

New Trend In Phishing: Conversation Hijacking

There's been a spike in the number of cyber-attacks that hijack ongoing email conversations and turn them into a vehicle for delivering malware.



Conversation-hijacking attacks are when hackers manage to infiltrate legitimate email threads between people, and use highly-customised phishing techniques [to make it look as if the victim is the one sending messages back and forth](#).

By ensuring that people believe they're interacting with a person they trust -- perhaps someone even within the same organisation -- the scammers hope victims won't be suspicious about downloading and opening attachments they might be sent as part of the conversation. That means victims can relatively easily be tricked into downloading malware.

Now researchers at email and web security firm [AppRiver](#) have uncovered what they refer to as "an unparalleled spike" in this form of phishing attack -- and a campaign is leveraging conversation hijacking to deliver the [Gozi banking trojan](#), providing the attackers with access to the victim's financial details and the ability to clean out their account.

The attackers begin with phishing campaigns designed to acquire the email login details of targets. Large numbers of phishing emails are sent, using lures with a variety of themes designed to trick targets into opening malicious documents and clicking on an embedded URL.

One example is an email around the theme of real estate, which requires users to enter their email address and password in order to 'unlock a protected document'. The victim is taken to a customised login page designed to look like the major email provider they selected and the attackers harvest the data.



A phishing message designed to steal email login details for use in further attacks.

Image: AppRiver

These attacks may be generic and widely targeted in spam blasts -- although some are more carefully crafted -- but if even a small number of people fall for the ruse, those behind the campaign have gained access to email login and password details they can use to extend their reach for the true aim of the campaign: distributing malware.

Rather than having to start brand new email threads in an effort to lure in victims, the attackers can use the trusted accounts to reply back to ongoing and previous legitimate conversations.

With control of the accounts, this stage of the campaign is relatively simple, as the attackers just send out replies with malicious attachments, which can easily be related to previous points in the discussion.

In January alone, AppRiver recorded more than 34,000 incidents of malicious emails being sent from compromised accounts over the course of the month, with peaks and troughs of activity.

"Since we began monitoring this we have seen an ebb and flow of sorts. Much in the same way that a botnet will reseed itself prior to a large email blast," Troy Gill, manager of security research at AppRiver, told ZDNet.

"These attackers seem to go through cycles where they are gathering credentials and later utilising those credentials by launching the malware attacks from the compromised accounts."

The Gozi trojan payload works like other banking trojans, and steals information relating to financial accounts. That means it could be extremely potent if the customised phishing emails managed to successfully trick anyone in an organisation with access to company accounts.

While the widespread use of Gozi means it can't be used to pinpoint any potential perpetrators of these attacks, those behind it are "likely part of a highly organised crime ring", said Gill.

While the conversation-hijacking attacks are currently being used to distribute a banking trojan, it's possible that in future, those behind the campaign could move onto distributing other forms of malware -- and in greater numbers.