FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000030-TT

(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**.

SUMMARY

(U) The FBI is providing the following information with HIGH confidence. Today the Western District of Pennsylvania unsealed an indictment naming five members of the People's Liberation Army of the People's Republic of China on 31 counts, including conspiring to commit computer fraud (18 U.S.C. §§ 371, 1030), accessing a computer without authorization for the purpose of commercial advantage and private financial gain (18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)), damaging computers through the transmission of code and commands (18 U.S.C. § 1030(a)(5)), aggravated identity theft (18 U.S.C. § 1028A), economic espionage (18 U.S.C. § 1831(a)(1)), and theft of trade secrets (18 U.S.C. § 1832(a)(1)). Each of the defendants provided his individual expertise to a conspiracy to penetrate the computer networks of six US companies while those companies were engaged in negotiations or joint ventures with or were pursuing legal action against state-owned enterprises in China. The following technical details are indicators released in the indictment related to these actors' activity.

(U) For additional details on the Indictment, please refer to FBI Private Industry Notification 140519 – 002 and/or the Department of Justice's Press release.

TECHNICAL DETAILS

(U) The aforementioned actors have used the following usernames/monikers, domain names and malware to conduct cyber espionage against US companies. The FBI is distributing the indicators associated with these actors for awareness and to enable network defense activities. The FBI has high confidence in these indicators.

(U) The following usernames are associated with the indicted actors:

- Jack Wang
- Uglygorilla
- Jack Sun
- Winxyhappy
- Win_XY
- Lao Wen
- Hzy_lhx
- KandyGoo

FBI FLASH

(U) The following domains/domain accounts are associated with the indicted actors and connected to malicious cyber activity:

- Financeanalysis.com (dns.diy.net)
- gmailboxes.com (dns.diy.net)
- busketball.com (dns.diy.net)
- arrowservice.net (eNom.com) – owned
- bigish.net (dns.diy.net)
  - finekl.bigish.net
- businessconsults.net (eNom.com) owned
- businessformars.com (eNom.com)
- marsbrother.com (eNom.com) owned
- purpledaily.com (eNom.com) owned
  - klwest.purpledaily.com
- newsonet.net (eNom.com) owned
- comrepair.com (dns.diy.net)
- oplaymagzine.com (dns.diy.net)
- hugesoft.org (namecheap.com)

(U) The following malicious software/hacking tools have been associated with the indicted actors:

- agenda.zip
- wiam.exe
- ccapp.exe
- gu.exe
- ugls.exe
- i.exe

(U) The following file name has been associated with exfiltration/data theft conducted by the indicted actors:

- wd.rar

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**