**Cyber Security Advisories**

**Date: 12 February 2025**

1. **TA-MAW-2025-02-12-012**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

stresser.pw

**Hashes:**

1cf613c80e8bfab9095cb822e2c35c25bcc1158f05ef0d573cb9886f8224b96d

272e82409d73a99bd0d0bddf17f9fba8a64ee19a270c505663613c993ba1f975

37e700e7388bf976908ba9f0123377718fa2f6e128d5fb4ebc1d59ea2a13f32a

4b2d6c00e8960e0862bae557bd58d9d54b60a16c6f964b7b0e393e503ab35db5

4c061dbb1c111157c54a3df1f91abdc1923ba4e797a24ae3f50d29ee05a00840

5b6bc07c886df32ea4c41f2351124549ec40eb8ed38b4177869ae64a0b0caf7f

6836ee6e55549436f28fc221725689d61d3043d2a468a3afa12dbb2f646ed71f

7b21d08e8dc3dc1811f98dd9838bf52083bb1c3f9a88c6181b8c79d00480eb0b

a18348c96c06111c05cdbd757657da3be15b30aadf3674eeb24119ae57d5866c

b8db134d110f977a2317b9b0d360a41982ff50ed6d6c5087feccb4ac130c36cf

c37a3ecda58d2c73200beef947749265990dcc8de356aad31e9bbf1b0a7ca013

d5f6059fb7fc276f92ccd4e1994b2f8e92680d3882b679dedcec902414d8b8ca

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

1. **TA-PHI-2025-02-12-009**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains that are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

www.email.gov.in.indiandefenceforces.link

email.gov.in.indiandefenceforces.link

gov.in.indiandefenceforces.link

\*.indiandefenceforces.link

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Install and regularly update antivirus software.
* Install Updates and Patches regularly.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Implement Multi-Factor Authentication (MFA).
* Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.
* Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.
* Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

1. **TA-RAN-2025-02-10-004**

It has been observed that TitanPlus is deploying multiple ransomware variants that include Cactus & Black Basta, as part of an expanding cyber-attack campaign. This threat is characterised by the use of sophisticated techniques to deliver malware, including Remote Access Tools (RATs) and multiple payloads through a variety of channels.

The adversary uses DLL sideloading and masquerading techniques to evade detection and deliver multiple malware payloads through sophisticated methods.

**Distribution Methods:**

TitanPlus employs a variety of distribution methods to deliver malware:

* Phishing Emails: Leading victims to malicious URLs or attachments that execute the infection chain.
* Internet Shortcuts: Using shortcut files that download and execute malicious scripts upon opening.
* ZIP Archives: Hosting malicious content within ZIP files that contain URL files directing users to download malware.
* WebDAV Servers: Utilizing a network of WebDAV servers to host and distribute malware.
* Cloud Services: Abusing services like Cloudflare to create temporary tunnels for malware distribution.

**Key Characteristics:**

* Multiple Payloads: Adversary involve simultaneous deployment of several malware families like Cactus and Black Basta ransomware variants.
* Phishing Tactics: The initial access is typically gained via phishing emails, which may include malicious URLs or attachments that lead to infected files.
* Obfuscation Techniques: The malware employs various obfuscation methods to evade detection, using tools like BatchShield to obscure BAT files and Python scripts.
* WebDAV Infrastructure: Threat actors utilize WebDAV servers to host malware, allowing for easy updates and management of payloads.
* Adapting to Defenses: Regular adaptations to the infection chain are made to improve evasion tactics, such as adding antivirus checks within scripts to alter payload delivery based on the security environment.

**Impacts:**

* Data Loss: Critical data may be encrypted or stolen, leading to the potential loss of sensitive information.
* Operational Disruption: Ransomware attacks can halt business operations, significantly impacting productivity and revenue.
* Financial Costs: Organizations may incur hefty costs related to ransom payments, recovery efforts, and system repairs.
* Reputational Damage: Breaches can harm an organization’s reputation, leading to loss of customer trust.
* Regulatory Consequences: Violations of data protection regulations can result in fines and legal action against affected organizations.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IPs & Ports

195.123.233.148

89.185.80.170

195.211.96.135

45.8.157.146

207.90.238.67

38.180.138.15

185.190.251.114

38.180.138.167

45.8.157.144

185.190.251.16

207.90.238.52

89.185.80.86

38.180.25.3

45.8.157.199

5.181.3.164

**Hash:**

C9471F5CF7D75495622036FE35AFC532B7A05423C05EECA5BDA08BBE91CF9D71

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*