Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 199 **25-08-2023**

Name: Identification of WannaCry Family

Source IP Address: 198.96.155.3

Threat Classification: Malware

Affected Software / Services:

- Microsoft Windows operating system's Server Message Block (SMB) protocol

Summary:

A critical threat has been identified within the enterprise network environment on the publicly exposed assets of the organization. The IP address "**198.96.155.3**" has been positively linked to the WannaCry ransomware family. This notorious ransomware is known for its widespread impact on systems by encrypting data and demanding ransom payments for decryption. Immediate action is required to mitigate potential risks associated with this IP address.

Severity	**Critical**
Attack Vector	Network

Recommendations:

- Isolate the affected system from the network immediately to prevent further spread. Block all inbound and outbound network traffic to and from the IP address "198.96.155.3" using network firewalls or security appliances.
- Activate your incident response plan and involve your security team to assess the extent of the potential threat and its impact on your network.

- Ensure all systems, including servers and endpoints, have the latest security patches and updates applied. This includes critical patches related to the WannaCry vulnerabilities.
- Verify the integrity of your backup systems and ensure that critical data is regularly backed up and stored offline to protect against ransomware attacks.
- Strengthen your email security measures to prevent phishing attempts and malicious attachments that could introduce ransomware into your network.
- Educate employees and users about the risks of opening attachments or clicking on links from unknown or unverified sources.
- Implement robust intrusion detection systems (IDS) and network monitoring tools to detect any unusual or suspicious activity related to this IP address.
- Stay updated on the latest threat intelligence related to the WannaCry ransomware family and collaborate with cybersecurity experts to implement effective countermeasures.
- Please treat this advisory with the utmost urgency. The identification of the IP address "198.96.155.3" as belonging to the WannaCry ransomware family requires immediate action to safeguard your network from potential attacks.