What Talos Incident Response learned from a recent Qakbot attack hijacking old email threads

By Jonathan Munshaw

Published: 2022-07-27 · Archived: 2026-04-05 23:22:59 UTC

What Talos Incident Response learned from a recent Qakbot attack hijacking old email threads

Wednesday, July 27, 2022 08:00

By Nate Pors and Terryn Valikodath.

Executive summary

- In a recent malspam campaign delivering the Qakbot banking trojan, Cisco Talos Incident Response (CTIR) observed the adversary using aggregated, old email threads from multiple organizations that we assess were likely harvested during the 2021 ProxyLogon-related compromises targeting vulnerable Microsoft Exchange servers.
- This campaign relies on external thread hijacking, whereby the adversary is likely using a bulk aggregation of multiple organizations' harvested emails to launch focused phishing campaigns against previously uncompromised organizations. This differs from the more common approach to thread hijacking, in which attackers use a single compromised organization's emails to deliver their threat.
- This many-to-one approach is unique from what we have generally observed in the past and is likely an indirect effect of the widespread compromises and exfiltration of large volumes of email from 2020 and 2021.

- Understanding the difference between external and single-victim thread hijacking is essential for detecting these threats. Below, we have several tips for defenders on how to identify key indicators of this activity.

External thread hijacking

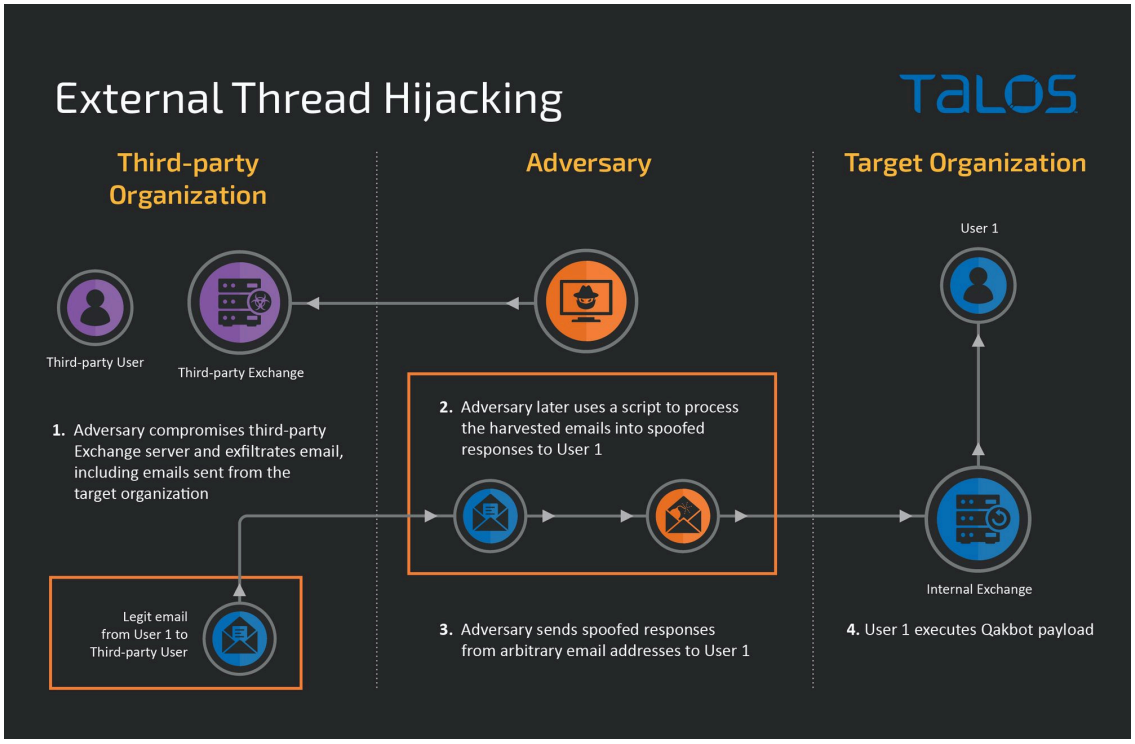
Cisco Talos has observed threat actors using external thread hijacking, a method by which attackers weaponize emails previously harvested from other organizations. This differs from the more common approach to thread hijacking, in which adversaries compromise the victim organization's Exchange server to obtain email threads that are then weaponized. We recently observed this in June 2022 as part of a broader campaign that delivered the Qakbot banking trojan. In this threat activity, the attackers used old emails harvested months to years ago during the 2021 ProxyLogon campaign, tracked as CVE-2021-26855, targeting vulnerable Exchange servers.

External thread hijacking is not dependent on the threat actor gaining initial access to the victim environment. This is notable from a digital forensics and incident response (DFIR) perspective because the target organization only saw inbound phishing emails with its own legitimate emails as the source material, with multiple external organizations represented in the email threads. Our assessment of the adversary's use of emails obtained from the ProxyLogon compromises is based on a number of observations, including the timing of the emails and research into publicly acknowledged ProxyLogon compromises. The attackers selectively used these emails to target senders or recipients from the target organization.

In the external thread hijacking attack observed by CTIR, the adversary likely took the following steps:

1. The attacker took control of multiple third-party organizations' Exchange servers or individual inboxes and exported emails for later use. The adversary selected the emails relevant to the target organization from the email dumps. This could have been accomplished with a regex search for "[@]company[.]com" in the "To" or "From" fields, although we did not directly observe the adversary's selection process.
2. With the emails selected, the adversary ran a script to format the text of each legitimate thread into a phishing email by adding malicious content.
3. The attacker then sent the phishing emails to the original "[@]company[.]com" address in each legitimate thread from many adversary-controlled external mailboxes, completing the phishing attack.

See the graphic below for a visual depiction of those steps. Note that the graphic shows only one third-party organization for simplicity, but emails harvested from multiple external organizations were involved in the attack observed by Cisco Talos.



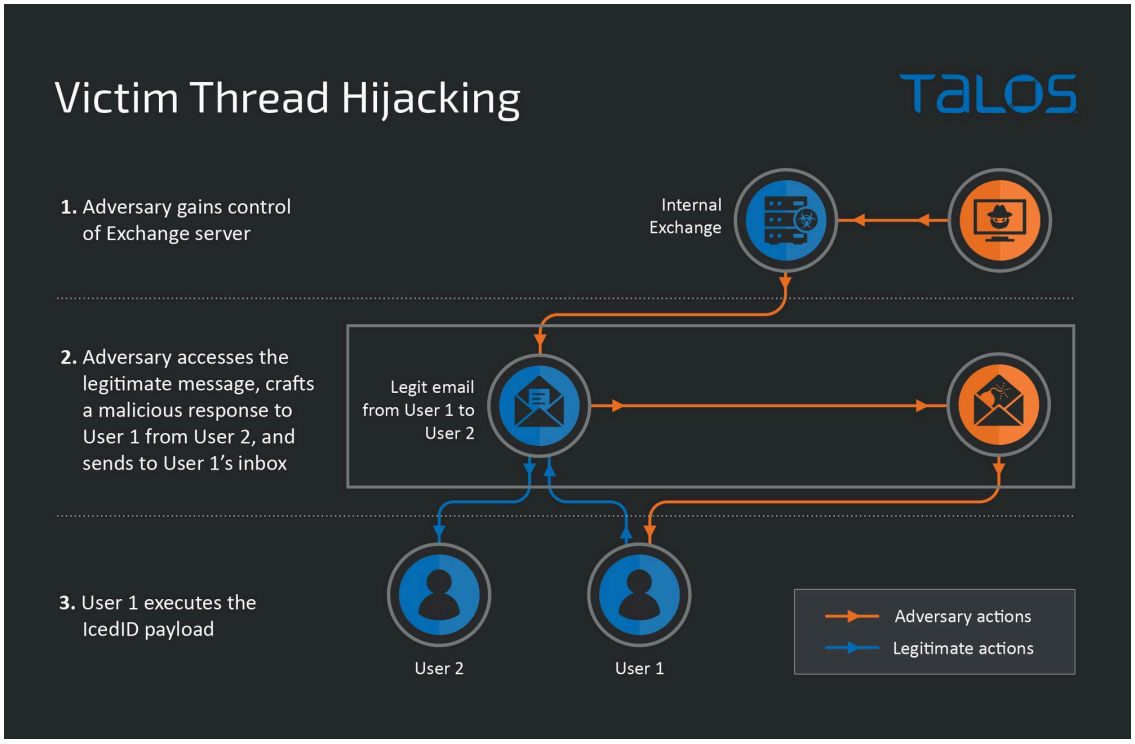
Victim thread hijacking

To help showcase the unusual nature of the external thread hijacking, a brief breakdown of the more common victim thread hijacking is instructive. In 2021 and early 2022, adversary methods for thread-hijacking primarily depended on access to a victim's Exchange server or individual email account. Most recently, this was seen in an IcedID campaign in early 2022 where the adversary compromised a victim's Exchange server and used it as a base of operations to craft and send malicious emails based on recent legitimate email threads.

In the past, in a standard malspam campaign delivering IcedID, an attacker would have taken control of the target organization's Exchange server, then hijacked threads between internal users and/or their external partners. The key point is that the victim's Exchange server served as both the source for the legitimate email thread and the sender for the malicious reply. These attacks were usually conducted immediately post-compromise, or shortly after.

In a victim thread hijacking attack, the adversary would take the following steps:

1. Take control of the target organization's Exchange server via ProxyLogon or another Exchange vulnerability.
2. The adversary would then use a legitimate email to craft a reply, inserting malicious content. Next, the adversary would send a malicious reply to the target user via the target organization's Exchange server. This step of the attack would work equally well for internal-to-internal and internal-to-external phishing.
3. The target user, seeing the legitimate sender, source and thread history of the email, would be reasonably likely to click the link, thereby executing the IcedID payload on the system.



Regarding the malware delivered in this campaign, there are numerous Snort rules and ClamAV signatures users can deploy to detect the deployment of Qakbot. While the primary focus of this post covers the process of how an attacker delivered this attack, if a user were to be infected with this particular campaign, Qakbot can steal financial data and login information from targeted systems. It also loads additional malware from its C2 servers, which Snort rules can detect and prevent.

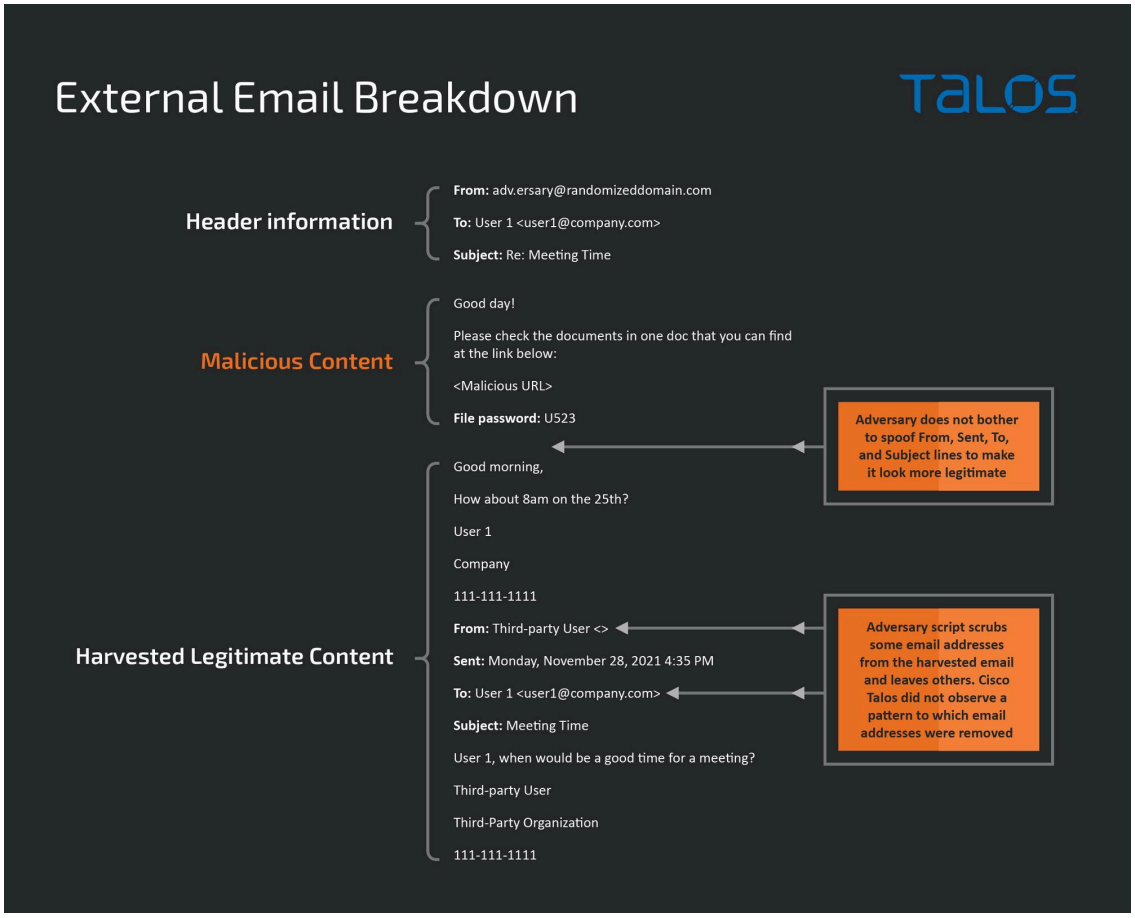
With a clear understanding of the difference between external thread hijacking versus victim thread hijacking, the next question is how to detect external thread hijacking, particularly in the current campaign using emails harvested through ProxyLogon attacks. This is a very relevant topic for DFIR professionals because accurate identification of this attack method might lower the priority of in-depth forensic examination of internal Exchange servers.

Tips for Defenders

Look for the following indicators as key signs of the external thread hijacking method:

- **Spoofed senders.** Since the adversary did not have access to the victim's Exchange server, all emails originate from spoofed, external addresses.
- **Old email threads, primarily from 2020 and 2021.** However, Cisco Talos has observed at least one email thread as recent as May 2022, indicating that the adversary in question is actively using newly harvested emails.
- **No or very limited internal-to-internal threads.** Since the emails were harvested from external sources, there should be very few internal-to-internal threads seen in the legitimate content.
- **Malformed replies.** The adversary concatenated the old, legitimate content with the new, malicious content within the email body. This created a malformed appearance, as seen in the example below.

- **Partially scrubbed email addresses.** The adversary's script removed some email addresses from the bodies of the legitimate emails during the construction of the malicious emails, as noted in the example below.
- **Repetitive use** of the same harvested legitimate email threads in multiple phishing waves. The example below was created by Cisco Talos to avoid displaying identifying information but is highly similar in all aspects to the external thread hijacking emails observed in the wild.



Conclusion

By early 2022, the direct effects of ProxyLogon, most famously exploited by the HAFNIUM group, largely quieted down. The external approach to thread hijacking, not necessarily specific to one adversary, appears to be one of the many indirect effects of the widespread compromises that resulted in exfiltration of large volumes of email from 2020 and 2021. Although those emails are relatively old by now, we will likely continue to observe adversaries leveraging bulk email aggregations from multiple organizations to launch focused phishing campaigns. Accurately recognizing the difference between external thread hijacking and victim thread hijacking can potentially avoid incorrect assessment of an incident and save dozens of hours of hunting for an internal breach that does not exist.

Source: https://blog.talosintelligence.com/2022/07/what-talos-incident-response-learned.html