Spürbarer Anstieg von Schadcodeverteilung via E-Mail

Seit Kurzem ist ein spürbarer Anstieg von E-Mails zu verzeichnen, mittels derer Schadcode an die Empfänger ausgeliefert werden soll. Die Mails werden teilweise von Viren- und Spamfiltern nicht als solche erkannt, auch die Erkennung des Schadcodes durch Virenscanner ist oftmals erst verzögert gegeben.

Mittels unterschiedlicher Phishingwellen wird derzeit verstärkt versucht, diverse Trojaner bzw. Downloader für Trojaner zu verteilen. Die Zustellung der Mails scheint hierbei nicht zielgerichtet zu sein, sondern darauf ausgelegt zu sein, eine große Masse an Empfängern zu erreichen. Teilweise werden hierbei auch Phishingmails an deutsche Empfängerkonten zugestellt, bei denen der nachgeladene Online-Banking-Trojaner auf deutschen Bankingseiten momentan gar nicht funktioniert.

Die offenbar am stärksten verbreitete Phishingwelle wird derzeit in Kombination mit dem Trojaner Dridex beobachtet. Dridex entstammt der gleichen Familie wie der Online-Banking-Trojaner GEODO und nutzt auf deutschen Bankingseiten unserer Kenntnis nach auch ähnliche oder identische "Webinjects" (Masche "Demokonto"). Um Dridex auf die Systeme der Mailempfänger zu bekommen verschicken die Betrüger Mails mit Word- oder Excel-Dateien im Anhang, welche ein schädliches Macro enthalten. Durch das Macro wird der Downloader "MDropper" oder ein anderer Downloader auf das System geladen, welcher wiederum Dridex nachlädt. Die meisten derzeit im Umlauf befindlichen Mails dieser Phishingwelle sind auf englisch verfasst, viele von ihnen beinhalten im Betreff bzw. im Namen des Attachments den Begriff "Invoice".

Derzeit sind nicht alle auf diese Weise verteilten Dridex-Trojaner funktional. Es besteht aber das Risiko, dass die Trojaner sich zu einem bestimmten Zeitpunkt (beispielsweise wenn eine bestimmte Anzahl Systeme erfolgreich infiziert wurde) auf eine funktionale Version updaten, sodass auf einen Schlag sehr viele Phishingversuche stattfinden. Zudem eignen die Trojaner sich zum Abgreifen von Zugangsdaten und anderen sensiblen Informationen.

Neben Dridex werden momentan auch andere Schädlinge verstärkt verteilt. Die Mails der jeweiligen Phishingwellen sind unterschiedlich gut gestaltet und beinhalten zumeist exe-Dateien in ZIP-Archiven. Wir beobachten derzeit beispielsweise Mails mit sinnfreiem Betreff, die zum Verteilen von "Upatre" verwendet werden, sowie eine neue Masche mit angeblichen DHL-Mails, die diesmal nicht im Kontext von GEODO, sondern von ZeuS genutzt werden. Sprachlich sind die Mails zumeist eher schlecht gemacht. Das vertraute Layout beispielsweise bei den DHL-Mails könnte trotzdem dazu führen, dass die Empfänger den Text nur überfliegen und eher bereit sind, den Anhang zu öffnen.

In allen von uns beobachteten Fällen ist die Erkennung der via Mail verbreiteten Viren und Trojaner durch Virenscanner aktuell nicht besonders gut. Wir raten daher, sowohl Mitarbeiter als auch Kunden über die aktuellen Wellen zu informieren und entsprechend zu sensibilisieren. Vor allem die Phishingmasche "Demokonto" könnte in Kürze wieder verstärkt auftreten.

Quelle: intern