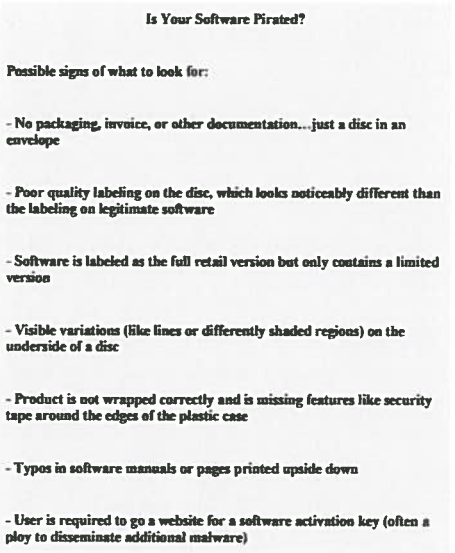
Intelligence Note
Prepared by the
***Internet Crime Complaint Center* (IC3)**
August 7, 2013

Consumer Alert: Pirated Software May Contain Malware

You decide to order some software from an unknown online seller. The price is so low you just can't pass it up. What could go wrong?

Plenty. Whether you're downloading it or buying a physical disc, the odds are good that the product is pirated and laced with malicious software, or malware.

Today, the National Intellectual Property Rights Coordination (IPR) Center—of which the FBI is a key partner—is warning the American people about the real possibility that illegally copied software, including counterfeit products made to look authentic, could contain malware.



Our collective experience has shown this to be true, both through the complaints we've received and through our investigations. It's also been validated by industry studies, which show that an increasing amount of software installed on computers around the world—including in the U.S.—is pirated and that this software often contains malware.

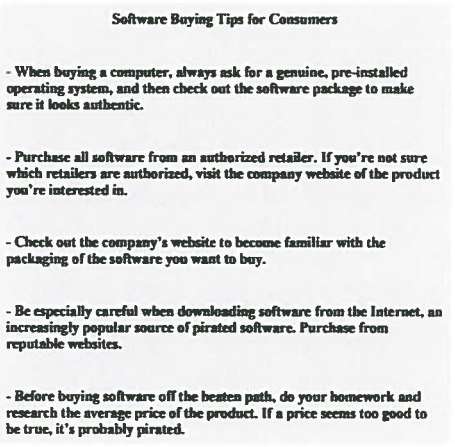
As in our above scenario, pirated software can be obtained from unknown sellers and even from peer-to-peer networks. The physical discs can be purchased from online auction sites, less-than-reputable websites, and sometimes from street vendors and kiosks. Pirated software can also be found pre-installed on computers overseas, which are ordered by consumers online and then shipped into the United States.

Who's behind this crime? Criminals, hackers and hacker groups, and even organized crime rings.

And the risks to unsuspecting consumers? For starters, the inferior and infected software may not work properly. Your operating system may slow down and fail to receive critical security updates.

But the greater danger comes from potential exposure to criminal activity—like identity theft and financial fraud—after malware takes hold of your system.

Some very real dangers:



- Once installed on a computer, malware can record your keystrokes (capturing sensitive usernames and passwords) and steal your personally identifiable information (including Social Security numbers and birthdates), sending it straight back to criminals and hackers. It can also corrupt the data on your computer and even turn on your webcam and/or microphone.
- Malware can spread to other computers through removable media like thumb drives and through e-mails you send to your family, friends, and professional contacts. It can be spread through shared connections to a home, business, or even government network. Criminals can also use infected computers to launch attacks against other computers or against websites via denial of service attacks.

To guard against malware and other threats, read our tips on how to protect your computer. If you think you may have purchased pirated software (see sidebar on how to spot it), or if you have information about sellers of pirated software, submit a tip to the IPR Center or the Internet Crime Complaint Center.

And know this: Pirated software is just one of the many threats that the IPR Center and the FBI are combating every year. The theft of U.S. intellectual property—the creative genius of the American people as expressed through everything from proprietary products and trade secrets to movies and music—takes a terrible toll on the nation. It poses significant (and sometimes life-threatening) risks to ordinary consumers, robs businesses of billions of dollars, and takes away jobs and tax revenue.

Learn more by visiting the IPR Center website and the FBI's Intellectual Property Theft webpage.

FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000023-BT

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

(U) The FBI is providing the following information with **high confidence**:

SUMMARY

(U) Since September 2012, US financial institutions have been under coordinated and timed DDoS attacks. In total, 50 U.S. financial institutions have been targeted in over 350 separate DDoS attacks with varying effects. The botnets used in the attacks, identified as "Brobot" and "Kamikaze/Toxin" consist of compromised high bandwidth webservers with vulnerable content management systems. The compromised bots are infected through a vulnerable customer account. Once the customer account is accessed, attack scripts are uploaded to a hidden directory on the customer web site.

TECHNICAL DETAILS

(U) The FBI is providing 3,375 URLs (546 CONUS and 2,829 OCONUS), which have been observed receiving status updates or have participated in previous attacks. These URLs are located within the United States and worldwide. The FBI is distributing these indicators to enable network defense activities and reduce the risk of similar attacks in the future. The FBI has **high confidence** that these indicators were involved in past DDoS attacks or will be used in future attacks. The FBI recommends that your organization help victims identify and remove the malicious code.

(U) Attached to this document are two Excel spreadsheets that contain indicators including the full paths of the attacking or uploader scripts, IP addresses, last seen date, city, state, country and ISP information.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or
FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937

InfraGard
a collaboration for
infrastructure protection

INFRAGARD
MEMBERS ALLIANCE

November 26, 2013

Dear InfraGard Member,

With 84 InfraGard Members Alliances and nearly 20,000 members actively registered on the InfraGard network, providing for the growing communication needs of a nationally dispersed organization presents a tremendous challenge. While new liaison roles, including those of FBI Regional Coordinator and Sector Chief, have already proven their value in expediting information through human channels, additional support is needed in order to guide the accompanying increase in communication traffic.

InfraGard's secure network provides a robust platform for information sharing, and has recently undergone a number of upgrades in order to allow FBI and INMA leadership to furnish the on-time email messaging and intelligence reports that lend membership much of its value. The network now supports secure, high priority messaging (FLASH) from InfraGard Headquarters to Coordinators, Presidents and members. Relevant intelligence products are also being processed and uploaded to the site far more rapidly than they have been prior, increasing their impact for members.

A redesign of public and member web interfaces for improved content, navigation, and usability will be deployed near the end of the 2013 calendar year, including a customizable home page for all current members. The iGuardian reporting tool will continue to be provided as a central resource by which members may submit cyber incidents directly to the FBI. Members will be required to register on the new site in order to view intelligence products and assets, and must log in and change passwords every 90 days in order to maintain site access and active member status.

At every level, seamless communication between InfraGard management and members is a priority and is key to preparedness and threat awareness. We are working to create an information rich environment—locally and online— that offers mutual benefit and encourages frequent engagement between government and private sector subject matter experts.

Sincerest regards,

FBI Cyber Division
Joseph M. Demarest
Assistant Director

Kenneth V. Jones, Chief
National Industry Partnership Unit

INMA
David Pekoske
Chairman of the Board

Sheri Donahue
President

NCRIC | Northern California Regional Intelligence Center

Fusing Information, Talent And Training For A Safer Society.

Summary for California State Lottery Commissioner Meeting 9/26/2013 for NCRIC AOR

24 October 2013

(U) SCOPE: The summary reflects all reported suspicious activity reports (SARs) related to the request, as well as an open source search and search of available intelligence databases. It is important to remember that in most cases SARs are raw reports that principally reflect the interpretation of the reporting party. Incidents rated Minimal or No Nexus lacked credible indications of threat activity. Incidents that presented possible pre-incident indicators consistent with current threat models are rated Elevated or higher, but even these incidents should not be interpreted as confirming threat presence, interest or activity. All SARs rated Elevated or higher have been referred to the FBI JTTF for assessment; any incidents that the FBI determined had a potential nexus to terrorism will be noted below. Please visit ncric.org for more information on SARs.

(U//FOUO) The NCRIC conducted a search of local suspicious activity reporting within the last year on the California State Lottery commissioners within the NCRIC AOR: Sheriff Greg Ahern and Phil Tagami of Alameda.

(U//FOUO) The NCRIC has no reporting indicating a current threat related to the California Commissioners Ahern or Tagami, or to the California State Lottery Commissioners meeting.

(U//FOUO) For situational awareness, the related Suspicious Activity Reports provided to the NCRIC within the past year are listed below. These are the same SARs reported last month; there are no new incidents. The reports involve sovereign citizen documents mailed to Sheriff Ahern's office. All of the reports were provided to the NCRIC from the Alameda County Sheriff's Office. The reports were originally rated as *Preliminary* by the NCRIC.

PRELIMINARY

- **(U//FOUO) Sovereign citizen type letter received by Alameda County Sheriff's Office** (09/04/13, Alameda County Sheriff's Office) The ACSO received a letter directed to the President and Vice President of the United States along with other state and federal officials as well as "Sheriffs of all California Counties." The letter contained information claiming to invoke various Indian Trade and Reorganization Acts from as far back as 1790. The letter also urges California homeowners to discourage and stop "illegal foreclosures and unlawful evictions by evidencing and proving good and superior titles issued by the Washitaw Empire under Usucapion." ***Usucapion is defined as the acquisition of property through long, undisturbed possession. The rhetoric is similar to that of the sovereign citizen movement and Moorish nation ideology.***[1]

UNCLASSIFIED

SPARTAN SAR RATINGS

ACTIONABLE: Activity consistent with terrorist operational preparations that strongly suggests convergence with specific, credible threat reporting.

ELEVATED: Unusual behavior or activity - consistent with terrorism indicators - that does not fit typical patterns for the venue and lacks a legitimate explanation.

PRELIMINARY: Ordinary behavior or activity - including routine criminal activity that witness interpreted as possibly consistent with terrorism indicators. Nexus indeterminate.

CRIMINAL: Observed activity, consistent with known crime trends, that presents no indications of a nexus to terrorism.

NO NEXUS: Incident resolved as not terrorism- or crime-related.

OFFICER SAFETY | UPDATED ITEM

DISPOSITION OF RATED SARs

SARs rated ELEVATED or higher are referred for FBI investigation; SARs rated PRELIMINARY may be entered into eGuardian for information only. SARs rated CRIMINAL are referred to the appropriate local agency.

URGENT THREAT INFORMATION?
Call the FBI-JTTF at (415) 553-7400

SUSPICIOUS ACTIVITY?
Report it to NCRIC at https://ncric.org

Provide your feedback on the Partner Update Brief by clicking here

- **(U//FOUO) Sovereign citizen mailed letter to Alameda County Sheriff** (02/17/13, Alameda County Sheriff's Office) A subject sent a letter to the Alameda County Sheriff titled "Notice of Claim & Demand for a Timely Response." The subject is currently undergoing foreclosure proceedings and is facing eviction from his residence in Livermore, CA. The subject claimed in the letter that the Livermore property is "Sovereign Land." ***The language used by the subject is consistent with the sovereign citizen movement. The subject was recently arrested for resisting a peace officer during a traffic stop. The subject was previously mentioned in NCRIC PUB 13-018 on 01/29/13 for suspicious behavior during a traffic stop***.[2]

- **(U//FOUO) Sovereign citizen mailed letter to Alameda County Sheriff** (01/17/13, Alameda County Sheriff's Office) An identified subject sent a letter to the Alameda County Sheriff titled "Notice of International Diplomatic Status." The subject requested that ACSO "update the database to reflect [his] diplomatic status." ***The language used by the subject is consistent with the sovereign citizen movement***.[3]

---

[1] (U//FOUO) NCRIC SAR 20130578
[2] (U//FOUO) NCRIC SAR 20130118
[3] (U//FOUO) NCRIC SAR 20130078