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

CYBER GUIDANCE ISSUE 00158

VISHING ATTACKS BYPASS EMAIL SECURITY

DATE ISSUED: 21st June 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A recent email campaign has bypassed native Microsoft email controls to deliver messages to victims requesting they call a scam phone number to obtain credit card details using billing and tech support ruses claiming to be from Norton Antivirus and Microsoft.

BREAKDOWN

Vishing is a type of social engineering attach where voice calling is used to scam victims out of sensitive information or charge exorbitant amounts for the phone call's duration. In this case fake receipts were sent to victims with a phone number to call for victims to apply for a refund or "processing order returns." While the Microsoft campaign was much more convincing than the Norton campaign, common evasion tactics were used to bypass Microsoft's native security features in both cases. Both emails were assigned a confidence level of -1 meaning they were considered to be from a safe sender to a safe recipient – in both cases a Gmail account was used. This method of attack can bypass security as there are no external links present and a phone number is not an Indicator of Compromise (IoC) tracked in the security community. The phone number for both campaigns has now been deactivated.

REMEDIATION STEPS

- Educate your users on all types of social engineering attacks – particularly those less commonly known or talked about such as Vishing. Provide guidance on what to do within your organisation if a user feels an email is suspicious including reporting processes and email isolation.
- Use validation checks to determine the sincerity of emails making similar claims or changes to any services you may be registered for such as checking bank statements for unexpected charges to your account or by logging in to your self-service account by visiting the website - never access the site through a clickable link in an email, but rather type it in to your web browser manually.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/geek-squad-vishing-bypasses-email-security/167014/
Armorblox https://www.armorblox.com/blog/tech-support-vishing-attacks/