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

CYBER GUIDANCE ISSUE 00179

PRAYING MANTIS TARGETS WINDOWS IIS

DATE ISSUED: 3rd August 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Attacks that are "operating almost completely in-memory" are being executed by a new threat actor dubbed Praying Mantis AKA TG1021 is targeting Windows Internet-facing servers and vanishing without a trace.

BREAKDOWN

Using a completely custom malware framework and deserialization attacks to load a completely volatile toolset specifically designed to target the Windows IIS environment, Praying Mantis is able to leave little trace of it's presence on infected systems. Volatile refers to the nature of memory or RAM (Random Access Memory) that requires power to sustain data and stored information and once the power is turned off, all data is deleted. Once the core component is loaded into IIS servers, it is able to intercept HTTP requests to the server and while the threat actor has access, they are able to carry out credential harvesting, lateral movement across the network, reconnaissance activities, establish a back door, and much more. This skilled attacker appears to have great knowledge of IIS and security operations as they employ numerous detection evasion tactics. Deleting all disk-resident tools means that although they cannot ascertain persistence, they are able to use stealth and have their activities go undetected.

REMEDIATION STEPS

- Patch .NET deserialization vulnerabilities
- Check the known IoC's provided in Sygnia's report in the resources below (pg20+).
- Use tools to discover compromise in Internet facing IIS servers.

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/praying-mantis-threat-actor-targeting-windows-internet-facing-servers-with-malware
Sygnia https://www.sygnia.co/praying-mantis-targeted-apt
The Cyber Wire https://thecyberwire.com/newsletters/research-briefing/3/30