TRENDS

The 2017 Internet Crime Report highlights the IC3's efforts over the past year, specifically focusing on their efforts regarding Business Email Compromise (BEC) and Email Account Compromise (EAC) scams and the Operation Wellspring Initiative (OWS).

Business Email Compromise :

Business Email Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The Email Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments. The IC3 received 15,690 BEC complaints in 2017 with losses over $675 million.

Ransomware:

A form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through spear fishing emails to end users. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of ransom, at which time the actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a preventive measure. The IC3 received 1,783 Ransomware complaints in 2017 with losses over $2.3 million.

2017 STATISTICS

$1,418,732,316
- Losses Reported

301,580
- Complaints Received

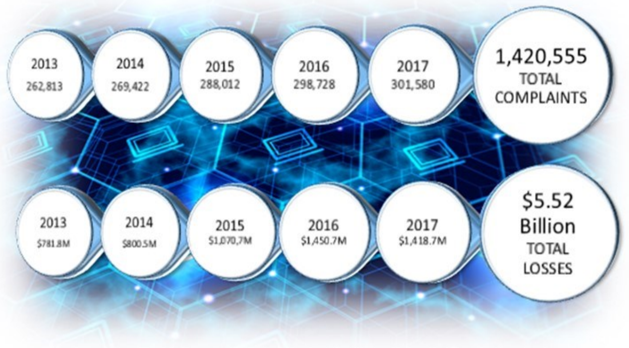
133,608
- Complaints Received that Reported Losses

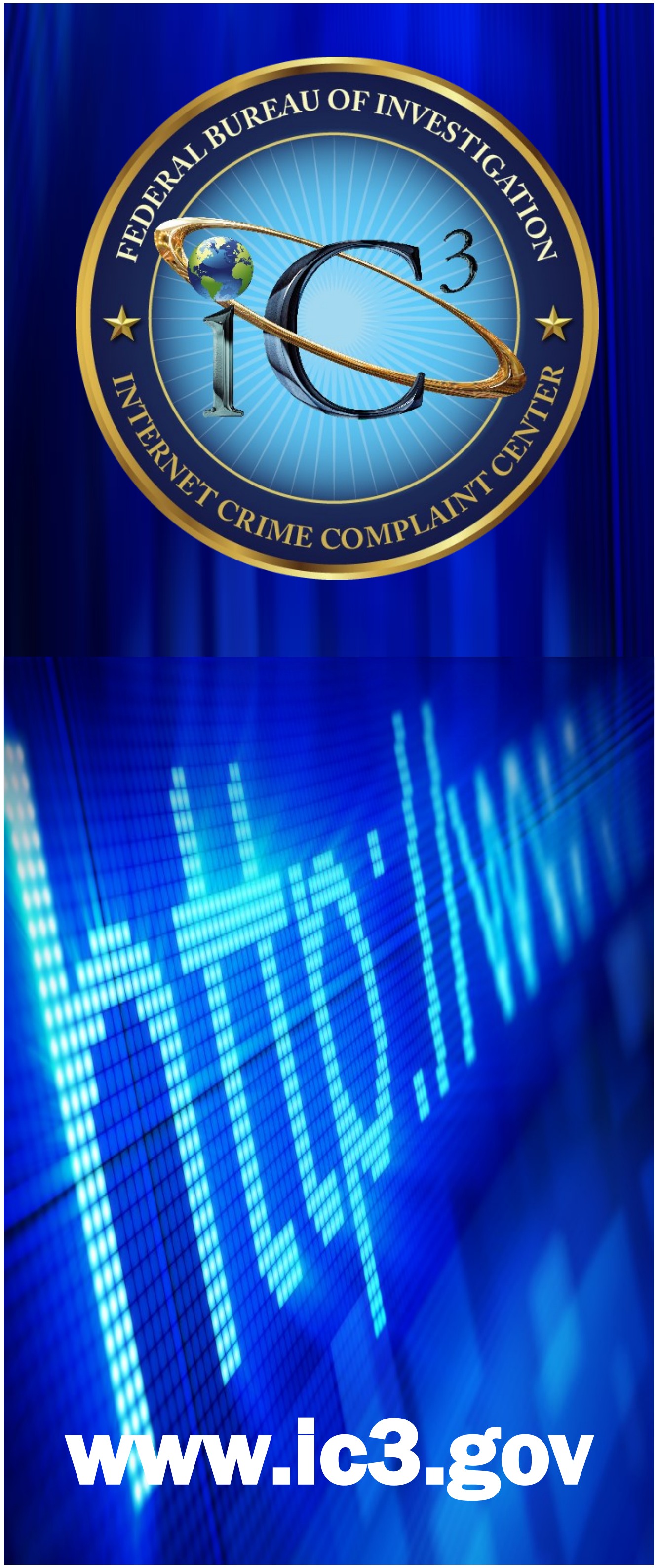
$10,619
- Average Loss For Complaints That Reported Losses

$4,704
- Average Loss For All Complaints

$681
- Median Loss

Five-Year Review:
(Complaints and Losses Reported to the IC3)




FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

www.ic3.gov

AN INVESTIGATIVE LOOK INTO THE IC3

Mission of the IC3:

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

Operation Wellspring:

The Operation Wellspring (OWS) Initiative launched in August 2013 with the Salt Lake City FBI Cyber Task Force (CTF), in partnership with the Utah Department of Public Safety, and has expanded to multiple offices across the nation. OWS serves as a national platform to receive, develop, and address Internet-facilitated criminal cases, and through collaboration builds the Internet investigative capability and capacity of the state and local law enforcement community.

Internet Crime and the IC3:

As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of Internet crime through its complaint system.

IC3 Complaints:

The complaints submitted to the IC3 cover an array of Internet crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Searching the IC3 Database:

A remote search capability of the IC3 database is available to all sworn law enforcement through the FBI's Law Enforcement Enterprise Portal (LEEP). Users can connect directly to the IC3 Complaint Search after authenticating through LEEP from the user's Identity Provider (IDP) or through the user's Law Enforcement Online membership at www.cjis.gov. Users may also contact the IC3 for analytical assistance.

IC3 users have the ability to gather complaint statistics by city, state, county, and country and sort by crime type, and age. Users can also run overall crime type reports and sort by city, state, and country. The report results can be returned as a PDF or exported to Excel. This search capability allows users to better understand the scope of cyber crime in their area of jurisdiction and enhance case development.

Public Service Announcements:

The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends. Public service announcements (PSAs) and other publications outlining specific scams are posted to the www.ic3.gov website.