FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

The following are indicators of possible compromise:

Network-Based Indicator
Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36. The below is a SNORT signature related to this activity:

alert tcp any any -> any any (content:"|6E|"; depth: 1; content:"|36 36 36 58 36 36 36|"; offset: 3; depth: 7; msg: "Beacon C2"; sid: 1000000001; rev:0)

Host-Based Indicator
The malware runs as a Windows service "RasWmi (Remote Access Service)" from the malicious .dll C:\Windows\system32\wbem\raswmi.dll. The implant is installed from an executable file (the file has been observed under a variety of names) which drops the raswmi.dll file into the same directory and sets it to run as a service.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or
FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937