Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:117 **30-11-2020**

Name: Linux malware posing as an Apache Web Server

Threat Classification: Malware/ Trojan

Summary:

It has been reported that a new version of Linux trojan **Stantinko** has rolled out to **pose as the legitimate Apache Web server process** (httpd) in order to make detection harder on infected hosts. This is done to prevent server owners from spotting the malware, as the Apache web server is often included **by default in many Linux distributions**.

For more technical details and analysis, please visit following links:

- https://www.intezer.com/blog/research/stantinkos-proxy-after-your-apache-server/
- https://www.bankinfosecurity.com/linux-botnet-disguises-itself-as-apache-server-a-15461

Recommendations:

- **Update all software** including Operating Systems, Servers, web browsers etc to the latest and stable versions with appropriate patches.
- Ensure the **principle of least privilege** and **disable unnecessary services**/ ports as malware often exploit such services.
- Maintain and implement a **strong password policy** throughout the infrastructure.
- **Regularly maintain data backups** and also ensure that backups are stored offline at a secure site.
- **Install, regularly maintain and update Antivirus solution** from a well reputed vendor.

- **System Administrators/ Network Administrators** to **configure host-based firewalls to block outbound connections from Excel.exe, Winword.exe, Wordpad.exe, Mshta.exe, Noptepad.exe, Eqnedt32.exe and ctfmon.exe** as Anti-malware solutions alone cannot fully protect against APT attacks.
- **Execution of unsigned executables** from sensitive webservers and endpoints must be blocked.
- Regularly **provide Cyber security awareness trainings** to the employees.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.