UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00086

SYSTEMBC BACKDOOR LEVERAGED FOR RANSOMWARE

DATE ISSUED: 21st December 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Numerous attempts to deploy the SystemBC backdoor have been detected in recent months in conjunction with Ryuk and Egregor ransomware attacks

BREAKDOWN

First discovered in 2019, the SystemBC backdoor malware has recently evolved in automate activities and anonymise the Tor platform in an effort to obscure the command and control (C2) destination and traffic. It is suspected to be utilised by Ransomware as a Service (RaaS) groups to establish a persistent connection with victims and deploy various attacks, including launching Ryuk and Egregor ransomware. By acting as a Virtual Private Network (VPN) via the SOCK5 proxy, traffic is obscured as it travels to the C2 destination. This malware has also been seen to be used in conjunction with Cobalt Strike, Buer loader, QBot and ZLoader as the initial attack vector to gain a foothold and move laterally across a system before establishing persistence by deploying the SystemBC backdoor for added persistence. By automating these attacks, a lesser degree of interaction is required by the attacker and therefore, a greater number of attacks can be deployed quickly.

REMEDIATION STEPS

- Educate users on the dangers of social engineering and malicious emails to avoid exposure to malicious software
- Monitor system and network behaviour for suspicious activity and outbound requests
- Ensure an up-to-date Business Continuity and Disaster Recovery plans are in place, and includes mitigations and contingencies for ransomware attacks, test back-ups and run through restore scenario exercises regularly. Ensure at least one back up is kept offline (unable to be accessed through network)

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/ryuk-egregor-ransomware-systembc-backdoor/162333/