die GUTEN
die BÖSEN
und die
AHNUNGSLOSEN

G DATA | ADVANCED ANALYTICS

eDAY:16 | Unternehmen Sicherheit

CLUELESS

http://img02.deviantart.net/1c5d/i/2013/262/9/b/the_good_the_bad_and_the_ugly___movie_poster_by_zungam80-d6mwe2c.jpg

GDATA | ADVANCED ANALYTICS


MARION MARSCHALEK
Principal Malware Researcher
GDATA Advanced Analytics
GDATA
ADVANCED
ANALYTICS
http://www.fyqyfz.com/data/uploads/68/519072-western-wallpaper-hd.jpg

Der wilde wilde Westen

G DATA | ADVANCED ANALYTICS

Oder:

Wie zur Hölle kam der wilde Westen in unsere **Wohnzimmer**, **Büros** und an das **Spielzeug**

http://www.freewallpaperfullhd.com/wp-content/uploads/2015/03/wallpapers/cactus_3-wallpaper-1920x1080.jpg

Der wilde wilde Westen

https://upload.wikimedia.org/wikipedia/commons/thumb/3/3a/Natanz_nuclear.jpg/800px-Natanz_nuclear.jpg

http://media.nbcsandiego.com/images/652*367/Hello-Barbie.jpg

https://commons.wikimedia.org

https://pixabay.com/static/uploads/photo/2013/07/13/10/42/router-157597__180.png

https://commons.wikimedia.org

https://www.youtube.com

Router, Heimautomatisierung, Autos, ...

Zahnbürsten, Spielzeuge ...

Voll funktionstüchtige Betriebssysteme

Botnetze auf Routern durch Multi-Plattform Malware

Royale Botnetze

Bots, bots, überall, BOTS!

„IoT ist wie Windows vor 15 Jahren!“

UK Government Used 'Rolling Thunder' DDoS Attacks Against Anonymous, LulzSec and Syrian Electronic Army

By David Gilbert
February 5, 2014 10:59 GMT

A protestor poses in a Guy Fawkes mask in front of police protecting Westminster Abbey as part of Anonymous' Million Mask March. (IBTimes UK)

The UK government's spy wing, GCHQ, has been using distributed denial of service (DDoS) attacks - known as 'Rolling Thunder' - against members of the online hacking collectives such as Anonymous, LulzSec and the Syrian Electronic Army according to leaked documents from Edward Snowden.

The UK government has now been labelled as the first western government to carry out DDoS attacks against its own citizens and faces a lot of criticism for attacking what is seen as free speech.

http://www.ibtimes.co.uk/uk-government-used-rolling-thunder-ddos-attacks-against-anonymous-lulzsec-syrian-electronic-1435186

G DATA ADVANCED ANALYTICS

Ihre Majestät, die Kanonen sind schussbereit!

http://www.webwandtattoo.com/de/img/mag289-png/folder/products-detalle-png/kinderzimmer-wandtattoo-piraten-kanone.png

Die Spionin im Kinderzimmer

SmartBarbie:

- Mikrophon & Lautsprecher
- Spracherkennung auf Knopfdruck
- Wifi Support

When children or other users talk with Hello Barbie by pressing and holding the “Talk” button, **we may capture Recordings** . These Recordings are considered personal information under the Children’s Online Privacy Protection Act (“COPPA”). We **cannot prevent children from providing personal information** when they talk with Hello Barbie, and such information may be captured in the Recordings.

https://www.toytalk.com/hellobarbie/privacy/

Die Spionin im Kinderzimmer

SmartBarbie:

- Mikrophon & Lautsprecher
- Spracherkennung auf Knopfdruck
- Wifi Support

„In Russia,
TV is watching you!“

First known hacker-caused power outage signals troubling escalation

Highly destructive malware creates "destructive events" at 3 Ukrainian substations.

by **Dan Goodin** - Jan 4, 2016 8:36 pm UTC

Share Tweet Email 112

Krzysztof Lasoń

Highly destructive malware that infected at least three regional power authorities in Ukraine led to a power failure that left hundreds of thousands of homes without electricity last week, researchers said.

http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

G DATA ADVANCED ANALYTICS

Black Energy: Malware Kit

Seit ca. 2007 für 700 USD käuflich erwerbbar

Energie, Medien, Telekommunikation & Regierungsinstitutionen

Ukraine seit 2014/15

Stromausfall in der Ukraine

Betriebsspionage

Targeted Attacks

Data Breaches

Advanced Persistent Threats

G DATA ADVANCED ANALYTICS

http://www.howtobeadad.com/wp-content/uploads/2014/12/8-ball-header-575x250.jpg

Staatlich gesponsorte

Betriebsspionage

Kanada, wie sie das Brasilianische Ministerium für Berbbau und Energie ausspionieren

US‘ NSA, wie sie die Brasilianische Petrobras ausspioniert

Frankreich, wie sie IBM und Texasinstruments ausspionieren in den 80ern

Politisch motivierte Malware

Stuxnet und Konsorten

Nämlich:

Duqu 1&2	The Dukes	
Gauss	Turla	
Equation	VolatileCedar	
Babar & AnimalFarm	PawnStorm	
Packrat	Regin	
APT28	Agent.btz	uvw.

Ethische Herausforderungen im APT-Research

ADVANCED ANALYTICS

*"... if the malware is detected, it will also make it **easier for extremists to protect themselves** against cyber spying attempts."*

*" ... the researcher's insight into the operation [...] is always superficial. At first glance, it might appear that the **targeted entity is "innocent"**, such as an academic or a journalist, but in reality they **could be a radical academic or a terrorism-facilitating journalist.**"*

http://www.securityweek.com/long-term-strategy-needed-when-analyzing-apts-researcher

Im Internet sind alle Katzen grau

Citizen Lab 2014: Network Injection Appliances modifizieren Internettraffic direkt beim ISP

HackingTeam und FinFisher:

Lawful Interception

Überwachungssoftware für kleine

Im Internet sind alle Katzen grau

HT: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan

FF: Australia, Austria, Bahrain, Bangladesh, Bulgaria, Canada, the Czech Republic, Eston Germany, Hungary, India, Indonesia, Japan, I Macedonia, Malaysia, Mexico, Mongolia, Neth Pakistan, Panama, Qatar, Romania, Serbia, S South Africa, Turkey, Turkmenistan, the Unite the United States, and Vietnam

https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/
https://citizenlab.org/2013/04/for-their-eyes-only-2/

die GUTEN

http://www.freewallpaperfullhd.com/wp-content/uploads/2015/03/wallpapers/cactus_3-wallpaper-1920x1080.jpg

die BÖSEN

http://www.freewallpaperfullhd.com/wp-content/uploads/2015/03/wallpapers/cactus_3-wallpaper-1920x1080.jpg

die Ahnungslosen

http://www.freewallpaperfullhd.com/wp-content/uploads/2015/03/wallpapers/cactus_3-wallpaper-1920x1080.jpg

MARION MARSCHALEK

marion.marschalek@gdata-adan.de
@pinkflawd

http://www.hqwfz.com/data/uploads/68/510072-western-wallpaper-hd.jpg

Referenzen

Operation „Rolling Thunder“, IBTimes
http://www.ibtimes.co.uk/uk-government-used-rolling-thunder-ddos-attacks-against-anonymous-lulzsec-syrian-electronic-1435186

About Hello Barbie, Mattel
http://hellobarbiefaq.mattel.com/about-hello-barbie/

BlackEnergy, SecureList
https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

Ukraine Power Outage, CNN
http://edition.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/

Russian hackers used Windows bug to target Nato, BBC
http://www.bbc.com/news/technology-29613247

Which countries are we spying on, CBC News
http://www.cbc.ca/news/canada/brazil-canada-espionage-which-countries-are-we-spying-on-1.1930522

US government spied on Brazil‘s Petrobras, Bloomberg
http://www.bloomberg.com/news/articles/2013-09-08/u-s-government-spied-on-brazil-s-petrobras-globo-tv-reports

French said to spy on US computer companies, New York Times
http://www.nytimes.com/1990/11/18/world/french-said-to-spy-on-us-computer-companies.html

Schrodinger‘s cat video and the death of clear text, CitizenLab
https://citizenlab.org/2014/08/cat-video-and-the-death-of-clear-text/

Here are all the sketchy goverment agencies buying HackinTeam‘s spy tech, Motherboard
http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech