UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00113

MALICIOUS MOZILLA EXTENSION GMAIL TAKEOVER

DATE ISSUED: 2nd March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Friarfox is a newly discover extension for the Mozilla Firefox web browser software that allows complete takeover of a victim's Gmail account. The Advanced Persistent Threat (APT) group known as TA413 is suspected to be behind the attacks.

BREAKDOWN

The effects of this malicious browser extension allows attackers to search, read, label, delete, forward and archive any emails in the victims account. They have also been seen to access victims browser history and browser tabs, user data for websites, alter privacy settings and provide access to notifications – which may be another point of entry or malicious activity. These attacks have been seen to leverage the Scanbox malware and appear to be deployed by way of phishing emails containing malicious links impersonating sites such as YouTube. Once clicked, the link activates JavaScript files which scan the system and decide whether to deploy the malicious extension. While this attack has so far only been seen on Tibetan organisations, it is an important reminder that attackers are using web-browsers more to gain access to victim's devices and their data and a great deal of caution should be employed by users when surfing the web and accessing commonly used services, websites and social media.

REMEDIATION STEPS

- Only install browser extensions from reputable sources and known locations
- Disable the installation of web browser extensions across all browsers known to be in use in your organisation.
- Educate users on the dangers of social engineering and phishing attacks and how they should respond to suspicious emails.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/malicious-firefox-extension-allowed-hackers-to-hijack-gmail-accounts/

Threatpost https://threatpost.com/malicious-mozilla-firefox-gmail/164263/