Darknet und Javascript, reloaded

Das Torprojekt hat zur Verhaftung des Darknet-Providers „Freedom Hosting“ ausführlich Stellung bezogen.

The person, or persons, who run Freedom Hosting are in no way affiliated or connected to The Tor Project, Inc., the organization coordinating the development of the Tor software and research. In the past, adversarial organizations have skipped trying to break Tor hidden services and instead attacked the software running at the server behind the dot onion address. Exploits for PHP, Apache, MySQL, and other software are far more common than exploits for Tor. The current news indicates that someone has exploited the software behind Freedom Hosting. From what is known so far, the breach was used to configure the server in a way that it injects some sort of javascript exploit in the web pages delivered to users. This exploit is used to load a malware payload to infect user’s computers. The malware payload could be trying to exploit potential bugs in Firefox 17 ESR, on which our Tor Browser is based. We’re investigating these bugs and will fix them if we can.

Hier sind die Details.

Auch Heise berichtet „Tor-Nutzer über Firefox-Lücke verfolgt“. „Ältere, zum Tor-Browser-Bundle gehörende Firefox-Browser enthalten eine Javascript-Sicherheitslücke, über die sich Code einschleusen und ausführen lässt. “

Deswegen schreibt meine Lieblings-Torfrau Runa ganz richtig : „Firefox vulnerability was Windows-specific and targeted older versions of the Tor Browser Bundle“.

Wer über Tor surft und Javascript aktiviert hat, kann auch gleich das Schloss vor die Tür nageln. Diese

„Sicherheitslücke“ betrifft nur Leute, die sich um Sicherheit wenig kümmern.

Leserbrief c’t Security II

Lieber Kollege Holger Bleich,

in der aktuellen c’t Security schreiben Sie (S. 11), man solle die „Möglichkeiten der Ermittler“ nicht unterschätzen. So weit, so gut und nachvollziehbar. „Seit 2010 ist bekannt, dass hierzulande auch die sogenannte ‚Quellen-TKÜV‘ zum Einsatz kommt, also das Belauschen von Verdächtigen direkt an ihrem Endgerät. Auf diese Weise haben Behörden bereits verschlüsselte Skype-Telefonate mitgehört und Mails nach der Entschlüsselung am PC abgfangen.“

Gestatten Sie, dass ich „der Kaiser ist nackt!“ rufe. Der Begriff „Quellen-TKÜV“ stammt aus dem Propaganda-Fundus des Innenministeriums und suggeriert, dass Behörden sich ohne Wissen eines Verdächtigen „von fern“ einen Remote-Access-Zugriff auf dessen Rechner verschaffen können. Das ist Unfug, wenn dieser Verdächtige sich einigermaßen vernünftig verhält und zum Beispiel Meldungen wie „cipav.exe is an unknown application. Install anyway?“ ignoriert.

Skype kann abgehört werden. Das Programm kann sogar andere Malware heimlich nachladen. Wer aber das Programm installiert, hat diese Features mit einer freien Willensentscheidung a priori akzeptiert und darf sich über die Folgen dann nicht wundern. Und wie sollen Behörden diese Spionage-Software ohne physikalischen Zugriff auf den (geöffneten!) Rechner installieren können? Dürfte ich auf Ihrem Laptop einfach so Programme installieren? Mir ist nicht bekannt, dass Skype zwangweise installiert werden könnte, ohne dass der Nutzer des

jeweiligen Rechners das mitbekommt.

Thesen wie „Online-Durchsuchung: LKA installiert Spionage-Software bei Flughafenkontrollen“ würde ich gern zunächst auf Fakten überprüfen. Die Behörden können mir also Programme auf meinen Laptop installieren, ohne dass ich das merke? Da wüsste ich doch gern mehr über die Details (Ich nutze Windows und Linux und denke mitnichten daran, die BIOS- und Truecrypt-Passworte auf einem Zettel bei mir zu tragen).

Mails nach der Entschlüsselung am PC abgefangen? Ist Ihnen irgendeine technisch nachvollziehbare Möglichkeit bekannt, gezielt (!) verschlüsselte Mails „von fern“ zu lesen, wenn der Verdächtige KEINE Mal- und Spionagesoftware vorher selbst installiert hat? Ich halte das, mit Verlaub, für eine Verschwörungstheorie, die aber so „sexy“ ist, dass sie gern wiederholt wird. „Seit 2010 ist bekannt“ bedeutet nur, dass das irgendwo in der Zeitung stand. Damit wird es nicht richtig. Die Methode „Stille Post“ ist aber für journalistische Standards kein gültiges Referenzsystem.

Kopie an Jürgen Kuri, der – wie ich – zu der leider nur kleinen Gemeinde der Ungläubigen und Zweifler gehört.

Mit freundlichen Grüßen
Burkhard Schröder
(Autor des Buches „Die Online-Durchsuchung“, Telepolis)

Das Terrorgespenst

„Der konservative [den Namen des Politikers bitte selbst eintragen] malt das Terrorgespenst an die Wand, um die Ausweitung der Schnüffelbefugnisse zu rechtfertigen.“

Welches Land könnte wohl gemeint sein?

Leserbrief c’t Security s. 38ff

Guten Tag,

Sätze wie „einen Virenschutz braucht jeder Windows-Anwender“ (S. 38) regen mich maßlos auf. Wie kann die c’t so etwas drucken? Ich habe noch nie ein Anti-Virenprogramm besessen und plane auch nicht, so etwas auf meinen Rechnern zu erlauben, zumal die Anbieter derartigen „Schlangenöls“ die Frechheit besitzen, mir penetrant bei der Installation zusätzlich Software unterjubeln wollen, z.B. die Datenkrake Google Chrome. Ist das seriöses Geschäftsgebaren?

Software schafft keine Sicherheit, sondern nur vernünftiges Verhalten. Das Problem sitzt immer vor dem Monitor und hat zwei Ohren.

Die Gegner sicherheitsbewussten Verhaltens sind ignorante Webdesigner, die Surfer um jeden Preis zwingen wollen, aktive Inhalte (etwa Javascript) zuzulassen. Sicheres Surfen unterbinden die Geschäftsmodelle fast aller Medien – und „sozialer“ Netzwerke sowieso -, die vom Verkauf der Nutzerdaten leben und nicht nur Myriaden von Cookies implementieren wollen. Mit das größte Problem ist die Unsitte, elektronische Postkarten (E-Mails) unverschlüsselt und ausschließlich in HTML verschicken zu wollen, weil es so chic aussieht und weil es alle machen. Phishing lässt grüßen.

Mit virenfreien Grüßen
Burkhard Schröder

Mastering the Internet

Die Süddeutsche analysiert, welche große Firmen mit den US-amerikanischen Geheimdiensten zusammenarbeiten.
Es ist die Crème de la Crème jener Firmen, die große Teile der weltweiten Internet-Infrastruktur beherrschen. Sie besitzen Unterseekabel, ihnen gehören sogenannte Backbone-Netze – die das Rückgrat des Internets sind – und sie unterhalten riesige Rechenzentren. Mit ihrer (manchmal unfreiwilligen) Hilfe steht den Spähern vom Dienst das gesamte Internet offen. Ein Programm der GCHQ heißt „Mastering the Internet" und das ist kein leerer Slogan: Das Internet beherrschen sie.

Übrigens: Deutschland ist „auf einer Landkarte der NSA als einziges europäisches Land gelb eingefärbt ist – als Indikator für besonders intensive Überwachung."

Noch mal übrigens: Gibt es hier noch irgendjemanden, der E-Mails im Klartext schreibt? Nicht an mich bitte!

Tutorial (für Windows): „E-Mails verschlüsseln in 30 Minuten".

Die Parteien und die Überwachungsgesetze

Daten-Speicherung.de: „Übersicht deutscher Sicherheits- und Überwachungsgesetze, ihres kritischen Inhalts und des Stimmverhaltens der Fraktionen im Deutschen Bundestag".

Deutsche Daten nur für Deutsche

„Die gierigen Datensammler in den USA und Großbritannien haben kein Recht, deutsche Bürger auszuforschen. Die Bundesregierung muss die Menschen vor dem Zugriff fremder Geheimdienste schützen – sie muss jetzt handeln.“ (