U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00225

PHISHERS USE TINY FONTS TO FOOL EMAIL FILTERS

DATE ISSUED: 17th November 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

The 'One Font' Business Email Compromise (BEC) phishing campaign discovered by researchers at Avanan is targeting Microsoft 365 users with a range of sophisticated obfuscation techniques to avoid detection, including using tiny 1pt font size to hide text within phishing emails.

BREAKDOWN

Using tiny the tiny font in their phishing emails is allowing attackers to trick natural language processing filters present in email scanners like Microsoft's NLP, and making the text difficult to detect by end users. Not only that, they are also hiding clickable URLs in the Cascading Style Sheets (CSS) of emails using the <font> tag – a formatting technique commonly used to alter the look and styling of HTML formatted emails. This disrupts the semantic analysis of most tools and the emails are then treated as simple marketing emails, allowing them to slip through filters. The ZeroFont campaign of 2018 used similar tactics to compromised business emails to be used in subsequent attacks. BEC is often the initial step to further malicious campaigns, as attackers can use the legitimate email address they have compromised to distribute phishing emails from and increases the likelihood of victims falling for the phish.

REMEDIATION STEPS

- Educate users on social engineering and phishing emails – how to detect them and what to do with any emails they deem suspicious received within your organisation.
- Implement a Next Generation Secure Email Gateway to assist with detecting malicious email activity, both inbound and outbound. Spam filters are no longer enough on their own.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/tiny-font-size-email-filters-bec-phishing/176198/
Heimdal Security	https://heimdalsecurity.com/blog/email-filters-duped-by-tiny-font-size-in-bec-phishing-attacks/
Avanan	https://www.avanan.com/blog/zerofont-phishing-attack