National Cyber Security Centre

2111171241-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Exploited Exchange Servers Leading to Ransomware
2021-11-18

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

Multiple threat researchers including CIRCL and CERT-SE have recently highlighted ongoing criminal campaigns involving **Microsoft Exchange** servers. Attackers have been observed making use of compromised Exchange servers to perform **Email Conversation Thread Hijacking**[1] in order to distribute a number of malware loaders.

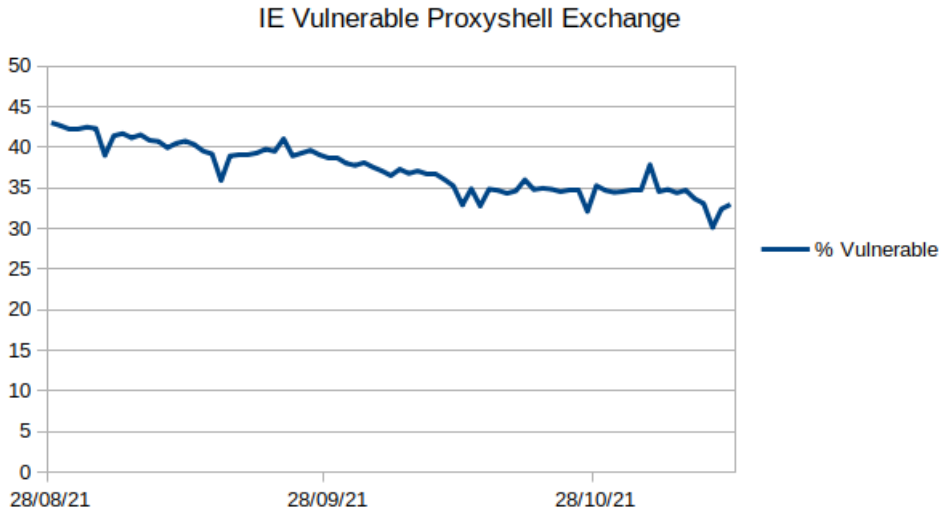
This practice involves attackers identifying email threads with potentially high value targets and introducing malicious documents or links into responses. Email Conversation Thread Hijacking has proven extremely effective due to the trust associated with the sender and the content of the email conversation.

Malware observed in these campaigns include **SquirrelWaffle, Danabot and Qbot/QakBot**. These types of malware are generally used as pre-cursor malware in the initial or early stages of an attack, in order to deploy **Cobalt Strike** or similar and often lead to an organisation suffering from a **Ransomware attack**.

The attacking emails arrive from organisations with **a compromised MS Exchange server**. The threat actors are believed by researchers to use information gained from the compromised server to craft emails to be inserted into current threads. These attacking emails contain text and a URL or attachment that leads to malware arriving on the system.

These attacks have been observed exploiting a particular set of chained vulnerabilities known as **ProxyShell**. Microsoft Exchange servers that were compromised prior to patching are now being used to perform Email Thread Hijacking. The NCSC advisory on the Microsoft Exchange ProxyShell Vulnerabilities can be viewed here.

The NCSC estimates that circa 30% of exposed Microsoft Exchange servers in Ireland are still unpatched and are vulnerable to ProxyShell. Owners of unpatched servers should proceed under the assumption that they are compromised.



[1] https://www.barracuda.com/glossary/conversation-hijacking

Impact

Compromised Systems, Data & Financial Loss, Ransomware.

Recommendations

Patching the vulnerability alone is not enough. The NCSC recommends organisations who have servers that have been found to be compromised by the previous vulnerabilities in MS Exchange to restore them completely as soon as possible.

The NCSC strongly advises all constituents to establish a regular patching schedule. In addition, organisations should carry out Incident Response investigations to establish if they have been compromised before patching.

Advising users about the escalated risk from email thread hijacking, and providing a reporting structure for suspect emails may mitigate part of this risk.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie