Calendar

- 30.01.2014
  OpenChaos im Chaos Computer Club Cologne
- 30.01.2014
  Chaosradio
- 05.02.2014
  C-RaDaR Darmstadt
- 12.02.2014
  Chaosdorf: Themenabend

Chaos Computer Club analysiert Staatstrojaner

2011-10-08 19:00:00, admin

Der Chaos Computer Club (CCC) hat eine eingehende Analyse staatlicher Spionagesoftware vorgenommen. Die untersuchten Trojaner können nicht nur höchst intime Daten ausleiten, sondern bieten auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Schadsoftware. Aufgrund von groben Design- und Implementierungsfehlern entstehen außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen können.

Nicht erst seit das Bundesverfassungsgericht die Pläne zum Einsatz des Bundestrojaners am 27. Februar 2008 durchkreuzte, ist von der unauffälligeren Neusprech-Variante der Spionagesoftware die Rede: von der "Quellen-TKÜ" ("Quellen-Telekommunikationsüberwachung"). Diese "Quellen-TKÜ" darf ausschließlich für das Abhören von Internettelefonie verwendet werden. Dies ist durch technische und rechtliche Maßnahmen sicherzustellen.

Der CCC veröffentlicht nun die extrahierten Binärdateien [0] von behördlicher Schadsoftware, die offenbar für eine "Quellen-TKÜ" benutzt wurde, gemeinsam mit einem Bericht zum Funktionsumfang sowie einer Bewertung der technischen Analyse. [1] Im Rahmen der Analyse wurde vom CCC eine eigene Fernsteuerungssoftware für den Behörden-Trojaner erstellt.

Die Analyse des Behörden-Trojaners weist im als "Quellen-TKÜ" getarnten "Bundestrojaner light" bereitgestellte Funktionen

nach, die über das Abhören von Kommunikation weit hinausgehen und die expliziten Vorgaben des Verfassungsgerichtes verletzen. So kann der Trojaner über das Netz weitere Programme nachladen und ferngesteuert zur Ausführung bringen. Eine Erweiterbarkeit auf die volle Funktionalität des Bundestrojaners – also das Durchsuchen, Schreiben, Lesen sowie Manipulieren von Dateien – ist von Anfang an vorgesehen. Sogar ein digitaler großer Lausch- und Spähangriff ist möglich, indem ferngesteuert auf das Mikrophon, die Kamera und die Tastatur des Computers zugegriffen wird.

Es ist also nicht einmal versucht worden, softwaretechnisch sicherzustellen, daß die Erfassung von Daten strikt auf die Telekommunikation beschränkt bleibt, sondern – im Gegenteil – die heimliche Erweiterung der Funktionalitäten der Computerwanze wurde von vorneherein vorgesehen.

"Damit ist die Behauptung widerlegt, daß in der Praxis eine effektive Trennung von ausschließlicher Telekommunikationsüberwachung und dem großen Schnüffelangriff per Trojaner möglich oder überhaupt erst gewünscht ist", kommentierte ein CCC-Sprecher die Analyseergebnisse. "Unsere Untersuchung offenbart wieder einmal, daß die Ermittlungsbehörden nicht vor einer eklatanten Überschreitung des rechtlichen Rahmens zurückschrecken, wenn ihnen niemand auf die Finger schaut. Hier wurden heimlich Funktionen eingebaut, die einen klaren Rechtsbruch bedeuten: das Nachladen von beliebigem Programmcode durch den Trojaner."

Der Behördentrojaner kann also auf Kommando – unkontrolliert durch den Ermittlungsrichter – Funktionserweiterungen laden, um die Schadsoftware für weitere gewünschte Aufgaben beim Ausforschen des betroffenen informationstechnischen Systems zu benutzen. Dieser Vollzugriff auf den Rechner, auch durch unautorisierte Dritte, kann etwa zum Hinterlegen gefälschten belastenden Materials oder Löschen von Dateien benutzt werden und stellt damit grundsätzlich den Sinn dieser Überwachungsmethode in Frage.

Doch schon die vorkonfigurierten Funktionen des Trojaners ohne nachgeladene Programme sind besorgniserregend. Im Rahmen des Tests hat der CCC eine Gegenstelle für den Trojaner geschrieben, mit deren Hilfe Inhalte des Webbrowsers per Bildschirmfoto ausspioniert werden konnten – inklusive privater Notizen, E-Mails oder Texten in webbasierten Cloud-Diensten.

Die von den Behörden so gern suggerierte strikte Trennung von genehmigt abhörbarer Telekommunikation und der zu schützenden digitalen Intimsphäre existiert in der Praxis nicht. Der Richtervorbehalt kann schon insofern nicht vor einem Eingriff in den privaten Kernbereich schützen, als die Daten unmittelbar aus diesem Bereich der digitalen Intimsphäre erhoben werden.

Der Gesetzgeber ist hier gefordert, dem ausufernden Computerschnüffeln ein Ende zu setzen und endlich unmißverständlich zu formulieren, wie die digitale Intimsphäre juristisch zu definieren und wirksam zu bewahren ist. Leider orientiert sich der Gesetzgeber schon zu lange nicht mehr an den Freiheitswerten und der Frage, wie sie unter digitalen Bedingungen zu schützen sind, sondern läßt sich auf immer neue Forderungen nach technischer Überwachung ein. Daß der Gesetzgeber die Technik nicht einmal mehr überblicken, geschweige denn kontrollieren kann, beweist die vorliegende Analyse der Funktionen der behördlichen Schadsoftware.

Die Analyse offenbarte ferner gravierende Sicherheitslücken, die der Trojaner in infiltrierte Systeme reißt. Die ausgeleiteten Bildschirmfotos und Audio-Daten sind auf inkompetente Art und Weise verschlüsselt, die Kommandos von der Steuersoftware an den Trojaner sind gar vollständig unverschlüssselt. Weder die Kommandos an den Trojaner noch dessen Antworten sind durch irgendeine Form der Authentifizierung oder auch nur Integritätssicherung geschützt. So können nicht nur unbefugte Dritte den Trojaner fernsteuern, sondern bereits nur mäßig begabte Angreifer sich den Behörden gegenüber als eine bestimmte Instanz des Trojaners ausgeben und gefälschte Daten abliefern. Es ist sogar ein Angriff auf die behördliche Infrastruktur denkbar. Von einem entsprechenden Penetrationstest hat der CCC bisher abgesehen.

"Wir waren überrascht und vor allem entsetzt, daß diese Schnüffelsoftware nicht einmal den elementarsten Sicherheitsanforderungen genügt. Es ist für einen beliebigen Angreifer ohne weiteres möglich, die Kontrolle über einen von deutschen Behörden infiltrierten Computer zu übernehmen", kommentierte ein CCC-Sprecher. "Das Sicherheitsniveau dieses Trojaners ist nicht besser, als würde er auf allen infizierten Rechnern die Paßwörter auf '1234' setzen."

Zur Tarnung der Steuerzentrale werden die ausgeleiteten Daten und Kommandos obendrein über einen in den USA angemieteten Server umgelenkt. Die Steuerung der Computerwanze findet also jenseits des Geltungsbereiches des deutschen Rechts statt. Durch die fehlende Kommando-Authentifizierung und die inkompetente Verschlüsselung – der Schlüssel ist in allen dem CCC vorliegenden Staatstrojaner-Varianten gleich – stellt dies ein unkalkulierbares Sicherheitsrisiko dar. Außerdem ist fraglich, wie ein Bürger sein Grundrecht auf wirksamen Rechtsbehelf ausüben kann, sollten die Daten im Ausland verlorengehen.

Gemäß unserer Hackerethik und um eine Enttarnung von laufenden Ermittlungsmaßnahmen auszuschließen, wurde das Bundesinnenministerium rechtzeitig vor dieser Veröffentlichung informiert. So blieb genügend Zeit, die vorhandene Selbstzerstörungsfunktion des Schnüffel-Trojaners zu aktivieren.

Im Streit um das staatliche Infiltrieren von Computern hatten der ehemalige Bundesinnenminister Wolfgang Schäuble und BKA-Chef Jörg Ziercke stets unisono betont, die Bürger müßten sich auf höchstens "eine Handvoll" Einsätze von Staatstrojanern einstellen. Entweder ist nun fast das vollständige Set an staatlichen Computerwanzen in braunen Umschlägen beim CCC eingegangen oder die Wahrheit ist wieder einmal schneller als erwartet von der Überwachungswirklichkeit überholt worden.

Auch die anderen Zusagen der Verantwortlichen haben in der Realität keine Entsprechung gefunden. So hieß es 2008, alle Versionen der "Quellen-TKÜ"-Software würden individuell handgeklöppelt. Der CCC hat nun mehrere verschiedene Versionen des Trojaners vorliegen, die alle denselben hartkodierten kryptographischen Schlüssel benutzen und mitnichten individualisiert sind. Die damals versprochene besonders stringente Qualitätssicherung hat weder hervorgebracht, daß der Schlüssel hartkodiert ist, noch daß nur in eine Richtung verschlüsselt wird oder daß eine Hintertür zum Nachladen von Schadcode existiert. Der CCC hofft inständig, daß dieser Fall nicht repräsentativ für die besonders intensive Qualitätssicherung bei Bundesbehörden ist.

Der CCC fordert: Die heimliche Infiltration von informationstechnischen Systemen durch staatliche Behörden muß beendet werden. Gleichzeitig fordern wir alle Hacker und Technikinteressierten auf, sich an die weitere Analyse der Binaries zu machen und so der blamablen Spähmaßnahme wenigstens etwas Positives abzugewinnen. Wir nehmen weiterhin gern Exemplare des Staatstrojaners entgegen. [5]

Addendum zum Bericht des Chaos Computer Clubs über den Staatstrojaner vom 8. Oktober 2011

Links:

[0] Binaries

[1] Bericht über die Analyse des Staatstrojaners

[4] BigBrotherAwards 2009, Kategorie Business: companies selling internet and phone surveillance technology

[5] 0zapftis (at) ccc.de mit folgendem PGP-Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (Darwin)

mQINBE6OIJYBEADA8V/CA60MHsizwIEk46q3Tw2/DceWdN5jpqr8xD00vhjLMjBx
kFgbZdou6yrYnZbrTC72dQbqj/e0KJaj5gmDjzEb29GKxFRbZkhjMSxYPBb4rawJ
MRQdv/o/Olsf7ucLCEMRjuNxxczpo5dayDZC1yT4P/PcERscOM1RIOkM+Iaqde4v
ApEZavNMrXBlV/s/cQ6gMnzqyzv9dNRaUN8BbNWufWmvue22DUR2kUpsEWYfXBe6
o70k8nxe91uHBDnfjL12n2E7kI79+umniOdXYPQgfzBLTnAgCjHjt+Xy75LOiYXt
ea7KPaGZoe9RuV+gAcK0G+NElDF7PjeuHbsV3YLXuQ7wjmbsn6qjpxl2E6C+vY30
29+4Si7FgwKLlJ/NVrAg90OGEQ13BvPGFUq5rES/ILs31fa7jcIXKaF+ADcMs9o3
ymXQF/wU1ENyUMtLsEz9DZ8yKgLVmLlieVmaiMPaJXSFYyHTccJoJ48QfYQARuMa
OR+bMhW/wWoubIKgj1tL35GF9fJ0hYpwtMG+Xfyi/JG8fJHV8J01sKG5w/UaBAY1
T4quFIHcdMjoRXwtExCsDjyqHRJAakL4WZEjulb3ReGVfuk+pVXTG4Hsp3E8oVKT
v62ahMg7X5ugek232DwUTzfU77sNkcTiuXokPMswbEIfp5zmm9pUhalcnQARAQAB
tDcwIFphcGZ0IElzISBSZXZlcnNlIEVuZ2luZWVyaW5nIElucHV0IDwwemFwZnRp
c0BjY2MuZGU+iQI+BBMBAgAoBQJOjiCWAhsvBQkHhh+ABgsJCAcDAgYVCAIJCgsE
FgIDAQIeAQIXgAAKCRDwbQurk8EwoEHBD/4vkbPzdBw9Ra7IBJCFe6aTUlw4qskU
WM+2hyC06wOWgZM8KiGABFabInJ+2krc+humAuRJoZPySoHyOi/QY9ND033FgkhX
Vea9EJpZRm0tJmbFMlFLzwT9fZ5r7GL0xLrQKoMEK3vUd0b3xQBqeaFEpB+VfU8Q
vKmgTG4dO8pYKVe3/MnjAkS6fUUFOsl9QvHCW8+u2Qn4fl7mUygBTLfK4y2KDruh
rh3EjeSuSaMdkNlXLDyEI5Hxttn0fTDp8K2Sh15qaeR1uMrwtxPHZRuSUw7jZ7xH
24eUjJ4ipnwLMqeTNiL5JBwzQIRp9pb1cjiNuhxUCT4tGBPTeHgPR2MeEbBfFuYJ
JnSEEO8VRStZXWWAKHj1ku8+YQ90SmFloRAbjlrkZpJn+vrj66wyGyzVbe1bD3Gy
jokwVEhcierUaSpUq9ChBIB+vbMQZlchUfIGZPln/WOuwSgo2L6CNTfcA/6FvHYu
+2Mg5VoeHOxQm28ZXjqCsODx3+j476S9VlHIDsBRmqPbOUoEzY2VIAyDzTlQE5Kn
kBGp8FXk68QYVSS+ZI00cLtoDZlDD22scjn6qDk1y6oHuUnP9UoIF8t2kR1j9xG3
FKrSNufwivgkZ3Fr2n+s9jYMom8YfZi15coNntyYSo7WQOgA29Ssfu8dfG56cdUc
WPrcjLfEcjvPMrkCDQROjiCWARAA4dsiBRvVSRN0YFW8iYJNqH0jzu/CwbjsQAOt
N6xM8OrjEsu3y82q0g/NryJJ4cVq3kl4r+WDoCwD2wR+oT4oMmg5jWtrs8lSikaG
6Gl1W8e81zkyvDol8+BQLFEDxyyOZ313rQznP8RsBzk8u8x1YBPNyeHEJMF3dusm
HUgQW2DY/eUUZQJARb9CHp2DTduTlQbkTPeDnFm6lrvduJyee98QeP+nCw9vTok0
uWc5o9p4VgY+koX10E++iFRlz9rwNzFT2vHPm5MeG1ZITbWjS17ZQNHsgbOdMDUk
08zQOYl29N4IuXRD1zRhs96oDwuxlo1rUE7A8vtf/6S6RETxkS7ykH1csCWrw6s/
CjaioVVoyWIEvCzn60P8kUCsLJCiXTE4rcdaY9eysM1jeNC2t7BpmuY6gSqBwM5m
0VfL86mCIZcE0Aaxtrifjjwg8hlnlodyD0Ugi9tO87rPq204wplTMm6iZblKya5a
vzQdKckXOXd4DBSB1fKoZBWAFIuZ2asHa57CsZLXAsM1a1b/eGUIilBN6/bXboum
Gv2q+yF91kEP4tv+5fWLRJOgyUOiljB4g0JN1n9JfnM2iHaX7wcFh+jCnpX+1xZJ
E8urrUEPpt4IOCHB/mJAk2rCrCY69WWJTjuaXIc178TioWDWr+eDuDyENa9pbTCx
5paebg8AEQEAAYkERAQYAQIADwUCTo4glgIbLgUJB4YfgAIpCRDwbQurk8EwoMFd
IAQZAQIABgUCTo4glgAKCRBebJ87j17H3iJID/9UVR9HIxmQtQPADWXZxjnNePw1
32O1+Syd9j9JgYczHooudki6mx55ydFHEyu4oDJ7az0UiV92GEl7XV3iwBppf9Ja
WvZ5WvWMX4F/ZmmDWENXqQeniqIUlKa9XmA9jhYAEwy7198pbD/qsGBMioDVai0f
GTYUiBwHt2spu1uopx30spK/RwBKvbH6cbtGmOvfpXmgsFagtg6kPZPbfGZ3Iumh
yWHP4zd/+VcAOkjJv844Nuloh4VMPfwiInakG9bZzg4Ky5kGqB+Vl2WCZSOiVVGo
C4JmdMO7IMkBPMRNXQw23rhWWJVjsnF+nT/TnDlnH7g067IZ5YOZftwSun78Cjb1
sRmwCaj9iNbTwEUnES8Clni/AAirYvXs0Isu67WN1lJWUSwAavs6Thswhvpnrsq7
v0svvtmOU1pZVmYGmOFn8xAC+iK1PHFL4BH8NEhkiCMqBfH0pGIjl/hZk60r6Gtf
BNB0Fjt/HOQYVHNaQvbpPhWCLYxeVEUfMk9rRE1FlyzYGhBa/pG5ECoJGNQGriGC
bB4hzSmwjVqaP7N3qzfeP6xQT4y5A7Xe2zN9FnOO8+vjQ6hMMX4Ch4YDaxuHS3C7
4eQTgmJ9CWERuUBz/AdEobY+sakH+2PHN2eBgwbLBX5ti3YKy1L7DE3EZibKwWm5
D4C9KHCwUpT/unjQ9gM9EACHIFOBbxZF/2o4w6VdrsYYBUcihaEtDMc9sywNTwBF
jsxbJM4GHvtwlJlunMp1Iz62f9dL+hAUe76UCq2i7W9eVlT8Pp3xR0+z2Ini1PbG
nfgpsbI9q0ncUlGyo+o/fVNASQqqvfGsfU6SuKapwvMdqK6p7G4y+1XodRHChzli
v9WV2GRXNSp5jTuU7FZzCUaHilIU1Xh9P2eo/5/QwTvxkHdEssbCtK6hsWNS/ot9
9IRRB5x3Sr2pnb8JiiZrvwh2YlqaD0cs0gViA5gZXTsOVb6IzcaMgnG4M4xu+fgz
U+G9jHbwWj9UHcEUPEl5rRmrMTpeu5f2xRZddlbDW1QKREATXZkROsP3GLmXMESe
af7BF3+JtUTajYjxQxYwW6hQLkGc4wsIO4nWDFbk/lBh9T25mzTpo54WblDEq9yQ
K83zwI2BC3NFqRoZ9IrC3wJsic5T0/bIKALFXo5quK4pE7xt2+c6VQosymeWBk5q
Exy6jS1C6RjZGF4qXVPznejivZ9jEv4xUh+BXSMKnZCN9SZIzhWU3K6aqacY8LVm
mWE4MA8GJ0dUiw+egWacFBJFRg1I6p1NbuUIlU1WdGne2hyz7djbFofLay15x1Lo
wYTTAi2gmp8vxHoZoI30dCJZTtVKb1vIEOE9Tz5Cl/UOVMxtqANGr9/GdVLPY2NB
ZQ==
=jS/I
-----END PGP PUBLIC KEY BLOCK-----
```

Sponsoren

Tags

- update
- pressemitteilung
- staatstrojaner

Featured

Cancel