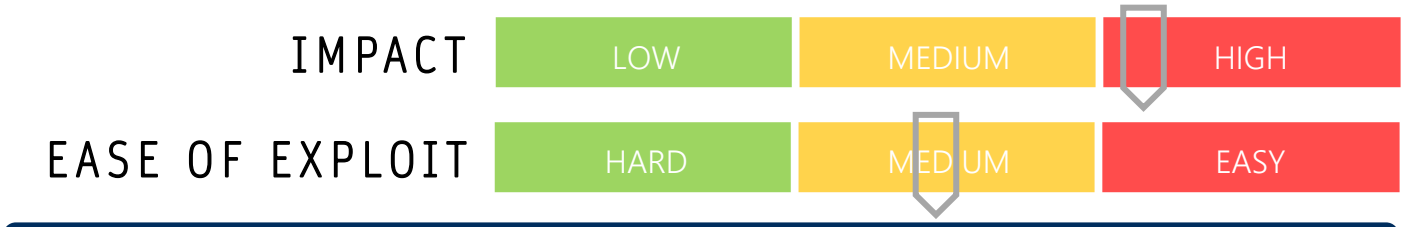
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00073

BLACKROTA GOLANG BACKDOOR IN DOCKER

DATE ISSUED: 30th November 2020



OVERVIEW

Written in the 'Go' Language, this new backdoor known as Blackrota targets a security flaw in Docker that uses a number of techniques to avoid detection and is nearly impossible to reverse analyse for researchers.

BREAKDOWN

First discovered in a honeypot, the malware made attempts to break through an unauthorised access vulnerability in the remote access API for Docker. Named by researchers after its Command and Control (C2) domain, this malware is known to effect Linux systems in Executable and Linkable Form (ELF) file format in x86/x86-64 CPUs. The malware uses a beacon known as a "geacon" to communicate with the C2 to determine instructions for data collection and exfiltration in a similar manner to CobaltStrike. This geacon enables the execution of shell commands, upload and download of files, browsing and setting a sleep delay time. The open-source tool gobfuscate is used to hide source code using randomized character substitutions for package names, global variable names, function names, type and method names, before compiling, which is what makes this malware so difficult to reverse engineer and catch using traditional methods. This tool replaces all strings with XOR ciphers and an associated decoding function to act at program execution. Normally, Go language malware creates binary files using static links and when disassembled displays a list of functions and the obfuscation of the symbolic and type information achieved by the implementation of gobfuscate in this malware makes analysis near impossible.

REMEDIATION STEPS

- Use URL filtering to prevent any access to the blackrota.ga
- Use network monitoring tools to identify suspicious outbound requests

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/blackrota-golang-backdoor-obfuscation/161544/
Netlab 360 https://blog.netlab.360.com/blackrota-an-obfuscated-backdoor-written-in-go-en/