



CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

Internet Crime Complaint Center

Bill Hinerman- Unit Chief

Mission: To conduct analysis and develop referrals for investigative entities on cyber crimes





The screenshot shows the IC3 website interface. At the top, there is a navigation menu with links for Home, File a Complaint, Press Room, About IC3, and Contact Us. The main content area is titled 'Filing a Complaint with the IC3' and contains a paragraph explaining the process, followed by a list of required information: name, mailing address, telephone number, and details of the complaint. A red 'File a Complaint' button is located below the list. On the right side, there is a 'Welcome to the IC3' section with the NW3C logo and a description of the center as a partnership between the FBI and the National White Collar Crime Center. Below this is a 'Site Navigation' menu with links for FAQs, Disclaimer, Privacy Notice, Internet Crime Prevention Tips, Internet Crime Schemes, and Public/Private Alliances. Further down is an 'Alerts' section with a warning icon, and a 'Protect Yourself With The Latest IC3 Consumer Alerts!' banner. At the bottom, there is a 'Flyer/Poster' section with links for Mass Market Fraud, IC3 Flyer, and IC3 Safety Poster.

www.ic3.gov
52,688,925 hits in 2013

All PSAs and Scam Reports are available via Really Simple Syndication (RSS)



Law Enforcement Enterprise Portal



What is the Law Enforcement Enterprise Portal?

The FBI's Law Enforcement Enterprise Portal (LEEP) is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources. These resources will strengthen case development for investigators, enhance information sharing between agencies, and be accessible in one centralized location!

The resources available include:

- Virtual Command Centers
- Nationwide criminal justice records
- Global cyber-complaint data
- Information sharing networks
- Intelligence centers
- Plus many more...

Along with these great resources being in one centralized location, you are also able to gain access by logging in using a single sign-on process. In other words, by using one username and one password, you can obtain access to many different resources and services within the LEEP.

Who Can Access the LEEP?

Any user from a local, state, tribal, and federal law enforcement agency that is an Identity Provider (IdP) to the LEEP.

(An IdP is an agency that partners with the LEEP, which gives their users easier access to the LEEP resources. To become an IdP, send request to leoportal@leo.gov.)

or

Anyone who has a Law Enforcement Online (LEO) account. *(To become a LEO member, go to www.leo.gov.)*

How Do I Access the LEEP?

If your agency is an IdP, simply log onto your agency workstation.

or

If your agency is not an IdP, go to www.leo.gov and use your LEO account username and password.

How LEEP Works:

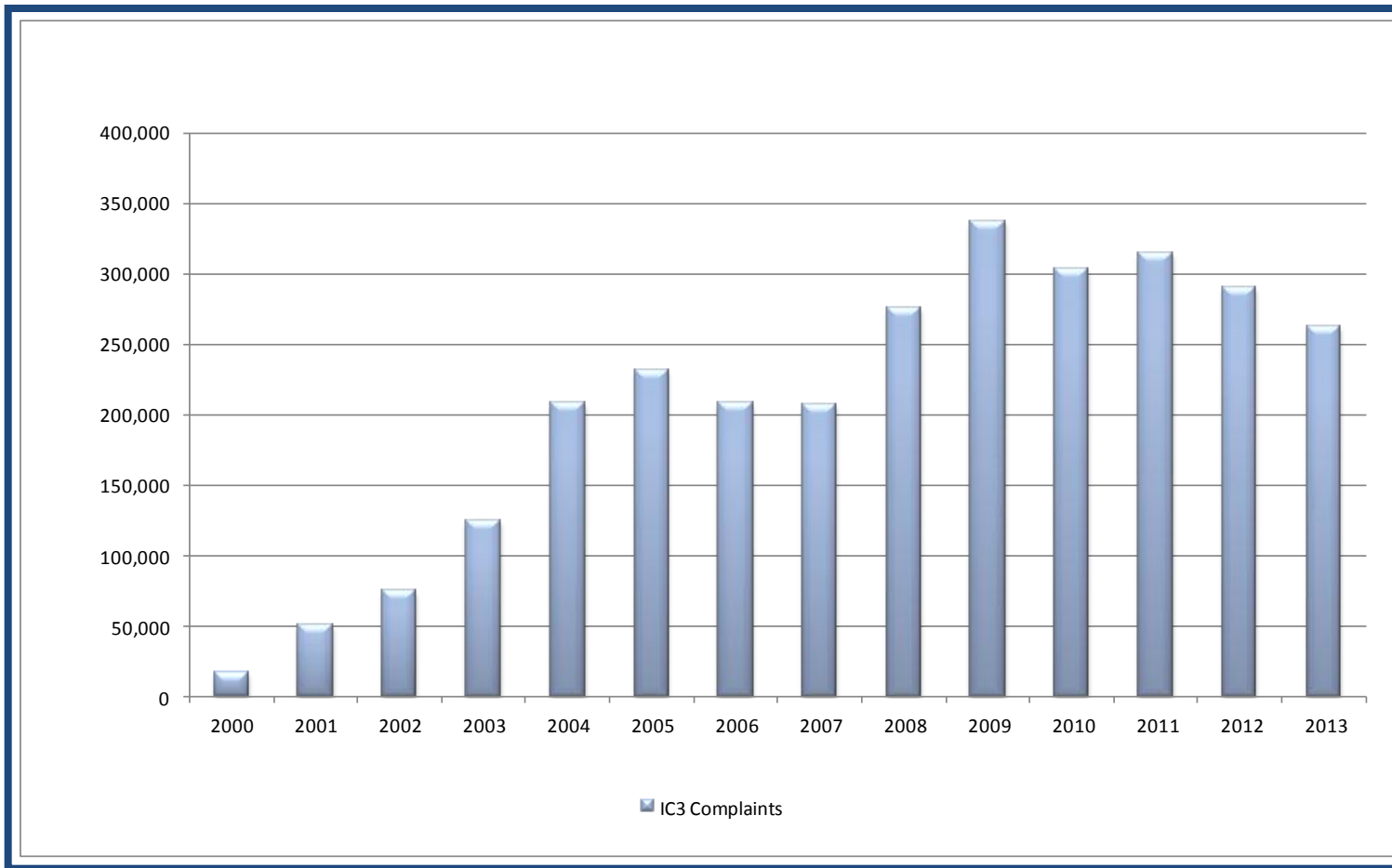




- **Complaints Received: 262,813**
- **Complaints reporting loss: 119,477**
- **Total adjusted loss: \$782,159,556**
- **Average loss overall: \$2,976**
- **Average loss for those reporting loss: \$6,547**



IC3 Complaints Received Annually



Crimes Reported to the IC3



Urgent/Violent

Fraud

Terrorism

Identity Theft

Hacking/Intrusion

Intellectual Property

Phishing/Spam

Stalking/Harassment

Presidential Threats

Child Exploitation





The screenshot shows the website's header with the logo and navigation menu. The main content area features a 'Welcome' message, a cartoon illustration of a man with a wheelbarrow full of money, and a search bar. Below the search bar is a 'Click for Our Fraud Risk Test' button. A red banner for 'FBI Scam Alerts!' is visible, along with a 'FakeChecks.org' logo. The left sidebar contains a list of links including 'Types of Fraud', 'Victim Stories', 'FAQs / Tips', 'Share Your Experience', 'Privacy Policy', 'Site Map', 'Action Center', 'Consumer Alert!', 'Spotlight Company', and 'Teen Center'.

Launched in October 2005, a joint effort between law enforcement and industry designed to protect consumers against Internet crimes.

Remember, if it looks too good to be true, it probably is!





- **Access to consumer complaint database**
- **Research open and closed Internet sources**
- **Analyze and organize case data**
- **Liaise with numerous industry contacts**
- **Coordinate investigative effort**
- **Continually update ongoing investigations**
- **Send case referrals to state, local, and federal law enforcement**



IC3 Dissemination of Intelligence



The Internet Crime Complaint Center's (IC3) August 2013 Trend Analysis and Intelligence Brief



Tactical Intelligence:

MICROSOFT SUPPORT SCAM NOW USING THE IC3

The IC3 has produced Scam Alerts in the past advising the public of an ongoing telephone scam in which callers purport to be an employee of a major software company. The callers speak with very strong accents, which most complainants described as Indian, and report the user's computers are sending error messages and a virus has been detected.



Monthly Trend Analysis: Disseminated to Legats, InfraGard, LEO, and Cyber coordinators in FBI Field Offices



Intelligence Note Prepared by the Internet Crime Complaint Center (IC3) September 18, 2013



BETA BOT MALWARE BLOCKS USERS ANTI-VIRUS PROGRAMS

The FBI is aware of a new type of malware known as Beta Bot. Cyber criminals use Beta Bot to target financial institutions, e-commerce sites, online payment platforms, and social networking sites. Beta Bot blocks programs, leaving

Beta Bot infects message box na "Windows Comm with the request, spread via USB t websites.



To view PSAs, you may visit www.ic3.gov, www.fbi.gov, and/or www.lookstoogoodtobetrue.com



Internet Crime Complaint Center's (IC3) Scam Alerts July 13, 2013]

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

SPAM CONTINUING TO CAPIT

The IC3 continues to receive rep fraud schemes. Although there a typically notified that they are t use the name of James Conroy.

The IC3 has posted multiple PS/ FBI's name. Some messages ca <http://www.ic3.gov/media/2013/11/>

DHS NOTES RISE IN BRUTE-F

SCMagazine featured the follo

A subgroup of the U.S. Departm has increasingly been targeted b Hackers using some 50 IP addre to natural gas companies, accor Cyber Emergency Response Te

The campaign leveraged brute-f or characters to gain access - a gas compressor stations, from F however

The newsletter also said that bet incidents targeting the critical inf against energy companies.

In most cases, attackers used w their targets, as well as SQL inje - victims to click malicious links or

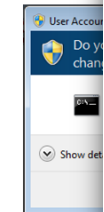


Figure 1, Beta B

Although Beta B perform modifia appears on your system's config changes.

Remediation str date anti-virus software on the infected computer, download the latest anti-virus updates or a whole computer, save it to a USB drive and load and run to subsequently re-format the USB drive to remov

"blogs.rsa.com; nbnews.com

If you have been a victim of an internet scam or was an attempted scam, please file a complaint at




To view Scam Alerts, you may visit www.ic3.gov



Internet Crime Complaint Center Report (IC3R)

Unclassified/Law Enforcement Sensitive



Internet Crime Complaint Center

Internet Crime Complaint Center Report:
IC3R Number:
of Complaints:
Total Reported Loss:

IC3 MISSION STATEMENT

The IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local, and international level, the IC3 provides a central referral mechanism for complaints involving internet-related crimes.





Questions, Comments?

Bill Hinerman

Unit Chief

Internet Crime Complaint Center

