Karl-Friedrich-Gymnasium Mannheim

**ElternMedienMentoren am KFG**

# RATs – die unterschätzte Gefahr im Kinderzimmer

Was sind RATs? Die Abkürzung steht für Remote access trojans. Dabei handelt es sich um Schadsoftware, die in einen Computer eingeschleust wird und dem Hacker eine Fernsteuerung verschiedener Funktionen des infizierten Computers ermöglicht. Besonders beliebt ist die Fernsteuerung der in viele Laptops integrierten Webcam, um so die Wohnung oder die Aktionen einzelner Personen auszuspionieren. Dabei werden Kinderzimmer zu immer beliebteren „Tatorten".

Bereits 2010 konnte man Zeitungsmeldungen lesen wie: „Ein 44-jähriger Mann soll mit manipulierten Webcams Kinderzimmer ausspioniert und sich mehr als drei Millionen Bilddateien verschafft haben. ... Die Aufnahmen zeigen überwiegend Kinder und Jugendliche, die sich an- und ausziehen oder auf ihrem Bett liegen [ ... ]" [1]
oder:
„Images of children's bedrooms and living rooms in the UK are being broadcast on the internet by a Russian website." [2]

Nach einem Bericht des Nachrichtendienstes BBC News „werden Kameras zunehmend ferngesteuert, um in Schlaf- und Kinderzimmer zu blicken. Rund um die gekaperten Kameras floriert mittlerweile ein Schwarzmarkt. [...] Eine erfolgreiche Webcam-Attacke bedeutet für den jeweiligen Hacker bares Geld, denn die Zugänge lassen sich verkaufen.
Halbwegs lukrativ sind jedoch nur Zugänge zu Webcams von Frauen. Wie berichtet wird, gab ein Hacker an, gekaperte Webcams von Frauen für jeweils einen US-Dollar … verkaufen zu können. Die Webcam eines Mannes sei nur ein Hundertstel dessen wert." [3]

Man muss heutzutage kein Profi mehr sein, um derartige Hacks vorzunehmen. Im Internet lassen sich bereits fertige Softwarepakete zu erstaunlich geringem Preis kaufen, was zu einem rasanten Anstieg von Hobby- und gewerbsmäßigen Voyeuren geführt hat.
Auch in Syrien wurden von regierungsfreundlichen Hackern solche RATs zum Ausspionieren rebellischer Aktivisten eingesetzt. Seit 2012 war dafür ein leicht zugänglicher, weit verbreiteter Trojaner namens „Blackshades" im Einsatz.[4]

---

[1] http://www.nordbayern.de/kinderzimmer-mit-webcams-ausspioniert-1.319979
[2] http://news.sky.com/story/webcam-hacking-five-previous-attacks-10381827
[3] http://www.t-online.de/computer/sicherheit/id_64144650/hacker-spaehen-durch-webcams-in-kinderzimmer.html
[4] www.eff.org/deeplinks/2012/07/new-blackshades-malware

2014 konnten die Entwickler von Blackshades festgenommen werden. Nach Angaben des FBI waren bereits über eine halbe Million Computer damit infiziert. Auslöser für die Festnahmen: Ein „Fan“ schleuste die Software in den Computer der „Miss Teen America“ ein und konnte so ihre Webcam kontrollieren, um Hunderte heimlicher Photos von ihr in ihrem Schlafzimmer zu machen. Als er sie über eine E-mail davon in Kenntnis setzte und ihr drohte, einige besonders kompromittierende Photos zu veröffentlichen, falls sie nicht diverse sexuelle Handlungen für ihn vor laufender Kamera vornehme, ließ sich der Teenager nicht einschüchtern, sondern wandte sich an die Polizei. Dieser als „Sextortion“ (engl.: extortion= Erpressung) bezeichneten Form der Erpressung widmen sich auch kriminelle Organisationen auf den Philippinen, die damit bis zu 2000 $ pro Opfer erpressen. Ein 17-jähriger Brite, der Opfer derartiger Erpressung wurde, nahm sich das Leben. Umso mutiger ist die Reaktion der jungen Amerikanerin einzustufen, die zudem zu einer erfolgreichen Maßnahme führte:
Der amerikanischen Polizei gelang es daraufhin in einer großangelegten Aktion, den Täter dingfest zu machen und die weitere Verbreitung des Trojaners zu stoppen.

Schnell erwies sich die Eliminierung dieses Trojaners jedoch als bloßer Scheinsieg: Hacker wurden dadurch animiert, eine zweite Generation solcher Trojaner zu entwickeln, die mehr Vorteile, mehr Möglichkeiten und mehr Funktionen aufwiesen. War nämlich „Blackshades“ nur für Windows konzipiert, so können die neuen RATs nun auch auf Linux- und OS-Betriebssystemen eingesetzt werden.
Außerdem sind sie in der Lage, das Kontroll-Licht der infizierten Webcam auszuschalten, so daß eine Überwachung kaum zu bemerken ist.
Darüber hinaus weisen sie Funktionen auf, die eine vollständige Kontrolle über die infizierten Computer ermöglichen, unter anderem: Keylogger, Screengrabs, Remote-Codeausführung, Webcam-Überwachung, Mikrofon-Recorder, Remote-Verwaltung, Passwort-Stealer, Infostealer, Facebook-Controller und Anti-analysis protections.

Das bedeutet konkret für jugendliche Opfer im Kinderzimmer: nicht nur Aufnahmen mit der Webcam können vom Hacker kontrolliert werden, sondern auch alle eigenen Photos, die auf dem Computer gespeichert sind, können über einen RAT abgerufen und kopiert werden.

## Wie kann ich mich schützen?

**Eine 100%ige Sicherheit gibt es nicht!**
**Aber man kann die Gefahr deutlich eindämmen, indem man den Laptop nach Gebrauch regelmäßig zuklappt; manche Leute überkleben auch ihre Webcam mit dunklem Klebestreifen.**
**Keine kompromittierenden Photos auf dem Computer speichern.**
**Sensible Daten unbedingt verschlüsseln.**
**Ein regelmäßiges Update der Sicherheitssoftware bietet leider keine vollständige Sicherheitsgarantie, da die neue Trojanergeneration auch mit anti-analysis protections ausgestattet ist, kann aber das Risiko deutlich minimieren.**
**Keine E-Mails von dubioser Herkunft öffnen. Ist der Absender nicht eindeutig auszumachen, hilft oft ein einfacher Trick: Drücken Sie auf „Antworten“, um zu sehen, an welche Adresse die Mail geleitet wird. Es gibt auch Add-ons, die den gesamten Mail-header anzeigen (z. B. „Mailsleuth“ bei Thunderbird – über „Extras“ – „Add-ons“ zu finden).**