NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

BULLETIN

A-0020-NCCIC / ICS-CERT –120020110916

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR MISION PARTNERS AT THE "FOR OFFICIAL USE ONLY" LEVEL, ACROSS THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

(U//FOUO) ASSESSMENT OF ANONYMOUS THREAT TO CONTROL SYSTEMS

EXECUTIVE SUMMARY

(U) The loosely organized hacking collective known as Anonymous has recently expressed an interest in targeting industrial control systems (ICS). This product characterizes Anonymous' capabilities and intent in this area, based on expert input from DHS's Control Systems Security Program/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the other NCCIC components.

(U//FOUO) While Anonymous recently expressed intent to target ICS, they have not demonstrated a capability to inflict damage to these systems, instead choosing to harass and embarrass their targets using rudimentary attack methods, readily available to the research community. Anonymous does have the ability to impact aspects of critical infrastructure that run on common, internet accessible systems (such as web-based applications and windows systems) by employing tactics such as denial of service. Anonymous' increased interest may indicate intent to develop an offensive ICS capability in the future. ICS-CERT assesses that the publically available information regarding exploitation of ICS could be leveraged to reduce the amount of time to develop offensive ICS capabilities. However, the lack of centralized leadership/coordination and specific expertise may pose challenges to this effort.

DISCUSSION

(U//FOUO) Several racist, homophobic, hateful, and otherwise maliciously intolerant cyber and physical incidents throughout the past decade[a] have been attributed to Anonymous, though recently, their targets and apparent motivations have evolved to what appears to be a hacktivist[1] agenda. The section below highlights a recent interest Anonymous has developed in exploiting ICS, which the NCCIC assesses is a new tactic, technique and/or procedure (TTP). For more information on Anonymous's background or motivations, please see the NCCIC Bulletins: "*Anonymous Upcoming US Operations, Impact, and Likelihood*," and "*Anonymous and Associated Hacker Groups Developing New Cyber Attack Tools*."

[1] Hacktivist – A cyber exploitation or attack actor whose intent is driven by a social, religious, political or cultural ideology.

(U) Recent Examples of Anonymous' Interest in Control Systems

(U) On 11 July 2011 a suspected member of Anonymous, posted some materials to Pastebin[b]. This posting describes its cyber attack on Monsanto's websites and e-mail servers. Anonymous reported exfiltrating personally identifiable information (PII) data on 2,500+ employees and associates, including full names, addresses, phone numbers, and exactly where they work. They reported it took about two months to accomplish this attack.

- (U) Monsanto is a U.S.-based global biotech seed company. Tom Helscher, the company director of corporate affairs, in an e-mail to msnbc.com confirmed that Monsanto "experienced a disruption to its website that appeared to be from an organized cyber group."[c]

(U//FOUO) On 12 July 2011, Anonymous released a press report on a website titled "Anonymous Operation Green Rights \ Project Tarmaggedon."[d] The report outlined Anonymous' hacktivists concerns with global warming and called for protests against the Alberta Tar Sands (Canada) project along Highway 12 in Montana. As quoted from its posting, "Anonymous Operation Green Rights calls your attention to an urgent situation in North America perpetuated by the boundless greed of the usual suspect: Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd. Imperial Oil, the Royal Bank of Scotland and many others." On 13 July 2011, according to open source reporting, seventy protesters ascended on the Montana state capitol building to protest the Alberta Tar Sands project and the Keystone, XL 36 inch underground pipeline project.[e] The NCCIC assesses that Anonymous' participation in peaceful protests carries a moderate likelihood of being accompanied by cyber attacks or exploitations, though no malicious cyber activity was reported in association with this protest.

(U) On 19 July 2011, a known Anonymous member posted to Twitter the results of browsing the directory tree for Siemens SIMATIC software. This is an indication in a shift toward interest in control systems by the hacktivist group.

(U) ICS-CERT Assessment of Capabilities [f,g,h, i]

(U//FOUO) An anonymous individual provided an open source posting on twitter of xml and html code that queries the SIMATIC software. The individual alleged access to multiple control systems and referred to "Owning" them.[2] The Twitter posting does not identify any systems where privileged levels of access to control systems have been obtained.

(U//FOUO) The posted xml and html code reveals that the individual understands the content of the code in relation to common hacking techniques to obtain elevated privileges. It does not indicate knowledge of ICS; rather, it indicates that the individual has interest in the application software used in control systems. The posted xml and html contained administration code used to create password dump files for a human-machine interface control system software product from Siemens. The code also contained OLE for Process Control (OPC) foundation code that is used in server communication with control system devices such as programmable logic controllers, remote terminal units, intelligent-electronic devices, and industrial controllers. No indication of exploitation capability was observed by ICS-CERT. The information assessed indicates that the individual was able to recognize and post the portions of code that would ensure others knowledgeable in control systems would take notice.

(U//FOUO) The same individual also posted the directory browse history of the software application installation. In the twitter posting the server information was not identified. This does not indicate that

[2] "Owning" is a common term referring to having super-user or privileged access to a computer system.

the individual was trespassing on an operational control system - the information could have been posted based on others work or a demonstration installation on the individual's personal systems.

(U//FOUO) The capability of the individual to recognize and post code that would gain the attention of those knowledgeable in control systems, as well as their claims to have access to multiple control systems, indicates the individual has an increased interest in control systems, but does not demonstrate capabilities. There are no indications of knowledge or skill in control systems operations, design, or components. The individual may possess the necessary skill to exploit elevated privileges by hijacking credentials of valid users of the ICS software product posted based on traditional exploitation methods, not anything ICS specific. No posting by the individual indicated direct malicious activity.

DHS/NCCIC ASSESSMENT

(U//FOUO) The information available on Anonymous suggests they currently have a limited ability to conduct attacks targeting ICS. However, experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly. Free educational opportunities (conferences, classes), presentations at hacker conferences, and other high profile events/media coverage have raised awareness to ICS vulnerabilities, and likely shortened the time needed to develop sufficient tactics, techniques, and procedures (TTPs) to disrupt ICS. Control system exploits are released in common penetration testing software such as Metasploit release 4.0 that can be directly used with novice level skills in hacking and little to no background in control systems. Common packet inspection tools such as WireShark and Netmon have improved to the point where industrial protocols are supported minimizing the effectiveness of security-by-obscurity.[j,k,l,m] In addition, there are control systems that are currently accessible directly from the Internet and easy to locate through internet search engine tools and applications. These systems could be easily located and accessed with minimal skills in order to trespass, carry out nefarious activities, or conduct reconnaissance activities to be used in future operations.[n,o,p]

(U//FOUO) Anonymous has recently called on their members to target energy companies based on "Green Energy" initiative performance. This targeting could likely extend beyond Anonymous to the broader hacktivist community, resulting in larger-scope actions against energy companies.[q,r] Asset owners and operators of critical infrastructure control systems are encouraged to engage in addressing the security needs of their control system assets.

POINTS OF CONTACT

(U) This NCCIC Bulletin was produced by the NCCIC Analysis Group and the DHS Control Systems Security Program/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the other NCCIC Functional Groups and Operational Components.

---

a (U) The New York Times, "Malwebolence, The World of Web Trolling," http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html, 3 August 2008, accessed 16 September 2011.
b. (U) PASTEBIN, "Untitled," http://pastebin.com/vrDGwuUH, accessed July 29, 2011.
c. (U) Suzanne Choney, "Anonymous hacks Monsanto computers; posts employee info," MSNBC, July 13, 2011. http://technolog.msnbc.msn.com/_news/2011/07/13/7076220-anonymous-hacks-monsanto-computers-posts-employee-info, accessed July 29, 2011.

d. (U) Anonnews.org, “Anonymous Operation Green Rights \ Project Tarmaggedon,” http://www.anonnews.org/?p=press&a=item&i=1021, last accessed July 24, 2011.
e. Adams, John S., “Pipeline protesters hit Montana governor’s office” , USA Today, http://www.usatoday.com/news/nation/2011-07-13-montana-oil-protest_n.htm, accessed September 12, 2011.
f. (U) Pastie, “#2243211 – Pastie,” http://pastie.org/2243211, last accessed July 20, 2011.
g. (U) PasteBay, “PasteBay.com – Free uncensored text hosting,” http://pastebay.com/133000, last accessed July 20, 2011.
h. (U) PASTEBIN, “[Prolog]pr0f – Pastebin.com,” http://pastebin.com/DDbmJK90, last accessed July 20, 2011.
i. (U) PASTEBIN, “[HTML] pr0f – Pastebin.com,” http://pastebin.com/wY6XD97L, last accessed July 21, 2011.
j. WireShark, “Display Filter Reference: Common Industrial Protocol,” http://www.wireshark.org/docs/dfref/c/cip.html, last accessed September 15, 2011.
k. WireShark, “Display Filter Reference” EtherNet/IP (Industrial Protocol)” http://www.wireshark.org/docs/dfref/e/enip.html, last accessed September 15, 2011.
l. Hulsebos, Rob, “Network Analysis and the challenge of Industrial Automation protocols,” Industrial Ethernet Book, http://www.iebmedia.com/index.php?id=5597&parentid=63&themeid=255&hft=41&showdetail=true&bb=1&PHPSESSID=rro01ah93rh2kkrjao3r01p152, last accessed September 15, 2011.
m. Morris, Jeff, “Re: [tcpdump-workers] request for DLT_WIHART for Wireless HART”, SECLISTS.ORG, July 25, 2011, http://seclists.org/wireshark/2011/Jul/511, last accessed September 15, 2011.
n. Mills, Elinor, “Researchers warn of SCADA equipment discoverable via Google” CNET, August 2, 2011, http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/, last accessed September 13, 2011.
o. ICS-CERT, “ICS-ALERT-10-301-01 – Control System Internet Accessibility,” October 28, 2010, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, last accessed September 13, 2011.
p. Goodi, Dan, “Hackers tap SCADA Vuln Search Engine” theregister.co.uk, November 2, 2010, http://www.theregister.co.uk/2010/11/02/scada_search_engine_warning/, last accessed September 13, 2011.
q. Vallance, Chris, “Activists turn ‘hacktivists’ on the web”, BBC, March 16, 2010, http://news.bbc.co.uk/2/hi/technology/8567934.stm, last accessed September 12, 2011.
r . (U) Lacey, Stephen, “In a Cable Released by WikiLeaks, State Department Officials Encourage Canada to Spin News Coverage of Tar Sands Pipeline” thinkprogress.org, July 13, 2011, http://thinkprogress.org/romm/2011/07/13/268391/wikileaks-state-department-tar-sands-pipeline/, last accessed September 12, 2011.