The 2016 Dyn cyberattack

I. Problem definition and analysis (including timeline)

On Friday, October 21, 2016, up to three separate but related Distributed Denial of Service (DDoS) cyberattacks were observed against Dyn, Incorporated, an Internet performance management company and Domain Name System (DNS) provider. The first wave of attacks were recorded at approximately 11:10 UTC, (5:10 AM CDT) and lasted until approximately 13:20 UTC, (7:20 AM CDT). A second wave of outages occurred from 15:50 UTC (9:50 AM CDT) until 17:00 UTC (11:00 AM CDT), with residual impacts lasting until approx 20:30 UTC, (2:30 PM CDT). Ironically, the attack took place while a number of cybersecurity professionals were delivering a packed-house roundtable discussion, presented by Verizon Communications (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/) at Webster University's Community Music School Auditorium on that Friday morning.

II. Business impact and implications of the attack

The intent of the malware was to prevent the successful resolution of domain names (for example https://www.bankofamerica.com/) which correspond to numeric IP addresses (for example 171.161.160.10) via an exploitation of Internet of Things (IoT) devices such as laptop webcams, residential gateways and routers, interconnected baby monitors, and printers. These IoT devices were coordinated into a massive automated network (or "botnet") via elementary "script-kiddies". These bots, in turn, were subsequently programmed to attack and remove the availability of HTTP (web) services from several websites including but not limited to: Amazon, CNN, DirecTV, iHeartRadio, The New York Times, Paypal, Quora, Reddit, Starbucks, Twitter, Verizon Communications, Visa, and Walgreens.

Subsequent investigations have found that a specific open-sourced software codebase called "Mirai" was responsible for taking down these companies' servers. A detailed background on Mirai is provided below.

III. Recommendations to defend against the DYN attack and Mirai botnet

"Mirai" is a Japanese word meaning "the future". Supposedly, this "future" was to refer to the Internet of Things, a next-generation gradual migration towards the interconnectivity of household devices. These household devices have a plethora of vulnerabilities up to and including factory-set usernames and passwords, default I/O ports, and possibly as-of-yet unpatched firmware, which Mirai successfully exploited.

Since the Mirai codebase is open sourced and freely available (written in the C and Go programming languages), it is at the risk of any organization NOT to study and prepare their servers against such traffic requests. Professional anti malware toolkits include the Kali Linux operating system, installed with Netcat and Wireshark software packages.

Respectfully Submitted 2016-12-09 by Erik A. Buschardt

References:

Krebs, Brian (September 21, 2016). "KrebsOnSecurity Hit With Record DDoS". Brian Krebs. Retrieved 7 December 2016 from https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

"Blame the Internet of Things for Destroying the Internet Today". Motherboard. Retrieved 2016-12-07 from http://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today.

Hilton, Scott. (2016, October 26). Dyn Analysis Summary Of Friday October 21 Attack [Web log post]. Retrieved from http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.