



रक्षा लेखा नियंत्रक (सेना)

Controller of Defence Accounts (Army)

बेल्वेडेर परिसर, आयुध पथ, मेरठ छावनी -250001

Belvedere Complex, Ayudh Path, Meerut Cantt-250001

e-mail: cdaedp.dad@hub.nic.in



Through Website

No. IT&S/III/Cyber Security/2024

Date: 17-01-2024

To

All Sections of Main Office

All sub-offices under the aegis of CDA (Army) Meerut

Sub: Raising Awareness about malicious use of 'Mythic C2 Framework'

In regard to the above subject, a copy of HQrs Office letter No. Mech/IT&S/810/Cyber Security/Misc dated 21.12.2023 is hereby forwarded for information and strict compliance.

This is issued with the approval of CDA.

Encl: As stated above.

M. M. M. M.
Sr. AO (IT&S)

“ हर काम देश के नाम ”

रक्षा लेखा महानियंत्रक



उलान बटार रोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt.- 110010

(IT&S Wing)



Phone: 011-25665588 Fax: 011-25675030 email: cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security/Misc **Circular**

Date: 21/12/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)
(through DAD WAN/email)

Sub: Mythic C2 Framework.

Mythic is a free to use, open source tool, written predominantly in Python. It provides cross platform payload options (Linux, Win and MacOS). It has an active development community and ‘plug n play’ functionality for its various agents. Mythic is attractive to threat actors of varying skill sets, for low skilled actor the ‘plug-n-play’ capabilities mean that they can use the framework very easily and effectively.

2. It has been observed that the Mythic framework is being used to target diplomatic, defense, research organizations in Indian government and the Indian Armed forces or related assets in India by unknown threat actors.

Mythic Framework:

3. Mythic is a powerful post exploitation red teaming framework built with python3 docker, docker-compose and a web browser UI. Mythic can be used to build, distribute and manage custom implant agents, also known as “myths” to interact with compromised systems. It supports various communication channels, including HTTP, HTTPS and DNS. Threat actor makes the victim download malicious files in their computer either by embedding the malicious link in ads of water hole websites or by sending malicious attachments in unsuspecting emails as part of phishing email campaigns.

4. Malicious files then try to establish communication with C2 server and upon successful connection with C2 server, the malicious payload gets dropped to the victim’s computer. Threat actors can either get complete access of the victim’s computer or the agent can exploit as per the commands loaded into the payload. These Remote Access Trojans can leak info, take screenshots and record webcam streams.

Modus operandi:

5. Threat actor creates fake domains that mimic legitimate military and defense organizations as a core component of their operations. It was found that the threat actor used several delivery methods in a campaign. These are executables masquerading as installers of

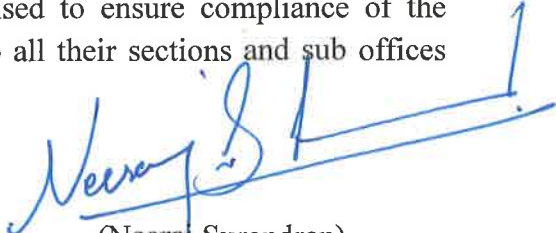
legitimate applications, archive files and malicious docs to target Indian entities and individuals. These chains of infection were seen in the placement of different types of implants not observed before.

6. It has been observed that threat actor use phishing attacks to gain initial access and take advantage of the vulnerabilities in the existing systems. The steps followed by attackers to compromise systems can be listed as follows:

- a. Step 1: User downloads malicious attachment namely LTC1.pdf through phishing email or by clicking on malicious hyperlink embedded in fake websites.
- b. Step 2 : Pdf checks for connectivity with C2 server and on establishment of servers communication, it downloads and drop trojan as per the OS being used .
- c. Step 3: Further, the Trojan checks for communication with sanic server (C2 server) which facilitates downloading of customized malicious files from where it downloads and drops malicious payload on victim's computer.
- d. Step 4 : Various types of payloads can be dropped on the victim's computer thereby granting the threat actor access to various files in the victim's computer.

Recommendations:

- a. Make sure that multi factor authentication is enabled for all accounts using in the network.
 - b. Internet dependency should be minimized for all critical systems and control system devices should not be connected directly to the internet.
 - c. All unused legacy applications should be removed from all machines on the network to avoid abuse.
 - d. Critical networks, behind firewalls must be isolated from all the external network.
 - e. To negate known security vulnerabilities, updates and patch OS applications periodically.
 - f. Strong passwords should be implemented.
 - g. Organisations should keep backup of important data, systems and configurations.
 - h. Conduct of cyber security awareness training to acquaint the users of the potential threat.
 - i. Always install applications from trusted source only, be careful while clicking on email links, even if they seem to come from a legitimate source.
7. In view of the above, all the Controllors are advised to ensure compliance of the recommendations given above and disseminate these to all their sections and sub offices for strict compliance.


(Neeraj Surendran)
Sr. ACGDA (IT&S)