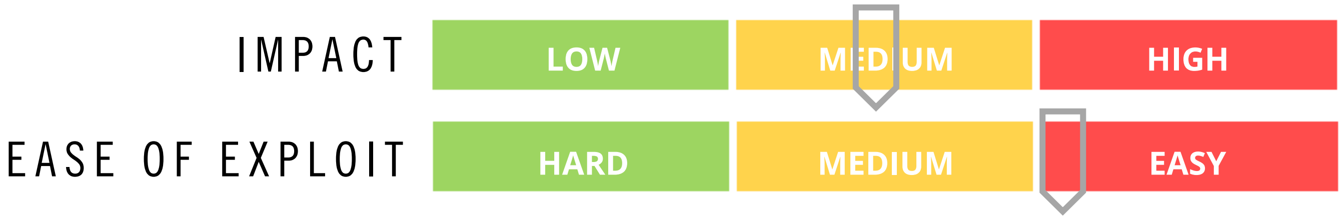
UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 0028

SQUIRRELWAFFLE NEW EXPLOIT FOR PROXYLOGON

DATE ISSUED: 1st March 2022



OVERVIEW

First discovered in September 2021, this relatively new malware is using a new twist on its modus-operandi to exploit ProxyLogon/ProxyShell in unpatched Microsoft Exchange Servers (of which there are still thousands) by hijacking email threads and malspamming users.

BREAKDOWN

While SquirrelWaffle continues to use tactics of hijacking email threads to distribute malware to unwary users through unpatched MS Exchange Servers, it seems the group is upping their game by conducting reconnaissance to look for money transfer information in a new campaign. The Sophos Raid Response Team discovered the campaign set to launch a financial fraud attack using typo squatting as a means to continue sending emails through Exchange even after patches had been applied. By registering a domain name similar to the intended victim (with a minor spelling error), the attackers then used this to send replies to an email thread in an effort to set up a money transfer. Creating numerous emails to appear as though internal support was being requested and employing social engineering techniques to instil a sense of urgency, attackers attempted to redirect funds to their controlled bank account

REMEDIATION STEPS

- Apply the latest patches to vulnerable on-premises Microsoft Exchange Servers immediately
- Implement industry standards for email authentication (SPF, DKIM, DMARC) to assist organisations in identifying whether emails are legitimate or spoofed.
- Implement Next Generation Email filtering tools such as Secure Email Gateway that employ machine learning to identify increasingly sophisticated social engineering attacks, phishing emails and impersonation attacks.
- Educate users on how to spot suspicious emails and how to deal with them within your organisation.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/squirrelwaffle-fraud-exchange-server-malspamming/178434/
Sophos	https://news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/
ZDNet	https://www.zdnet.com/article/squirrelwaffle-loader-leverages-microsoft-exchange-server-vulns-for-financial-fraud/