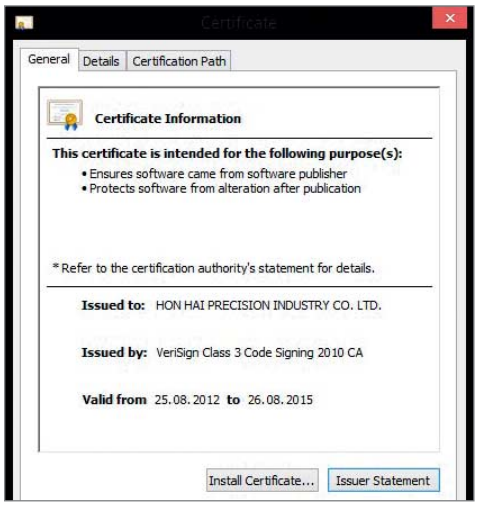
Virus befällt Antivirenfirma

Die Antivirenfirma Kaspersky ist Opfer eines Hacker-Einbruchs geworden. Das Unternehmen hat einen Spionage-Trojaner aufgespürt, der seit Monaten unentdeckt im Firmennetz sein Unwesen trieb. Laut Kaspersky ist ein Mitarbeiter im asiatisch-pazifischen Raum auf eine Trojaner-Mail reingefallen und hat die Schadsoftware im Anhang ausgeführt. Anschließend verbreitete sich der Schädling im Netzwerk. Der Vorfall wurde erst im Frühjahr dieses Jahres entdeckt.

Die Angreifer haben im Zuge der Attacke das Netzwerk unter anderem nach zukünftigen Schutzmechanismen für Betriebssysteme und Informationen über die Untersuchungen von sogenannten Advanced-Persistent-Threat-Hacker-Gruppen (APT) durchforstet. Kasperksy versichert, dass während des Angriffs keine Daten von Kunden erbeutet wurden. Zudem soll die Arbeitsweise der Software des Unternehmens zu keinem Zeitpunkt eingeschränkt gewesen sein.

Den Untersuchungen zufolge ist der Spionage-Trojaner fast identisch aufgebaut wie der Duqu-Wurm, der Ende 2011 etwa Betriebsgeheimnisse aus verschiedenen industriellen Zielen abziehen wollte. Kaspersky vermutet, dass dieselben Angreifer hinter dem Übergriff stecken. Dabei handele es sich wohl um staatliche Akteure, da das Spionage-Werkzeug äußerst komplex aufgebaut ist und viel Geld in der Entwicklung verschlungen hat. Teile der Software hatten sogar eine gültige digitale Signatur des Elektronik-Herstellers Foxconn.

Kaspersky hat russische und britische Sicherheitsbehörden eingeschaltet, um die Aufklärung voranzutreiben. Auch Microsoft wurde informiert, da die Angreifer bisher unbekannte Schwachstellen in Windows als Einfallstor genutzt haben sollen. Microsoft zufolge wurden die Sicherheitslücken im Zuge des Juni-Patchdays geschlossen. (des@ct.de)



Der Super-Trojaner im Netz von Kaspersky hatte eine gültige digitale Signatur.

Sicherheits-Notizen

Der Passwortspeicherdienst **LastPass** wurde gehackt. Der Betreiber rät seinen Nutzern, ihre Master-Passwörter zu ändern.

Die **PHP**-Versionen 5.6.10, 5.5.26 und 5.4.42 schließen Sicherheitslöcher, die sich unter anderem zum Einschleusen von Shell-Befehlen ausnutzen lassen.

OpenSSL ist nach einem Update auf die Version 1.0.2b, 1.0.1n, 1.0.0s oder 0.9.8zg vor Angriffen durch die Logjam-Lücke gefeit.

Vier Sicherheitslücken in **Drupal** 6 und 7 kann ein Angreifer unter anderem zum Kapern des Admin-Kontos missbrauchen. Abhilfe schafft ein Update auf Version 6.36 respektive 7.38.

Firmware-Updates sichern das Web-Interface von 16 **Asus-Routern** vor unbefugten Zugriffen. Näheres erfahren Sie unter dem c't-Link.

Amerikanische Behörden haben die belgische Polizei dabei unterstützt, **WhatsApp** zu belauschen. Dass die USA den Messenger-Dienst anzapfen können, wurde bislang nur spekuliert.

c't Weitere Informationen: ct.de/ypdq

Sicherheitslücke in Samsung-Smartphones

In der vorinstallierten Bildschirmtastatur zahlreicher Samsung-Smartphones klafft eine kritische Sicherheitslücke, durch die Angreifer die Kontrolle übernehmen und Daten abgreifen können. Dies hat die auf mobile Anwendungen spezialisierte Security-Firma NowSecure herausgefunden. Betroffen sind unter anderem die Modelle Galaxy S5 und S6.

Die Lücke steckt in der angepassten Version des SwiftKey Keyboard, die Samsung fest in die Firmware seiner Smartphones integriert. Das Keyboard lädt Zip-Archive aus dem Netz, die normalerweise Updates für die aktiven Sprachpakete enthalten. Da der Download unverschlüsselt über HTTP erfolgt, kann ein Angreifer in der Position des Man-in-the-Middle die Übertragung abfangen und Schadcode injizieren, den das Smartphone anschließend ausführt. Gerade in öffentlichen Netzen wie WLAN-Hotspots sind solche Eingriffe mit geringem Aufwand machbar.

Laut der Sicherheitsfirma sind wahrscheinlich Galaxy S4 Mini, S5 und S6 anfällig. Samsung machte hierzu bislang keine Angaben. Derzeit muss man davon ausgehen, dass alle Modelle betroffen sind, auf denen die Samsung-gebrandete Version der SwiftKey-Tastatur vorinstalliert ist (Samsung IME). Ab dem Galaxy S4 soll eine automatisch verteilte Aktualisierung des Security-Tools Knox die Lücke schließen. Für ältere Geräte will der Hersteller korrigierte Firmware-Images bereitstellen. (rei@ct.de)

Passwortklau durch Sicherheitslücken in iOS und OS X

Bösartigen Apps ist es laut einer Studie von sechs Sicherheitsforschern möglich, vertrauliche Daten anderer Programme einzusehen, im systemeigenen Schlüsselbund gespeicherte Passwörter auszulesen und iCloud-Zugangs-Token abzugreifen. Die Sicherheitslücken betreffen Mac OS X und iOS.

Der Angriffspunkt liegt in verschiedenen Systemdiensten, die Apps zur Kommunikation untereinander nutzen können. Eine Sicherheitslücke im Schlüsselbund von Mac OS X, der systemweit unter anderem Benutzerdaten und Passwörter verwaltet, erlaubt einer App beispielsweise, die von einer anderen App gespeicherten Daten abzufragen. Sie hätten auf diese Weise erfolgreich Zugangsdaten ausgelesen, die die Systemeinstellung „Internetaccounts“ verwaltet; darunter das iCloud-Token zum Zugriff auf Apples Cloud-Dienste. Der Konzern habe sich ein halbes Jahr für einen Patch erbeten und in OS X 10.10.3 sowie der Beta von 10.10.4 erste Schutzmaßnahmen integriert. Diese lassen sich aber offenbar umgehen.

Durch das „Entführen“ von URL-Schemata soll es neben OS X auch unter iOS möglich sein, mit einer in den App Store eingeschleusten App, Passwörter oder Anmelde-Token bei der Kommunikation zwischen anderen Apps einzusehen. Eine im Rahmen der Studie durchgeführte Prüfung von über 1600 Mac-Apps und iOS-Apps habe gezeigt, dass insgesamt mehr als 88 Prozent für mindestens eine der Schwachstellen anfällig sind. Ein Teil der Lücken könne nur auf Systemebene durch Apple behoben werden. Der Hersteller kündigte an, erneut nachzubessern. (lbe@ct.de)