radware

ERT Threat Alert

Attacks Against Medical Institutions

May 25, 2016

Abstract

Turkish citizens are the latest victims in a worldwide cyber assault on medical institutions and healthcare providers. Hackers, including those from the global hacktivist group Anonymous, have hacked the databases of several Turkish medical institutions and gained control of patient records in retaliation for a series of ransomware attacks against U.S. hospitals earlier this year. These recent cyber assaults underscore the growing threat to medical institutions and insurance companies worldwide, raising the concern that medical records and patient data will be compromised.

Hackers have launched this new round of cyber-attacks leveraging denial of service, SQL injections and ransomware attacks targeted against the organization’s email servers. These medical institutions are being targeted by hackers for various reasons, and have suffered from extortion schemes/ransomware and HTTP floods throughout the year.

Recent Attacks

- **Turkey Hospitals**[i] – Anonymous hacker leaked personal health information for what they claim is retaliation for a sting on ransomware attacks seen across the United States. Through SQL injections, authorization error, short passwords and other vulnerabilities the hackers where able to gain access and leak sensitive information.

- **Ottawa Hospital**[ii] – A Ottawa Hospital was the victim of a ransomware campaign that resulted in four computers being infected. In this case a user clicked on a link that activated the malware. The hospital did not pay the ransom and just wiped the drives.

- **York Hospital**[iii] - York Hospital in Maine suffered from a data breach that resulted in the compromises of employee information. Information like names, addresses, SSN and W-2’s where includes in the data breach. It is likely that this information was stolen from the network via an SQL injection.

- **Flint, MI Hospital**[iv] - A day after Anonymous threaten to take action over the water crisis in Flint Michigan, Hurley Medical Center was the target of a cyber-attack, followed by DDoS assaults on the city website as well as the state of Michigan.

Attack Methods

1. **Ransomware**

   Ransomware is a malware that manipulates files in order to extort their owners. It typically propagates as a Trojan, disguised as a seemingly legitimate file through infected USB flash drives or email attachments. Perpetrators often make use of social engineering techniques, which are designed to lure the recipient into opening the attachment.

   The attack methodology and payload delivery are both simple and effective. Hackers require access to internal servers, which can be accomplished via downloads and phishing emails. Others exploit vulnerable JBOSS servers commonly found inside hospitals and medical institutions. In addition, hackers leverage tools like JaxBoss[i] and JBOSS auto pwn[ii], and JBOSS vulnerability scanners to look for vulnerable servers before launching these attacks (see Figure 1). These tools can also tell the user which vulnerabilities can be leveraged on the JBOSS application platform. This is the second step.
   Lastly, the perpetrator will upload the malicious program (AKA Webshell) to the system, which then modifies server configurations or spreads itself across the network

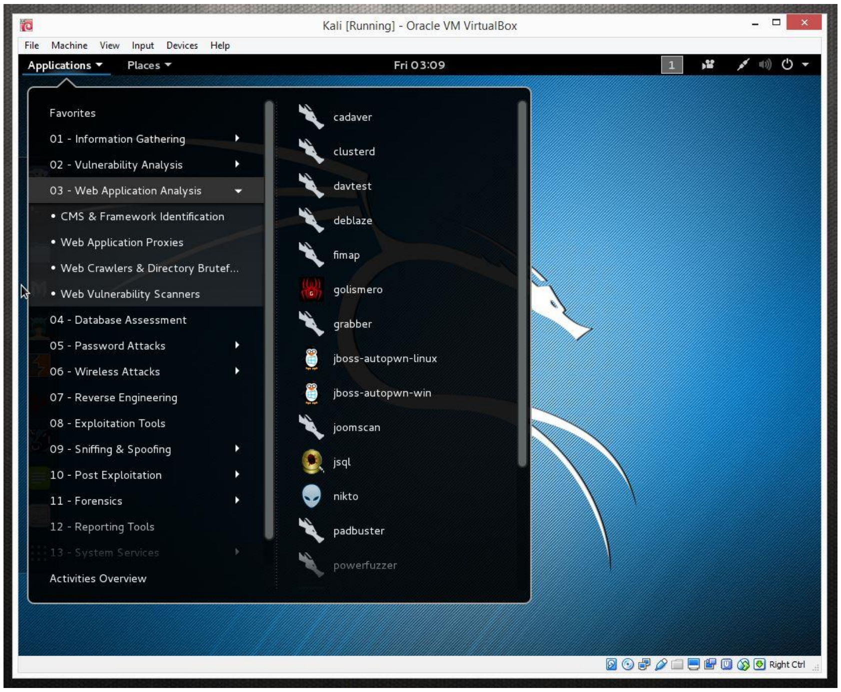

Figure 1: JBOSS auto pwn standard on Kali Linux

2. **SQL Injection**
   This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

   In dark markets, medical records have greater value than credit card numbers. This financial motive drives hackers to attain these records in the effort to turn greater profits. Medical institutes should be aware of the growing use of SQL injections.

3. **Denial of Service**
   a. **UDP Flood** – In a UDP flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is “connectionless” and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC IP
   b. **NTP Monlist flood** – The NTP Amplification attack is an emerging form of Distributed Denial of Service (DDoS) that relies on the use of publically accessible NTP servers to overwhelm a victim system with UDP traffic. The NTP service supports a monitoring service that allows administrators to query the server for traffic counts of connected clients. This information is provided via the “monlist” command. The basic attack technique consists of an attacker sending a "get monlist" request to a vulnerable NTP server, with the source address spoofed to be the victim’s address.
   c. **HTTP Flood** - A method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests that are designed to consume a significant amount of server’s resources, and can result in a denial-of-service condition - without necessarily requiring a high rate of network traffic.

Most network security devices can’t distinguish between legitimate and malicious HTTP traffic, resulting in a high number of false-positive detections. Rate-based detection engines are also not successful at detecting HTTP flood attacks, as the traffic volume of HTTP floods may be under detection thresholds. It is necessary to use several parameters detection including rate-based and rate-invariant.

Organizations Under Attack Should Consider

Protection from UDP & HTTP Floods, reflection attacks and other DDoS techniques:

- A hybrid solution combining on-premises detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and internet pipe saturation.
- The solution must distinguish between legitimate and attack traffic, blocking it while protecting the SLA.
- An integrated, synchronized solution that can protect from multi-vector attacks by combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts.

Protection from SQL injections and web application vulnerabilities:

- IP-agnostic device fingerprinting – having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time.
- Automatic and real time generation of policies to protect from zero-day, unknown attacks.
- Shortest time from deployment to a full coverage of OWASP Top-10.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

DDoS attacks or malware outbreaks can create unwanted emergency situations. Radware offers a service to help respond to these emergencies, neutralize the security risk, and better safeguard operations before irreparable damages occur. If you’re under attack and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] http://pastebin.com/wZ4sQtZq
[ii] http://www.cbc.ca/news/canada/ottawa/hospital-cyber-attack-1.3489388
[iii] http://www.scmagazine.com/york-hospital-breach-compromises-pii-of-1400-employees/article/479549/
[iv] http://www.mlive.com/news/flint/index.ssf/2016/02/anonymous_claims_responsibilit.html