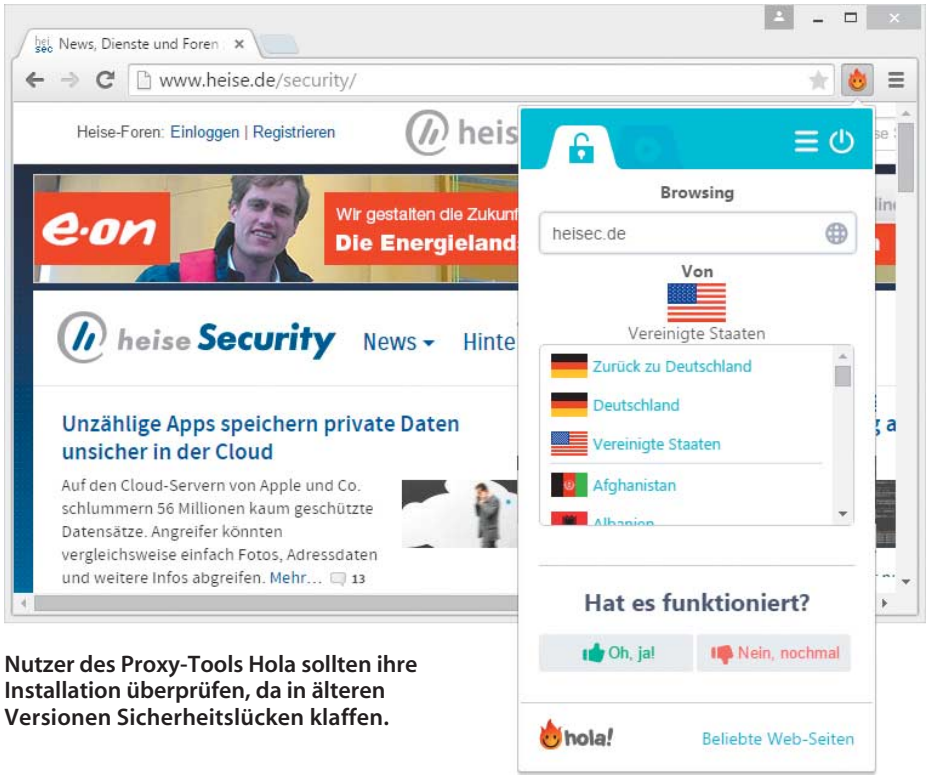
Mehrere Schwachstellen in Proxy-Tool Hola gestopft

Im Proxy-Tool Hola haben Sicherheitslücken geklafft, durch die ein Angreifer Code auf dem Rechner seines Opfers ausführen konnte. Den Entwicklern zufolge wurden die Schwachstellen mittlerweile auf allen Plattformen geschlossen. In Zukunft soll es ein Bug-Bounty-Programm geben, das Sicherheitsforschern einen Finderlohn zusichert, die neu entdeckte Sicherheitslücken an das Unternehmen melden. Wer Hola installiert hat, sollte unmittelbar überprüfen, ob der Client respektive die Browser-Erweiterung auf dem aktuellen Stand (Version 1.7.333) ist. Zudem kann man über eine Testseite sicherstellen, dass der Demo-Angriff tatsächlich vereitelt wird (siehe c't-Link).

Die Entdeckung der Schwachstellen geht auf das Konto von einer Gruppe von Whitehat-Hackern. Denen zufolge startet Hola auf dem Loopback-Interface (127.0.0.1) einen Webserver, der auf Port 6853 lauscht. Mehrere JSON-APIs dienen dazu, auf das Dateisystem zuzugreifen oder auch Programme zu starten. Der Server lieferte diese APIs mit dem HTTP-Header „Access-Control-Allow-Origin: *“ aus. Dies hebelt die sogenannte Same-Origin-Policy aus, die sonst verhindert, dass Code von der Seite evil.com darauf zugreift. Die Webseite des Angreifers konnte deshalb per JavaScript auf den lokalen Server zugreifen, der auf dem Rechner des potenziellen Opfers läuft. Er konnte alle API-Funktionen nutzen, also etwa Programme starten oder Dateien vom Rechner des Nutzers abziehen. Die Hacker demonstrierten dies mit einer Proof-of-Concept-Seite, die unter Windows den Taschenrechner startet. Zudem liest sie drei eindeutige Ziffernfolgen aus, die sich zum Tracking von Hola-Nutzern eignen. (rei@ct.de)

ct Sicherheit von Hola überprüfen: ct.de/yh26



Nutzer des Proxy-Tools Hola sollten ihre Installation überprüfen, da in älteren Versionen Sicherheitslücken klaffen.

Android-Malware stiehlt Geld von Kreditkarten

Eine Malware für Android-Geräte kann den NFC-Sensor missbrauchen, um NFC-Kreditkarten anzuzapfen. Das kann gelingen, wenn sich der Geldbeutel in der benachbarten Hosentasche befindet. Das perfide dabei: Der Zugriff kann aus der Ferne gesteuert werden, wie zwei Sicherheitsforscher erfolgreich vorführten. Die präparierte App müsste sich natürlich erst mal in Google Play schmuggeln, doch so etwas ist schon öfter passiert. Das Smartphone muss für die Installation nicht gerootet sein.

Im Zuge des Angriffs scannt die Malware die Umgebung via NFC. Sobald eine geeignete Kreditkarte in der Nähe ist, bekommt der Angreifer von der Malware eine Nachricht auf sein Smartphone. Anschließend kann dieser mit einem passenden Lesegerät eine Transaktion durchführen. In der Regel könnten Angreifer hierzulande aufgrund der Limits für kontaktloses Zahlen aber nur kleine Beträge bis 25 Euro stehlen. Aktuell sind keine Übergriffe bekannt, die einen solchen Angriff durchführen. (des@ct.de)

Krypto-Trojaner entschuldigt sich und entschlüsselt wieder

Der Erpressungs-Trojaner Locker hat seit Ende Mai auf Windows-Rechnern sein Unwesen getrieben. Den Todesstoß hat ihm nun der mutmaßliche Entwickler selbst versetzt, indem er der Malware befahl, alle verschlüsselten Dateien wieder zu entschlüsseln. Einem Bekennerschreiben zufolge wollte er die Malware eigentlich nie veröffentlichen. Zudem hat er eine Liste aller Schlüsselpaare ins Netz gestellt, die jemals zum Einsatz kamen. Darüber hinaus gibt es ein Tool von einem Nutzer des Computerhilfe-Forums Bleepingcomputer.com, das die verschlüsselten Dateien automatisch wieder lesbar macht (siehe c't-Link). Locker hat in seiner Schaffensphase vor keinem Dateityp haltgemacht und vom Office-Dokument bis zum Zertifikat vieles verschlüsselt. Perfiderweise löschte der Schädling im Anschluss die Schattenkopien auf Laufwerk C. Diese automatisch erzeugten Dateikopien sind für Opfer von Krypto-Trojanern oft der letzte Rettungsanker – insbesondere, wenn kein Backup vorhanden ist (siehe auch „Desinfec't hilf!“ auf Seite 92).

Wer wieder Zugriff auf die Dateien erhalten wollte, musste den zur Entschlüsselung nötigen, individuellen Krypto-Schlüssel innerhalb von drei Tagen beim Entwickler freikaufen. Im Vergleich zu anderen Verschlüsselungs-Trojanern war das Lösegeld mit 0,1 Bitcoin (rund 20 Euro) niedrig angesetzt. Erst nach Ablauf der Frist wurde die geforderte Summe auf 1 Bitcoin erhöht. (rei@ct.de)

ct Tool zum Entschlüsseln: ct.de/yh26

Der Trojaner „Locker“ zeigt Reue und dekodiert alle Dateien wieder.

Facebook setzt auf PGP-Verschlüsselung

Über die neue Funktion „Füge einen öffentlichen Schlüssel hinzu“ können Facebook-Nutzer ab sofort ihren öffentlichen PGP-Schlüssel in den Kontaktinformationen ihres Profils verankern. Dort landet neben dem Schlüssel auch der zugehörige Fingerprint. Anschließend kann man sich auf Wunsch alle Statusnachrichten von Facebook verschlüsselt zusenden lassen. In den Mails findet sich auch die PGP-Signatur von Facebook.

Zudem will das soziale Netzwerk ab Oktober dieses Jahres seine Server auf SHA-2 umstellen, um die Kommunikation im sozialen Netzwerk effizienter vor Manipulation zu schützen. Apps mit schwacher Krypto will der Konzern künftig vor dem Zugriff auf Facebook aussperren.

(rei@ct.de/des@ct.de)

Exploit-Kit nimmt 50 Router-Modelle unter Beschuss

Angreifer nutzen derzeit ein Exploit-Kit, um etwa 50 Router-Modelle zu attackieren. Darunter befinden sich Modelle von Asus, Belkin, D-Link, Edimax, Linksys, Netgear, TP-Link, Trendnet und Zyxel. AVM-Router sollen nicht dazugehören. Da das Exploit-Kit aktiv weiterentwickelt wird, können mittlerweile mehr Modelle betroffen sein. Der c’t-Link führt zu einer vollständigen Liste. An dieser Stelle kann man auch testen, ob der eigene Router kompromittiert ist.

Wie der Virenforscher Kafeine herausgefunden hat, nutzen Angreifer bestimmte Schwachstellen in den Routern aus, um den eingestellten DNS-Server zu manipulieren. So können sie den Internetverkehr ihrer Opfer umleiten. Der Angriff erfolgt, wenn ein Opfer eine verseuchte Webseite besucht. Dabei soll verschlüsselter Java-Code die interne IP-Adresse des Routers und dessen Modell ermitteln. Der maßgeschneiderte Angriff nutze dann Sicherheitslücken aus oder klopft Standardzugangsdaten ab. Gelingt dies, ändert das Kit den im Router eingestellten DNS-Server auf eine IP-Adresse, die unter der Kontrolle der Angreifer steht. Sie können den Datenverkehr ihrer Opfer dann beliebig umleiten und den Router für Phishing- und DDoS-Angriffe missbrauchen.

Schützen kann man sich vor solchen Angriffen, indem man regelmäßig überprüft, ob die Router-Firmware aktuell ist. Sofern der Hersteller den Router mit einem Standardkennwort für das Webinterface ausliefert, sollte man dieses unbedingt ändern, da das Exploit-Kit auch Wörterbuchangriffe durchführt.

(rei@ct.de)

c't Betroffene Router und Test: ct.de/yh26