New phishing attacks appear to use Google Translate as a disguise

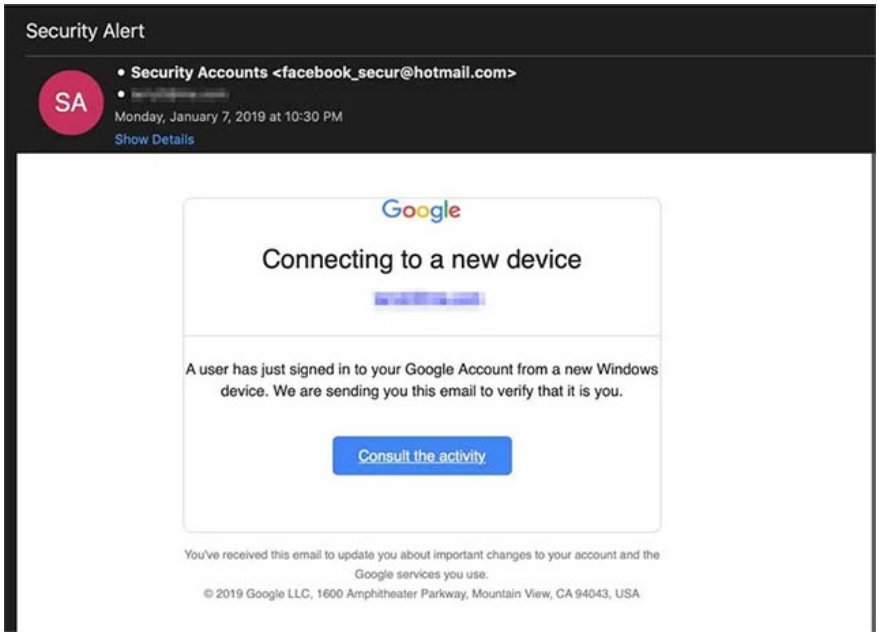
Recently, a phishing campaign to steal Google accounts and Facebook login information has been discovered using Google Translate (Google Translate) as a disguised location on mobile browsers.

Recently, a phishing campaign to steal Google accounts and Facebook login information has been discovered using Google Translate (Google Translate) as a disguised location on mobile browsers.

Specifically, according to new research by Larry Cashdollar, a member of Akamai Security Intelligence Response Team (SIRT), the latest phishing campaign has been discovered, targeting both Google and Facebook accounts.What makes this campaign so effective is that it will use Google Translate to make the phishing page look like it originated from a Google domain, while also making the site malicious. Mobile browser platforms become much more difficult.

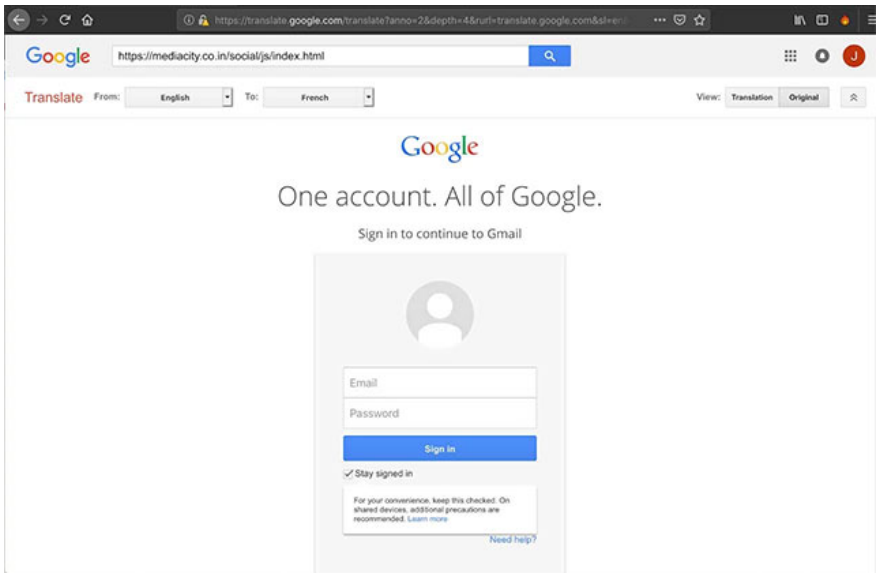
1. New USB cable type allows hackers to perform remote attacks

First, these phishing emails will pretend to be a Security Alert from Google with content indicating that the service provider has discovered that your account is being logged on from a Windows device. new.It will then trick you into clicking on the malicious link (Consult the activity) to see more details about this security warning.

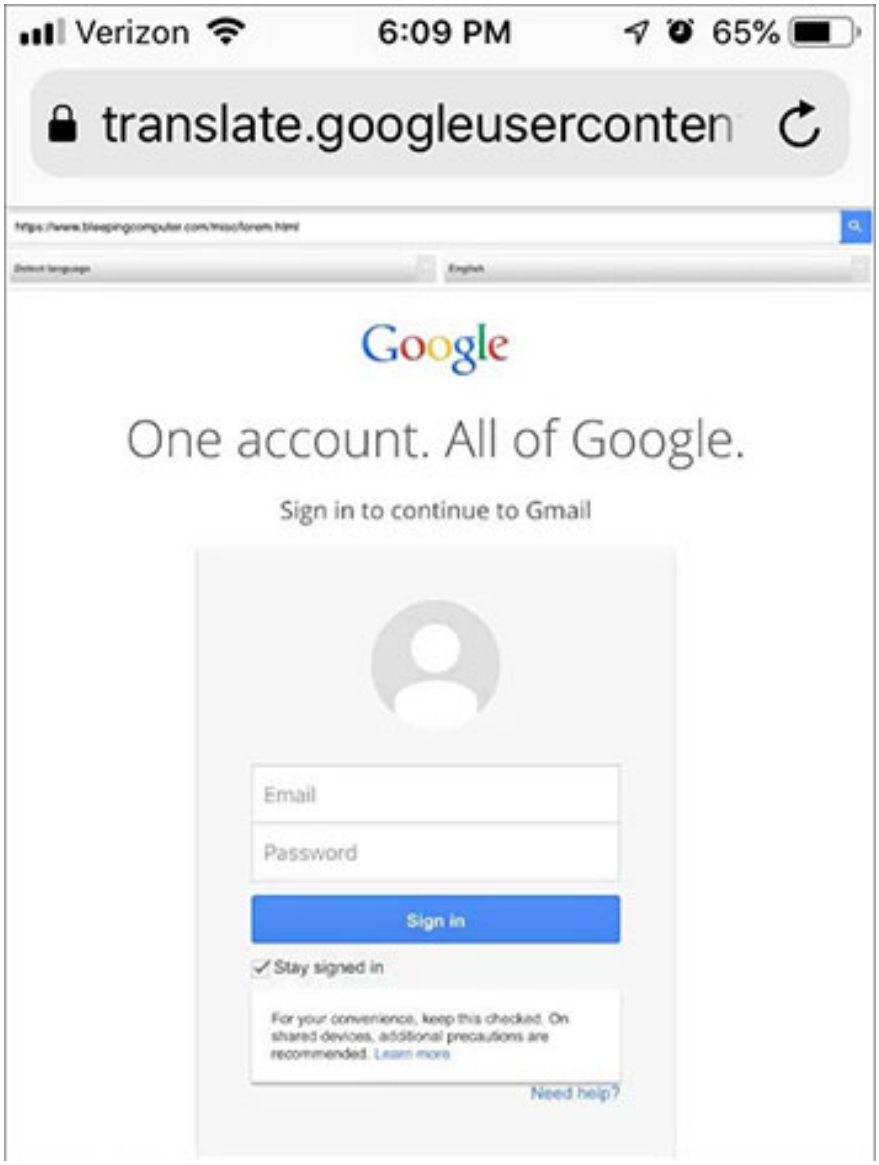


1. Detecting new electronic phishing malware, redirecting payment transactions to attackers

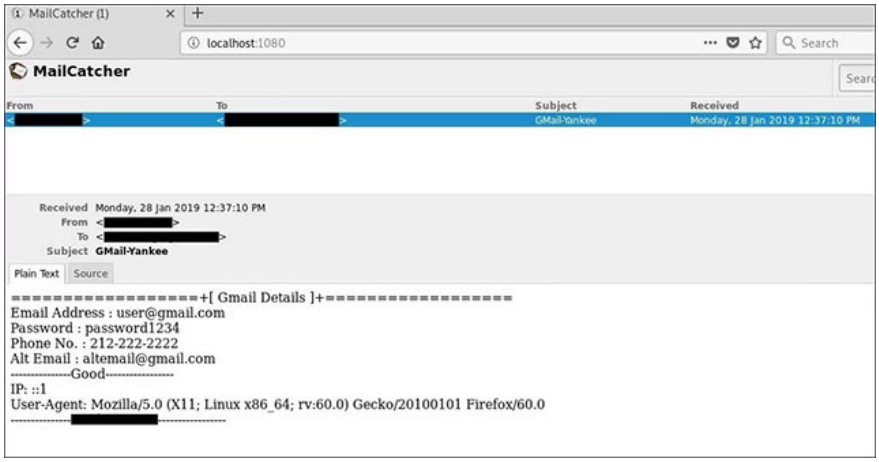
When users click on the link, they will be taken to the Google Translate page, which is actually a shadowed phishing site - requiring you to enter your Google account login information.On desktop browsers, we can easily discover that phishing pages are being displayed through Google Translate.However, for mobile browsers, detecting the difference is much more difficult because Google Translate will display the minimal interface when opened on a mobile device.



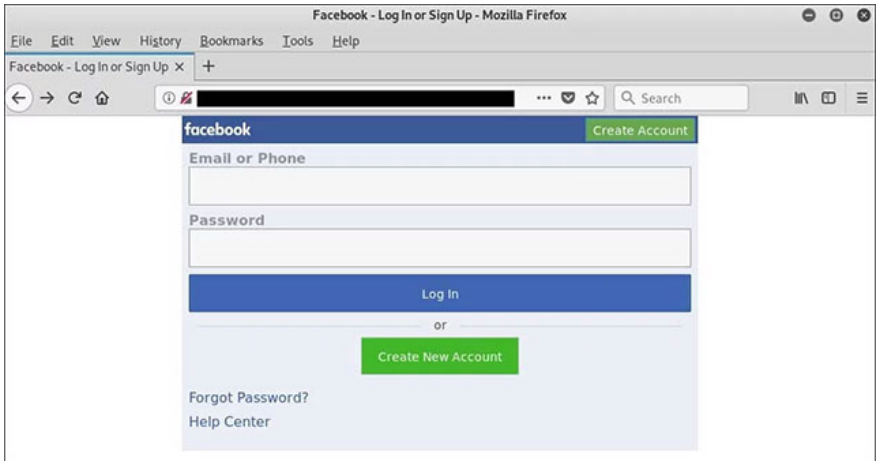
For example, here, we created a test page containing fake Google account login information and opened it via Google Translate on a mobile browser.As you can see, this Google Translate interface is not much different, and this page shows that we are accessing the Google.com domain.For general users, this is enough to convince them to trust the source and security of this site.



When a user types their login information into a phishing page, a script will be executed to send an email containing the information entered to the attacker, as you can see from the email below:



At this point, the attackers have obtained the victim's Google account login information, they will perform another redirect to the Facebook phishing page and try to get both their Facebook username and password. victim.However, luckily, this Facebook shadow phishing page is not optimized for mobile devices and can therefore be easily discovered if users pay close attention.



1. Azorult Trojan steals user passwords while running in the background like Google Update

As you can see, an attacker constantly offers more creative ways to deceive users to provide their login information.After all, raising awareness and protecting yourself against online fraudulent acts is still the best solution for every situation.Users must always be alert before logging their personal information into any website, and do not forget to analyze a URL carefully to see if anything is different before taking the next steps.In addition, you should also be aware that Google or any legitimate service provider will never ask you to log in through a questionable redirection site.Equip yourself to protect yourself!