Previous article

Next article

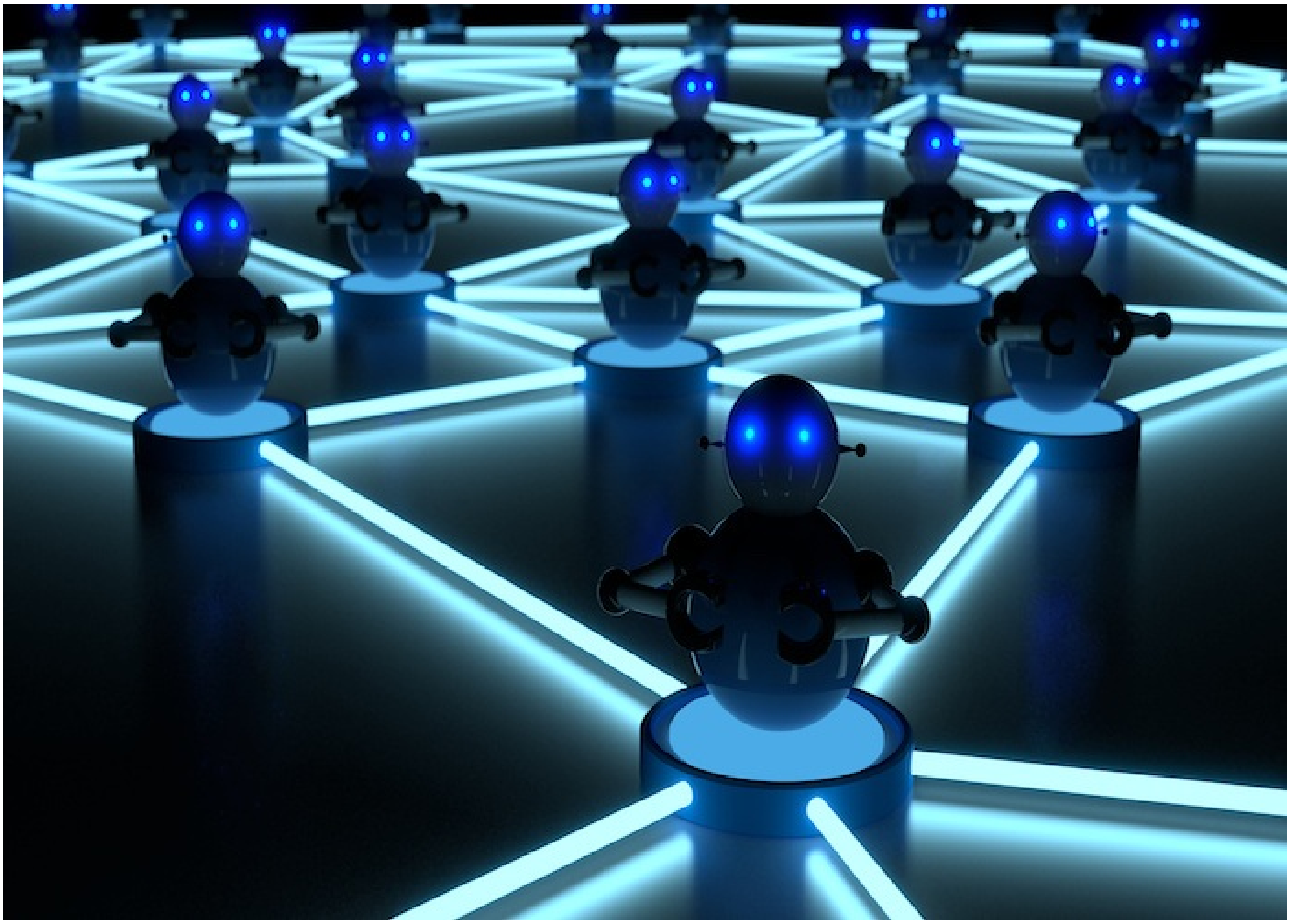
Forget BlueKeep: Beware the GoldBrute

Author:

Tara Seals

June 7, 2019 / 1:15 pm

Share this article:



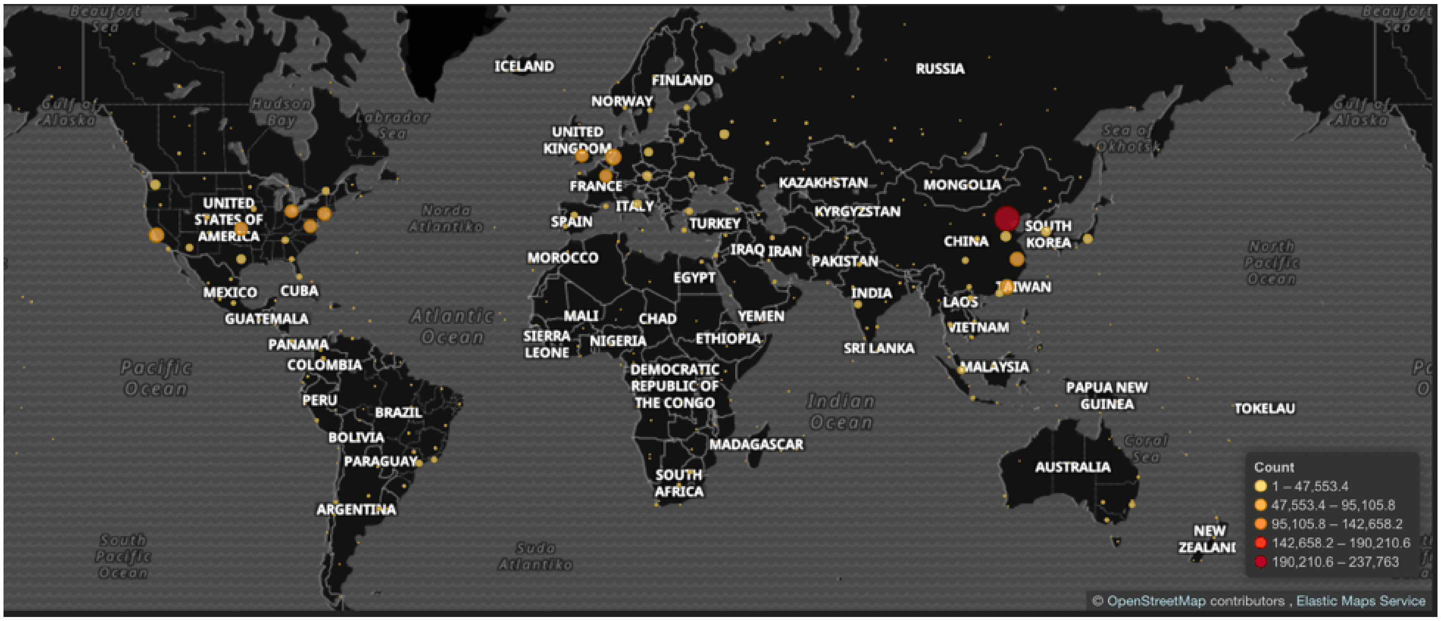
A botnet has appeared that has attempted to brute-force 1.5 million RDP connections to Windows systems in the last few days — and counting.

While everyone's talking about the BlueKeep Mega-Worm, this is not the main monster to fear, according to recent web attack activity. Rather, a researcher is warning that the GoldBrute botnet poses the greatest threat to Windows systems right now.

In the past few days, GoldBrute (named after the Java class it uses) has attempted to brute-force Remote Desktop Protocol (RDP) connections for 1.5 million Windows systems and counting, according to Morphus Labs chief research officer Renato Marinho. The botnet is actively scanning the internet for machines with RDP exposed, and trying out weak or reused passwords to see if it can gain access to the systems.

After initially spotting the activity earlier this week, "after six hours, we received 2.1 million IP addresses from the C2 server from which 1,596,571 are unique," Marinho wrote in a posting on Thursday, adding that the botnet continues to swell in size (though he didn't quantify it). There are plenty of hosts to be had: Shodan reveals nearly 2.5 million exposed RDP instances as of this writing

machines remotely; it's also sometimes used by teleworking employees. Once an attacker has access to the connection, he or she has access to the Windows desktop and can set about doing anything the legitimate user would have permission to do. Obviously, pivoting into corporate networks, implanting malware, stealing information, and marshaling CPU resources for cryptomining or distributed denial-of-service attacks could all be on the cyberattack menu du jour for the GoldBrute operators.



GoldBrute distribution as of June 6, 2019.

Speaking of whom, it turns out that the GoldBrute botnet is controlled by a single command-and-control (C2) server, associated with an IP address in New Jersey. These adversaries could in theory carry all of the aforementioned attacks out on a large scale, all at once.

According to the researcher, the C2 is exchanging data with the bots via AES-encrypted WebSocket connections to port 8333. An infected system will first be instructed to download the bot code (which is a very large 80MB package that includes the complete Java Runtime, Marinho said); once it has burrowed into its host, it starts scanning random IP addresses to find more hosts, and reporting the IP addresses back to the C2.

"After the bot reports 80 new victims, the C2 server will assign a set of targets to brute-force to the bot," Marinho said. "Each bot will only try one particular username and password per target. This is possibly a strategy to fly under the radar of security tools, as each authentication attempt comes from different addresses."

The virulence of the activity should give admins pause, he added: "While the reporting around this 'Bluekeep' vulnerability focused on patching vulnerable servers, exposing RDP to the internet has never been a good idea."

The BlueKeep critical remote code-execution vulnerability (CVE-2019-0708), for which a fully functioning exploit has been developed (but kept private by researchers), also lays open remote desktop services for attack. It's widely seen as the next big corporate threat, because it's wormable and requires no user interaction to spread. Th

"GoldBrute highlights the fact that the bulk of scanning activity) for RDP isn't BlueKeep related," they wrote in a posting on Thursday. "When attackers can just bypass locked screens or guess weak RDP credentials, IT departments need to focus on making sure machines are not unnecessarily exposing RDP on the internet (putting a layer in between, such as a VPN, would help) and that users know how to use RDP properly."

That said, patching the BlueKeep flaw – which affects older version of Windows, including Windows 7, Windows XP, Server 2003, Server 2008 and Server 2008 R2 – should obviously also be on the top of the to-do list. Millions of systems remain vulnerable to it.