Vulnerable Exchange server hit by Squirrelwaffle and financial fraud

news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/

February 15, 2022

The Sophos Rapid Response team recently investigated an incident where the Squirrelwaffle malware loader was used in conjunction with the ProxyLogon and ProxyShell exploits to target an unpatched Microsoft Exchange server. The attackers leveraged the vulnerable server to mass distribute Squirrelwaffle to both internal and external recipients by inserting malicious replies into employees' existing email threads (known as email thread hijacking.)

Sophos has encountered this approach before, but, on this occasion, there was also something new going on. The incident investigators discovered that while the malicious spam campaign was being implemented, the same vulnerable server was also used for a financial fraud attack using knowledge extracted from a stolen email thread.

What is Squirrelwaffle?

Squirrelwaffle is a malware loader that is distributed as a malicious office document in spam campaigns. It provides attackers with an initial foothold in a victim's environment and a channel to deliver and infect systems with other malware. When a recipient opens a Squirrelwaffle-infected document and enables macros, a visual basic script typically downloads and executes Cobalt Strike Beacons, giving control of the computer to an attacker.

The twist

In a typical Squirrelwaffle attack leveraging a vulnerable Exchange server, the attack ends when defenders detect and remediate the breach by patching the vulnerabilities, removing the attacker's ability to send emails through the server.

In the incident investigated by Sophos Rapid Response, however, such remediation wouldn't have stopped the financial fraud attack because the attackers had exported an email thread about customer payments from the victim's Exchange server. (Further, as noted below, patching isn't the final solution for remediating vulnerable Exchange servers, you also need to investigate to see if there was any other impact, such as the installation of web shells.)

Using knowledge obtained from the thread, the attackers registered a "typo-squatted" domain (one that appears to be the victim's domain but with a small typo) that they then used to reply to the email thread. Moving the conversation out of the victim's email infrastructure gave the attackers operational control over what happened next.

The attackers replied to the email thread using email addresses from the typo-squatted domain and attempted to redirect the victim's customer's payments to themselves.

To add further legitimacy to the conversation, the attackers copied additional email addresses to give the impression that they were requesting support from an internal department. In fact, the additional addresses were also created by the attacker under the typo-squatted domain.

The attackers set the stage for a legitimate financial transaction to be redirected to a bank account under their control:

That's very understandable, I shall wait for your updates.

Finance department is cc'ed in this email and would provide the updated banking details to you shortly.

A follow up email references the new banking details and tries to create a sense of urgency. The attackers followed up almost every day for the next six days with the tone growing increasingly agitated:

Hi [redacted],
I hope things are going well in school. I rang this morning hoping to have a quick chat with you. I appreciate how busy you are but wondered if you could give me an update regarding the renewal? And, also it's important to know the status on payment, as you well know by now we updated our banking operations from [redacted] to [redacted].
Accounting department @Operations , have noted we may have to change yet again.
Sorry about this as it's down to our internal financial control.

Kind regards,
[redacted]

The attacker changed their tone after receiving an email indicating that the payment was being processed:

Hi [redacted],
I have processed your renewal for you and our Operations Team are in the process of generating your invoice.I have asked if they can get this to you asap.
Kind regards,
[redacted]

The attackers very nearly achieved their goal. The victim organization initiated a transfer of money to the attackers, however, one of the financial institutions involved in the transaction flagged the transaction as fraudulent and so the transfer did not complete.

Protecting against malicious email attacks

The single biggest step defenders can take to prevent the compromise and abuse of on premises Microsoft Exchange servers is to ensure that they have been patched with the most recent updates from Microsoft.

Next, defenders can make it easier for other organizations to determine the legitimacy of emails coming from their domain, for instance by implementing industry recognized standards for email authentication, such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain Message Authentication Reporting and Conformance.) Using these standards can make it harder for an attacker to send spoofed emails impersonating your domain.

As attackers become increasingly skilled at social engineering, creating sophisticated phishing lures and impersonation messages, and more, it may be time to start using email security products that integrate artificial intelligence.

Last but not least, defenders need to protect the recipients of such emails and ensure that users in their organization can spot phishing attempts and know how to report and respond to them.

I've been attacked – what now?

If you suspect you have been the target of a Squirrelwaffle or financial fraud attack, there are some practical steps you can take.

- Use the Sophos Rapid Response Squirrelwaffle Incident Guide to help you investigate, analyze and respond to an incident involving Squirrelwaffle.
- Implement your incident response plan. If you don't have one or don't feel you have the right resources to contain and neutralize the attack, call on a third party incident response team, such as Sophos Rapid Response.
- Get patching. Update the software on any vulnerable on premises Microsoft Exchange servers – and check after patching for any web shells left behind by the attackers for later access.
- If your domain has been typo-squatted, you can file an abuse complaint with the domain registrar of the typo-squatted domain. This process will vary depending on the registrar.
- If a malicious spam campaign was conducted from your compromised Exchange server, make sure your organization's legitimate domain or email infrastructure has been flagged as a spam sender. Check whether you have been blacklisted. You can ask to be removed from the list, but it is sometimes worth staying on it until no further spam is detected from your domain as that could help to prevent some of your legitimate emails from being inadvertently delivered to external recipients.

Conclusion

The combination of Squirrelwaffle, ProxyLogon, and ProxyShell has been encountered by the Sophos Rapid Response team multiple times in the last few months, but this is the first time we have seen attackers use typo-squatting to maintain the ability to send spam once the Exchange server has been remediated.

Kyle Link and Mauricio Valdivieso from the Sophos Rapid Response team also contributed to this article.