TATA CONSULTANCY SERVICES
Experience certainty.

Malware Advisory

OTP-based 2FA Breach

14th December, 2018

Contents

1. Overview

ArsTechnica has reported a recent phishing campaign targeted US government officials, activists, and journalists that has succeeded in bypassing the two-factor authentication protections offered by Gmail and Yahoo Mail. The 2FA authentication technique bypassed was SMS-based OTPs which has been considered more or less secure owing to the fact that the OTP is sent to the user’s mobile which is in possession of the user.

The report alleges that attackers working on behalf of the Iranian government collected detailed information on targeted individuals and then sent them spear-phishing emails containing a hidden image that alerted the attackers in real time when targets viewed the messages. This enabled the attackers to present false login pages that collected user-supplied credentials and used them on the real login page in real time to compromise their email accounts.

Arstechnica has reported the involvement of Iranian cyber-espionage groups Charming Kittens and Rocket Kittens in these attacks. This is of particular concern as emails are used for spreading Shamoon virus.

Severity: Critical

Release Date: 14th December 2018

Target: Gmail and Yahoo Mail as of current reports

Distribution Method: Email

Discovered by: Certfa Lab and ArsTechnica

2. Technical Detail

The user receives an email containing a hidden image that alerts the attackers when the recipient views the message. The attackers are perpetrating these phishing attacks through:

1. Unknown email or social media and messaging accounts

2. Email or social media and messaging accounts of public figures, which have been hacked by the attackers

Once the user clicks on the image, they are taken to a fake Gmail or Yahoo Security Page. When targets entered passwords into the fake security page, the attackers would almost simultaneously enter the credentials into the corresponding real login page. This will lead to a push notification from the phone app which will make the user enter the received OTP on the fake page presented by the attackers. As long as the target responds within an allotted amount of time (usually 30 seconds), the attackers will gain access.

In theory, this attack can work against any 2fa app that uses SMS-based OTP or asks the user to click an approval button. Apart from bypassing 2fa, the phishing campaign reported by Certfa was effective in hosting malicious pages on sites.google.com. Additionally, emails were sent from addresses such as notifications.mailservices@gmail.com and noreply.customermails@gmail.com to give the impression the content was officially connected to Google. The phishers are supposed to have dedicated more than 20 Internet domains targeted to suit their targets' use of email services on computers and phones.

Certfa said that some of the domains and IP addresses used in the campaign connect the phishers to “Charming Kitten,” a hacker group previously linked to the Iranian government. Charming Kittens is also linked with Rocket Kittens or Magic Hound - an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia.

3. Mitigation Measures

1. Users should immediately update their passwords for their email accounts
2. Users should be advised not to click on random links or images received in emails even if they appear genuine
3. If a user has observed a sudden change in their email account credentials, it should be reported
4. Users should check their Sent Mail to verify that no unaccounted for emails have originated from their accounts

4. Preventive Measures

1. As per ArsTechnica, this attack is impossible, at least in theory, against 2fa that uses an industry-standard security key. These keys connect through a computer USB or by using Bluetooth or Near Field Communication on a phone.
2. Gmail and other types of Google accounts currently have the ability to work with keys that conform to U2F, a standard developed by an industry consortium known as the Fido Alliance.
3. Google also offers an Advanced Protection Program that requires security keys to be used as the sole means of 2fa when accessing Gmail and other types of Google accounts.

5. References

1. https://arstechnica.com/information-technology/2018/12/iranian-phishers-bypass-2fa-protections-offered-by-yahoo-mail-and-gmail/
2. https://blog.certfa.com/posts/the-return-of-the-charming-kitten/