05/07/2012

EPR07/2012
www.enisa.europa.eu

EU-Internetsicherheitsagentur ENISA; „High-Roller"-Online-Bankeinbrüche entlarven Sicherheitslücken

Viele Online-Banking-Systeme verlassen sich in gefährlicher Weise darauf, dass PCs sicher sind. Doch stattdessen sollten Banken davon ausgehen, dass die PCs der Nutzer infiziert sind, schließt ENISA, die EU-Agentur für Cybersicherheit, aus den Berichten über den „High-Roller"-Cyberangriff.

Die jüngsten gezielten „High Roller"-Cyberangriffe auf millionenschwere Bankkonten wurden in einem neuen Bericht von McAfee und Guardian Analytics analysiert. Der Bericht beschreibt die technischen Details und den Einfluss dieser Serie von Cyber-Angriffen. Das alte Sprichwort, dass „Kriminelle dorthin gehen, wo das Geld ist" bedeutet heute, dass "*Bankräuber online gehen*", wie der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, erklärt. Es sollte keine Überraschung sein, dass große organisierte Verbrechergruppen Onlinebanking-Seiten angreifen. Aus den folgenden drei Gründen haben die Angriffe dennoch viel Aufmerksamkeit auf sich gezogen:

1. Hochautomatisiert: Die Angreifer reduzierten manuelles Eingreifen auf ein Minimum und verließen sich hauptsächlich auf Automatisierung. Die Angriffe waren außerdem schnell und vom Nutzer als solche kaum zu erkennen.

2. Ausgeklügelt: Die Sicherheitsmaßnahmen der Banken, wie die Zwei-Schritt-Authentifizierung und die Betrugserkennung, wurden umgangen. Die Nutzer bemerkten dies nicht sofort, weil die betrügerischen Transaktionen durch Malware verborgen wurden (durch Einfügen von JavaScript Code auf den Seiten).

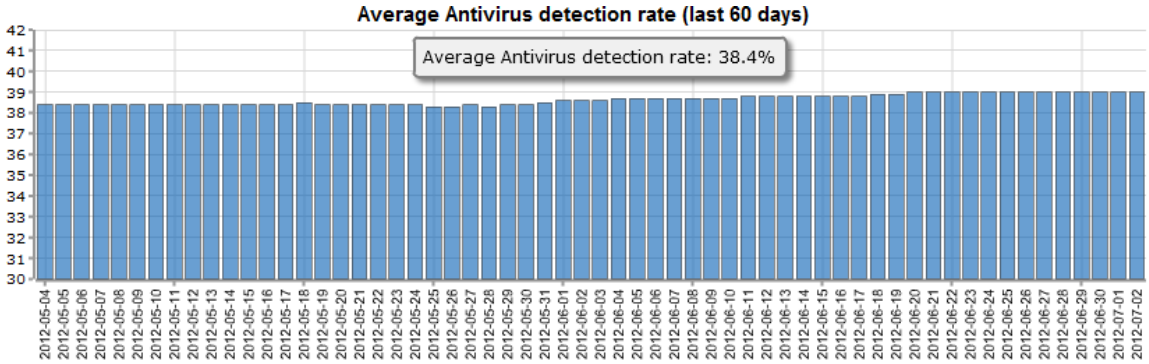
3. Gezielt: Nur PCs von Nutzern mit entsprechend hohem Kontostand wurden angegriffen (z.B. etwa 5000 PCs in den Niederlanden).

Die Cyberangriffe bestanden aus drei Phasen. Zunächst wurden die Ziele identifiziert, indem Onlineerkennung und (Spear-)Phishing genutzt wurde. Opfer mit Zugang zu Konten mit hohem Kontostand wurden ausgewählt (daher der Name „High Rollers"). Als zweites wurde Malware (SpyEye, Zeus und Ice 9) auf den PC des Opfers geladen, der für die Onlinebanking-Websites des Opfers eingerichtet war. Die Malware wurde beim Start einer Onlinebanking-Sitzung des Opfers ausgelöst. SpyEye, Zeus und Ice 9 sind typische Malware-Ausrüstung und für diesen Angriff zugeschnitten. Danach wurden im Namen des Nutzers betrügerische Transaktionen ausgeführt und vor diesem hinter Warn- und Wartemeldungen versteckt. Die Malware transferiert dann Beträge von Sparkonto auf Girokonten und dann zu Mittelsmänner im Ausland, die das Geld abheben, und es dann mit Hilfe von Person-zu-Person-Geldtransfer (z.B. Western Union) weitersenden. Eine detaillierte Analyse und eine Anzahl an Empfehlungen von McAfee und Guardian findet man online.

Empfehlungen

1. Davon ausgehen, dass alle PCs infiziert sind: Die Angreifer benutzen Zeus, ein Do-It-Yourself-Virus-Kit, der für etwa tausend EURO erhältlich ist. Zeus ist seit 2007 als Standardvirus erhältlich, wobei seine Erkennungsrate

gering ist.[1] Für eine Bank ist es in der aktuellen Situation sicherer anzunehmen, dass die PCs aller Nutzer infiziert sind, und die Banken sollten daher Schutzmaßnahmen ergreifen, um damit umzugehen.



Statistik zu Zeus: Nur etwa 40% aller Zeus-Malware wird entdeckt.

2. Onlinebanking-Instrumente sicherer machen: Viele Onlinebanking-Systeme, manche davon mit einmaligen Transaktionscodes, Rechnern oder Smartcard-Lesern, funktionieren auf Basis der Annahme, dass der Nutzer-PC nicht infiziert ist. In Anbetracht der aktuellen Lage der Computersicherheit ist diese Annahme gefährlich**. Banken sollten stattdessen davon ausgehen, *dass* die PCs infiziert sind, und dennoch Schritte unternehmen, um Nutzer von betrügerischen Transaktionen zu schützen.** Zum Beispiel schützt eine einfache Zwei-Schritt-Authentifizierung nicht vor Man-in-the-middle- oder Man-in-the-browser-Angriffen[2] auf Transaktionen. Daher ist es wichtig, mit dem Nutzer den Wert und das Ziel bestimmter Transaktionen gegenzuchecken; über einen sicheren Kanal, mit einem sicheren Gerät (z.B. eine SMS, einen Anruf, ein selbstständiger Smartcard-Reader mit Bildschirm). Sogar Smartphones könnten hier verwendet werden, vorausgesetzt, die Sicherheit von Smartphones lässt dies zu.

3. Enge Zusammenarbeit ist erforderlich, um die internationalen Kommandozentralen zu bekämpfen: Der Cyberangriff wurde mit Kommando- und Kontrollservern durchgeführt, die dynamisch über den gesamten Globus verteilt waren, unter Verwendung von z.B. Fast-Flux-Botnets[3] und kugelsicheren[4] Hosting-Anbietern. Kriminelle

---

[1] *Die Antivirus-Ermittlungsrate für Zeus-Binärcodes liegt durchschnittlich bei etwa 38,4%. Mit anderen Worte, selbst bei der Verwendung eines aktualisierten Antivirus-Programmes gibt es noch ein beträchtliches Risiko, infiziert zu werden.*

2 *Selbst, wenn der Nutzer jedes Mal für die Authentifizierung einen neuen und geheimen Code eingeben für die Transaktion auf dem Server eingeben muss, kann der Betrüger dennoch diesen Code abfangen und ihn auf dem Server erneut abspielen, um eine betrügerische Transaktion durchzuführen.*

3 Fast Flux ist eine Technik, bei der ein Domainname auf eine große Menge von schnell wechselnden IP-Adressen (also Computern) verweist.

nutzen diese Tricks, um Strafverfolgung sowie Erkennung und Bekämpfung noch komplizierter zu machen. **Daher ist eine enge Zusammenarbeit sowohl bei Prävention, als auch bei Strafverfolgung nötig.** Die ENISA arbeitet daran, engere Verknüpfungen und mehr Informationaustausch zwischen den nationalen Computer Emergency Response Teams (CERTs), den Ermittlungsbehörden und EU-Mitgliedsstaaten zu befördern, um grenzübergreifend die Reaktion auf Zwischenfälle zu verbessern.

Die Prävention von Cyberangriffen ist wichtig, aber es ist trotzdem notwendig, auf Angriffe vorbereitet zu sein. Die ENISA arbeitet mit den einzelnen EU-Mitgliedsstaaten daran sicherzustellen, dass jedes Land über gut funktionierende CERTs verfügt, um mit Cybersicherheits- Zwischenfällen umgehen zu können. Die ENISA organisiert große internationale Cybersicherheits-Übungen (zum Beispiel Cyber Europe 2010, Cyber Atlantic 2011, und die bevorstehende Cyber Europe 2012) um die internationale Zusammenarbeit bei großen Sicherheits-Zwischenfällen zu verbessern. Die ENISA arbeitet mit den Mitgliedsstaaten auch daran, die Berichterstattung über Zwischenfälle zu verbessern, um mehr Transparenz über die Gründe, die Häufigkeit und die Schwere von vergangenen Zwischenfällen zu erreichen. Derzeit sind Nutzer, Unternehmen und Politiker zu groben Schätzungen gezwungen. Die Europäische Kommission hat vor kurzem eine Strategie für Internetsicherheit angekündigt, einschließlich der Möglichkeit Artikel 13a (verpflichtende Fehlerberichterstattung und Sicherheitsmaßnahmen) für den Bereich jenseits der elektronischen Kommunikation auszuweiten.

In Zukunft werden Browsersicherheit und Smartphone-Sicherheit eine immer wichtigere Rolle spielen, da immer mehr Transaktionen auf Smartphones oder Tablets durchgeführt werden. Die schnelle Verbeitung von Smartphones bietet eine wichtige Möglichkeit, um die End-point-Sicherheit zu erhöhen (zum Beispiel durch die Nutzung von geprüften Appstores oder von Smartphones as Sekundärfaktoren) aber wir sollten Smartphone-Sicherheit nicht als gewährleistet ansehen.[5]

Für Interviews: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Mobil: + 30 6948 460 143, oder cert-relations@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu

4„Kugelsicherer Hosting-Anbieter" ist die Bezeichnung für eine Anbieter, der keinerlei Bedingungen oder Prüfungen an hochgeladenes Material knüpft. Cyber-Kriminelle nutzen kugelsicheres Hosting um Server, Malware-Infektionsseiten, Phishing-Sites etc. zu steuern und zu kontrollieren.

[5] Auch wenn viele Smartphone-Händler die Chance genutzt haben, die PC-Sicherheit zu verbessern, sollten wir dennoch vorsichtig sein: Es gibt bereits zahlreiche Fälle, bei denen Kriminelle sowohl den PC als auch das Smartphone des Opfers infizieren, um die SMS-basierte Zwei-Wege- Authentifizierung zu umgehen, durch Verwendung von Zitmo.