Staatliche Malware in Deutschland

Colin Benner

12. Februar 2012

Bezeichnungen

- Online-Durchsuchung
- Remote forensic software (RFS)
- Quellen-Telekommunikationsüberwachung
- Bundestrojaner
- Staatstrojaner
- Behördentrojaner
- Computerwanze
- ...

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung
- 11. Dezember 2006: Bundesgerichtshof: keine Rechtsgrundlage für Online-Durchsuchung vorhanden

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung
- 11. Dezember 2006: Bundesgerichtshof: keine Rechtsgrundlage für Online-Durchsuchung vorhanden
- 27. Februar 2007: Bundesverfassungsgericht: nordrhein-westfälisches Verfassungsschutzgesetz verfassungswidrig

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung
- 11. Dezember 2006: Bundesgerichtshof: keine Rechtsgrundlage für Online-Durchsuchung vorhanden
- 27. Februar 2007: Bundesverfassungsgericht: nordrhein-westfälisches Verfassungsschutzgesetz verfassungswidrig
- 25. Dezember 2008: Neufassung des BKA-Gesetzes

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung
- 11. Dezember 2006: Bundesgerichtshof: keine Rechtsgrundlage für Online-Durchsuchung vorhanden
- 27. Februar 2007: Bundesverfassungsgericht: nordrhein-westfälisches Verfassungsschutzgesetz verfassungswidrig
- 25. Dezember 2008: Neufassung des BKA-Gesetzes
- 8. Oktober 2011: Veröffentlichung der Analyse des CCC

Geschichte

- März 2005: Schily erlaubt Verfassungsschutz die Online-Durchsuchung
- Oktober 2006: Schäuble fordert Online-Durchsuchung
- 11. Dezember 2006: Bundesgerichtshof: keine Rechtsgrundlage für Online-Durchsuchung vorhanden
- 27. Februar 2007: Bundesverfassungsgericht: nordrhein-westfälisches Verfassungsschutzgesetz verfassungswidrig
- 25. Dezember 2008: Neufassung des BKA-Gesetzes
- 8. Oktober 2011: Veröffentlichung der Analyse des CCC
- 26. Oktober 2011: Analyse eines neueren Trojaners

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server
- AES-128 im ECB-Modus

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server
- AES-128 im ECB-Modus
- Hartkodierter Schlüssel

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server
- AES-128 im ECB-Modus
- Hartkodierter Schlüssel
- Bei verschiedenen Fällen derselbe

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server
- AES-128 im ECB-Modus
- Hartkodierter Schlüssel
- Bei verschiedenen Fällen derselbe
- Unzulässige Funktion zum Nachladen beliebigen Codes

Technische Analyse des CCC

Analysiert wurde eine Version des Trojaners von 2008

- Keinerlei Authentifizierung
- Verschlüsselung nur vom überwachten Rechner zum Server
- AES-128 im ECB-Modus
- Hartkodierter Schlüssel
- Bei verschiedenen Fällen derselbe
- Unzulässige Funktion zum Nachladen beliebigen Codes
- Screenshot-Funktion

Zweite Version

Analysiert wurde eine Version des Trojaners von 2010

- Verschlüsselung in beiden Richtungen

Zweite Version

Analysiert wurde eine Version des Trojaners von 2010

- Verschlüsselung in beiden Richtungen
- mit gleichem Verfahren

Zweite Version

Analysiert wurde eine Version des Trojaners von 2010

- Verschlüsselung in beiden Richtungen
- mit gleichem Verfahren
- mit gleichem Schlüssel

Zweite Version

Analysiert wurde eine Version des Trojaners von 2010

- Verschlüsselung in beiden Richtungen
- mit gleichem Verfahren
- mit gleichem Schlüssel
- rudimentäre Authentifizierung

Schluss

Fragen? Anmerkungen?