John Chesson
FBI Special Agent
SFBay InfraGard Coordinator

INFRAGARD CYBER INTELLIGENCE BRIEF

Redacted

FBI Intelligence Process Overview

- Sources:
  - Open Source media, blogs, social media
  - FBI investigations and confidential source reporting
- Products:
  - IIR (Initial Intelligence Report) – raw intel
  - Intelligence Bulletin – collection of multiple IIRs
  - Intelligence Assessment - detailed analysis of issue
- Requirements:
  - What don't we know?

InfraGard Secure Portal

Image Removed

Intelligence Product Feedback

Image Removed

InfraGard Message Board

Image Removed

Hacker Groups

- "Anonymous"
  - LulzSec
    - Antisec Movement

Tactics, Techniques, and Procedures

- Anonymous used Internet to:
  - Recruit and Train new personnel
  - Conduct recon on targets
  - Exploit vulnerabilities
  - Deny access to resources
  - Alter information presented to public
  - Steal sensitive data

Recent News

- 19 July 2011, Authorities arrest 16 Anonymous and LulzSec affiliates for computer crimes.

- 9 Aug 2011, Hacker group Anonymous vows to destroy Facebook on 5 Nov 2011

Hacker Group Anonymous Vows To Destroy Facebook On November 5

Ellis Hamburger | Aug. 9, 2011, 12:59 PM | 407,602 | 244

Share 1,394 Tweet 4,371 +1 799 Email AAA

641

Hacktivist group Anonymous, which has been responsible for cyber-attacks on the Pentagon, News Corp, and others, has vowed to destroy Facebook on November 5th (which should ring a bell).

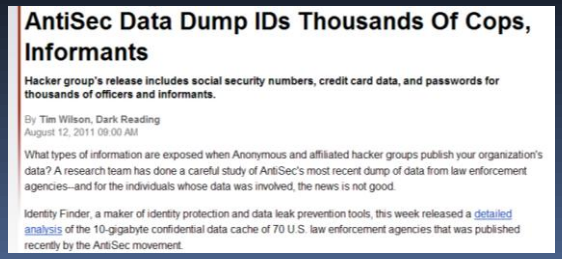
Citing privacy concerns and the difficulty involved in deleting a Facebook account, Anonymous hopes to "kill Facebook," the "medium of communication [we] all so dearly adore."

UPDATE: Anonymous leadership disowned Operation Facebook on

Image: AP

See Also:

- 11 Aug 2011, AntiSec Data Dump IDs Thousands Of Cops, Informants. …includes social security numbers, credit card data, and passwords for thousands of officers and informants.



AntiSec Data Dump IDs Thousands Of Cops, Informants

Hacker group's release includes social security numbers, credit card data, and passwords for thousands of officers and informants.

By Tim Wilson, Dark Reading
August 12, 2011 09:00 AM

What types of information are exposed when Anonymous and affiliated hacker groups publish your organization's data? A research team has done a careful study of AntiSec's most recent dump of data from law enforcement agencies--and for the individuals whose data was involved, the news is not good.

Identity Finder, a maker of identity protection and data leak prevention tools, this week released a detailed analysis of the 10-gigabyte confidential data cache of 70 U.S. law enforcement agencies that was published recently by the AntiSec movement.

Advanced Persistent Threats

- Expected State sponsored actors targeting
  - Businesses with global market advantages
  - US Gov't classified projects
- Suspected State goals
  - Gain competitive edge for global business
  - Steal research and intellectual property
  - Use your trusted relationships to propagate compromises in and outside your company

APT attack vectors

- Spear Phishing attacks has most success
  - Emails to C*, Dir, Scientist, Engineers, HR, Sales, etc…
  - Targets business, home or personal email accounts…
- Target reconnaissance methods
  - Uses social media sites , public conferences, and foreign travel to recon human targets…
- Stolen user credentials
  - Used to access through corporate VPN
  - Used to escalate privileges on your corporate network

APT indicators

- Compromised systems beacon out to Dynamic DNS registered domain
- Exfiltration of data through US domains
- Using commonly open ports for uncommon protocols (like FTP on port 80)
- "Compromised system" attempts recon on multiple systems inside your domain

APT response

- Increase logging and monitoring before any mitigation actions.
  - Place Firewall inline with VPN (for logging)
  - Start logging DNS queries
  - Inspect outbound traffic for anomalies
    - Verify protocol used on common ports
    - Look for spikes in exfiltration of data
- Capture victim system connection state to preserve volatile data.
- Image victim systems (using dd) and collect relevant logs.
- Keep your notes and establish a chain of custody.
- Call FBI as soon as compromise is confirmed.

FBI proactive response

- Consent Monitoring of Victim Computers
  - Active "Computer Trespasser"
  - Non-production system intrusion attempts
- Computer Intrusion Threat Assessment System – pilot project
  - Redirects a single non-production IP address to a Law Enforcement (LE) monitored honeypot
  - Allows LE and participants to correlate network attacks across infrastructure sectors in real-time

Situational Awareness

- National Terrorism Advisory System: http://www.dhs.gov/alerts
- MS-ISAC: http://www.msisac.org/index.cfm
- IT-ISAC: https://www.it-isac.org
- ES-ISAC: http://www.esisac.com/
- FS-ISAC: http://www.fsisac.com/
- US CERT: http://www.us-cert.gov/nav/t01/
- InfraGard members only: URL Redacted

Questions?

John B. Chesson

Special Agent

Federal Bureau of Investigation

San Francisco Division, San Jose Resident Agency

Counter Intelligence Computer Intrusion Squad (CY-4)

(408) 558-1065

john.chesson@ic.fbi.gov

FBI InfraGard Coordinator

San Francisco Bay InfraGard Chapter

www.sfbay-infragard.org