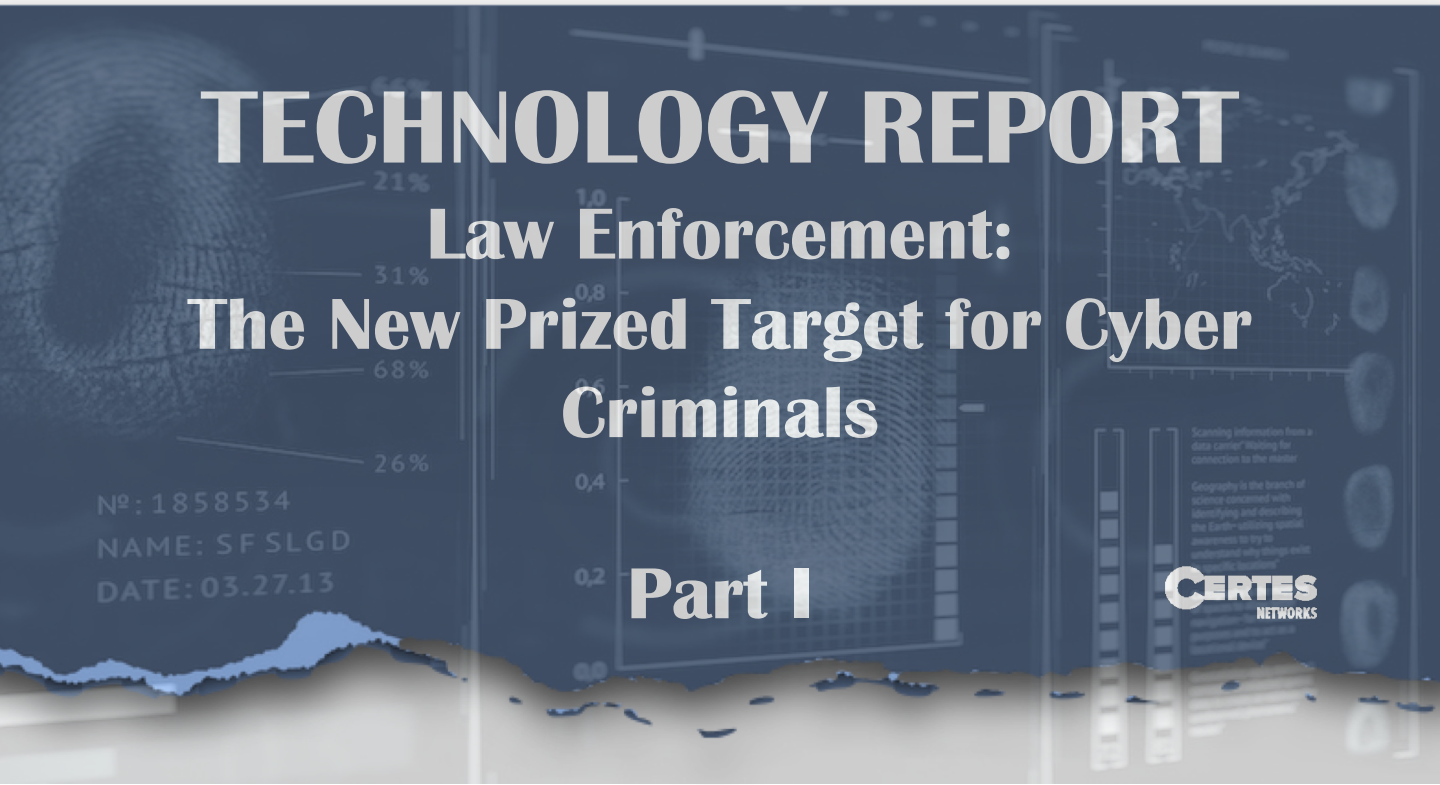
CERTES NETWORKS



Law enforcement is a highly-focused target for cyber criminals

Introduction

Extensive data breaches and cybercrimes including ransomware are increasing throughout the world. And law enforcement is a highly-focused target for cyber criminals whose sole purpose is to exploit sensitive information and impact a region's critical infrastructure. The complexity and reach of cyberattacks can present challenges that might seem overwhelming for most local law enforcement agencies. And, the idea that a breach or malware attack is noticed after the fact runs contradictory to the preventive nature of law enforcement itself.

Even more troubling, police departments and emergency services are highly dependent on computer-aided dispatching, alert systems and other information technology in order to bring essential personnel and equipment to locations where they are most needed. But, equally as important is this intelligence is shared primarily through the internet, which is one of the most vulnerable points in the network infrastructure.

How Critical Is It?

Malicious actors engaged in very sophisticated and continuous hacking efforts often leverage malware to gain undetected access to IT systems in order to disrupt essential emergency and/or government services. Ransomware is a form of malware used to deny users access to critical data and systems. Once an organization's systems are infiltrated, the cyber criminals demand a ransom payment in exchange for allowing access to their critical data.

In December 2016, a law enforcement agency near Dallas, Texas, was the victim of a ransomware attack when an employee clicked on a link in a phishing email that appeared to be from another law enforcement agency. The agency lost a substantial number of digital files, including video evidence.

On March 22, 2018, a ransomware attack encrypted data on the City of Atlanta's (Georgia) government servers, affecting various internal and customer-facing applications, including those of the Atlanta Police Department. During the same month, the City of Baltimore, Maryland, had its dispatch system taken offline for more than 17 hours due to a cyberattack.

Law enforcement agencies are at constant risk of a critical data breaches which often coincide with media-focused events such as the implementation of controversial policies that can draw inquiry from the public, or other high-profile events that receive media attention, such as officer-involved shootings. The civil unrest in Ferguson in August 2014 resulted in many officers being "doxxed," meaning their home addresses, social security numbers, and phone numbers were published online, creating a significant threat to their personal safety and that of their families. In another very alarming cyberattack on law enforcement, the ISIS-affiliated Caliphate Cyber Army divulged personally identifiable information of 36 Minnesota police officers, and called for the officers to be killed.

And the list goes on.

The Implications

A recent U.S.-wide survey of local government cybersecurity showed that local governments are under "near-constant attack." The unauthorized access or loss of law enforcement data due to a cyberattack has serious operational and privacy implications. The importance of a robust cybersecurity strategy must include an almost impenetrable set of network security protocols and a cybersecurity culture that is hyper vigilant at all times.

The unwilling forfeiture of such sensitive data is not just a consequence of not fully protecting data but needs to be weighed and thought-through from multiple perspectives—those of employees, community, crime victims, witnesses, informants, and prosecutors. A cyberattack could potentially affect the public's confidence in local law enforcement, eroding trust and credibility.

Many U.S. states have laws that mandate notification protocols if an organization suspects that their data have been breached in a manner that compromises the confidentiality of an individual's personal information. Compliance can be both labor intensive and publicly embarrassing. Law enforcement agencies have an ethical and legal obligation to maintain the security of their data. It is without question that the monetary cost of a cyber breach could have not only substantial fiscal implications but also disrupt essential government services for prolonged periods of time.

How the Department of Homeland Security is Lending Assistance

Stay tuned for Part II of this Tech soundbite which will outline how the Department of Homeland Security (DHS) is offering free assistance to help law enforcement agencies prepare for, prevent, and respond to cyber incidents that could degrade or overwhelm U.S. strategic assets. Or go to https://www.certesnetworks.com/resources/ for more information.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.