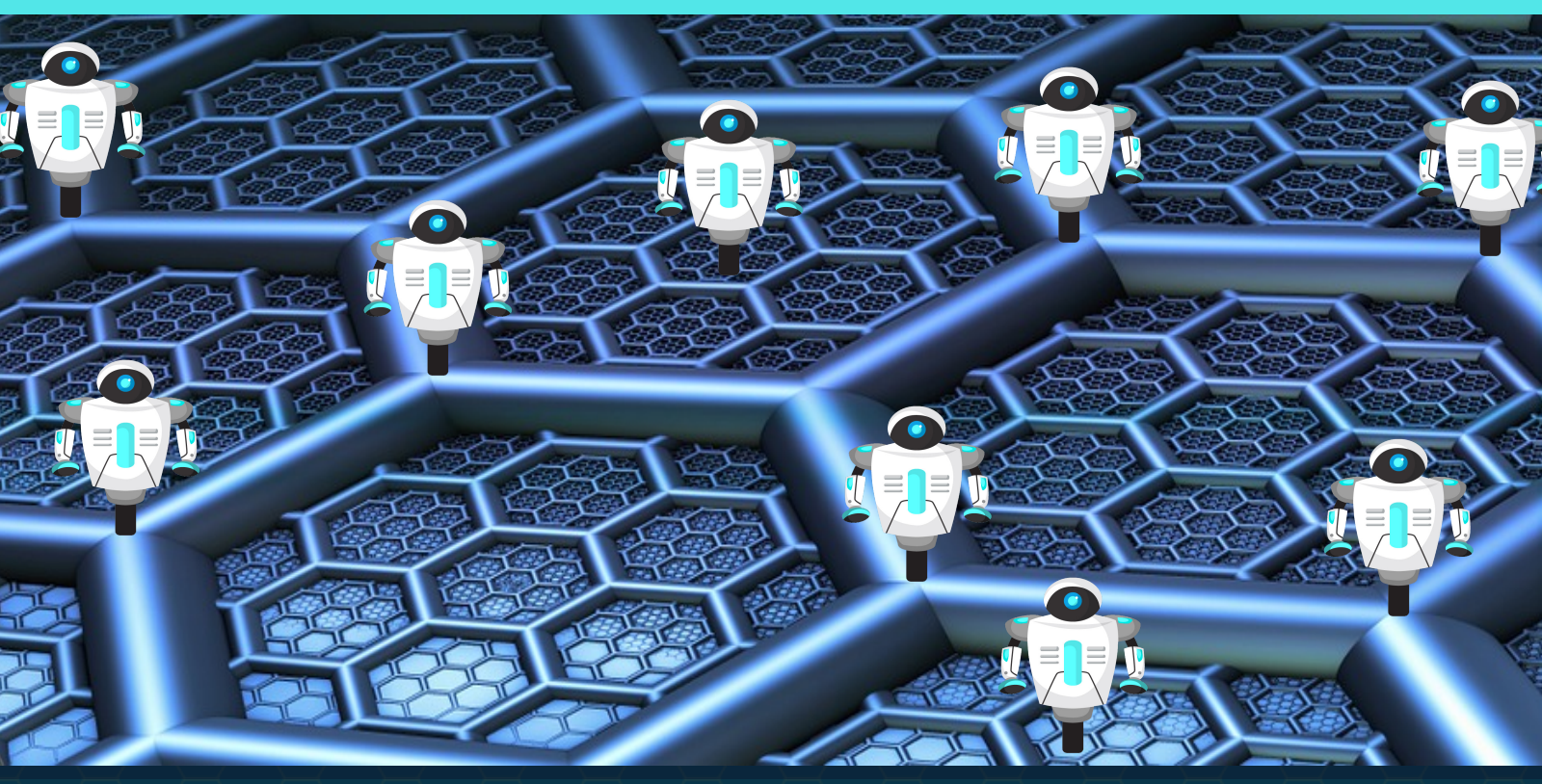
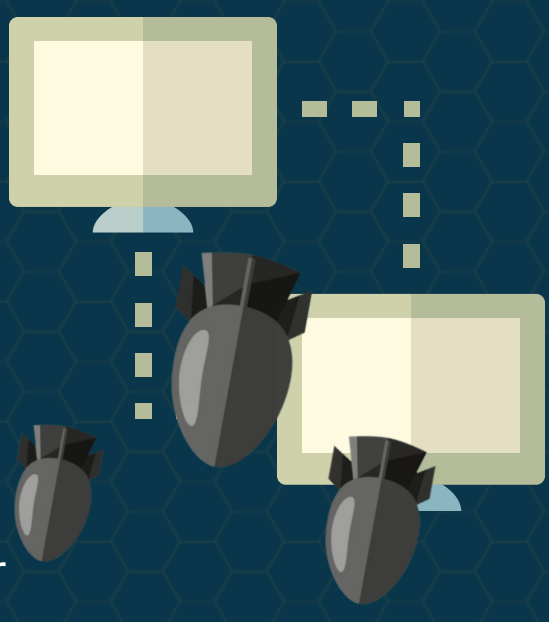
Necurs Botnet



01 Necurs botnet uses a hybrid architecture to communicate.

02 It uses a direct C2 server to obtain new instructions or configuration information.

03 The details about new C2s are distributed through Domain Generation Algorithm or through P2P communication.



04 The botnet follows an on-off strategy; it establishes communication to deliver commands and goes offline for weeks/months before resurfacing.

05 This strategy has helped the botnet to avoid detection and led it to become the second most prevalent botnet.

History Of Necurs Botnet

2012	Inception
2013	Acted as rootkit to spread Zeus Banking Trojan
2014	Distribution of ransomware such as CryptoLocker
2015	Distribution of CryptoWall ransomware
2016	DDoS and proxy capabilities implanted in the botnet
2018	Cryptocurrency feature added to deploy Monroe-mining malware

www.thecentexitguy.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road, Suite # 1100, Dallas, TX 75240
Phone: (972) 375 - 9654

501 N. 4th Street, Killeen, TX 76541
Phone: (254) 213 - 4740

1201 Peachtree St NE, Suite 200, Atlanta, GA 30361
Phone: (404) 994 - 5074

7600 Chevy Chase Drive, Suite 300, Austin, TX 78752
Phone: (512) 956 - 5454