ROLL CALL RELEASE
INTELLIGENCE FOR POLICE, FIRE, EMS, AND SECURITY PERSONNEL

8 May 2015

(U//FOUO) Criminal Hackers Target Police to Protest Perceived Injustices

(U//FOUO) Disruptive cyber attacks by criminal hackers—primarily distributed-denial-of-service (DDoS) attacks—targeting local law enforcement websites have increased since August 2014. We judge that this is almost certainly a result of the heightened coverage surrounding the alleged use of excessive force by law enforcement and an increased focus on incidents of perceived police brutality. The primary impact from the majority of these attacks has been the temporary disruption of the targeted public-facing websites.

UNCLASSIFIED

(U) Figure 1. Criminal Hackers Targeting Police

» (U//FOUO) In 2014, the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 53 separate incidents of criminal hackers conducting cyber operations against state and local entities in response to incidents of alleged use of excessive force by law enforcement. The majority of these incidents were low to moderate in effect, most frequently resulting in temporary disruption to targeted websites.

» (U//FOUO) On the morning of 30 December 2014, unknown criminal hackers disabled a Midwestern police department's public website using a DDoS attack. A post later that morning on a US social-networking site containing the hashtag "#BlackLives Matter" announced that the targeted website was down. The disabling of this website was the third successful attack to disable a law enforcement website in the state within a week—the attacks were limited to the temporary disablement of targeted websites, according to DHS field reporting.

» (U//FOUO) A criminal hacker using the moniker (at)DigitaShadow claimed responsibility on a US social-media site for disrupting access to a Northwestern city police department's website in early December 2014. The DDoS attack, which lasted approximately 10 minutes, prevented the department's in-car terminals from transmitting or receiving traffic, including 911 dispatch requests, according to FBI reporting.

(U//FOUO) MS-ISAC Distributed-Denial-of-Service Mitigation Recommendations

(U) Proactive protections include:

» (U) Establish connections with multiple Internet service providers (ISPs) for redundancy,
» (U) Ensure service-level agreements with ISPs contain provisions for DoS prevention (such as IP address rotation),
» (U) Conduct rate-limiting of traffic at the network perimeter, and
» (U) Create backup, remote-site network infrastructure using multiple addressing schemes.

(U) Reactive protections include:

» (U) Execute ISP address rotation,
» (U) Block source IP addresses generating DoS traffic at enterprise boundary or within ISP infrastructure, and
» (U) Acquire increased bandwidth capability from the ISP.

(U//FOUO) See MS-ISAC's "Guide to DDoS Attacks" for additional information: http://msisac.cisecurity.org/resources/reports/ documents/GuidetoDDoSAttacks_000.pdf.

(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-0181-15