Sparkasse stopft Lücke in ihren Geldautomaten

Die Sparkasse hat bundesweit eine Sicherheitslücke gestopft, die der Mitarbeiter einer Sicherheitsfirma in Geld- und Kontoführungsautomaten der Firma Wincor Nixdorf entdeckt hatte. Wenn die Automaten ein Sicherheitsupdate einspielen, unterbrechen sie die momentan laufende Transaktion und spucken die Karte des Kunden aus. Dann zeigt der Automat auf dem Bildschirm an, dass er temporär nicht benutzbar ist. Wenn man in diesem Moment die Karte mit Druck wieder in den Automaten schiebt, sorgt ein Fehler in der Software dafür, dass das Kommandozeilen-Fenster, in dem das Update läuft, im Vordergrund angezeigt wird.

Bei Kontoführungsautomaten ist eine Tastatur vorhanden, damit Kunden Überweisungen tätigen können. Der Sicherheitsforscher fand heraus, dass diese benutzt werden kann, um in die Kommandozeile eigene Befehle zu tippen – mit Administrator-Rechten. Und selbst ohne solch direkten Zugang enthält der Output des Update-Fensters immer noch eine Menge sensible Informationen wie interne IPs, Nutzernamen und Passwörter aus dem Netz der Bank. Mit diesem Wissen bewaffnet könnte sich ein Angreifer dann Zugang zum LAN der Bank verschaffen und Man-in-the-Middle-Attacken auf die Automaten starten. (fab@ct.de)

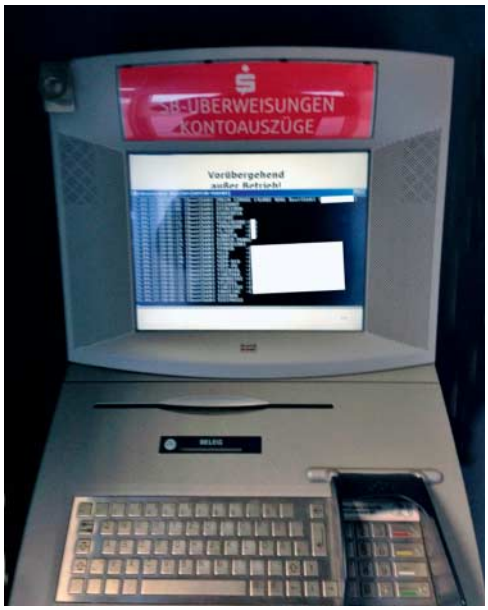

Bild: Evolution Security

Dieser Kontoführungsautomat der Sparkasse führt gerade ein Update aus. Dank der eingebauten Tastatur kann ein Angreifer direkt in die Windows-Kommandozeile tippen.

Verschlüsselungstrojaner Chimera veröffentlicht Daten seiner Opfer

Wer sich den Trojaner Chimera einfängt, der muss damit rechnen, dass die persönlichen Fotos im Netz veröffentlicht werden. Denn genau damit drohen die Erpresser hinter der Ransomware. Wie andere vergleichbare Trojaner verschlüsselt Chimera die privaten Daten auf dem Rechner des Opfers. Zahlt dieses kein Lösegeld (Bitcoins im Wert von umgerechnet etwa 580 Euro), sind die Daten aber nicht nur unzugänglich, sie werden angeblich auch in Zusammenhang mit dem Namen des Opfers im Netz verteilt. Besten Schutz vor solchen und ähnlichen Angriffen bietet ein aktuell gehaltenes Antivirenprogramm und natürlich regelmäßige Backups.

Verschlüsselungstrojaner boomen momentan, da sie ein sehr lukratives und einfach umzusetzendes Geschäftsmodell für Kriminelle darstellen. Diese sparen sich eine umständliche Geldwäsche-Infrastruktur und die Trojaner können aus Kits, die auf dem Schwarzmarkt angeboten werden, einfach zusammengeklickt werden. (fab@ct.de)

TextSecure und RedPhone verschmelzen zu Signal

Der quelloffene Messenger TextSecure verschlüsselt Chats zwischen Android-Geräten Ende-zu-Ende (siehe Test in c't 13/15, S. 144) und ist voll kompatibel zur iOS-App Signal. Die kann seit einiger Zeit auch Gespräche verschlüsseln. Android-Nutzer brauchten bisher die alleinstehende App RedPhone, um diese Gespräche anzunehmen oder selbst untereinander Ende-zu-Ende-verschlüsselt zu telefonieren. Das ist jetzt vorbei, da TextSecure und RedPhone nun zu einer App kombiniert wurden, die ebenfalls Signal heißt. TextSecure-Nutzer, die das Update einspielen, werden mit einer Nachricht begrüßt, die sie auf die Namensänderung hinweist. Nutzer von RedPhone erhalten einen Hinweis, der ihnen empfiehlt, Signal zu installieren.

Sowohl Signal auf Android als auch auf iOS nutzen nach wie vor das eigenständige Verschlüsselungsprotokoll von Open Whisper Systems. Dieses wird von vielen Kryptografen als sehr verlässlich angesehen und kommt mittlerweile auch bei WhatsApp zum Einsatz. Allerdings ist es dort auf fragwürdige Weise umgesetzt (siehe c't 11/15, S. 88). Auch Star-Whistleblower Edward Snowden vertraut der App von Open Whisper Systems. So gab er vor kurzem über Twitter bekannt: „Ich nutze Signal jeden Tag." (fab@ct.de)

TextSecure ist jetzt Signal. Ab sofort sind auch verschlüsselte Anrufe möglich.

Angriffe auf Joomla-Seiten

In den Versionen 3.2 bis 3.4.4 des Content Management Systems Joomla steckt eine Sicherheitslücke, die aktiv von Angreifern missbraucht wird, um Webserver zu kapern. Admins sollten die von ihnen betreuten Systeme unbedingt auf das nicht verwundbare Joomla 3.4.5 aktualisieren. Außerdem sollten Admins sich immer aus Joomla ausloggen, wenn sie das CMS gerade nicht nutzen, da dies Angreifern erschwert, die Session mit Admin-Rechten zu kapern.

Server-Hoster haben schon in der ersten Woche nach Bekanntwerden der Sicherheitslücke massiv Angriffe auf Joomla-Seiten registriert. Der Hoster 1&1 spricht von Hunderttausenden von Angriffen in wenigen Tagen. Es sei offensichtlich, dass Angreifer das Netz gezielt nach verwundbaren Joomla-Versionen abgrasen. (fab@ct.de)

Sicherheits-Notizen

Betrüger, die sich als Support-Mitarbeiter von **1&1** ausgeben, rufen momentan Kunden an und versuchen diesen per Fernwartungssoftware Malware unterzuschieben. Am besten lässt man sich in solche Gespräche gar nicht erst verwickeln und legt auf.

Die Foren-Software **vBulletin** ist in den Versionen 5.1.4 bis 5.1.9 verwundbar gegenüber Angriffen. Ein Update, welches die Lücke stopft, steht auf der Seite der Entwickler bereit.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover