Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

16 June 2016

Alert Number

160616-001

Please contact the FBI with any questions related to this Private Industry Notification Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

United Cyber Caliphate Releases Personally Identifiable Information of Individuals in US Business Personnel Directory

Summary

As of 5 May 2016, the Islamic State of Iraq and the Levant (ISIL) Sympathizer hacking group United Cyber Caliphate (UCC) defaced a Nigerian-hosted Web site, posting an html file containing the heading "USA Online Company Data Dumped by United Cyber Caliphate," there was no other message or threat associated with the file. The file contained approximately 1,137 entries, many of which appeared to be US-based individuals with corresponding personally identifiable information (PII) fields such as name, company, e-mail, phone, city, state, and zip code. The PII was doxed[1] from the personnel directory of a US business, according to FBI and open source reporting.

According to FBI reporting, the most recently released information was obtained using a new technique for UCC, a simple letter query[2] on the personnel registry database of a US-based business. UCC exfiltrated the PII by exploiting the open source nature of the personnel directory search function by entering each letter from A to Z, yielding all users within the directory which started with each respective letter. The resulting file was posted to the defaced Web site. FBI reporting indicates this is the first time UCC has used a simple letter query to exfiltrate data, but this does not reflect an expansion of UCC's cyber capabilities.

UCC is responsible for a number of computer intrusions, data exfiltrations, Web site defacements/injects, and PII doxing of victims around the globe. UCC utilizes social media sites and applications to publish the results of its criminal acts, typically by posting PII of its victims. UCC actively promotes allegiance to ISIL, and its publications

[1] "**Doxing**" involves searching for and publishing personally identifiable information about a specific person on the Internet.
[2] "**Simple Letter Queries**" are a basic search and sort request using letters to filter for users within a database.

call for ISIL-inspired attacks against the victims whose PII has been released. ISIL and its sympathizers have repeatedly called for attacks by US-based ISIL supporters against military, law enforcement (LE), security and intelligence personnel via data exfiltrations and incitement of lone-wolf attacks through doxing of PII. Between 21 April 2016 and 2 May 2016, UCC began expanding its doxing efforts to include private citizens with the release of PII belonging to approximately 2,100 New York-based individuals and 1,500 Texas-based individuals, according to FBI and open source reporting. This expansion further validates the group's anti-American sentiments, as well as an increased threat to targets of opportunity.

Threat

The FBI is unaware of any specific, credible threats by ISIL or its sympathizers against LE or private sector partners, and previous doxing releases have not successfully instigated physical attacks. However, ISIL supporters and US-based homegrown violent extremists present LE with limited opportunities to detect and disrupt plots, which frequently involve simple plotting against targets of opportunity.

Defense

Despite the lack of current specific targeting of the private sector by UCC, precautionary measures to mitigate a range of potential cyber threats by this group include:

- Implementing more stringent search parameters for querying personnel directories.
- Implementing password protecting personnel directories.
- Implement a data backup and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Implement a DDoS mitigation strategy and keep logs of any potential attacks. Enable network monitoring and logging if feasible.
- Scrutinize links contained in e-mail attachments.
- Regularly mirror and maintain an image of critical system files.
- Maintain and enforce a strong password policy, including changing passwords frequently, and do not reuse passwords for multiple accounts.
- Be cognizant of information available on open sources that may make you a target. Use caution when posting information on social media.
- Be aware of social engineering tactics aimed at obtaining sensitive information.
- Regularly update and patch software.

- Establish a relationship with local law enforcement and participate in IT security information sharing groups.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at NPO@ic.fbi.gov or 202-324-3691.

Administrative Note

This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

There is no additional information available on this topic at this time. For comments or questions related to the content or dissemination of this product, please contact CyWatch.