[redacted]

b6
b7C
b7E

From: [redacted]
Sent: Tuesday, August 07, 2007 9:15 AM
To: [redacted]
Subject: Computer Intrusion Program Intelligence

UNCLASSIFIED
RECORD 288-JN-C31765-INTEL

The below items are provided for review and discretionary dissemination by supervisory agents due to potential investigative program overlap. Please note and share with liaison contacts in the banking industries the two items at the bottom concerning an increase in Phishing schemes and hacking.

Thanks,
[redacted]

SSA [redacted]
FBI Jackson Division - [redacted]
[redacted]
"One Nation, Under God"
"Lead, Follow, or Get Out of the Way"

b6
b7C
b7E

Intelligence Products Disseminated

(U) Intelligence Information Report

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~)

b7E

43

Other Items

(U) Flaw Exposes Hack Threat

- (U) Terrorists and other criminals could exploit a newly discovered software flaw to hijack massive computer systems used to control critical infrastructure like oil refineries, power plants, and factories.
- (U) The software is used to manage supervisory control and data acquisition or SCADA systems – computers that regulate the functioning of important infrastructures.
- (U) The intrusion works by attacking sensors within the facilities that are linked to the Internet through encrypted connections.
- (U) The flaw could crash certain systems, particularly older ones.
- (U) [redacted] a security researcher with 3Com's TippingPoint, Austin, TX, demonstrated the vulnerability to Defcon attendees.
- (U) [redacted] declined to identify the software company whose product he hacked, but says his firm has notified the company so the problem can be fixed.
- (U) Authorities have become increasingly concerned about the vulnerabilities of SCADA

b6
b7C
b7E

8/7

44

123 pages / em

[redacted]

288-JN-C31765-INTEL

systems as they've moved from closed networks to being connected to the Internet.
- (U) Source: USA Today

(U) Public Wi-Fi Use Raises Hacking Risk

- (U) Wi-Fi hot spots that let you hop onto the Internet anywhere you travel leave you wide open to hackers.
- (U) The basic problem: T-Mobile and AT&T - the largest providers of Wi-Fi hot spots in coffee shops, bookstores, and airports -- don't require encryption of data traveling wirelessly between laptops and the Internet.
- (U) Anyone with a Wi-Fi equipped laptop can download free Wi-Fi monitoring programs, eavesdrop from up to 100 feet away, and monitor what you do on the Internet.
- (U) There are no estimates of how often this has happened and there have been no arrest for Wi-Fi hacking.
- (U) T-Mobile and AT&T supply hot spots at more than 15,000 locations in the USA.
- (U) Source: USA Today

(U//~~FOUO~~) Hackers Informed of Ways to Breach Card Systems and Locks at White House and Pentagon

- (U//~~FOUO~~) [redacted] demonstrated how Medeco deadbolt locks relied on worldwide at embassies and banks can be opened in seconds with a strip of metal and a thin screwdriver. b6 b7C
- (U//~~FOUO~~) [redacted] has notified Medeco repeatedly through e-mail regarding the breach, but has not received a response.
- (U//~~FOUO~~) [redacted] has refused to publish details of defeating the locks.
- (U//~~FOUO~~) [redacted] demonstrated a device that can be spliced into wires connecting key card readers to computers systems that control door locks on many businesses.
- (U//~~FOUO~~) [redacted] identified easy targets as electronic key scanner pads at doors where workers step out for cigarette breaks.
- (U//~~FOUO~~) According to [redacted] walk up, pop off a cover held on by two screws, insert the device and it's done.
- (U//~~FOUO~~) Once the device is spliced into place, encoded cards can be used to command it to replay the last valid entry code or have the system deny access to people with legitimate cards.
- (U//~~FOUO~~) Source: CIA Threat Intelligence Highlights on 6 August 2007 citing an online article on timesofindia.com entitled, *White House, Pentagon Locks Can be Easily 'Breached'*.

(U//~~FOUO~~) Consumer Report Projects US Consumers Have Lost More Than $7 Million to Viruses, Spyware, and Phishing Schemes

- (U//~~FOUO~~) According to the 2007 "State of the Net" report, consumers face a one in four chance of becoming a cyber crime victim, a slight decrease since last year.
- (U//~~FOUO~~) The survey was conducted by the Consumer Reports National Research Center using a sample of more than 2,000 households with Internet access.
- (U//~~FOUO~~) The survey found the rate of virus infections remained steady compared to last year, which Consumer Reports calls a mark of progress for consumers and software vendors because threats have grown more complex.
- (U//~~FOUO~~) According to the report, 38 percent of respondents reported a computer virus in the last two years and 17 percent did not have anti-virus software installed.
- (U//~~FOUO~~) During the past six months, 34 percent of respondents' computers were exposed to spyware.
- (U//~~FOUO~~) Source: CIA Threat Intelligence Highlights on 6 August 2007, citing an online article on post-gazette.com entitled, *Report: Consumers Lost $7 Billion Over Last Two Years Due to Cybercrime.*

(U//~~FOUO~~) SecureWorks Announced the Number of Hacking Attempts Against Banking Clients Up 81 Percent Since January

- (U//~~FOUO~~) SecureWorks has blocked 167 million hacker attacks in the last 30 days.
- (U//~~FOUO~~) Most of the hackers stealing financial data are located in Russia and Eastern Europe, however, a growing number are coming out of China.
- (U//~~FOUO~~) Gozi, Prg and BBB trojans alone found millions of dollars of data sitting in stolen repositories.
- (U//~~FOUO~~) These data caches contained thousands of bank account and credit card numbers, social security numbers, online payment accounts, and user names and passwords.
- (U//~~FOUO~~) Source: CIA Threat Intelligence Highlights on 6 August 2007 citing an online article on tmcnet.com entitled, *SecureWorks Reports 81 Percent Increase in Financial Institution Hacking Attempts*

UNCLASSIFIED