

Rexspy – Trojaner oder Marketing. Was ist dran an der Geschichte um den SMS-Trojaner?

In den Medien wird seit Oktober des Jahres 2006 berichtet, dass der Security Dienstleister SecurStar aus München die wohl schlimmste Sicherheitslücke bei Handys überhaupt gefunden hat.

Der Inhaber der Firma SecurStar, Herr Hafner, rühmt sich damit, selbst diesen Trojaner namens „Rexspy“ entwickelt zu haben.

Wen wundert es da, dass SecurStar hierfür auch gleich passend ein Gegenmittel anzubieten hat: Eine Verschlüsselungssoftware für Handys.

Gehen wir zum Anfang der Geschichte zurück und beleuchten die inzwischen bekannt gewordenen Details zu „Rexspy“.

In einem Interview und in einer Demonstration für das Magazin Focus wird gezeigt, wozu Rexspy in der Lage sein und welche Bedrohung diese Lücke darstellen soll.

Hafner, der selbst die Demonstration durchführt, geht mit dem Reporter von Focus in einen Handyladen und kauft 2 vermeintlich neue Mobiltelefone, mit denen er die Sicherheitslücke demonstrieren will.

Dann ruft der Reporter mit einem dieser Handys in der Redaktion an, während Hafner dem zweiten der gekauften Handys eine kryptisch anmutende SMS schreibt und diese absendet.

Ob und wo die SMS ankommt, ist weder bekannt noch ersichtlich.

Während der Reporter das Gespräch beginnt, klingelt auch schon das eigene Handy von Hafner und er kann das Gespräch mithören.

Auf diese Art und Weise soll gezeigt werden, dass es möglich ist mittels einer angeblich verschlüsselten SMS andere Handys anzuzapfen und Gespräche mit zuhören.

Über diese Sicherheitslücke sei es möglich, jedes Mobiltelefon zu einer Wanze umzufunktionieren.

Mehr noch und wie anscheinend in der Demonstration bewiesen – der Nutzer bemerke von diesem Vorgang nicht einmal etwas.

Laut Aussage des Inhabers der Firma, Wilfrid Hafner, funktioniere diese Lücke vermeintlich mit Hilfe einer Service-SMS.

Es wurden jedoch hierzu keine Details veröffentlicht oder Screenshots gezeigt.

Hierbei sei zusätzlich erwähnt: Vor einigen Jahren noch beschäftigte sich Wilfrid Hafner mit dem „Hacken von Telefonleitungen“ (Phreaking).

Da sich der Artikel im Focus mehr als interessant und im Ergebnis etwas unglaublich gelesen hat, versuchten wir, einen Demotermin zu bekommen, um uns die Sache genau anzuschauen.

Dazu kam es nicht, da angeblich terminliche Probleme auftraten.

Dies jedenfalls wurde aus der PR-Agentur bekannt gegeben, bei der Hafner bis vor kurzem seine Pressearbeit erledigen ließ.

Um die Zeit nicht ungenutzt verstreichen zu lassen, recherchierten wir und fanden interessante Details zu Rexspy.

Wir telefonierten mit vielen Experten und nahmen Kontakt zu Herstellern von Mobiltelefonen sowie zu Mobilfunkbetreibern auf.

Wenn man Hafner Glauben schenken darf, handelt es sich um die erfolgreiche Ausnutzung einer Schwachstelle im Service-SMS Protokoll.

Um weitere Details zu erfahren, nachdem der spannende Bericht im Focus erschienen war, nahmen wir Kontakt zu Herr Hafner persönlich auf und bekamen tatsächlich einen

Rückruf aus München.

Im Gespräch mit dem Entdecker der Schwachstelle wurde uns erklärt, was Service-SMS sind, was Blueboxing sei, und dass Herr Hafner wohl lediglich eine Konferenzschaltung aktivieren könne.

Herr Hafner erklärte während des Telefonates weiterhin, dass man alle Gespräche mithören und auch die SMS des betroffenen Handys auslesen könne.

Desweiteren berichtet Hafner von Schwachstellen und Angriffsmöglichkeiten auf Windows Mobile, die wohl zusätzlich noch ausnutzbar wären.

Auch zu diesen Schwachstellen wurden wieder einmal keine weiteren Details bekannt gegeben.

Im Gespräch mit Hafner wurde schnell deutlich, dass deutsche Mobilfunkprovider nicht bereit waren, für die entdeckte Schwachstelle eine angemessene Summe an ihn zu zahlen.

Aber auch dies bezüglich sind von ihm keine konkreten Namen oder Unternehmen genannt worden.

In einem Interview mit der BILD-Zeitung wurde von SecurStar verkündet, die Provider würden die Schwachstelle nicht ernst nehmen.

Wir gingen diesen Aussagen nach und konfrontierten die Netzbetreiber in Deutschland mit den Fakten von Rexspy, die uns durch Pressemeldungen vorlagen.

So wie die Aussagen der Netzprovider zu lesen sind, gab es anscheinend keine Gespräche mit Hafner.

Grund hierfür: Hafner war nicht erreichbar für die Mobilfunkbetreiber.

Die Provider waren zudem auch nicht bereit, ohne weitere Details zum Beweis für die angebliche Schwachstelle Rexspy eine uns unbekannt Summe zu zahlen.

Wirklich interessant wird es in dem Moment, in dem man Zeilen wie diese liest: „Mit Rexspy kann man auch verschlüsselte Telefonate abhören!“ (Hafner in einem Interview) Diese Möglichkeit allein würde den BigBrother Supergau auslösen, sofern es sich hierbei um eine tatsächlich entdeckte Schwachstelle handeln würde.

Hafner legt im gleichen Atemzug nach und verspricht, dass die SecurStar eigene Software „PhoneCrypt“ die Sicherheit bietet, um auch in diesem Fall sicher vor Rexspy zu sein.

Was sagen die Mobilfunkprovider und Hersteller von Mobilfunkgeräten dazu?

Vodafone Deutschland äußerte sich auf Anfrage folgendermaßen:

„Um den von Ihnen genannten Trojaner Rexspy ist es still geworden, da der von einer Sicherheitsfirma entwickelte "Spion" sich als nicht reproduzierbar erwiesen hat.

Selbst auf mehrfache Nachfrage war die Firma SecureStar nicht bereit, eine Ihrer "Schad-SMS" zur Verfügung zu stellen, um die "Infizierung" des Handys nachstellen zu können.

Es wird generell angezweifelt, dass die von SecureStar behauptete mögliche "Herrschaft" über das mit einer SMS infizierte Handy ohne Interaktion des Nutzers stattfinden kann.

Außerdem stellt eine SMS einfach nicht genug Platz zur Verfügung, um Schadcode - der immerhin einige Bytes an Platz benötigt - zu verbreiten.

Selbst wenn eine Verbindung zu einem dritten Handy - ohne dass der Nutzer dies bemerkt - möglich wäre, was Vodafone ausschliesst; spätestens bei Erhalt der nächsten Rechnung mit Verbindungsübersicht ist eine Enttarnung möglich, da für diese Maßnahme die Anwahl einer Rufnummer erforderlich ist.

Rexspy wird demzufolge nicht als Bedrohung angesehen, jedoch sollten trotzdem Sicherheitsvorkehrungen beim Umgang mit Handys (insbesondere der Multimediageräte neuester Generation) getroffen werden.“

Da die Firma Ericsson auf der Homepage der Firma SecurStar als Referenz angegeben wird, erkundigten wir uns auch bei Ihnen.

Die Aussage des Pressesprechers liest sich indes sehr klar:

„Laut EICTA Security Issue Group und Bitkom handelt es sich bei der Geschichte um einen klassischen "Hoax".“

Ein Hoax ist vereinfacht ausgedrückt eine Information, die keine echten Inhalte enthält und Dinge vortäuscht, also eine Falschmeldung.

Ebenso gab Ericsson bekannt, dass keinerlei Geschäftsbeziehungen zwischen SecurStar und Ericsson bestanden hätten oder bestehen würden.

Warum aber gibt es eine Software, die Rexspy von betroffenen Handys entfernen soll, wenn doch Rexspy gar nicht im Umlauf sein kann?

Hafner selbst äußerte sich während des Telefonats und auch in weiteren Interviews dazu mehr als deutlich.

Die Schwachstelle werde von ihm nicht veröffentlicht, und so kann Rexspy auch keine echte Bedrohung darstellen.

Welchen Sinn macht eine Entfernungssoftware für einen Trojaner, der aber doch angeblich nicht im Umlauf sein soll?

Rexspy funktioniert nach Aussage von Hafner auf jedem Mobiltelefon - also auf Mobiltelefonen mit SymbianOS, auf Windows Mobile und auf Handys mit eigener Firmware.

Die Schwachstelle liege nicht direkt im Betriebssystem der Mobiltelefone, sondern sei im Service-SMS Protokoll zu suchen.

Auf der Homepage von SecurStar wird das Removaltool angeboten, mit dem man Rexspy entfernen kann.

Wir beschlossen also, uns rexkiller.exe – das Removaltool – etwas genauer anzusehen und stellten dabei fest:

Die beiden folgenden Registry-Keys werden gelöscht:

- \CLSID\{2AB4C11E-673C-494C-98A2-CC2E91A48115}
- \Software\Microsoft\Inbox\Svc\SMS\Rules\{2AB4C11E-673C-494C-98A2-CC2E91A48115}

Es werden alle laufenden Prozesse im System via Toolhelp32 aufgelistet.

Geht der Call schief, meldet das Programm: Device not infected with REXspy

Es sucht nach einen Prozess "ac.exe" und beendet diesen, sollte er gefunden werden.

Es löscht eine Verknüpfung namens "ac.lnk".

Es de-registriert eine DLL mit Namen "ac.dll".

Es sagt "REXspy was successfully removed!".

Trifft dies nicht zu, meldet das Removaltool: "Device not infected with REXspy"

Werden also keine ac.* Dateien gefunden, erscheint diese Meldung.

Codeanalyse: Felix „FX“ Lindner, Reurity Labs GmbH.

Nach der Analyse des Rexspy Removaltools kann man davon ausgehen, dass mit der Installation von rexkiller.exe eine Software auf dem Windows Mobile Smartphone installiert wird die entsprechende ac.* Dateien anlegt.

Auch zeigt das Löschen der Registry Keys im Speicherbereich der SMS, dass in der Tat eine manipulierte SMS eingegangen sein könnte.

Hierbei könnte es sich durchaus um eine Backdoor handeln, die eine Aktion auf dem betroffenen Mobiltelefon auslöst. Schließlich wird ja ein SMS-Handler deinstalliert.

Dies ist jedoch auch mit dem Removal Tool nie bewiesen worden.

Rexspy stand uns ja nicht zur Verfügung.

Zweifel:

In einer letzten Möglichkeit mit Herr Hafner via E-Mail in Kontakt zu treten wurden keine weiteren Details genannt.

Einzig zu lesen ist, dass Hafner die Technologie an einen Geheimdienst nach Brasilien verkauft haben will.

Welchen Hintergrund dieser angebliche Verkauf haben soll, bleibt unklar.

Hafner beteuerte in Interviews, dass er die Technologie (die angebliche Schwachstelle) unter Verschluss halten will.

Aus einem Telefonat heraus ist zweifelsfrei bekannt geworden, dass ein deutsches Unternehmen bei der Geschichte um Rexspy keine unwesentliche Rolle spielt.

So hat uns ein Geschäftsführer versichert, man habe für die Demonstration von Rexspy eigens eine Telefonanlage entwickelt, die diese Täuschung vornimmt.

Es wurde uns ebenfalls telefonisch versichert, dass für die Demonstration entsprechend gekauften Handys und SIM-Karten bereits vorher bekannt waren und somit auch die Rufnummern.

Es ist anzuzweifeln, ob eine echte Demonstration zustande gekommen wäre, wenn ein Mobilfunkladen durch uns ausgewählt worden wäre.

Hierbei sei jedoch zu erwähnen, dass ein Beweis der Firma ausgeblieben ist und Details dazu nicht übermittelt wurden.

Die Zweifel an der Echtheit des Rexspy bleiben jedoch erhalten.

Ein Beweis zu 100% kann hier nicht erbracht werden.

Zusammenfassung:

Es ist mit großer Wahrscheinlichkeit davon auszugehen, dass es sich nicht um einen SMS Trojaner namens Rexspy handelt.

Die Existenz von Rexspy konnte nicht nachgewiesen werden.

Die Analyse des Removal Tools zeigt außerdem, dass nicht alle Handys wären betroffen, selbst wenn Rexspy existieren würde.

Die zusammen getragene Informationen lassen darauf schließen, dass „Rexspy“ als Schwachstelle nicht ernst zu nehmen ist.

Eine Erklärung für die Funktionsweise der Demonstration ist deutlich einfacher als vermutet.

Eine gut programmierte ISDN/MSISDN/GSM Anlage wäre durchaus in der Lage, solche Funktionalitäten zu bieten.

Seltsam mutet es schon an, dass ausgerechnet eine Software der Firma SecurStar gegen Rexspy helfen und Gespräche wieder sicher machen soll.

Der bittere Beigeschmack eines schlechten Marketingfeldzuges bleibt zurück.

Verweise, Quellen:

EICTA Security Issue Group

<http://www.eicta.org>

Phonecrypt:

http://www.securstar.com/products_phonecrypt.php

Collin Mulliner:

<http://www.mulliner.org/blog/blosxom.cgi/security/rexspy.html>

Marko Rogge:

http://shakal.blog.de/2007/03/31/rexspy_trojaner_fur_alle_handys~2007417

Zone-H:

<http://www.zone-h.org/content/view/14370/31/>

Focus Online:

http://www.focus.de/digital/handy/sicherheitsluecke_nid_44790.html

Pressemeldung SecurStar:

http://www.securstar.com/press_2006_10_31.php

IMSI-Catcher:

<http://de.wikipedia.org/wiki/IMSI-Catcher>

Das Gesetz dazu & der Datenschutz:

<https://www.datenschutzzentrum.de/material/themen/divers/imsicat.htm>

Recurity Labs:

<http://www.recurity-labs.com>

Danksagung:

Ich möchte mich für die Hilfe bei der Recherche, der Korrektur und der Umsetzung bei folgenden Personen und Unternehmen bedanken:
Collin Mulliner, Birgit Haase, Vodafone Deutschland, Felix „FX“ Lindner, SABRE Labs GmbH, T-Mobile Deutschland, Ericsson, Nokia, Paul Sebastian Ziegler, Martin J. Muench, E-Plus und allen anderen Firmen und Personen die geholfen haben.

Marko Rogge, September 2007

<http://www.marko-rogge.de>

Anmerkung:

Alle hier genannten Informationen sind zusammen getragen worden aus persönlichen Gesprächen mit beteiligten Personen und betroffenen Unternehmen.

Die E-Mails von Mobilfunkbetreibern und weiteren Fachexperten liegen vor .

Angemerkt sei hierbei ebenfalls, dass Geheimdienste schon seit je her in der Lage sind, Gespräche von Mobiltelefonen zu belauschen.

Hierzu sei Verweis auf den IMSI-Catcher aufgeführt.

In der Welt wäre eine Schwachstelle sicherlich einem Supergau gleich zu werten.

Eine Service SMS wird im übrigen immer mit einer Passwort Abfrage versendet.

Ich möchte hier ausdrücklich erwähnen, dass ein 100% Beweis für die Existenz von Rexspy nicht erbracht werden konnte.

Ein Gegenbeweis jedoch auch nicht.

Dies ist kein Tatsachenbericht.