SECURITY INSIGHTS:

Tails of the Email Flood Attack

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

The two most common attacks targeting users in our industry are credential theft and unauthorized remote access. Tech Support scams that have been around for decades. Recently, these scams have evolved to be presented as calls from a company's IT. Since we all require IT assistance at some point, a call from an IT technician claiming to help with a problem may seem perfectly normal. Now, one needs to create a plausible "problem."

The attack begins by flooding the user's inbox with a large number of emails, overwhelming their mailbox. Shortly after this, the user receives a phone call (or Teams connection) from the IT, who claims they want to help address the email issue. Under the guise of assisting, they say they need to remotely connect to the user's computer to resolve the problem. Feeling overwhelmed, the user may want a quick solution and agree to this request. Next, the attacker sends the user an email containing a link or directs them to a website to download remote access software. If the victim complies, the hackers gain complete control over the user's computer. This not only gives them access to the user's work network but also allows them to move through other systems.

This approach is not new; numerous runbooks have been created for it. What's particularly interesting is how it generates a deluge of emails. Many email services have started blocking mass mailings, but hackers have found a clever workaround. They use scripts to coordinate simultaneous subscriptions to dozens, hundreds, or even thousands of mailing lists, utilizing victims' email addresses on websites that lack CAPTCHA protection. They execute these subscriptions all at once, resulting in users receiving a flood of subscription confirmations in a very short time. Since these emails originate from various locations around the world and different mail services, they evade detection by email providers and are not blocked.

It's not uncommon to see these attacks during our busiest times - the end of the week or month. Threat actors know our business.

TAKEAWAYS:

- If you receive a sudden influx of emails, especially from subscription services you did not sign up for, this is a significant warning sign. Notify your security team immediately
- A few threat actors groups are notorious for using Microsoft Teams to connect with users under the pretense of local IT support - lockdown your Teams not to allow guest access
- If you get a phone call from someone claiming to be from an IT, ask for a ticket number and then hang up. Call the IT team or technician directly and reference the ticket number. If you are using an IT Managed Service Provider, establish the protocol on how they will communicate with your users. Educate your users accordingly
- MSPs frequently take shortcuts and **pre-install** Remote Assistance tools on all user's computers. That is a disaster waiting to happen. Rearchitect your remote services program with your MSP so your users are in full control of when the Remote Assistance tools are used
- Be aware that the remote access tool, **Quick Assist**, is built into the Windows operating system. An attacker does not need a user to install anything on their computer; they simply ask you to enable it. Train your user on how to respond to these requests.