hakin9

Eine neue Virengeneration: ist niemand mehr sicher?

Mikko Hypponen

Interview

Eine neue Virengeneration: ist niemand mehr sicher?

Interview mit Mikko Hypponen

Mikko Hypponen – ein Mensch, der einen Teil seines Lebens dem Schutz von tausenden Computern vor digitalen Schädlingen gewidmet hat. Im letzten Jahr hat er als erster die ganze Welt vor dem Angriff des Sasser-Virus gewarnt. Das von ihm geführte Team hat auch die Folgen der Slapper-Angriffe im Jahre 2002 eingedämmt. Außerdem hat das Team das weltweite Netz deaktiviert, welches vom Sobig.F-Wurm im Jahre 2003 verwendet wurde.

h9: Den Großteil Deines Auftrittes auf der F-Secure-Konferenz hast Du der Sache der Viren, Würmer und Trojaner für Mobilgeräte gewidmet. Du hast dabei über die aktuelle Situation gesprochen. Wir möchten allerdings wissen, wie sieht Deiner Meinung nach die Zukunft des schadhaften Codes in WLAN- und Bluetooth-Netzwerken aus?

MH: Potentielle Gefahren für drahtlose Netze sind das zentrale und auch schwerwiegendste Thema, dem sich unsere Teammitglieder widmen. Bisher haben wir wirkliche Gefahren noch nicht angetroffen, doch man muss wachsam sein. Stellen wir uns einen Angriff vor, der sich selbständig über tausende von Funkverbindungen ausbreitet. Es ist dabei unwichtig, ob es sich dabei um Bluetooth oder WLAN handelt. Solche Viren und Trojaner verbreiten sich in einem einzigen Augenblick - von einem Laptop auf einen anderen, von dort aus auf einen Palmtop, von dem Palmtop auf das Handy eines Bankdirektors, und von dort aus in das interne Banknetz.

h9: Katastrophal. Und was passiert danach?

MH: Somit bekommt der Virus einen leichten Zugriff auf einen durch keine Firewalls und Filter geschützten Bereich. Es sei zu bemerken, daß all dies sehr leicht und ohne die Notwendigkeit, irgendwelche Schutzmaßnahmen zu umgehen, geschieht. Genauso, wie es Würmer vom Typ Zotob machen. Seine Verbreitungsmethoden in strategisch wichtige Bereiche, sehen beispielsweise folgendermaßen aus: ein Mitarbeiter hat seinen Laptop zu Hause unbewusst infiziert und ihn dann mit an die Arbeit genommen, wo er ihn an das Firmennetz angeschlossen hat. Dies war ausgereichend, damit Zotob ins interne Netz der Firma gelangen konnte.

h9: Wird der Infektionsprozess erleichtert, wenn WLAN- und Bluetooth-Viren erscheinen?

MH: Wesentlich leichter! Es reicht, mit einem infizierten Laptop zu reisen. Von einem Moment zum anderen ist der Virus nicht nur im eigenen Netz, sondern auch im Netz des Nachbarn, der nebenan wohnt. Des Weiteren wird man auch das Handy des Pizza-Zulieferers infizieren, der gerade das Büro betritt. Damit ein solcher Angriff erfolgreich sein kann, müssen jedoch erst diverse Remote-Exploits vorhanden sein, die auf den Stacks von Bluetooth und WLAN Geräten anwendbar sind.

h9: Gab es bereits erste Anzeichen einer solchen Gefahr?

MH: Leider ja, zum Beispiel fanden sich Löcher in Sicherheitsmechanismen des Bluetooth-Stacks

von Vidcom. Die meisten Arbeitsstationen mit installiertem Windows-System waren über zwei Jahre lang für einen Remote-Exploit anfällig, welches verwendet werden kann, um über Bluetooth einen beliebigen Code auf dem angegriffenen System auszuführen. Wir befürchten, dass Sicherheitslücken in populären WLAN-Standards entdeckt werden und wissen, dass eine solche Entdeckung nicht nur möglich, sondern sogar höchst wahrscheinlich ist.

h9: Bei Deinem Auftritt hast Du über das System Symbian OS gesprochen. Meines Wissens ist es bisher das einzige Betriebssystem für Handys, das infiziert werden konnte. Woher kommt es, dass man einen Virus gerade für Symbian erstellen kann und beispielsweise nicht für das mobile Linux?

MH: Es gibt keine einzige Sicherheislücke. Jedes Virus, jeder Wurm und Trojaner, die wir gesehen haben, wollte nicht ein konkretes Sicherheitsloch ausnutzen, sondern hat eher auf der Unachtsamkeit des Benutzers basiert. Solche Viren funktionieren nach genau demselben Prinzip, wie auch E-Mail-Viren.

h9: Genauso wie LoveLetter?

MH: Exakt. Leute, die sich von dem Betreff und Inhalt der Nachrichten täuschen lassen, öffnen das Attachement. Auf dem gleichen Prinzip basieren heutzutage Viren, die Handys infizieren und sich über Bluetooth verbreiten. Der Benutzer selbst ist immer noch die größte Gefahr, die zur Infektion eines mobilen Geräts führen kann. Wenn man die Systeme Windows und Symbian vergleicht, kann man interessante Schlußfolgerungen ziehen. Symbian warnt den Benutzer vor einem Startversuch einer unbekannten Applikation – Windows nicht. Unter diesem Aspekt betrachtet ist also Symbian... sicherer als Windows.

h9: Mit welchen gefährlichen Trojanern habt Ihr im Laufe der letzten Monate zu tun gehabt?

MH: Wenn es um Infektionen von Mobilgeräten geht, müssen solche Trojaner erwähnt werden, die sogar das Starten des Geräts nicht mehr ermöglichten. Es gab Infektionen, durch die man das infizierte Handy gar nicht mehr benutzen konnte – man konnte nicht einmal mehr die Notrufnummer wählen.

Die Reparatur eines solchen Gerätes kann auf verschiedene Arten erfolgen. Man kann das Handy auf Herstellereinstellungen zurücksetzen, was eine Formattierung des gesamten Speichers und einen Verlust aller Daten zur Folge hat. Und das will ja keiner. Man kann auch ein anderes Handy benutzen, um eine Speicherkarte mit unserer Software vorzubereiten, die das bösartige Programm vom infizierten Handy entfernt.

Der letzte interessante Trojaner war *blank phone*. Er erhielt seinen Namen auf Grund seiner speziellen Funktionsweise - es ist nach einer Infektion nicht mehr möglich, irgendetwas im Gerät zu lesen, denn es gibt zwar Symbole und Bilder aber man kann keine Fonts mehr sehen. Es ist verzwickt, denn selbst wenn man ein Antivirenprogramm installiert hat, sieht man keinen Text und kann es nur sehr schwierig aufrufen. Man muss wissen, welche Tastenkombination zu drücken ist, damit man den Virus los werden kann.

h9: Gibt es eine Gefahr, dass man sein Handy durch ein heruntergeladenes Java-Spiel infiziert?

MH: Erstens – wir haben noch kein Java-Spiel gesehen, das einen Virus enthalten würde. Es gibt dahingehend sicherlich Gefahren, die wir allerdings noch nicht entdecken konnten. Alle bösartigen Programme, mit denen wir zu tun hatten, waren ein nativer Code von Symbian.

h9: Welchen Ratschlag kannst Du Besitzern von Mobilgeräten mit einem Symbiansystem und Bluetooth geben, um ein Maximum an Sicherheit zu erreichen?

MH: Praktisch alle Gefahren betreffen das Symbian der 60er-Serie. Wenn das Mobilgerät mit einem anderen Betriebssystem ausgestattet ist, wie Symbian 40 oder 80, Windows oder Linux, ist das Risiko sehr, sehr gering. Wenn es sich um ein Handy mit Symbian 60 handelt, existiert eine Infektionssgefahr in dem Moment, in dem unbekannte Applikationen installiert werden. Um sich dagegen zu schützen, sollte man Bluetooth ausschalten oder zumindest in den versteckten Modus übergehen und Applikationen nicht akzeptieren – es sei denn, dass sie erwartet werden. Man darf nicht Applikationen unbekannter Herkunft installieren.

h9: Hat F-Secure die Absicht, in der Zukunft ein Antivirenprogramm für andere Systeme zu entwickeln, wie z.B. für Linux?

MH: Zu diesem Thema darf ich leider nichts sagen, was aber nicht bedeutet, dass wir unsere Linux-Software nicht weiterentwickeln. Jeder weiss, dass Finnland ein sehr Linux-freundlicher Staat ist. Linus Torvalds hat mal gleich neben unserem Büro gewohnt. Wir interessieren uns immer für die Unterstützung jeder Linux-Plattform.

h9: Ich bin sehr gespannt, wie Du Dein eigenes privates System und Dein eigenes Handy vor Angriffen schützt...

MH: Nach über 15 Jahren Arbeit in dieser Branche habe ich eine ein bisschen paranoide Einstellung in der Sache der Schutzmaßnahmen und verwende mehrschichtige Schutzmittel. Mein Handy hat ein Antivirenprogramm, ich schliesse auch alle offenen Ports, die für einen Angriff verwendet werden könnten. Auf der Seite meines Rechners benutze ich zwei Hardware-Firewalls – die eine basiert auf einem BSD-System, die andere befindet sich in meinem Router. Auf meinem Laptop benutze ich eine Software-Firewall mit einer Antiviren-Software, die das System in Echtzeit scannt. Wenn es um den Antispam-Schutz geht, verwende ich seit über 10 Jahren eine Email-Adresse, die allgemein bekannt ist. Wie man sich leicht denken kann, bedeutet dies täglich eine Unmenge von Spam. Ich schütze mich davor mit Hilfe von *procmail* auf meinem Unix-Server, der einen großen Teil des Spam entfernt. Nach dem Herunterladen der restlichen Nachrichten verwende ich zwei weitere Filter. Somit empfange ich lediglich 5 bis 10 Spam-Nachrichten pro Tag.

h9: Ich bedanke mich für das Interview, Mikko.

MH: Ich danke auch und begrüße die Leser des *hakin9*-Magazins.