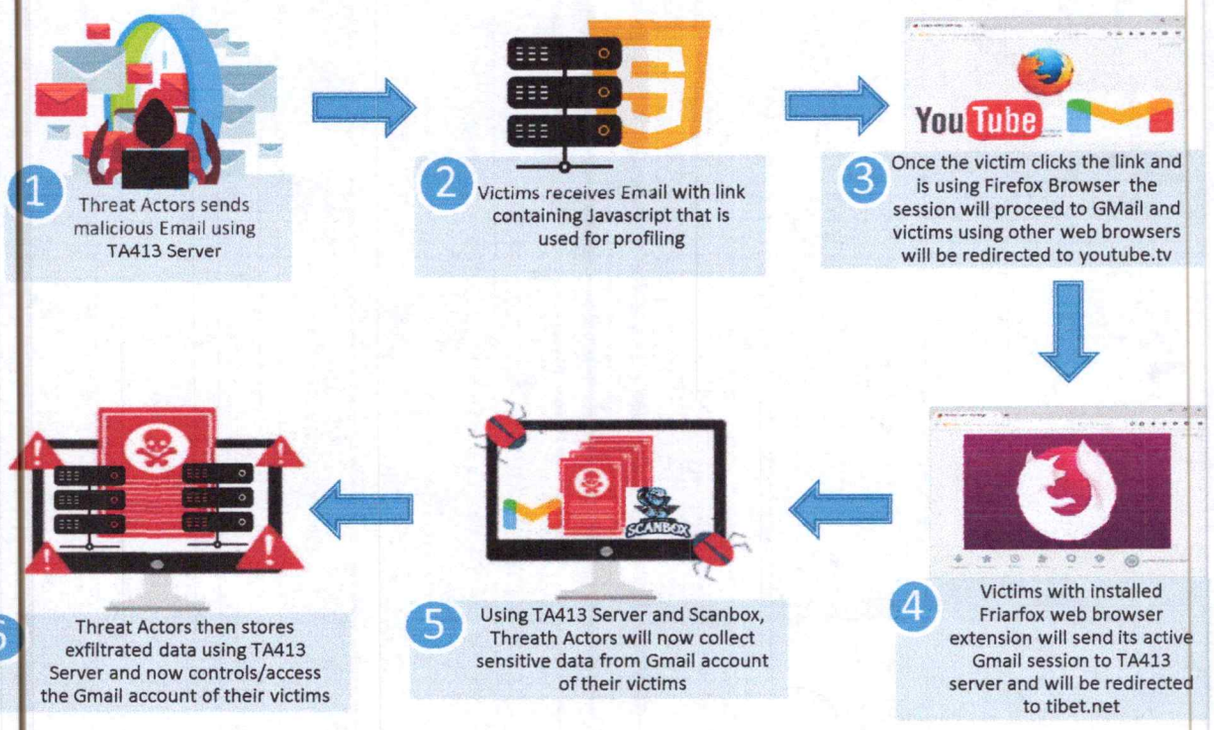
FriarFox Browser Extension Malware (CSB21-05)

April 8, 2021

Security researchers have intercepted a sneaky, albeit low-volume phishing campaign designed to plant malware via a malicious Firefox browser extension. Targets of the campaign typically receive a fraudulent email inviting them view video content of a malicious site that poses as YouTube.

Users who install this browser add-on will find their systems infected with a malicious Mozilla Firefox browser extension, dubbed '**FriarFox**'. The attack, geared towards gaining access to the Gmail accounts has been linked to **APT TA413**, a threat group that's aligned with the Chinese Communist Party's state interests, the same group was seen slinging the Scanbox and Sepulcher malware earlier this year.

HOW IT WORKS



IMPACT

- Data can be altered, damaged, deleted, and infused with additional computer viruses.

MITIGATIONS

- Do not pay the ransom.
- Coordinate with IT Project Officer assigned in your office/unit.
- Remove infected computer within the network.
- Perform a full system scan in safe mode to remove any infections.

PREVENTION

- Do a regular file back-up using cloud backup and storage or an unplugged storage device.
- Consider encrypting the data on your backup.
- Update your operating system, software, and antivirus frequently.
- Ignore all emails from unknown sender. Avoid opening or downloading files attached to spam emails.
- Do not use cracked or untrusted program
- Regularly run a complete scan to check the computer for present of malware.

REFERENCE

- https://www.ncert.gov.ph/wp-content/uploads/2021/03/CERT-PH_ThreatsFeed_20210301.pdf
- https://www.bleepingcomputer.com/news/security/malicious-firefox-extension-allowed-hackers-to-hijack-gmail-accounts/