solutions [AB1] to address these new threats, including IoT malware, like Mirai. Last fall, Mirai was used to arm hundreds of thousands of webcams to attack the ...

Feb. 14, 2017

More than 90 percent of IT security professionals said that connected devices will be a major security issue this year. However, 66 percent aren't sure how many devices are in their environment, according to new research from Pwnie Express.

In a report titled, The Internet of Evil Things (IoET), researchers found a common

"Mirai demonstrated what the right malware could do if unleashed onto poorly configured or inadequately secured devices," said Paul Paget, Pwnie Express CEO. "When you consider the exploding number of connected devices, many with poorly configured or no security and the fact that security teams can't see these devices, it becomes clear that security programs need to shift spending to adapt more quickly."

Mirai made headlines globally and 84 percent of those surveyed admitted that Mirai changed their perception about threats from IoT devices. Yet, over 65 percent said they either haven't checked or don't know how to check their connected devices for Mirai. With Mirai and its inspired offshoots in the wild, determined attackers see the potential to use vulnerable connected devices for nefarious large-scale purposes and to target and compromise specific networks and companies.

Key report findings include:

One in five of the survey respondents (20%) said their IoT devices were hit with ransomware attacks last year. 16% of respondents say they experienced Man-in-the-middle attacks through IoT devices. Devices continue to lend themselves to problematic configurations. The default network from common routers "linksys" and "Netgear" were two of the top 10 most common "open default" wireless SSID's (named networks), and the hotspot network built-in for the configuration and setup of HP printers – "hpsetup"- is #2.

In addition, survey respondents shared their top device threat concerns for 2017:

Misconfigured healthcare, security, and IoT devices will provide another route for ransomware and malware to cause harm and affect organizations. Unresolved vulnerabilities or the misconfiguration of popular connected devices, spurred by the vulnerabilities being publicized by botnets, including Mirai and newer, "improved" versions, in the hands of rogue actors will compromise the security of organizations

purchasing these devices. Mobile phones will be the attack vector of the future,

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.