Law Enforcement Hacking Hydra: For Any Answer, Ten New Questions

Yale ISP – 'Law Enforcement Hacking', 18.02.14

@axelarnbak
2013/14 Fellow Berkman Center & CITP
Your computer is infected!

If this Browser has opened automatically then your computer has been infected with malware. Your computer has become part of a bot network.

This message has been sent to you by the High Tech Crime Team of the Dutch National Crime Squad and aims to notify all owners of infected computers.

Dutch National Crime Squad takes down infamous botnet

On October 25th 2010, the High Tech Crime Team of the Dutch National Crime Squad took down a very large botnet, containing at least 30 million infected computer systems worldwide since July 2009. These computers were infected with the malicious Bredolab trojan, through infected websites. Through these botnets, cybercriminals can spread large amounts of other viruses and create new botnets.

In close cooperation with a Dutch hosting provider, The Dutch Forensic Institute (NFI), the internet security company Fox-IT and GOVCERT, the computer emergency response team of the Dutch government, shut down 143 computer servers today.

More information:

For more information about removing Bredolab from your computer, visit:

Technical Aspects

- Botnet: botherder (C&C server), botclients (infected device)
  - Botnet as a platform: botherder rented botnet to other cybercriminals
- Ran on rented servers of legit hosting company LeaseWeb
- Botnet scale exaggerated, unknown to date
  - Not “30 million”, rather 1.5 million infected machines
- No encryption on cookie used for VPN botherder with botclients
- 2 hacks by Dutch police, without basis in criminal law (illegal):
  - 1. C&C server infiltrated, observed 1 month, “shut down” (for TV!)
  - 2. All botclients (!) to install unpublished (!) .exe warning screen
- Hacking across borders: Armenia, 'The Internet'
- Only C&C server shut down, botnet resurfaced within days
  - Setting up new C&C server and taking over the botnet infrastructure
Last week: UTOPIA (good old undercover)
BUNDESTROJANER
German Constitutional Court: 2008 'Online Durchsuchung' Case

- Hacking IT violates core of privacy, personality
  - Beyond 'Communication', Beyond the Home
- IT-systems particularly sensitive
  - IT intertwined with daily life
  - Target structures data for the police: the 'easy way'
  - Networked, 'cloud': third parties & data concentration
- **Human Right to Confidentiality & Integrity IT-Systems**
  - Any Storage Device: PC, Smartphone, MP3 Player
    - Internet of Things: if device 'general purpose' possibility
- Not absolute, but strictest legal criteria

[see: http://www2.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp]
Chaos Computer Club analyzes government malware

2011-10-08 19:00:00, admin

The largest European hacker club, "Chaos Computer Club" (CCC), has reverse engineered and analyzed a "lawful interception" malware program used by German police forces. It has been found in the wild and submitted to the CCC anonymously. The malware can not only siphon away intimate data but also offers a remote control or backdoor functionality for uploading and executing arbitrary other programs. Significant design and implementation flaws make all of the functionality available to anyone on the internet.
Technical Aspects

• False claims about technical aspects
  – “Trojan for 'source wiretap', not 'remote search”
  – “Case-specific: custom made and quality audit”
• But 'upgrade path for remote search' built-in from start
• Similar software, functionality even same cryptographic keys
• Additional serious security issues: commands to trojan unencrypted, intercept data poorly encrypted
  – Evidence highly contentious; burden of proof
  – Man in the middle attack on law enforcement systems
  – Impersonate authorities for hacking
EXPERTS CALL UPON THE VENDORS OF ANTIVIRUS SOFTWARE FOR TRANSPARENCY

An international coalition of more than 25 civil rights organizations and security experts is concerned about the level of security provided by antivirus software companies. "The users of this software should be able to rely on the security of their systems. We fear this might be a false feeling of security," says Ton Siedsma of the Dutch digital rights organization Bits of Freedom.

According to the coalition, these companies have a vital position in providing security and maintaining the trust of internet users engaging in sensitive activities such as electronic banking. There should be no doubt that your antivirus software provides the security needed to maintain this trust.

In the letter, the coalition asks the antivirus companies for transparency on whether there have been any requests by governments to not detect the
Law Enforcement Hacking Hydra: New Questions for Any Answer

- Hacking Tools: obscure, falls claims, never transparent
- Function: Wiretapping, Remote Search, Spillover?
- Scope: Individual, Group or 100,000 Routers?
- 'Cybersecurity': Role AV Companies, Individual OpSec
- Constitutional values up to date: new rights, e.g. Germany?
- Hacking Law: technology neutral, or specify techniques?
- Function Creep: 'Parallel Construction' (NSA?)
- Jurisdiction: 'Citizenship', 'Region', 'Device', 'The Internet' ...
- Pandora's Box: 'We hack Armenia, so Armenia hacks us'?
- Cost-benefit: Do we need this in Surveillance Golden Age?
Law Enforcement Hacking Hydra: For Any Answer, Ten New Questions

@axelarnbak
2013/14 Fellow Berkman Center & CITP