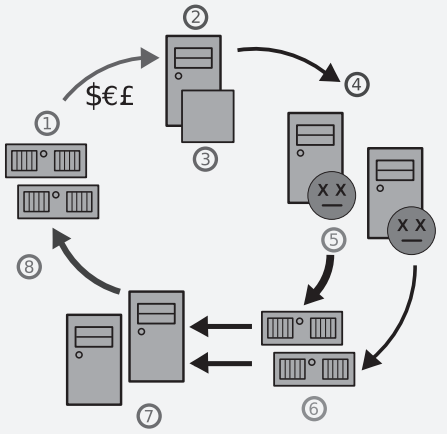
The Spamhaus Project (2015). The Policy Block List. The Spamhaus Project Lt. URL: https://www.spamhaus.org/pbl/ (Stand: 05.01.2016)

Verizon (2015). 2015 Data Breach Investigations Report. Verizon Enterprise Solutions. URL: http://www.verizonenterprise.com/de/DBIR/2015/

Wood, P. et al. (2014). Internet Security Threat Report 2014. Bd. 19. Symantec Corporation. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Wood, P. et al. (2015). Internet Security Threat Report 2015. Bd. 20. Symantec Corporation. URL: https://know.elq.symantec.com/LP=1542


**Kreislauf des Spamverkehrs im Internet**




(1) Spamwebseite
(2) Spammer
(3) Spam
(4) Infizierte Computer
(5) Virus oder Trojaner
(6) E-Mail-Server
(7) Computernutzer
(8) Internetverkehr

*Fubar Obfusco & Admrboltz, CC BY-SA 2.5*