TR-64 - Exploited Exchange Servers - Mails with links to malware from known/valid senders

circl.lu/pub/tr-64/

What have we observed?

Several organizations received complaints about the fact that their email accounts are sending spam, phishing and infected emails to their partner organizations. The emails are usually replies to ongoing email threads, where an attacker pastes a greeting sentence and URLs above the original mail content.

Attackers/adversaries do that to improve the social acceptance rate of their malspam. Indeed this strategy seems to be very successful.

Here a sample in English: (URLs are disarmed)

```
Subject:        Re: Demande de Remboursement

Greetings! I send here a recordwith a thorough description of the recent problem.
Please examine it here:

1)hXXps://ooforms[.]com/omnisquod/voluptatummodi-3313010
2)hXXps://karafarinenovin[.]com/estsit/estsed-3313010

Gudde Moien,
```

Here a sample in French: (URLs are disarmed)

```
Objet : Re: Nouveau dossier// REFTP 27791

Bonne journée! Dans cette lettre, j'envoie le Doc mentionné avec votre signature.
Vous pouvez trouver via le lien ci-dessous.

1)hXXps://catechismo.ravaldino[.]it/quiatemporibus/ideligendi-1590551
2)hXXps://tradingview.dharwadinternationalschool[.]com/delectusquia/officiisexpedita-
1590551

Monsieur,
```

If you receive emails like this, take care. These are links to QBot/QakBot/DanaBot/SquirrelWaffle malware, which is a “Information Stealing” / “Cobalt Strike Loader” malware. An infection will most likely end up in a ransomware case.

If you receive complaints about emails like this being sent from your infrastructure, be prepared to alert your IT team or IT supplier and feel free to contact CIRCL for assistance.

Root Cause

Recently we had to deal with several critical security vulnerabilities in Microsoft Exchange.

In March 2021, CIRCL warned about critical vulnerabilities which were initially exploited by an activity group (called HAFNIUM by Microsoft) starting in late 2020.

TR-61 - Critical vulnerabilities in Microsoft Exchange

In late October CIRCL got notified about MS Exchange servers vulnerable for the recent critical Exchange RCE vulnerabilities CVE-2021-26427.

Microsoft Exchange Server Remote Code Execution Vulnerability CVE-2021-26427

CIRCL immediately worked through the list of vulnerable IP addresses and notified the respective ISPs (service provider) with the request to warn their customers.

Since then, most of the vulnerable MS Exchange servers are patched (updated). But unfortunately sometimes patching alone is not sufficient.

If the server is already compromised before successful patching, the patch will likely close the vulnerability. But the server remains compromised. Patching alone is not sufficient

This situation is what we are looking at right now: the infrastructure is compromised, attackers read the emails and inject their malicious content into the mail threads by replying to the mail interaction.

Fixing and mitigation

There is only one single procedure to ensure that you completely fix and mitigate the situation, close all potential backdoors and kick-out the attackers: re-install every compromised server from scratch and then recover and copy the data over.

In all the cases, we recommend to initiate a full incident response process including the security review of the system.

One of the most important questions which must get answered: Did the attackers manage to laterally move within the internal network. If this happens your are at high risk of a crypto ransomware or data exfiltration. This means, you will find back all your data encrypted - or stolen.

If you have no resources for incident response and reinstall the Exchange server from scratch, Microsoft has published guidance for responders.

Guidance for responders: Investigating and remediating on-premises Exchange Server vulnerabilities

Do I need to patch internal and non-exposed exchange server?

Yes.

Have you seen exploited server in Luxembourg?

Yes.

New wave of malspam

Unfortunately the initial ‘Root Cause’ leads to the next stage of attacks. It seems the compromised Exchange servers not only were abused for spreading malspam by replying to existing email threads. CIRCL recently received evidences that the servers also got abused for data breach.

It seems the attackers exfiltrated a decent amount of emails from the compromised severs. These exfiltrated emails are now traded in the Internet and used to send new waves of malspam by replying to existing email conversations.

Here a sample in German: (URLs are disarmed)

```
>
> Objet: H
>
> Schönen Tag!
> Ich traf Komplikationen mit der Übertragung an Ihre Papiere. Deshalb sende ich es
noch einmal:
>
> hXXps://sade-cgth[.]az/guufiaq/tdtsl-ttarseaiaobsiumtcuto-aemlaoernoi
>
```

In case your organization was victim of the ‘Root Cause’ you should expect new waves of malspam sent in your name. Please warn all your contacts to be vigilant and not to click a link.

Since this kind of data leak also contains PII - personally identifiable information - we strongly advise to report to the local data protection agency CNPD, as soon as you learn about your organization being affected:

> Commission nationale pour la protection des données

References

Classification of this document

TLP:WHITE information may be distributed without restriction, subject to copyright controls.

Revision

- Version 1.0 - TLP:WHITE - First version - 10 November 2021
- Version 1.1 - TLP:WHITE - New wave of malspam - 16 February 2022