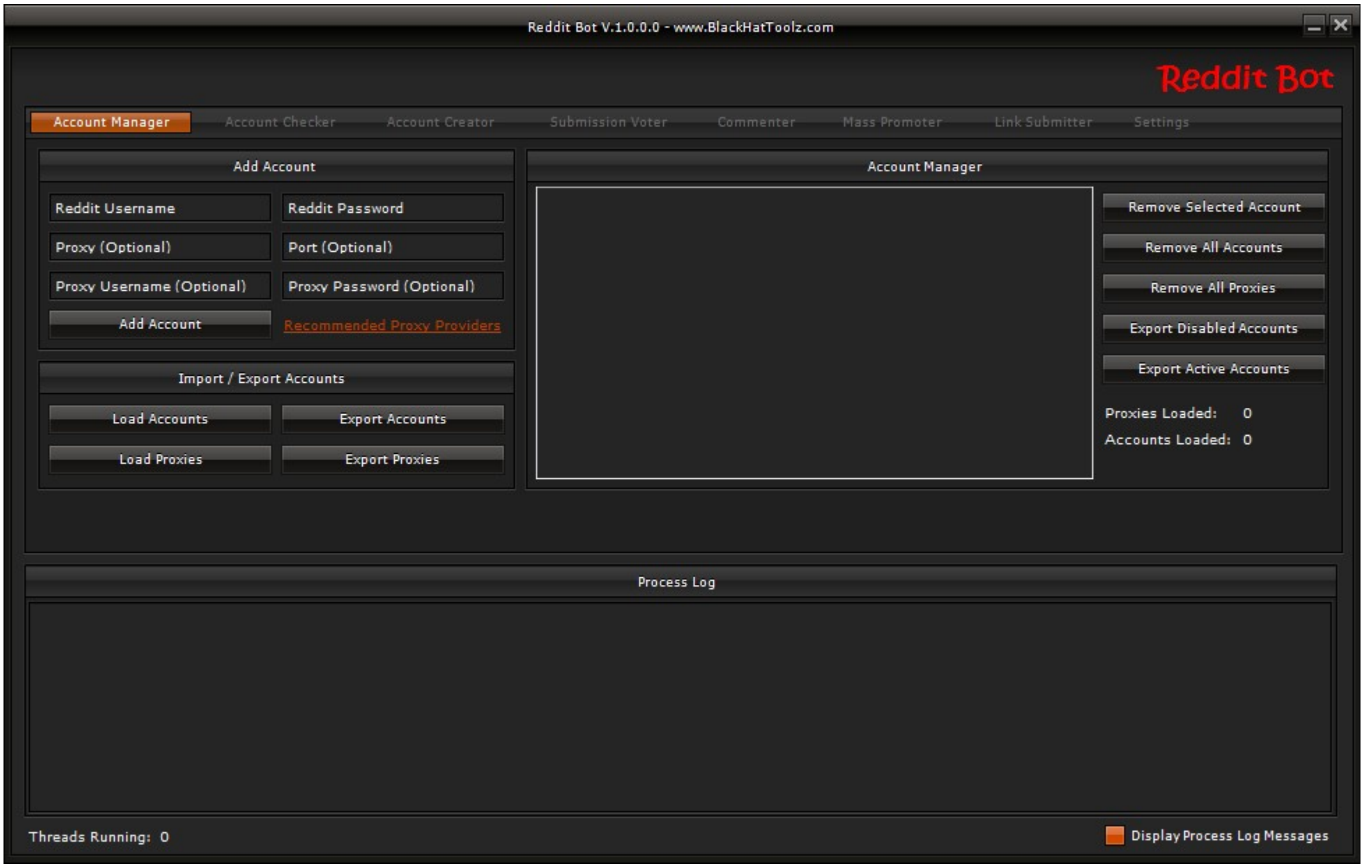
Ideensammlung zur Softwarehaftung

ERIS Assassin • January 18, 2019

https://events.ccc.de/congress/2016/wiki/Session:Eris_Rising Why hack machines, when you can hack people?



Proxies Loaded: 0
Accounts Loaded: 0

Threads Running: 0

A talk postulating a new type of hacker, the 'Eris': a blackhat sociologist who social engineers groups rather than individuals. Certain group ideologies or behaviors allow easy manipulation, and politically active communities like the hacker community will be in the targets in the coming era.

I want to get people talking about the threat of social engineering at the group level. In the internet age COINTELPRO techniques will not only be available to governments, but to anyone skilled in manipulation. This presents serious threats to communities, organizations and, as we've arguably seen recently, democratic systems. Politically active social groups like the hacker community will be especially targeted by nation states and other actors wanting to disrupt or discredit their activity. I believe we are already seeing the appearance of what I call an 'Eris': a professional hacker of social groups. Social media can be used as a laboratory in which to study and experiment with the art of group manipulation, and today's amateur Erises will be selling their skills to the highest bidder tomorrow. This, coupled with a growing corpus of human behavioral studies in the social sciences will see the rise of skilled attackers in an environment where few targets have even begun to think about defence.

I'll be discussing my own experiences in a community that was attacked by a proto-Eris and particularly focusing on what the vulnerabilities are that a skilled manipulator can exploit.

https://telegra.ph/Ideensammlung-zur-Softwarehaftung-01-18

https://www.blackhattoolz.com/redditbot.php Reddit Bot General Features:

```
Bypass API - Acts Like A Browser User
Fully Multi-Threaded - Run Up To 100 Threads Per Instance
Multi-Account Management - Support Unlimited Accounts
HTTP Proxy Compatible - User/Pass Authentication & IP Authentication
Link Proxies To Accounts / Load Proxies Seperately / Reload Proxies From URL Every X Minutes
Built In Proxy Checker - Checks For Valid Proxy Access & Also To Check If Banned From Site
Spintax Compatible - For Use With Commenter & Other Features
Full Process Logging - Reports All Actions - Can Be Disabled
Cookie Usage - Uses Cookies Between Sessions To Prevent Constant Logins
Captcha Support - Supports Manual Entry, De-Captcher & DeathByCaptcha
Built In Spintax Checker
Automatic Updates & Update Checking
```

Reddit Bot Main Features:

```
Account Checker - By Logging In / Check By Profile Page
Account Creator
Link Submitter
Submission Voter - Keyword Based Submission Finder & Vote Up/Down
```

```
Capabilities
Mass Promoter - Mass Vote Up Mode
Mass Promoter - Mass Vote Down Mode
Mass Promoter - Mass Friend Mode
Mass Promoter - Mass Comment Mode
Commenter - Keyword Based Submission Finder
Scheduling Abilities For: Liker, Commenter
Spintax Checker
Proxy Tester
```

Idea collection on software liability

Preparation for the workshop on 28.12.2016 on the 33c3

Thanks to the Internet of Things (IoT), the majority of devices will soon be made from cheapest webcams, light bulbs, toasters, etc., whose firmware is likely to have a number of security vulnerabilities and for which there was never an update path for cost reasons.

Already today we see (https://de.wikipedia.org/wiki/Mirai_(Malware)) that they can become powerful botnets, which represent a major threat to the Internet infrastructure.

From many sides, also from the policy (http://www.deutschlandfunk.de/hacker-angriff-auf-telekom-klingbeil-forderungen-dass.694.de.html?dram:article_id=372593), is demanded, the Manufacturer of faulty equipment more liable.

Such manufacturer's liability, if misused, entails greater collateral damage, which must be prevented in good time.

Now is the right moment to influence the political decision-making process.

The liability risk is likely to be enormous: By Mirai has failed in the episode Twitter for a weekend. That should mean a loss of sales of about 15 million US $.

Who is the manufacturer? Factory? Importer? Logo sticker (Telekom for Speedport)? Retailer (Saturn?) Software Developer (which at OpenSource? All? Author? Committer? Code Review?)? End customer modifying configuration?

Should the (usually not expert) owner of the hardware be liable who bought "too cheap"? Can this pass on the liability risk (guarantee?)?

If the end customer can negatively influence the security by misconfiguration, one must possibly take away the configurability from it. Result: more black boxes

Consequences of a liability for open source? Who would incur a liability risk if they only give away software / development services? Ggf exception for non-commercial (the experience, for example, with imprint obligation shows that one is very (too fast) commercial)? For source-open (by whose definition? RMS? This could also be a gap for the producers, which one wants to meet: Any sources are published and thus one escapes the liability)? Conversely, could this be a promotion for open source?

Is liability in general a barrier to the progress of startups that do not have a strong legal department?

Problem is international, liability outside of Germany but difficult to enforce

Security Certification ("Only proven devices are allowed on the net"): bureaucratic monster, by whom (BSI, TÜV ...)? Bureaucratic, guidelines should not be able to keep up with the progress, meaningful audit should be enormously expensive, otherwise snake oil.

At the time of the Federal Post only permitted devices were allowed to be connected to the telephone network, EDI did not come out of the starting blocks in D or only illegally.

Liability should incentivize manufacturers, regulation by market less bureaucratic than certification.

Complex Quadrilateral Ratio Manufacturer - Owner - Attacker - Victim, who has which interests, who turns to whom? Manufacturers and owners initially only danger or negligence, provide only tools, without attackers no harm.

Which products are we talking about? Demarcation IoT vs computer only gradually. Raspberry Pi, C.H.I.P., ...

"According to the state of the art"

Roughly negligent

Author: Robert Helling (helling@atdotde.de)

Co-writer gladly seen, for write access please send email!

Liability for gross negligence already at Heartbleed: http://www.golem.de/news/sicherheitsluecke-unternehmen-koennen-fuer-schaeden-durch-heartbleed-haftbar-sein-1404-105779.html

My blog post on the topic: https://atdotde.blogspot.de/2016/10/mandatory-liability-for-software-is.html

structure

Twitter -> DynDNS -> Webcams -> Chinese Manufacturer

T-Online -> Speedport -> Mirai gone wild

$ 5 and the fridge has an IP

$ 5 do not include security.

Liability for the responsible / causer of the damage

problems:

Enduser - Conrad - Logo - Importer - Factory - Designer

Many cooks - open source - user misconfiguration - locking in features

certification

Liability insurance

Verbandsklagerecht: Right for certain organizations, regardless of their own damage to warn foreign manufacturers of unsafe software (or similar)