New Reaper IoT Botnet Leaves 378 Million IoT Devices Potentially Vulnerable to Hacking

Submitted by: The PR Room
Tuesday, 24 October 2017

BullGuard CEO Calls on the Security Industry and Device Manufacturers to Address the Growing Cyber Threat from Unprotected Smart Devices; Dojo by BullGuard Stops Reaper Botnet Dead

SAN FRANCISCO and LONDON, OCTOBER 24, 2017 – In the wake of Reaper, the latest IoT botnet, Paul Lipman, CEO of award winning consumer cybersecurity company, BullGuard (https://www.bullguard.com/), today urged the security industry and device manufacturers to address the growing threat from unprotected smart devices. The call follows the discovery of the latest Internet of Things (IoT) botnet threat, known alternatively as Reaper or IoT Troop that has already enveloped smart devices on more than a million networks worldwide. Reaper uses actual software hacking techniques to break into devices – evolving beyond the October 2016 Mirai IoT botnet, which exploited weak or default passwords on impacted IP cameras and internet routers, and took down major websites across the U.S. including Twitter, Netflix and the New York Times. Reaper's potential for major Distributed Denial of Service (DDOS) attacks that rapidly take down online services is enormous, and makes last year's Mirai IoT botnet look like child's play.

"Reaper is a landmark evolution for hacked smart devices. Unlike Mirai it doesn't rely on exploiting devices with simple default credentials, rather it exploits numerous vulnerabilities in different IoT devices. It uses sophisticated techniques to hack routers and various smart devices," said Paul Lipman, CEO at BullGuard. "The industry must wake up and address this issue. Taking down websites may seem relatively innocuous, but Reaper has the potential to cause massive amounts of damage including crashing important online services. How long before we see organisations held to ransom or critical national infrastructure brought to a halt? These are very real and plausible scenarios, yet those responsible for security seem to have gone to sleep."

BullGuard protects consumer's smart homes with Dojo by BullGuard (https://dojo.bullguard.com/), a consumer cybersecurity product built from the ground-up as an enterprise-class network security service, and delivered in a way that is incredibly easy for consumers to use. Dojo utilizes unprecedented multi-layered cybersecurity protection including: Automatic Device Discovery and Categorization, Smart Firewall, Smart IPDS (Intrusion Prevention and Detection System), Secure Web Proxy and Network Behavior Anomaly Detection. Dojo's device and application aware cybersecurity service automatically adjusts the security envelope by constantly monitoring device behaviors.

378 Million Devices Potentially Vulnerable to Hacking in 2017.

The scale of poor IoT device security was recently revealed by an analysis of BullGuard's IoT Scanner (https://iotscanner.bullguard.com/), a tool that scans home networks searching for vulnerabilities. Approximately 310,000 users accessed the BullGuard IoT Scanner to scan their network for vulnerabilities. The scan analysis revealed that 4.5 per cent, or nearly 14,000 devices, could be easily hacked. Industry analysts at Garner forecast that 8.4 billion connected things will be in use worldwide in 2017, and will reach 20.4 billion by 2020 (https://www.gartner.com/newsroom/id/3598917). Extrapolating BullGuard's IoT Scanner results means 378 million devices are potentially vulnerable to hacking now, growing to more than

900 million potentially susceptible devices by 2020.

According to a recent consumer study conducted by BullGuard, 66 per cent of Americans and 55 per cent of Brits stated the number one thing that would prevent them from buying more IoT connected devices are security concerns. “The widespread adoption of IoT has brought with it tremendous convenience, but consumers are starting to have high expectations about the responsibility device manufacturers should bear to ensure their connected gadgets are secure from cyberattacks,” added Lipman. “Robust multi-layered protection needs to be adopted at a wider level in society if we don’t want to see globally coordinated IoT cyberattacks that could be potentially calamitous.”

About BullGuard

BullGuard is a leader in consumer cybersecurity. We make it simple to protect everything in your digital life – your data, your identity and your Smart Home. BullGuard combines technical expertise with a genuine understanding of your needs to deliver complete protections across all of your connected devices. As part of our ongoing promise to be champion of today’s digital consumer, we’ve added Dojo by BullGuard to our multi-award winning product portfolio. It’s the best custom-built solution to protect Wi-Fi enabled devices in the home, and gives customers the freedom to add as many Smart Home devices as they want without compromising privacy or security. Dojo is the cornerstone of a Smart Home, ensuring a connected world where every consumer, in every home, is smart, safe and protected.

Follow us on Twitter @BullGuard (http://www.twitter.com/BullGuard) and @DojoSafe (http://www.twitter.com/DojoSafe), like us on Facebook at BullGuard (https://www.facebook.com/BullGuard/?fref=ts) and Dojo (https://www.facebook.com/meetdojo/?fref=ts), or learn more at https://www.bullguard.com (https://www.bullguard.com/) or https://dojo.bullguard.com (https://dojo.bullguard.com/).

###

Media Contacts:
Michelle Cross
The PR Room
Michelle.cross@theprroom.co.uk