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

CYBER GUIDANCE ISSUE 00026

SCRIPT KIDDIES PLAY WITH DHARMA

DATE ISSUED: 25th August 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	LOW	MEDIUM	HIGH

OVERVIEW

Dharma A.K.A Crysis ransomware is being distributed by an Iran-linked group of script kiddies – unsophisticated or low-skilled attackers, highlighting that it is no longer large, mature, or state-sponsored operations deploying such attacks.

BREAKDOWN

The group has targeted a number of companies globally using a distributed Ransomware-as-a-Service (RaaS) style of attack using the source code for Dharma that was released in March this year. Targeting Remote Desktop Protocol (RDP) ports by scanning with Masscan and using publicly available tools for lateral movement across the network and discover weak credentials using NLBrute brute-force attacks and infecting vulnerable hosts with the ransomware. Some cases saw attempted escalation of privileges through CVE-2017-0213 in Windows systems and removal of built-in anti-virus software using other publicly available tools such as Defender Control and Your Uninstaller. Demands seen were between $12,000 and $59,000 USD.

REMEDIATION STEPS

- Close RDP port 3389 if not in use
- Monitor network for suspicious activity and set alerts for RDP connections in network monitoring software.
- Use third-party anti-malware and enable features that prevent its uninstallation or removal and create alerts for administrators where possible.
- Scan devices using anti-malware software to detect any running malware.
- Limit login attempts to lockout anyone trying to gain access with multiple incorrect login attempts

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/iran-linked-newbie-hackers-spread-dharma-ransomware-via-rdp-ports/158580/

Bank Info Security: https://www.bankinfosecurity.com/ransomware-darkside-debuts-script-kiddies-tap-dharma-a-14874

Info Security Magazine: https://www.infosecurity-magazine.com/news/lowskilled-iranian-hackers-dharma/

Tripwire: https://www.tripwire.com/state-of-security/security-data-protection/rdp-used-by-iranian-actors-in-international-dharma-ransomware-attacks/