DDoS attacks continue to morph

According to Bryan Hamman, territory manager for sub-Saharan Africa at Arbor Networks, while reflection and amplification techniques have come to characterise a large number of complex, multi-vector DDoS attacks, the latest approach is to use reflection to exploit connection-less lightweight directory access protocols (CLDAPs).

Bryan Hamman

Traditionally, large attacks based on reflection or amplification were the likes of NTP, DNS, SNMP, SSDP, SQL RS or Chargen. "But this new trend has now been discovered ‘in the wild’, with the force to generate highly efficient and destructive results,” he says.

What is CLDAP?

CLDAP is essentially a computer networking protocol designed for legitimate users to query and modify stored data on X.500 directory systems. It is typically used on Windows Exchange servers and domain controllers.

By providing directory and access control, one can use CLDAP to locate printers on a network, find a phone number of an employee, or see the security groups a user belongs to, for instance.

The modus operandi involves the attacker spoofing the source of a connectionless protocol, pinging the server with ultra-small queries. The server then responds to the victim with a far larger response. Initial findings suggest that this approach can amplify the initial response in the region of 46 to 55 times the size.

“This makes CLDAP attacks highly efficient. A well-orchestrated attack that exploits an organisation's vulnerabilities could very quickly achieve massive total attack size, and bring down the digital systems of all but the largest and best-protected organisations.”

Primary targets

Reports* from cloud giant Akamai show that the largest example of CLDAP reflection as the sole vector resulted in a payload of 52 bytes, amplified to as much as 70 times in this case – creating an attack data payload of 3,662 bytes, a peak bandwidth of 24Gbps, and 2 million packets per second.

CLDAP attacks have primarily targeted the software and technology industry. Other industries targeted include internet and telecom, media and entertainment, education, retail and consumer goods, and financial services.

Fighting back

To effectively resist this type of DDoS attack, organisations need to thoroughly address the potential threat at a network level, by covering a number of bases:

- **Prevent abuse:** Ensure that you have anti-spoofing deployed at the edges of your networks.
- **Detect attacks:** Leverage flow telemetry exported from all network edges to Arbor technology, to automatically detect, classify, traceback, and alert on DDoS attacks.
- **Ready mitigation techniques:** Deploy network infrastructure-based reaction/ mitigation techniques such as Source-Based Remotely-Triggered Blackholing (S/RTBH) and flowspec at all network edges.
- **Mitigate attacks:** Deploy intelligent DDoS mitigation systems at strategic points within your network.
- **Minimise damage:** Deploy Quality-of-Service (QoS) mechanisms at all network edges to police CLDAP traffic down to an appropriate level.
- **Remediate CLDAP services:** Proactively scan for and remediate abusable CLDAP services on the ISP and customer networks to reduce the number of abusable CLDAP servers.

“Like many other reflection techniques, organisations must always have ingress filtering in place. Unless there is a real need for your firm to have CLDAP available over the internet, you shouldn’t expose this protocol,” concludes Hamman.

*CLDAP reflection attacks may be the next big DDoS technique