Unpatched Exchange servers distribute phishing links (squirrelwaffle)

certitude.consulting/blog/en/unpatched-exchange-servers-distribute-phishing-links-squirrelwaffle/

Peter Wagner 29.11.2021

Beginning of November a customer reached out to us. Internal and external users reported suspicious mails sent from their mail accounts, which included suspicious links. These mails were sent as replies to messages already sent in the past, which made them appear legitimate.

First it was confirmed in the mail headers that the mail originated from the customers Exchange and was not spoofed from external sources. While further investigating the root cause it turned out that the on-premise MS Exchange server had not received updates for several months. Thus, it was affected by multiple vulnerabilities, e.g. “ProxyShell” (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) and “ProxyLogon” (CVE-2021-26855).

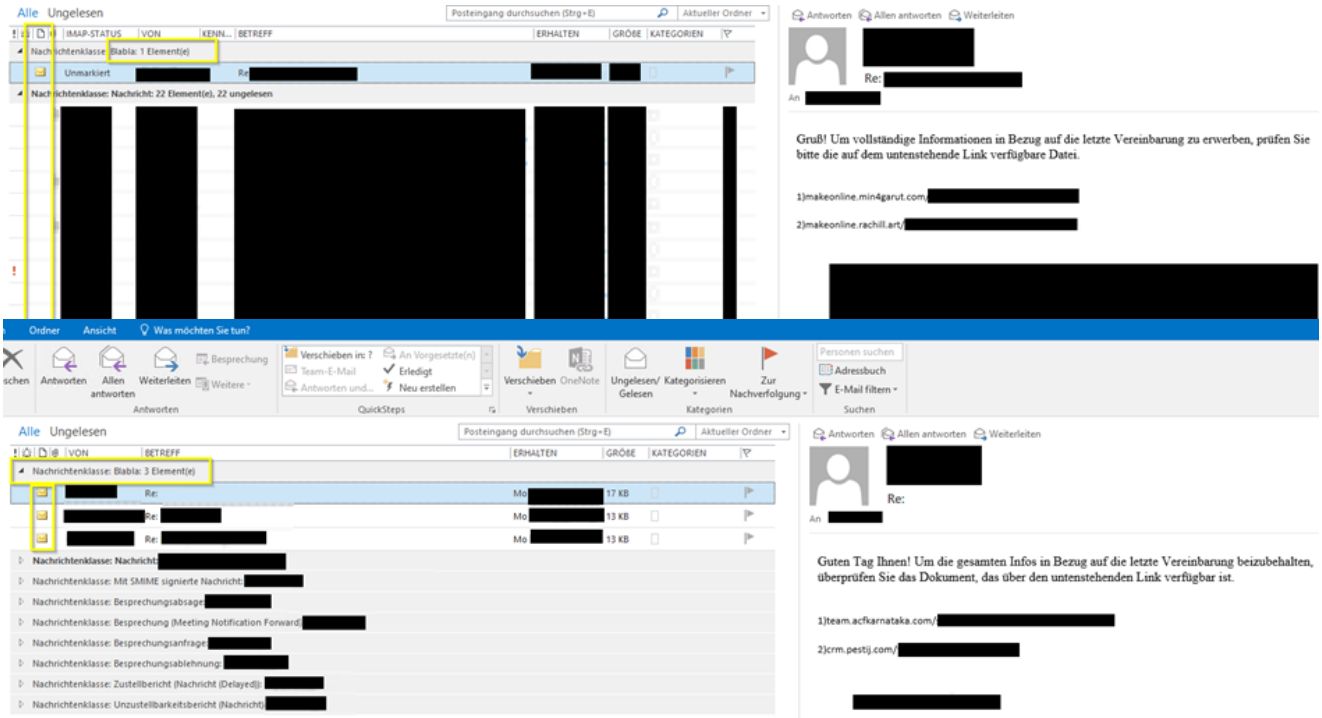
The IIS logs showed that special crafted server-side request forgery (SSRF) requests were used to exploit CVE-2021-26855, directed at the Exchange Web Services API endpoint. This allowed the attacker to perform unauthorized actions on behalf of legitimate users.

The corresponding IIS log lines looked like this:

```
2021-11-01 19:50:59 xxx.xxx.xxx.xxx POST /autodiscover/autodiscover.json
a=a@edu.edu/autodiscover/autodiscover.xml?=&Email=autodiscover/autodiscover.json?
a=a@edu.edu&CorrelationID=<empty>;&cafeReqId=1b241d99-89e8-4cfa-8b3c-f96c1ef40cf0;
443 - xxx.xxx.xxx.xxx Mozilla/5.0+(Windows+NT+10.0;+WOW64)+AppleWebKit/537.36+
(KHTML,+like+Gecko)+Chrome/92.0.4515.131+Safari/537.36. - 200 0 0 345
```

One thing that was also noticeable in the Exchange Logs is that the “ItemClass” of all mails created by the attacker was set to “IPM.Blabla”.

This allowed us to filter these mails in Outlook. However, this only worked for mailboxes of users who received these suspicious emails. We did not find emails in the “sent” folders of affected users. The pictures below show two mail accounts.



The format of the censored URLs conformed to the following regex pattern: `[a-z]+\.[a-z0-9]+\.com\/[a-z]+\/[a-z]+-[0-9]+`

Example: `sdf.wwkwe.com/tatamua/uzaro-3381926`

No malware could be identified on the Exchange server in the course of a quick analysis. Other forensic investigations came to a similar conclusion [1]. However, no full forensic analysis was conducted during this investigation.

Later it turned out that other organizations [1] were affected by similar attacks, seemingly related to an attack campaign titled “squirrelwaffle” [2].

We recommend everyone to update internet-facing applications in short cycles and apply patches as soon as possible after their release. Due to the high attack surface of the Microsoft Exchange product (multiple critical vulnerabilities have been published this year), it is also recommended to block access to the web interface from the internet and use a VPN if access from the internet is required.

Related URLs:
[1] https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
[2] https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

Photo by Maksim Goncharenok from Pexels.