COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< Target: Gmail users >

CSB17-014

Description:

Security researchers have discovered a new phishing campaign targeting Gmail users, which is so convincing and highly effective that even tech-savvy people can be tricked into giving away their Google credentials to hackers.

How do they do it?

1. Compromise a victim's Gmail account, once they're in, they
2. Start rifling through inboxes to launch secondary attacks in order to pass on the attack
3. The hackers first look for an attachment that victims have previously sent to their contacts and a relevant subject from an actual sent email.
4. Then the criminals will start gathering up contact email addresses
5. After finding one, the hackers create an image (screenshot) of that attachment and include it in reply to the sender with the same or similar subject for the email, invoking recognition and automatic trust.

This attack is so effective because the phishing emails come from someone the victim knows.

It uses image attachments that masquerade as a PDF file with a thumbnailed version of the attachment. Once clicked, victims are redirected to phishing pages, which disguise as the Google sign-in page. But it's a TRAP!

The URL of the fake Gmail login page contains the accounts.google.com subdomain, which is enough to fool the majority of people into believing that they are on a legitimate Google page.

Since the browser does not show the red warning icon usually used by Google to point out insecure pages, users fall for the Gmail hacking scheme.

Victims fall for the scam because of a clever trick employed by this attack, and they submit their credentials, which get delivered directly to the attackers. And as soon as the attackers get their credential, they log into the victim's Gmail account.

How to protect your account?

- Enable two-factor authentication
- Always be careful while opening any attachment in your email
- Always look for the lock icon next to the address bar
- Check the browser location bar and verify the protocol, then verify the hostname
- Check to see if your email account has been hacked
- Do an online search
- Watch for typos
- Know what phishing emails look like
- Use multi-level authentication
- Have strong security software

If the scam sounds familiar and you fear you've already fallen for it,

- Change your Gmail password, then
- Head to the Gmail account activity page

It will show you any current sessions that are logged it and you can kick off any that you think are suspicious.

References:

http://thehackernews.com/2017/01/gmail-phishing-page.html

http://www.ibtimes.co.uk/watch-out-this-convincing-gmail-phishing-scam-thats-rifling-through-users-emails-1601315

http://www.forbes.com/sites/leemathews/2017/01/16/gmail-phishing-attack-targets-your-contacts/#16b32dd41f9d

http://www.komando.com/happening-now/386804/top-story-fake-emails-from-gmail-look-legitimate-but-are-hiding-a-horrible-phishing-scam

https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/

http://securityaffairs.co/wordpress/55369/cyber-crime/phishing-gmail.html

http://mentalfloss.com/article/90966/phishing-scam-targeting-gmail-accounts-posing-your-contacts

http://www.theregister.co.uk/2017/01/16/phishing_attack_probes_sent_mail/