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

CYBER GUIDANCE ISSUE 00261

WHATSAPP ATTACKS TARGET O365 & GOOGLE USERS

DATE ISSUED: 13th April 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A new campaign using spoofed voice messages sent via WhatsApp is targeting Office 365 and Google Workspace users through a legitimate domain to spread information stealing malware to victims.

BREAKDOWN

Researchers at Armorblox discovered the campaign that appears to originate in Russia sent from a domain associated with the Center for Road Safety whereby victims receive an email that claims they have a new inbound voice message. The header and content of the email echoes this message presenting as a secure message from WhatsApp and includes a "play" button to listen to the message. If a user interacts with the button, they are redirected to a site that attempts to install the JS/Kryptik Trojan malware. After landing on the page, they are asked to confirm they are not a robot and if the victim selects "allow" on the pop-up notification then the payload is downloaded as a Windows application that can bypass User Account Control. The attacker is then able to steal any other sensitive information or credentials stored in the browser. As the emails are being distributed through a legitimate domain, they are able to slip past email filtering and security features. The level of sophistication, complexity and various techniques used in carrying out this attack make it difficult for unwary users to spot. While this attack appears to be targeting general users rather than businesses at this stage, there is speculation that this attack or other similar ones will begin targeting businesses in the near future.

REMEDIATION STEPS

- Educate users on social engineering and the dangers of phishing attacks, how to spot them, and what to do if they receive a suspicious email in your organisation
- Never accept push notifications when requested through a browser, as there is a multitude of attacks that can be carried out through these.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/attackers-whatsapp-voice-message/179244/
Tech Republic https://www.techrepublic.com/article/hackers-employ-voicemail-phishing-attacks-on-whatsapp-users/
Cyber News Group UK https://www.cybernewsgroup.co.uk/attackers-spoof-whatsapp-voice-message-alerts-to-steal-info/