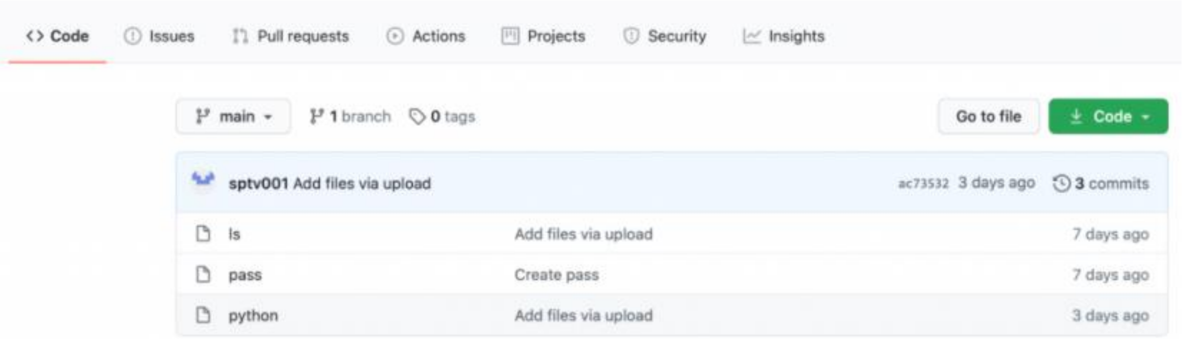
Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:122 **18-12-2020**

Name: Gitpaste-12 Botnet with a new Worm Targeting Linux Servers

Summary:

It has been recently reported that a new wormable botnet via GitHub and Pastebin repositories, has come up with expanded capabilities to compromise web applications, Routers and IP cameras by installing Linux-based crypto-miner and backdoors on target systems. It conducts a wide-range of attacks comprising at least 31 known vulnerabilities including F5 BIG-IP Traffic Management Interface (CVE-2020-5902), Pi-hole Web (CVE-2020-8816), Tenda AC15 AC1900 (CVE-2020-10987) and vBulletin (CVE-2020-17496), and an SQL injection bug in FUEL CMS (CVE-2020-17463).



sptv001 Add files via upload ac73532 3 days ago 3 commits

ls	Add files via upload	7 days ago
pass	Create pass	7 days ago
python	Add files via upload	3 days ago

Snapshot of GitHub repository hosting malicious files

For further details including technical analysis and relevant IDP signatures, Indicators of Compromise (IoCs), please visit following link:

https://blogs.juniper.net/en-us/threat-research/everything-but-the-kitchen-sink-more-attacks-from-the-gitpaste-12-worm

Recommendations:

- It is strongly recommended that the organization's Security team must perform **IoC sweeping** on every critical system running in enterprise environment available at following link: https://blogs.juniper.net/en-us/threat-research/everything-but-the-kitchen-sink-more-attacks-from-the-gitpaste-12-worm

- Implement filters at Email gateway to **filter out emails with known malware spamming indicators**. Also block the suspicious IP addresses at perimeter firewall.

- Implement Software Restriction Policies (SRP) to **block unsigned binaries running from %APPDATA% and %TEMP%** locations.

- **Block email attachments commonly associated with malware like .dll and .exe**, also block outbound network connections originating from **WinWord.exe, Powershell.exe, Powershell_ise.exe, Mshta.exe** and block inbound connections if remote access of system is not required.

- Ensure the **principle of least privilege** and **disable unnecessary services**/ ports as malware often exploit such services.

- **Regularly maintain data backups** and also ensure that backups are stored offline at a secure site.

- **Regularly update all software** including Operating System, Microsoft Office and other.

- Use **licensed antivirus software with heuristics and reputation ratings system** to identify and prevent malicious attachments, and also regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Regularly **provide Cyber security awareness trainings** to the employees.

- Avoid download/use of cracked and pirated software.

- In case of any incident, please report to this office.