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

CYBER GUIDANCE ISSUE 00187

LINUX & MS SERVERS VULNERABLE TO HOLESWORM

DATE ISSUED: 23rd August 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The HolesWorm (AKA Vuln) Botnet cryptominer is fast becoming one of the most successful and dubbed the "King of Vulnerability Exploitation" due to its ability to juggle multiple known vulnerabilities between attacks to gain access to a system – breaking into more than 1,000 cloud hosts since June.

BREAKDOWN

The HolesWarm virus has evolved over 20 different attack methods while carrying out its mission to deploy cryptomining software to mine for Monero cryptocurrency, steal user's credentials and offer system control to the attackers. Tencent Security were first to discover the malware and have observed exploitation activities across a number of common office server components (including Apache Tomcat, Jenkins, Shiro, Spring boot, Structs2, UFIDA, WebLogic, XXL-JOB and Zhiyuan). By using infected machines to audit numerous strings of blockchain, attacker's mine Monero at scale – the more machines they infect, the larger that scale grows. By constantly updating the HolesWorm modules, attackers can pivot to a new attack method and exploit other vulnerabilities making the behaviour unpredictable, as has been seen over the past two months – and it looks like they're just getting started.

REMEDIATION STEPS

- Tencent security are recommending that "organisations actively repair high-risk vulnerabilities in related network components" in order to prevent exposure and compromise.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/holeswarm-malware-windows-linux/168759/
WinBuzzer https://winbuzzer.com/2021/08/19/holeswarm-cryptomining-malware-found-in-windows-vulnerabilities-since-june-xcxwbn/