UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00206

TELEGRAM BOTS STEAL OTP TOKENS FOR PAYPAL ETC

DATE ISSUED: 4th October 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A number of big-name payment portal platforms are being targeted by malicious actors using Telegram Bots to steal One Time Password (OTP) Tokens and compromise users accounts including PayPal, Apple Pay, Google Pay and more.

BREAKDOWN

Researchers at Intel 471 discovered the campaign that has been operation since June using a range of tactic s to circumvent Multifactor Authentication (MFA) mechanisms to access protected online accounts. These tactics are based on social engineering to deceive users into giving them their OTP tokens and include calling or messaging victims impersonating banks, other service providers and trusted companies. The Telegram Bots are a Bot-as-a-Service product where threat actors pay to use the services or tools created by another malicious actor making their campaigns quicker to get going and see a lucrative turnaround when deployed in bulk. By entering victims phone numbers and using only a few simple commands the bot takes over and does all the hard work for them. Similar campaigns have seen up to 80% or users targeted surrendering their information to the attacker unwittingly.

REMEDIATION STEPS

- Never give out passwords or OTP tokens to anyone over the phone.
- If you're unsure of the origin of the call, or feel as though something is off, hang up and call back the service provider or bank directly. Some instances have seen bots able to make calls appear to be from a legitimate contact at a specific bank or similar.
- If you receive a suspicious phone call you believe to be impersonating a company, get in touch with them to let them know so they can warn their other customers.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/telegram-bots-compromise-paypal/175099/
Intel 471 https://intel471.com/blog/otp-password-bots-telegram
ZD Net https://www.zdnet.com/article/telegram-bots-are-trying-to-steal-your-one-time-passwords/
Krebs on Security https://krebsonsecurity.com/2021/09/the-rise-of-one-time-password-interception-bots/