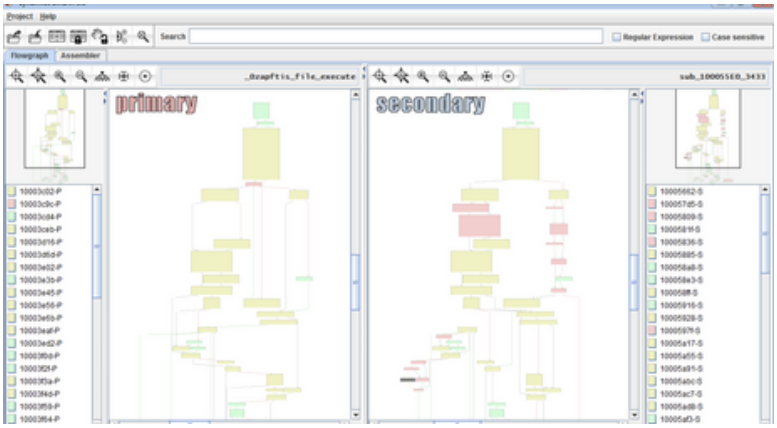
Calendar

- 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 aktuelle Version des Staatstrojaners

2011-10-26 11:00:00, presse

Dem Chaos Computer Club (CCC) wurde jüngst eine noch fast fabrikneue Version des Staatstrojaners zugetragen. Der Vergleich zur älteren, vom CCC bereits analysierten Version mit dem aktuellen Schnüffel-Code vom Dezember 2010 förderte neue Erkenntnisse zutage. Entgegen aller Beteuerungen der Verantwortlichen kann der Trojaner weiterhin gekapert, beliebiger Code nachgeladen und auch die angeblich "revisionssichere Protokollierung" manipuliert werden. Der CCC fordert daher einen vollständigen Verzicht auf Trojanereinsätze in Ermittlungsverfahren.



Am 8. Oktober 2011 veröffentlichte der CCC die Dokumentation und Binärdaten eines deutschen Staatstrojaners. [0] Dieser wurde für verharmlosend "Quellen-Telekommunikationsüberwachung" genannte behördliche Computerinfiltrationen genutzt. Der Einsatz in Ermittlungsverfahren und zur Repression wurde zwischenzeitlich von vielen Bundesländern eingeräumt.

Obwohl der CCC handfeste technische Beweise veröffentlicht hatte, dementierten die Behörden, verantwortliche Innenpolitiker und der Hersteller DigiTask die Existenz illegaler Funktionalitäten [1],[2],[10] und beriefen sich auf eine angeblich veraltete Softwareversion des analysierten Trojaners.

Die Ausflüchte variierten von "Testversion" bis "Prototyp", DigiTask beteuerte noch am 11. Oktober 2011 gegenüber seinen

Behördenkunden, daß fast alle Probleme in neueren Versionen gelöst seien. Die Funktion zum Code-Nachladen wird vom Hersteller DigiTask unisono mit den einsetzenden Behörden als "natürlich notwendig" angesehen, zum darin implizierten Grundrechtsverstoß wird in keiner Weise Stellung bezogen. Gemacht wird, was nutzt, der Zweck heiligt die Mittel.

Der CCC legte daher nun eine weitere detaillierte technische Dokumentation einer neueren Version des Staatstrojaners aus dem Jahre 2010 vor. [3] Die Aussagen von DigiTask in [10] erweisen sich anhand der im Bericht erläuterten Details als beschönigender Versuch, die rechtswidrige technische Realität zu kaschieren. Zeitgleich werden vom CCC kommentierte Disassemblate beider Trojaner-Versionen öffentlich zur Verfügung gestellt, um eine Nachvollziehbarkeit der Erkenntnisse zu gewährleisten und weitere Forschung durch Interessierte zu erleichtern. [4]

"Auch in den letzten drei Jahren waren die Behörden und ihr Dienstleister offensichtlich nicht in der Lage, einen Staatstrojaner zu entwickeln, der auch nur minimalen Anforderungen an Beweiskraft, Grundgesetzkonformität und Sicherheit gegen Manipulation erfüllt", faßte ein CCC-Sprecher die neuen Erkenntnisse zusammen. "Es steht aus prinzipiellen und konkreten Gründen auch nicht zu erwarten, daß dies in Zukunft gelingt."

Die Befunde des neuen CCC-Berichts stehen in scharfem Kontrast zu den Behauptungen des Innenstaatssekretärs Ole Schröder, der offenbar das kürzere Streichholz gezogen hatte und dem Bundestag Rede und Antwort stehen mußte. Dort behauptete er: "Die Software wird für jeden Einzelfall entsprechend konzipiert und vorher überprüft, damit sie eben nicht mehr kann, als sie darf." [8] Die Prüfung kann ausweislich der vorgefundenen Zustände nicht sehr intensiv gewesen sein – wie sollte sie auch, ohne verfügbaren Quellcode.

Der CCC fordert daher:

1. Kein weiterer Einsatz von Trojanern in strafprozessualen Ermittlungen,
2. Sofortige Offenlegung der Quellcodes und aller Prüfprotokolle über vergangene Einsätze von Trojanern durch deutsche Ermittlungsbehörden,
3. Zukünftige automatische Offenlegung von Quellcode, Binary und Protokollen des Trojaners nach jedem Einsatz.
4. Bei einer staatlichen Infiltration eines Rechners muß unwiderruflich die Möglichkeit erlöschen, Daten von der Festplatte des infiltrierten Systems gerichtlich zu verwerten.

"Der Kontrast zwischen den wohlfeil klingenden Beschwichtigungen des BKA-Präsidenten im Innenausschuß und den vorgefundenen technischen Realitäten könnte kaum größer sein", kommentierte ein CCC-Sprecher. "Das DigiTask-Trojaner-Modell 2010 entspricht wie seine Vorgängervarianten in keiner Weise dem Stand der Technik und enthält weiterhin die grundgesetzbrechende Funktion zum Nachladen beliebiger Erweiterungen. Es ist ein 'multifunktionaler Rohling' in einem ganz anderen Sinne."

Die nun analysierte Version 3.6.44 des von der Firma DigiTask entwickelten Trojaners entspricht in ihren Funktionen den Angaben des BKA-Präsidenten Ziercke im Innenausschuß des Bundestages, [1] nach denen inzwischen eine beidseitige Verschlüsselung und weitere Schutzmechanismen implementiert worden seien. Grundsätzlich stellte sich bei der Analyse heraus, daß sich die Trojaner-Version aus dem Jahre 2010 nur punktuell von der älteren Variante unterscheidet.

Wesentliche technische Neuerung des DigiTask-Trojaners Modell 2010 ist die von BKA-Präsident Ziercke betonte bi-direktionale Verschlüsselung, laut DigiTask seit dem 8. Oktober 2009 in Verwendung. [10] Die Analyse zeigt jedoch, daß diese genauso schlecht implementiert und anfällig für Angriffe ist, wie in den zuvor verwendeten Varianten. Der CCC konnte sein selbstgeschriebenes Trojaner-Steuerprogramm in nur wenigen Stunden anpassen, die Schadsoftware weiterhin steuern und Code auf den Opfer-Rechner nachladen.

Selbst DigiTask mochte die schwerwiegenden Manipulationsmöglichkeiten nicht in Abrede stellen. "Dies würde im Umkehrschluss bedeuten, dass die Behörden eigene nicht richterlich zugelassene Funktionen selbst schreiben und auf das ZÜA System laden. Dieser Vorwurf der Manipulation durch eine Sicherheitsbehörde ist technisch möglich, würde aber geloggt werden und mit einem MD5 Hash Wert versehen." (Agovis im Original) Wieso die manipulierende Sicherheitsbehörde dazu die DigiTask-Steuersoftware verwenden sollte, die möglicherweise den Code-Upload loggen könnte, bleibt wohl das Geheimnis des DigiTask-Geschäftsführers Achim Pulverich.

Wie von Herrn Ziercke zu Protokoll gegeben sind die Funktionen zum Anfertigen von Bildschirmfotos nicht mehr direkt aus der staatlichen Fernsteuersoftware heraus zugänglich. Die verfassungswidrige Nachladefunktion steht jedoch weiterhin scheunentorweit offen. Dies bedeutet, daß unbefugten Dritten vom spukhaften Fernlöschen von Dateien bis hin zur akustischen Raumüberwachung genausoviele Möglichkeiten geboten werden, wie den ermittelnden Beamten und ihren von Unkenntnis der technischen Sachlage geplagten Vorgesetzten.

Besonders bemerkenswert ist die Verwendung desselben, bereits mindestens drei Jahre alten und zudem fest eingebauten AES-Schlüssels für die Verschleierung der Datenübertragung. Laut der DigiTask-Stellungnahme ist erst seit dem 2. Juli 2010 überhaupt die Vergabe eines anderen AES-Schlüssels "global für eine Recording Unit" möglich. Eine angeblich neue, aber noch nicht veröffentlichte Version soll nun sogar bahnbrechenden Fortschritt ermöglichen und einen neuen Key pro Infiltrationsmaßnahme ermöglichen. Das dem CCC vorliegende Trojaner-Exemplar vom Dezember 2010 hat jedoch wiederum keinen abweichenden AES-Schlüssel. Kleinere Anpassungen versetzten den CCC innerhalb kürzester Zeit in die Lage, mit Hilfe seines selbstentwickelten Fernsteuer-Werkzeugs auch diesen neueren Trojaner zu kontrollieren, ein Programm hochzuladen und dieses zur Ausführung zu bringen. [5]

Der CCC zeigt zusätzlich zu den bisherigen Erkenntnissen, daß eine sogenannte "revisionssichere Protokollierung" im Falle eines Staats- oder Bundestrojaners nicht effektiv umsetzbar ist. In der Realität der Trojaner-Software kann sogar von unautorisierten Dritten eine Ermittlungsmaßnahme mit fingierten "Beweisen" irregeführt werden. Schon die erste Vorführung einer selbstgebauten Fernsteuer-Software des CCC hat gezeigt, daß ein Trojaner Befehle von unautorisierten Dritten erhalten kann, ohne daß die Behörden davon Notiz nehmen, geschweige denn revisionssicher protokollieren könnten.

Zur Veranschaulichung führte der Club nun eine Software vor, mit Hilfe derer jeder den Ermittlern gefälschte Bildschirmfotos senden kann. Bizarrerweise bestätigt die Herstellerfirma DigiTask in ihrer Stellungnahme diesen Fakt und behauptet allen Ernstes: "Das Unterschieben von falschen Beweisen kann z. B. über eine vorhandene DSL-Überwachung erkannt werden." Daß die DigiTask-Software keine nennenswerten Sicherungsmechanismen gegen einen solchen Angriff aufweist, wird nicht einmal bestritten.

Dahinter steckt der simple Fakt, daß ein Trojaner auf einem unkontrollierbaren System läuft, nämlich dem Computer eines Verdächtigen. Hier ist er potentiell immer unter Kontrolle des Besitzers oder eines weiteren Angreifers. Es ist nicht möglich, einen Trojaner zu entwickeln, den unautorisierte Dritte nicht imitieren könnten. Alles dazu notwendige Wissen steckt schließlich im Trojaner selbst, den man per Definition in dem Moment aus der Hand gibt, wenn man ihn auf dem

Fremdsystem installiert. Hier kann er jederzeit entdeckt und untersucht werden. Mit Trojanern erlangte Erkenntnisse sind daher generell nicht gerichtsfest. Der CCC fordert, diese einfache Erkenntnis zu verinnerlichen und gesetzlich zu verankern.

"Per Trojaner erlangte Beweise dürfen generell nicht vor Gericht verwertet werden. Die Exekutive darf kein rechtsfreier Raum sein", sagte ein CCC-Sprecher.

Ein weiterer wesentlicher Aspekt ist die Inkaufnahme von Risiken für die Betroffenen. Man halte sich das Beispiel des Zollkriminalamts vor Augen, das durch eine Infiltration deutscher Firmencomputer mit nachladefähiger Trojanersoftware etwaigen Wirtschaftsspionen und Konkurrenten die aufwendige Verwanzung ihrer Opfer erspart. Schlimmer noch: Die fahrlässige und schlecht geschützte Durchleitung der gewonnenen Betriebsgeheimnisse durch Netzwerke und Rechenzentren auf ihrem Weg in und durch die USA liefern unzähligen weiteren Parteien einen Zugriff frei Haus – 0zapftis.

Die Verantwortlichen für die Konzeptionierung, den Einsatz und die Überprüfung dieser Trojaner lassen den notwendigen Respekt vor dem Urteil des Bundesverfassungsgerichtes aus dem Jahr 2008 sowie eine ausreichende technische und rechtliche Ausbildung vermissen. Wer solch grundgesetzwidrige Vorgehensweise nach der Maxime 'der Zweck heiligt die Mittel' nicht nur billigt, sondern fortzuführen plant, hat in verantwortlicher Position in einem Rechtsstaat nichts verloren.

Links:

- [0] Die erste Pressemitteilung zum Staatstrojaner
- [1] http://netzpolitik.org/wp-upload/174366-Bericht-BKA-Prasident-Ziercke_TOP-24a-24c_53.-InnenA-Sitzug.pdf
- [2] http://www.bundestag.de/dokumente/protokolle/plenarprotokolle/17132.pdf
- [3] Technischer Report Die hier betrachtete Version des Trojaners stellte sich während der Analyse als identisch mit den an die Antivirus-Industrie über das Portal Virustotal übermittelten Binärdaten vom Dezember 2010 heraus. Virustotal bietet eine Plattform zum Online-Analysieren potentieller Schadsoftware und verteilt diese Dateien an die größten Antivirus- und Betriebssystemhersteller zur Entwicklung von Gegenmaßnahmen. Informationen aus der Antivirus-Indstrie zufolge hat vermutlich der Hersteller DigiTask selbst diese Version zu Virustotal übermittelt, um zu prüfen, ob aktuelle Virenscanner den Trojaner erkennen können.
- [4] kommentierte Disassemblate beider Trojaner-Versionen und die Binaries dazu
- [5] Videos: http://haha.kaputte.li/0zapftis-2_lowres-final.mov
  http://haha.kaputte.li/0zapftis-2_922x578-final.mov (medium resolution)
  http://haha.kaputte.li/0zapftis-2_1230x770-final.mov (high resolution)
- [6] Frank Braun: „0zapftis – (Un)Zulässigkeit von ‚Staatstrojanern'". In: Kommunikation & Recht 11/2011, S. 681-686
- [7] FAQ zum Staatstrojaner
- [8] Plenarprotokoll 17/132 des Deutschen Bundestages, 19. Oktober 2011, S. 15604,
- [9] Ulf Buermeyer, Matthias Bäcker: Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, HRRS
- [10] Dem CCC zugespielte Stellungnahme der Firma DigiTask an ihre Behördenkunden

Tags

- update
- pressemitteilung
- staatstrojaner
- 0zapftis

Featured

Cancel