NEWMEYER & DILLION LLP

BUILDERS BEWARE: SMART HOMES UNDER ATTACK BY "HIDE 'N SEEK" BOTNET

By: Scott L. Satkin & Amtoj Randhawa

Scott Satkin

Contact

949.271.7204
scott.satkin@ndlf.com

Practice Areas

Business Litigation
Business Transactions
Cybersecurity
Insurance Law
Real Estate Litigation
Real Estate Transactions

Amtoj Randhawa

Contact

949.271.7383
amtoj.randhawa@ndlf.com

Practice Areas

Business Litigation
Construction Litigation
Cybersecurity
Insurance Law
Real Estate Litigation

German manufacturer eQ-3 has found itself under siege by a botnet known as "Hide 'N Seek." This pernicious malware has infected tens of thousands of eQ-3's smart home devices by compromising the device's central control unit. Once a device has been infected, the malware spreads to other Internet of Things ("IoT") devices connected to the same wireless network. IoT devices have become the prime target for botnet attacks. As opposed to computers, laptops, or other larger computing devices, the smaller storage capacity and lower processing power of IoT devices limit the amount and complexity of the security measures that can be installed—making them an easier target for botnets.

What is a Botnet?

For those unfamiliar with the term, a botnet is a network of devices infected with a malware program allowing the infector to control and/or exploit the devices. Once a suitable number of devices are infected, the person or group controlling the botnet can harness the computing power of each infected device to perform activities which were previously constrained by a single device's capabilities (i.e. DDoS attacks, spamming, cryptocurrency mining, etc.).

Hide 'N Seek – History and Capabilities

The Hide 'N Seek botnet first appeared in January 2018 and has since spread rapidly. Its sophisticated design and capabilities have captivated the attention of many security watchdogs and researchers. While many botnets are designed to be "quick and dirty" (i.e. infect a few devices, eke out a little profit, and inevitably be cleared out or rendered ineffective by security updates and fixes), Hide 'N Seek was designed to maintain itself in the host's system indefinitely. When it was first released, Hide 'N Seek primarily targeted certain routers and internet-enabled security cameras; however, it has now began targeting digital video recorders, database servers, and most recently, smart home hubs.

Hide 'N Seek's communication capabilities are also more advanced than previous botnets. Previous botnets relied on existing communications protocols to communicate with one another, but Hide 'N Seek uses a custom-built peer-to-peer system to communicate. This advancement allows Hide 'N Seek to spread more rapidly than previous botnets.

Hide 'N Seek is also capable of extracting a device owner's personal information (i.e. name, address, e-mail, telephone numbers, etc.) whereas previous botnets were not.

Most importantly, Hide 'N Seek is consistently updated to increase its infection rate, decrease its detection probability, and bypass any security measures designed to detect and remove it from the system. This modularity has proved to be Hide 'N Seek's greatest strength.

Protecting Against Hide 'N Seek and Other Botnets

While many of the precautions will undoubtedly come from the device manufacturers vis-à-vis software programming and updates, homebuilders can still take some precautions to protect their customers.

1. When selecting a smart home system to incorporate into a home's construction, be sure to evaluate its security features including, but not limited to its: wireless connectivity, password/passphrase requirements, interconnectedness with other IoT devices, etc. Third-party reviews from tech-oriented outlets will likely have useful information on a device's security measures, vulnerabilities, and any recent security compromises.

2. Be vigilant in installing any eQ-3 smart home systems. The extent of the damage caused by Hide 'N Seek botnet remains unknown, as does damage from other potentially-infected technology. Thus, it may be prudent to avoid installing any eQ-3 device until it becomes evident that the threat has been neutralized and all security vulnerabilities have been remedied.

3. If a builder uses technology other than eQ-3, precautions must be taken. Ensure that technology providers are thoroughly researched. It is also recommended to include strong contractual indemnity provisions, and require vendors to carry cyber-specific insurance policies.

4. Homebuilders should consider purchasing their own stand alone cyber liability policies as a safety net, should potential exposure arise.

Scott Satkin and Amtoj Randhawa are associates in the Cybersecurity group of Newmeyer & Dillion. Focused on helping clients navigate the legal dispute implications of cybersecurity, they advise businesses on implementing and adopting proactive measures to prevent and neutralize cybersecurity threats. For questions on how they can help, contact Scott at scott.satkin@ndlf.com and Amtoj at amtoj.randhawa@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America© and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.