Rustock: Ein Jahr danach

14.03.2012, 14:25 | IT, New Media & Software

Pressemitteilung von: *eleven GmbH*
Presseagentur: *consense communications gmbh*

Quelle: eleven Research

Spam-Aufkommen auf Mehrjahrestief – Deutliches Wachstum bei Malware-E-Mails – Phishing-Aufkommen mehr als verdoppelt – Neue Botnet-Infrastrukturen im Aufbau

Berlin, 14. März 2012 – Am 16. März des vergangenen Jahres wurde das Rustock-Botnet abgeschaltet. Es war für einen Großteil des weltweit versendeten Pharma-Spams verantwortlich und steuerte hauptsächlich Bots in Westeuropa und den USA. Als Folge brach das Spam-Aufkommen innerhalb von 24 Stunden um mehr als 60 Prozent ein. Ein Jahr später hat das Research-Team von eleven, führender deutscher E-Mail-Sicherheitsanbieter, die Folgen der Rustock-Abschaltung analysiert und die wichtigsten Auswirkungen zusammengestellt.

Spam-, Malware- und Phishing-Aufkommen
Das Spam-Aufkommen lag im Februar 2012 um 61,2 Prozent unter dem Wert des gleichen Vorjahresmonats und damit auf dem Niveau unmittelbar nach der Rustock-Abschaltung. Im vierten Quartal 2011 war das Spam-Volumen zwischenzeitlich wieder gestiegen, nur um anschließend erneut einzubrechen. Dagegen hat die Anzahl gefährlicher E-Mail-Nachrichten deutlich zugelegt. Malware-E-Mails stiegen seit Februar 2011 um 50,5 Prozent, Virenausbrüche sogar um mehr als das Doppelte (107,0 Prozent). Den größten Sprung machten Phishing-E-Mails: Zwischen Februar 2011 und Februar 2012 wuchs ihre Zahl um 145,0 Prozent. (siehe Bild)

Die fünf wichtigsten Spam-Trends seit Rustock
1. Themenwechsel beim Spam
Rustock war weltweit die Hauptquelle für Pharma-Spam. In der Folge verlor dieser seine Stellung als wichtigstes Spam-Thema an Werbung für Online-Casinos. Seit Beginn des Jahres 2012 nimmt der Anteil von Viagra & Co. wieder zu , während die großen Casino-Wellen ausbleiben. Im Februar 2012 lag Pharma-Spam wieder auf Platz 1 mit einem Anteil von 26,9 Prozent am gesamten Spam-Aufkommen, gefolgt von Casino-Spam mit 14,4 Prozent.

2. Neue Spitzenreiter beim Spam-Versand
Einen Wechsel gab es auch bei den Herkunftsländern von Spam-E-Mails. Vor der Rustock-Abschaltung waren die USA unangefochtener Spitzenreiter im Spam-Versand, weitere westliche Industrienationen, darunter Deutschland, befanden sich in den Top 10. Deren Anteil ist deutlich zurück gegangen, stattdessen dominieren heute Schwellenländer aus Asien und Osteuropa den Spam-Versand. Spitzenreiter ist seit einigen Monaten Indien (9,5 Prozent im Februar 2012).

3. Aufbau neuer Botnet-Infrastrukturen
Seit Anfang 2012 beobachtet das eleven Research-Team erneute Verschiebungen bei Spam-Quellen und -Themen. So hat Pharma-Spam seine Position als wichtigstes Spam-Thema zurückerobert und auch der langjährige Spam-Weltmeister USA befindet sich wieder in der Spitzengruppe: Im Februar lagen die USA bei den Spam-Versendern hinter Indien und Russland mit einem Anteil von 6,9 Prozent auf Platz 3. Dies ist ein klares Indiz, dass derzeit massiv neue Botnet-Infrastrukturen aufgebaut werden, welche die durch die Abschaltung von Rustock und anderen Botnets im Jahr 2011 verlorenen ersetzen sollen. Ob es sich dabei um neue Botnets handelt oder um die Wiederbelebung alter Netze, ist derzeit noch unklar. (siehe Bild)

4. Phishing
„Gewinner" der Rustock-Abschaltung waren die Phisher. Nicht nur quantitativ legten sie zu – auch die Qualität ist spürbar gestiegen: Wichtigster Trend ist eine zunehmende Regionalisierung, bei der lokale Unternehmen als vermeintliche Absender genutzt werden und die E-Mails in der Landessprache verfasst sind. Damit sollen die Öffnungsquoten erheblich gesteigert werden. Ein weiterer Trend ist eine größere thematische Vielfalt: Neben Bank- und Kreditkartendaten stehen heute Zugangsdaten zu sozialen Netzwerken, Webhosting-Accounts und E-Mail-Konten im Visier der Phisher.

5. Plattformübergreifende Malware-Attacken
Der erste Schritt zum Spam-Versand per Botnet ist die Infektion einer möglichst großen Anzahl von Rechnern. eleven verzeichnet zurzeit einen Anstieg so genannter Drive-by-Angriffe. Dabei wird an die E-Mail ein vermeintlich harmloses Dokument (z. B. PDF) angehängt. Dies fungiert als Tor zum Rechner und versucht Sicherheitslücken zu finden, um darüber Schadsoftware einzuschleusen. Eine andere Methode stellen Links zu infizierten Websites dar. Dabei geschieht die Infektion durch das Öffnen der Seite im Browser (Driveby-Download). Die Standard-Programme bzw. Plugins aller Betriebssysteme sind davon betroffen.

Portrait

eleven - E-Mail-Sicherheit Made in Germany
eleven ist führender E-Mail-Sicherheitsanbieter aus Deutschland und bietet mit der Technologie eXpurgate einen weltweit einzigartigen Spam-Filter und E-Mail-Kategorisierungsdienst, der zuverlässig vor Spam- und Phishing-E-Mails schützt, potenziell gefährliche E-Mails erkennt und darüber hinaus zwischen individuellen Nachrichten und jeglicher Art von Massen-E-Mails unterscheidet. Zusätzlich bietet eXpurgate umfangreiche Virenschutzoptionen und eine leistungsfähige E-Mail-Firewall.

Mehr als 45.000 Unternehmen jeder Größe nutzen den eXpurgate Dienst. Täglich werden über 1 Milliarde E-Mails von eXpurgate geprüft und kategorisiert. Zu den Kunden gehören neben Internet Service Providern und Telekommunikationsdienstleistern wie T-Online, O2, Vodafone und freenet zahlreiche namhafte Unternehmen und öffentliche Einrichtungen, darunter SAP, Air Berlin, BMW, der Bundesverband deutscher Banken, DATEV, die Freie Universität Berlin, die Landesbank Berlin, RTL, SAP, ThyssenKrupp oder die Tobit Software AG. Mehr Informationen unter http://www.eleven.de.

eleven Securityblog: http://eleven-securityblog.de
eleven auf Twitter: http://www.twitter.com/elevensecurity

News-ID: 616158 • Views: 131 (Stand: 24.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/616158/Rustock-Ein-Jahr-danach.html