FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000031-PH

(U) The following information was obtained through a joint FBI/NCIS 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 and NCIS are providing the following information with **high confidence**:

SUMMARY

(U) The FBI and NCIS believe a group of cyber actors have been using various social networking sites to conduct spear phishing activities since at least 2011. FBI and NCIS investigation to date has uncovered 56 unique Facebook personas, 16 domains, and a group of IP addresses associated with these actors. These personas typically would attempt to befriend specific types of individuals such as government, military, or cleared defense contractor personnel. After establishing an online friendship the actor would send a malicious link (usually through one of the associated domains) to the victim, either through e-mail or in a chat on the social networking site eventually compromising the target's computer. While this FLASH specifically deals with Facebook personas, it is believed that many of these personas also maintain a presence on other social networking sites such as LinkedIn, Google +, and Twitter which are just as malicious. This group of cyber actors also has created and maintained multiple malicious Web sites, often spoofing a legitimate Web site and implanting malicious links into the actor's version of the Web site.

TECHNICAL DETAILS

(U) Based on investigative efforts, the FBI and NCIS believe the following names and Facebook User IDs (FBUID) are associated with fake personas and are involved in spear phishing activities on Facebook and additional social networking sites:

Abby Wilson FBUID 100001249857290	Abraham Gomez FBUID 100001545932069	Adia Mitchell FBUID 100003299460070	Alfred Nilsson FBUID 100004842848351
Alice Nilsson FBUID 100004672090339	Alice Taylor FBUID 100002924701430	Amanda Teyson FBUID 100004718351670	Barbara White FBUID 100002477442501
Berna Nani Achando FBUID 100003744333197	Brian Gibson FBUID 100003911053827	David Williams FBUID 100001537364844	Delia Carlsen FBUID 100001476095681
Donnie Eadense FBUID 103773899813841	Dorotha Baasch FBUID 100005436935593	Elizabeth Anderson FBUID 100002725315556	Gina McCarron FBUID 100002199199861
Heida Wagner FBUID 100001511282747	Jane Baker (Ava T. Foster) FBUID 100007144985923	Jeann Maclkin FBUID 100003591027097	Jinny Beyer FBUID 100004052511791
John Molavi FBUID 100001700742641	Joseph Nilsson FBUID 100004530097827	Josh Nilsson (Josh Furie) FBUID 100004516801118	Justin Snyder FBUID 100001450033215

Kendrick Babcock FBUID 100006297457628	Mahnaz Rahami FBUID 100001342226413	Mahsa Handyani FBUID 100001429057324	Marine Johnson FBUID 100003795818292
Mark Blyth FBUID 100002866859249	Mary Cole FBUID 100006363725699	Medhi Betterekoon FBUID 100002348575647	Mehdi Rastegar FBUID 100001483627448
Mehdi Sharooz FBUID 100002200349173	Michelle Hagerman FBUID 100002420632572	Mina Kasayi FBUID 100001881978783	Nancy William FBUID 100001739552330
Natasha Lovsky FBUID 100001778948301	Nilofar Shorabi FBUID 100001924237927	Olivia Johnson FBUID 100002864097606	Painfuol Strick FBUID 100002396473189
Rad Alborz FBUID 1431218901	Reza Salimi FBUID 100004568527560	Rozita Farhang FBUID 100001317388321	Sandra Maler FBUID 100006345461158
Sandy Laughlin FBUID 100001223376364	Sara Afsoon FBUID 100001667363382	Sara McKibben FBUID 100007150052891	Sharon Wilson FBUID 100002474596665
Sheida Zamani FBUID 100001867145251	Simin Rahnama FBUID 100001837158118	Susan Thomas FBUID 100003080928027	Thomas Clausen FBUID 100001560125984
Tim Caochoo FBUID 100001777117063	Tina Moradi FBUID 100002340489471	William Cooper FBUID 100003792613688	Zainab Osman FBUID 100002919467608

(U) The following fraudulent Web sites have also been identified as being involved in the malicious activity:

Domain	**IP address**
4techspot.com	173.193.136.193
Accounts.google.com-login.mobi	184.82.8.14 199.26.84.169
Com-login.mobi	199.26.84.169 198.20.182.55
Download.updatexplore.com	46.4.213.50 192.69.208.213
Downloadcenter.mcafeea.com	184.82.167.203
Eyeleo.com-login.mobi	199.26.84.169
Flycenter.ir	74.116.84.123
Fun4us.us	174.37.172.68 199.26.84.143 199.26.84.175 209.236.114.84 192.69.204.57 46.4.149.236
Internetexplorers.org	184.82.202.248 199.26.84.169 209.99.40.221 213.152.173.147
Login.yahoo.com-login.mobi	198.20.182.53 199.26.84.169
mcafeea.com	94.102.55.169 184.82.202.248

Domain	IP address
mediaplayercodec.net	64.130.216.21 174.37.172.68 209.99.40.219 192.69.208.213
Newsonair.org	199.26.84.143
Update.mcafeea.com	46.4.149.236 46.4.190.235 91.109.17.16 91.109.17.48 192.69.204.57 213.152.173.147
Updatexplore.com	70.168.71.240
Youtube.com-login.mobi	94.23.116.228 199.26.84.169

(U) The following IP addresses have also been identified as associated with these actors:

- 141.255.161.171
- 198.20.182.55

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**