ROLL CALL RELEASE

INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

7 July 2014

(U) Malicious Cyber Actors Use Advanced Search Techniques

(U) Malicious cyber actors are using advanced search techniques, referred to as "Google dorking," to locate information that organizations may not have intended to be discoverable by the public or to find website vulnerabilities for use in subsequent cyber attacks. "Google dorking" has become the acknowledged term for this malicious activity, but it applies to any search engine with advanced search capabilities. By searching for specific file types and keywords, malicious cyber actors can locate information such as usernames and passwords, e-mail lists, sensitive documents, bank account details, and website vulnerabilities. For example, a simple "*operator:keyword*" syntax, such as "*filetype:xls intext:username,*" in the standard search box would retrieve Excel spreadsheets containing usernames. Additionally, freely available online tools can run automated scans using multiple dork queries.

(U) **Google Dorking**

(U) Also known as "Google hacking," involves using specialized search parameters to locate very specific information. Examples include:

» (U) Site: Searches and lists all the results for that particular site.

» (U) Intext: Searches for the occurrences of keywords all at once or one at a time.

» (U) Inurl: Searches for a URL matching one of the keywords.

» (U) In October 2013, unidentified attackers used Google dorking to find websites running vulnerable versions of a proprietary Internet message board software product, according to security researchers. After searching for vulnerable software identifiers, the attackers compromised 35,000 websites and were able to create new administrator accounts.

» (U) In August 2011, unidentified actors used Google dorking to locate a vulnerable File Transfer Protocol server at an identified US university and compromised the personally identifiable information of approximately 43,000 faculty, staff, students, and alumni, according to an information technology security firm.

» (U) The Diggity Project is a free online tool suite that enables users to automate Google dork queries. It contains both offensive and defensive tools and over 1,600 pre-made dork queries that leverage advanced search operators.

(U) **Suggested measures for website administrators to protect sensitive information include:**

» (U//FOUO) Minimize putting sensitive information on the web. If you must put sensitive information on the web, ensure it is password protected and encrypted.

» (U//FOUO) Use tools such as the Google Hacking Database, found at http://www.exploit-db.com/google-dorks, to run pre-made dork queries to find discoverable proprietary information and website vulnerabilities.

» (U//FOUO) Ensure sensitive websites are not indexed in search engines. Google^{USPER} provides webmaster tools to remove entire sites, individual URLs, cached copies, and directories from Google's index. These can be found at: https://www.google.com/webmasters/tools/ home?hl=en.

» (U//FOUO) Use the robots.txt file to prevent search engines from indexing individual sites, and place it in the top-level directory of the web server.

» (U//FOUO) Test your website using a web vulnerability scanner.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

IA-0196-14

(U) Prepared by the Office of Intelligence and Analysis (I&A). Coordinated with Federal Bureau of Investigation. This product is intended to provide cybersecurity awareness to federal, state, local, and private sector first responders in matters that can affect personnel and network security of their respective organizations.

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.*

(U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label ^{USPER} and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures.