Hacker konzentrieren sich auf soziale Netzwerke

Auf Grund der wachsenden Beliebtheit von Online Communities konzentrierten Malware-Autoren ihre Anstrengungen auf das Hacken der Sicherheitsvorkehrungen von Social-Networking Plattformen, um an eine große Menge persönlicher Daten zu gelangen.

Auch in der ersten Jahreshälfte verbreiteten sich die meisten Virusinfektionen über das Internet, versteckt lauernd auf seriös scheinenden Webseiten. Oder sie tarnten sich als sogenannte **Scareware** und bewarben gefakte (geschwindelt, vorgetäuscht) Security-Software. Bei Scareware handelt es sich um Software, welche darauf ausgelegt ist, Computerbenutzer zu verunsichern oder zu verängstigen. Der Betriff ist ein englisches Kofferwort aus scare (Schrecken) und Software. Es handelt sich um eine automatisierte Form des Social Engineering. Fällt der User auf den Trick herein und glaubt sich bedroht, so wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten.

Alles unter dem Deckmantel von gefälschten Zertifikaten, die in ihrer seriösen Form eigentlich dazu dienen, die Sicherheit von Internetseiten zu verifizieren. Weiterhin gefährlich blieben auch

- PDF-Infektoren, die Schwachstellen im Adobe-Reader nutzen.
- Nicht minder aggressiv agierten die Autorun-Trojaner, die sich über Wechseldatenträger und die Windows-Autorun-Funktion verbreiten.

Kombinierte Malware-Angriffe im Kommen

Internetkriminelle entwickeln ihre Fähigkeiten auch in Zukunft weiter, Malware zu erstellen, sodass es sehr wahrscheinlich zu einer ganzen Flut neuer E-Threat-Attacken kommen wird. Hier geht die Tendenz hin zu kombinierten Einsätzen der digitalen Schädlinge. Denn viele aktuelle E-Threats verknüpfen scheinbar harmlose Programme, um eine ganze Infektionskette zu erzeugen. Beispielsweise nutzen Cyberkriminelle dem User unbedenklich erscheinende Download-Programme zum Nachladen von Malware auf einen ungeschützten Rechner.

Zudem sind einige Malware-Arten schon heute in der Lage, sich ständig zu modifizieren, um der Erkennung durch Sicherheitsprogramme zu entgehen. Unter Einsatz von Stealth-Technologien[1] wandeln sich viele Schädlinge beispielsweise zu so genannten Sleeper-Infektoren[2], die von konventionellen Schutztechnologien nur schwer identifiziert werden können.

Steigende Gefahr durch Botnetze

Da sich Botnetze zu einem ernst zu nehmenden Angriffsmechanismus entwickelt haben, werden Malware-Autoren weiterhin Wert auf deren Verwendung und Optimierung legen. So werden die Angriffe durch sogenannte Fast-Flux-Botnetze zunehmen. Dabei handelt es sich um abwechselnd missbrauchte „Zombie“-Netzwerke: Hier fungieren einzelne Bots als DNS-Proxies und setzen sich zwischen die Malware-Server und die attackierten Systeme. Die einzelnen Proxy-Rechner wechseln dabei in unregelmäßigen Abständen. Diese Methode erschwert die Erkennung der Malware-Attacken, denn Web-Hosting Provider konzentrieren sich zurzeit lediglich auf das Löschen einzelner Accounts, die für Phishing-Attacken, Exploit- oder Spam-Verbreitung verwendet werden.

Die E-Threat-Akteure konzentrieren sich weiter auf die Kompromittierung von beliebten **Social Networks**. Es ist zu erwarten, dass Internetkriminelle von ihrem bisherigen Kenntnisstand über die Funktionsweisen der Social-Networking-Plattformen profitieren und ihre Informationen nutzen, um noch raffiniertere Malware über diese zu verbreiten. Ein Teil der Angriffe konzentriert sich zudem auf den

[1] Tarntechnik, so wie es die Tarnkappenflugzeuge gibt, schleicht sich der Schädling getarnt als etwas Anderes in Ihr System ein.

[2] Der Schädling schläft so lange auf Ihrem System, bis eine gewisse Zeit abgelaufen ist oder der User eine bestimmte Tätigkeit macht.

Bereich des Social Engineering[3], während andere Angreifer wiederum bereits vorhandene Schwachstellen dieser Plattformen auszunutzen werden (z.B. Lücken im Datenschutz).

[3] Von Social Engineering spricht man immer dann, wenn ein Angreifer, z.B. für Zwecke der Industriespionage, menschliche Eigenschaften ausnutzt, um an Informationen zu kommen. Social Engineering Angriffe sind leider eine extrem effiziente Methode zur Informationsbeschaffung und zwar ohne Einsatz von technischen Hilfsmitteln. Angreifer nutzen dafür natürliche menschliche Reaktionen aus, positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz auf die Arbeit und das Unternehmen oder weniger positive Aspekte wie Gutgläubigkeit, Respekt vor Autoritäten oder gar Bestechlichkeit und auch Eigenschaften wie Konfliktvermeidung und Liebesbedürfnis und der Wunsch, ein guter Teamplayer zu sein