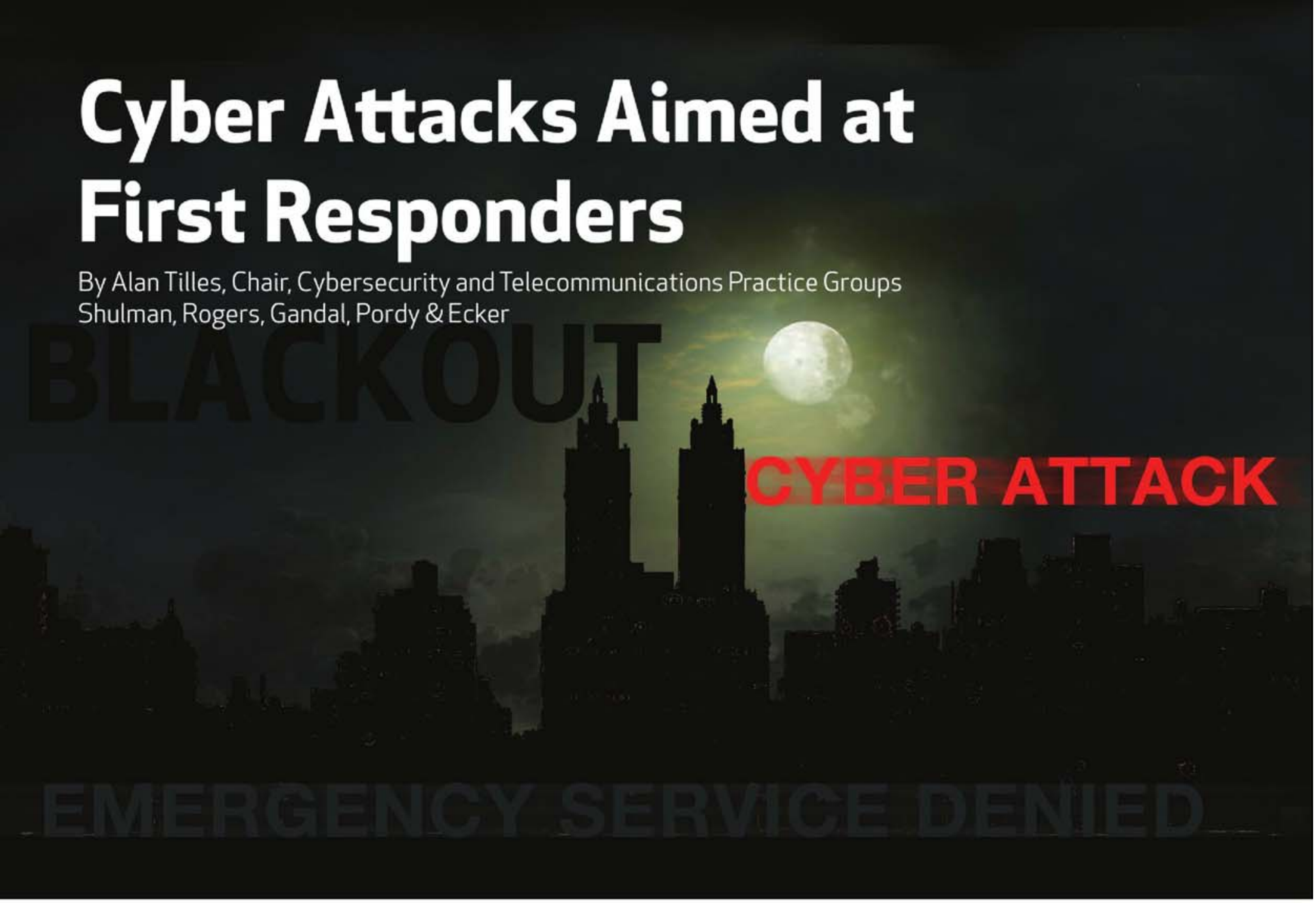
Cyber Attacks Aimed at First Responders

By Alan Tilles, Chair, Cybersecurity and Telecommunications Practice Groups
Shulman, Rogers, Gandal, Pordy & Ecker



Best Practice Checklist Developed for PSAP Lines to Minimize Risks

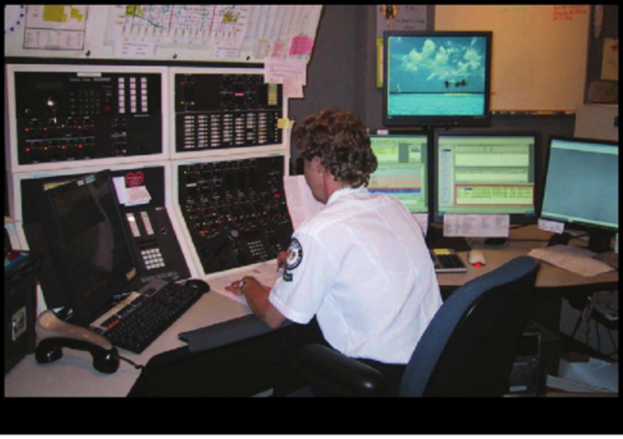
If you are a regular reader of this magazine, you are well aware of the problems that denial of service (DoS) attacks can have on a business or an individual. The dangers of cyber attacks on utilities has been written about and discussed over and over. One power utility stated that it fields 10,000 attempted attacks every month. The banking industry is under similar attack. The attack on the Associated Press's Twitter account, falsely reporting an explosion near the White house, caused the Standard & Poor's 500 Index to temporarily drop and wipe out $136 billion in market value.

Fortunately, action is being taken to respond to these incidences. The necessarily defensive tactics don't happen fast enough, but they are happening. However, rarely explored is the potential impact on public safety when that cyber attack is aimed at first responders.

You may have seen the movie Live Free or Die Hard (Die Hard 4), about a cyber-terrorist foiled by John McClane and young hacker Matt Farrell. And, you probably saw more than a few technical flaws in the movie's premise. These errors go from small (Lucy's SIM card has letters, when it should be all numbers) to large (there is no national power grid, there are three power grids for each geographic section of the country). But, something similar is very real, and already occurring. Specifically, Telephony Denial of Service (TDoS) attacks are being launched against public safety communications, targeting administrative public safety answering point (PSAP) lines.

A PSAP is the where a 9-1-1 call gets answered. Obviously, the ability to communicate at all times is crucial to public safety. Imagine a TDoS attack happening on a PSAP during a disaster, man-made or otherwise.

Telephony Denial of Service (TDoS) attacks are being launched against public safety communications, targeting administrative public safety answering point (PSAP) lines.



Typically, these attacks are part of an extortion scheme. A caller claims to be from a collection agency for payday loans, and is allegedly calling about an outstanding debt on an employee. When the dispatch center states that (in some cases) the alleged debtor is no longer an employee, the caller demands that the dispatch center pay. If payment isn't made, the TDoS attacks begin. The attacks can last for hours, or be intermittent. They may stop, but then resume.

Now that wireline voice telephony is primarily Voice over Internet Protocol (VoIP), it is possible for the attacker to robo-dial thousands of simultaneous calls using Session Initiation Protocol (SIP) computer software. The SIP software can spoof telephone numbers, which impedes the usefulness of black listing software. To keep the scheme going, Asterisk Private Branch Exchange (PBX) software can be programmed to dial recursively, keeping those lines open. If a person answers the phone line, noise or unintelligible speech can be programmed, which may keep the caller from immediately hanging up.

The attacks typically occur on PSAP administrative lines, not the 9-1-1 lines, distracting attention from real problems that are occurring. However, the impact can be significant, because resources become devoted to the administrative lines, distracting attention from the 9-1-1 lines. If there is enough call volume, there is a rollover to other PSAPs, exacerbating the problem.

As of March of 2013, there were reports of up to 50 such attacks in multiple jurisdictions across the U.S. The problem is very real.

Increasingly, municipalities are moving towards what's known as NG9-1-1 systems that accept text messages. Using text messaging or cellphones for TDoS attacks are more difficult, because PSAPs have the ability to work with cell providers to obtain location information (regardless of whether the cell phone has enabled location services).

To combat this problem, the Department of Homeland Security (and other federal authorities), the National Emergency Number Association (NENA) and the Association of Public-Safety Communications Officials (APCO) have developed a set of protocols, a best practices checklist, for PSAP to minimize the risks. From the outset, education is key, and adoption of the checklist vital.

The checklist can be found here:
https://www.nena.org/news/120618/Best-Practices-Checklist-for-Denial-of-Service-Attacks-Against-9-1-1-Centers.htm

Alan Tilles is a partner at the law firm of Shulman Rogers Gandal Pordy & Ecker, where he is the Chair of the Firm's Cybersecurity and Telecommunications practice groups. He can be reached at atilles@shulmanrogers.com.