Carlo Schäfer

Spam und Cybercrime im Jahre 2017

Spam wird häufig mittels kompromittierter E-Mail-Konten erzeugt, auf die zu diesem Zweck Botnetze zugreifen. Auf der FIfF-Konferenz 2017 in Jena (#FIfFKon17) wurde im Rahmen einer Demonstration im Foyer des Veranstaltungsgebäudes die Dimension solcher illegalen Zugriffe sowie deren Abwehr gezeigt.

Botnetze – die Quelle des Cybercrime

Das weltweite Malware-Aufkommen der letzten zwölf Monate entwickelte sich, wie in Abbildung 1 gezeigt, sehr dynamisch und fiel im Januar 2018 auf ein Vorkommen von einer in 786 E-Mails. Dies ähnelte dem Aufkommen von Anfang 2017, als vorübergehend die Botnetz-Aktivität des weltgrößten Spam-Botnetzes *Necurs* eingeschränkt war.

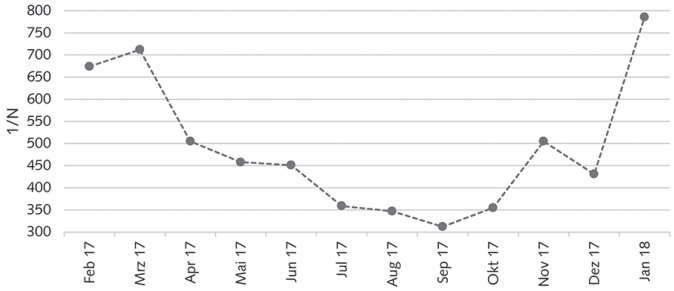

Abbildung 1: Weltweites Malware-Aufkommen 2017/2018 (Symantec 2018)

Das Aufkommen von Malware sank im Januar 2018, nachdem vermehrt Anti-Malware-Kampagnen durchgeführt wurden. Aktuell liegt die Anzahl an neuen Malware-Varianten pro Monat annähernd konstant bei 43 Millionen, das ist weniger als die Hälfte im Vergleich zu Februar 2017 mit 94 Millionen (Symantec 2018).

Im März 2017 wurde *Necurs* für Kampagnen zur Aktienmanipulation verwendet und somit weniger andere Malware wie zum Beispiel die Trojaner *Locky* und *Dridex* verbreitet. Ziel dieser Kampagnen war es, mittels *Pump-and-Dump-Nachrichten* – also Spam-Falschmeldungen – Aktienkurse künstlich in die Höhe zu treiben. Die Verantwortlichen der Kampagnen kauften zuvor Anteile dieser sogenannten Pennystocks billig auf, um sie nach dem künstlich gepushten Kursgewinn wieder zu veräußern (Baird et al. 2017).

Eingehender Spam

Im Januar 2018 waren 55 Prozent aller E-Mails Spam. Während der letzten zwölf Monate hat sich an diesem Wert nicht viel geändert. In den letzten fünf Jahren wurde auch die Anzahl der bei der Friedrich-Schiller-Universität (FSU) Jena eingehenden Spam-Nachrichten analysiert, das Ergebnis ist in Abbildung 2 zu sehen; der Trend entspricht der globalen Spam-Welle.

Ausgehender Spam

Dennoch kann man die Aktivität der einzelnen Botnetze deutlich erkennen. Bevor große Kampagnen gestartet werden, sind

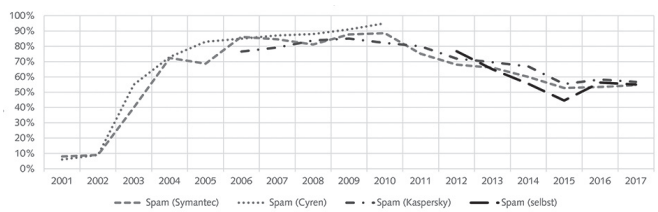

Abbildung 2: Weltweite Spam-Entwicklung der letzten 17 Jahre (Kaspersky 2018; Symantec 2017; Cyren 2018) und eigene Messungen an der FSU Jena

vermehrt Phishing-Nachrichten im Umlauf, die Zugangsdaten für E-Mail-Konten abgreifen sollen. Diese werden in den darauffolgenden Stunden beziehungsweise Wochen auf Funktionalität validiert und für die eigentlichen Kampagnen verwendet. Zugangsdaten, die einmal abgegriffen wurden, werden zyklisch – auch Jahre später – geprüft, um diese wieder zu verwenden. Deshalb sollten Passwörter niemals recycelt werden, da alte Zugangsdaten mit dazugehörigen Passwörtern nie in Vergessenheit geraten. Ein Botnetz verwendet anschließend diese kompromittierten Konten, um die eigentlichen Spam-Kampagnen durchzuführen. Im August 2017 wurde zum Beispiel das Botnetz *Onliner* identifiziert. Es verfügte zu diesem Zeitpunkt über 711 Millionen E-Mail-Adressen sowie rund 80 Millionen Zugangsdaten für E-Mail-Server, um über diese vertrauenswürdigen SMTP-Server Spam zu versenden (Westernhagen 2017). Dieser Missbrauch (Schäfer 2016b) und mögliche Gegenmaßnahmen (Schäfer 2014, 2015, 2017) wurden in der FIfF-Kommunikation 4/2015 im Beitrag *Die Rolle von Spam im Cybercrime* genauer betrachtet (Schäfer 2016a).

#FIfFKon17

Während der #FIfFKon17 wurde gezeigt, wie kompromittierte Konten missbraucht werden, um unerwünschte Nachrichten zu versenden. Um dem entgegenzuwirken, analysiert ein selbst entwickeltes System in Echtzeit automatisiert die entstehenden Metadaten, wodurch die missbrauchten Konten identifiziert werden können. Dieses Vorgehen sorgte für großes Interesse unter den Besuchern der Vorführung, vor allem, da sich lokal erzeugter ausgehender Spam komplett vermeiden lässt. Die eigene E-Mail-Reputation ist somit nicht mehr gefährdet, wodurch das Blacklisting der eigenen IP-Adressen verhindert werden kann. Erst das ermöglicht eine funktionierende Kommunikation mit den Empfängern – andernfalls gleicht dies einer sozialen Ausgrenzung.

Die *Necurs*-Bots, die gekaperte Konten nutzten, wurden für die Vorführung auf der #FIfFKon17 analysiert und geographisch zugeordnet. So war es möglich, während eines Zeitraums von 15

Stunden einen Missbrauch zu visualisieren. Während dieser Zeit wurden zwar alle unerwünschten Nachrichten entgegengenommen, um dem Botnetz funktionierende Konten vorzutäuschen. Diese E-Mails wurden jedoch nicht weitergeleitet, um die eigene Reputation nicht zu gefährden. Über 3.000 Bots des *Necurs*-Botnetzes versuchten, ein lokales Konto zu missbrauchen, und erzeugten in 15 Stunden mehr als 20 Millionen Spam-E-Mails.

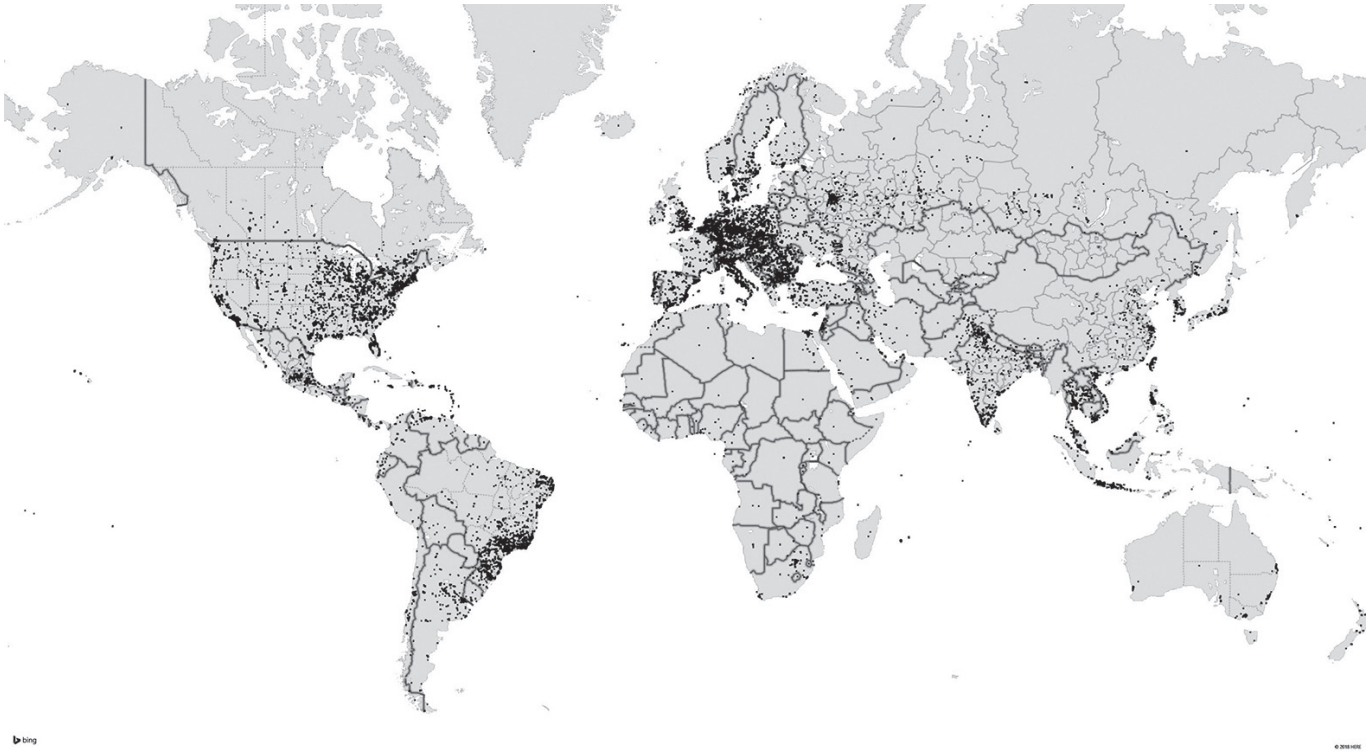

Abbildung 3: Geografische Herkunft von Angriffen des Necurs-Botnetzes innerhalb von 15 Stunden auf die E-Mail-Infrastruktur der FSU Jena

Ein solcher Missbrauch von Konten findet ständig statt und betrifft alle E-Mail-Anbieter. Des Öfteren werden auch große Provider von anderen geblockt, und deren Kunden finden einen gestörten E-Mail-Versand vor. Das lässt sich mit den richtigen Erkennungssystemen unterbinden, wie auf der #FIfFKon17 gezeigt wurde.

Referenzen

Baird S, Brumaghin E, Carter E, Schultz J (20. März 2017) Necurs diversifies its portfolio. http://blog.talosintelligence.com/2017/03/necurs-diversifies.html

Cyren Ltd. (2018) Resource center. https://www.cyren.com/resources

Kaspersky Lab (2018) Securelist Archive, Spam Statistics. https://securelist.com/all/?tag=126

Schäfer C (2014) Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata. 25th International Symposium on Software Reliability Engineering Workshops, IEEE, S 329–334. doi:10.1109/ISSREW.2014.32

Schäfer C (2015) Detection of compromised email accounts used for spamming in correlation with mail user agent access activities extracted from metadata. Symposium on Computational Intelligence for Security and Defense Applications (CISDA), IEEE. doi:10.1109/CISDA.2015.7208641

Schäfer C (2016a) Die Rolle von Spam im Cybercrime. FIfF-Kommunikation 32(4):27–29. http://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-4/fk-2015-4-content/fk-2015-4-p27

Schäfer C (2016b) Mail Infrastructure Traffic Analyzer – Erkennung kompromittierter E-Mail-Accounts. Dissertation, Univ. Jena

Schäfer C (2017) Detection of compromised email accounts used for spamming in correlation with origin-destination delivery notification extracted from metadata. 5th International Symposium on Digital Forensic and Security (ISDFS), IEEE. doi:10.1109/ISDFS.2017.7916494

Symantec Corporation (2017) Security Center Archived Publications. https://www.symantec.com/security-center/archived-publications

Symantec Corporation (2018) Internet Security Monthly Threat Report, Januar 2018. https://www.symantec.com/security_response/publications/monthlythreatreport.jsp?id=2018-01

Westernhagen Ov (30. August 2017) Spambot nutzt 711 Millionen Mail-Adressen zur Malwareverbreitung. Heise Security. https://heise.de/-3817207

Carlo Schäfer

Dr. **Carlo Schäfer** ist promovierter 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 Freistaat Thüringen.