Mit den Augen eines Phishers

Phishing hat sich in den letzten Jahren zu einer der größten Bedrohungen entwickelt. Die meisten Berichte über Phishing werden aus der Perspektive der Verteidiger geschrieben. Nun ist es den Betreibern des Forums ha.ckers.org gelungen einem Phisher seine Sichtweise zu entlocken.

Lesen Sie zunächst das Interview und danach die weiteren Reaktionen auf den Bericht und unsere Anmerkungen:

F: Wie würden Sie sich beschreiben? Alter? Sind Sie zur Schule gegangen? Interessen?

Lithium: Entschlossen ist das beste Wort, um mich zu beschreiben. Ich bin 18 Jahre jung. Ja, ich bin zur Schule gegangen. Ich ging nach der HighSchool ab. Meine Interessen sind MMA (mixed martial arts); Fitness und nicht zuletzt..das Internet!

F: Wie haben Sie mit Phishing angefangen? Was weckte Ihr Interesse daran?

Lithium: Die typischen Betrugs-Mails, die meine Eltern immer in Ihre Inbox erhielten. Sie waren soo schlecht gemacht! Trotzdem haben sie meistens funktioniert. Also wusste ich automatisch, dass ich effizientere Methoden entwerfen könnte und damit größeren Erfolg hätte.

F: Wie lange sind Sie schon Phisher?

Lithium: Ich habe mit dem Phishing angefangen als ich 14 wurde. Also fast 5 Jahre.

F: Haben Sie eine Vorstellung davon, wieviele Identitäten sie bis jetzt gestohlen haben?

Lithium: Weit über 20 Millionen. Mit Social Networking Würmern habe ich's gleich gehabt. Ich habe so viele Hunderttausend Accounts zu vielen Webseiten, dass ich noch keine Gelegenheit hatte sie durchzusehen.

F: Mussten Sie bestimmte Beziehungen zu Personen/Gruppen aufbauen, um loszulegen?

Lithium: Nein. Als ich anfing war ich solo. Viele Gruppen kamen zu mir und fragten, ob ich rein wollte. Ich lehnte ab.

F: Welche Art von Sites sind die besten Phishing-Sites?

Lithium: Social Networking Sites. Jede Seite, die Teenager ab 14 Jahre einbezieht.

F: Was tun Sie, um eine Phishing-Site aufzusetzen?

Lithium: Ich versuche einen Domainnamen zu finden, der am besten zum aktuellen Opfer passt. Versuche ein paar Ähnlichkeiten zu finden, die meine Site realistischer machen können. Dann, Registrieren! Dann suche ich einen verlässlichen Anonymouse-Host. (Ausländische sind am verlässlichsten) Obwohl, ich tendiere dazu kompromittierte Hosting Accounts zu verwenden.

Zweitens, ich schau mir den Sourcecode der Seite an. Dann veränder ich den Quellcode so dass die

Inhalte des Formulars in meiner Phishing-Site gepostet werden.

Drittens, ich erstelle eine PHP-Datei, die per POST die Inhalte des Formulars in eine Textdatei auf meinen Server überträgt, Dazu sind nur geringe Änderungen notwendig, da es nur ein paar Zeilen PHP Code sind.

F: Wie viele Leute werden pro geposteter Site abgephischt?

Lithium: Das hängt von der Größe der Website ab (Anzahl der Nutzer) Normalerweise pishe ich 30K pro Tag.

F: Wie werden die Identitäten zu Geld gemacht und wieviel bringt das Netto ein?

Lithium: Mit Social Networking Sites verdiene ich $500 bis 1K mit CPA Deals [Anm. G DATA: CPA = Cost per Action und heißt, dass jemand etwas gekauft oder abonniert hat]. 5 von 10 Personen benutzen das gleiche Passwort für ihren E-Mail Account. Der weitere Profit hängt davon ab, was in der Mailbox drin ist. Wenn der E-MailAccount einen der folgenden Accounts enthält Paypal/Egold/Rapidshare/Ebay und der E-MailAccount selbst. Ich verkaufe sie an Betrüger [Anm. G DATA: Scammer]. Alles zusammen genommen verdiene ich 3K bis 4K pro Tag. Ich phishe nur 3-4 Tage pro Woche. Hängt davon ab wieviel Zeit ich investiere. Je mehr Zeit ich investiere desto mehr kommt raus.

F: Sind mit Phishing auch Kosten verbunden?

Lithium: Ja es gibt Kosten. Ein dedizierter Server, VPN, Netzwerk-Verschlüsselungssoftware und Zeit.

F: Welche Hardware/Software brauchen Sie? Spezielle Tools (Phishing Kits, etc)? Was für eine Internetverbindung nutzen Sie?

Lithium: Für die MEISTEN Social Networking Sites benutze ich ein Programm namens MyChanger. Sie finden es auf dieser Website - www.myownchanger.com - Es macht Phishing auf Social Networking Sites viel schneller. Alles ist automatisiert! Messaging/Bulletins/Comments/Profiländerungen. Es ist großartig. Darüber hinaus erstellen Freelance Entwickler für mich VIELE maßgeschneiderte an meine Ansprüche angepasste Programme. Mein Internetverbindung ist nichts Besonderes. Eine normale 1MB ADSL Verbindung.

F: Wie schaffen Sie es nicht geschnappt zu werden?

Lithium: Ich nutze VPNs, dedizierte Server, Proxies und mein Netzwerkverkehr ist verschlüsselt. Alle Zahlungen erfolgen über eGold.

F: Gibt es Anti-Phishing Abwehrmaßnahmen (Tools oder Technologien), die das Leben eines Phishers erschweren?

Lithium: Ja sicher, Es gibt viele Dinge, die Phishing schwerer machen. Insbesondere seit Internet Explorer 7 und Firefox 2 einen Phishingschutz integriert haben. Diese beiden sorgen für den meisten Ärger.

F: Können Sie Änderungen in der Phishing-Industrie absehen, die erwähnenswert sind?

Lithium: Nein.

F: Sonst noch etwas, das Sie mitteilen möchten/ letzte Worte?

Lithium: Faule Webprogrammierer sind der Grund, warum ich immer noch phishen kann.

So weit das Interview, für das Lithium ein großer Dank gebührt. Die Reaktion auf diese Bekenntnisse in dem Forum war geprägt von zwei Gruppen. Eine wollte nicht glauben, was Lithium da geschrieben hat, und meinte, dass er nur ein aufschneiderischer Prahlhans wäre. Es meldeten sich aber Leser aus dem Blackhat-Lager zu Wort. Einer meinte, dass Lithium mit seinen lahmen Skripten ja ein Anfänger wäre. Er solle lieber mal einen Denial-of-Service Angriff auf einen DNS-Root-Server fahren (also auch ein Aufschneider). Ein weiterer Blackhat namens 'TehLeetPhisher' meinte, dass Lithium mit alten Sachen angibt. MyChanger sei 'funny shit' von Einem, den er kennt, und das Abphishen von Social Networking Plattformen sei seit einem Jahr aus der Mode. Außerdem verdiene er (TehLeetPhisher) täglich etwa $30K. Jeden Tag würde er 30.000 Accounts Phishen. An diese Leute und alle Leute aus deren Freundesliste kann er Spam verschicken - mit besonders hohen Click-Through-Raten (CTR), weil man Freunden ja normalerweise vertraut. Seit der Flash-Sicherheitslücke steige die Anzahl der ´Beworbenen´ exponentiell.

Was kann man nun daraus lernen? Nun Phishing ist offenbar ein lukratives Geschäft. Wenn man den Zahlen nur halbwegs Glauben schenken kann, verdient ein Phisher an einem Tag mehr als die meisten von uns in einem Monat. Phishing ist auch nicht mehr beschränkt auf den Diebstahl von Kontozugangsdaten. Alleine die Mailadresse und der Mailaccount sind auf dem Schwarzmarkt so wertvoll, dass man gut davon leben kann. Dadurch geraten insbesondere Social Networkting Sites wie wie MySpace, facebook, StudiVZ, XING etc. in den Fokus der Phisher. Faule Webentwickler und Sicherheitslücken in Standardanwendungen wie Flash stehen spezialisierter Phishing-Software und Tools gegenüber. So bleibt die Phishing-Industrie auch weiterhin profitabel.

Offenbar greifen aber auch die ersten Gegenmaßnahmen. Gut zu hören, dass IE7 und FF2 ein wenig Sand im Getriebe sind. Nutzer von Social Networking Sites sollten also ausgesprochen vorsichtig mit den dort bereit gestellten Daten umgehen. Außerdem sollten Sie jede Plattform und für ihren E-Mailaccount unterschiedliche Passwörter verwenden. Beim Besuch der Seiten könnte es nützlich sein, Flash auszuschalten, nicht auf jeden Link zu klicken und nicht alles zu glauben, was von angeblichen Freunden geschrieben wird.

(Veröffentlichung des übersetzen Interviews mit freundlicher Genehmigung der GDATA AG)

05/2007, Redaktion

Quelle:
http://www.securitymanager.de/magazin/artikel_1450_mit_den_augen_eines_phishers.html