JASK THREAT ADVISORY | TLP: WHITE | RISK FACTOR: HIGH

ACCOUNT TAKEOVER CAMPAIGNS TARGETING SMS AUTHENTICATION

OVERVIEW

A series of coordinated and targeted attacks against the cryptocoin community, continue to showcase the weakness of SMS (Short Message Service) used by many corporations and services as a form of multi-factor authentication. The modus operandi of malicious actors consists in pre-texting victims, acquiring previous knowledge of victims via open source intelligence means. Once this knowledge is acquired (email accounts, phone numbers, addresses, social media, etc) malicious actors proceed to port phones by calling cellphone carriers. In other cases they proceed to intercept messages via SS7 interception, publishing malicious applications in phone application stores or using multi-factor authentication phishing tools.

Once malicious actors have obtained SMS messages they proceed to reset and take over all users accounts starting with email accounts with access to financial, social media, corporate accounts. The attacks have mainly focused on cryptocoin holders and financial services, in some cases the attacks targeted corporate users, then proceeding to target user's corporate close circle or chain of command into changing authentication tokens and trying to access corporate resources.

Attacks have shown malicious actors using Google Voice numbers from foreign countries and calling cellphone carriers numerous times until representatives allow porting of phones. In some other cases malicious actors walk into phone dealerships and are able to get phone numbers ported. Things such as port freeze, PINs used for authentication, even one time password applications have been proven to be bypassable. As advised by National Institute of Standard and Technologies SMS as a form of authentication must be deprecated as it does not provide reliable protection from interception, theft and impersonation.

INDICATORS

There are multiple attack vectors being used for account take overs focusing on SMS:

TROJAN VIA MOBILE APPLICATION STORE

Malicious actors are using application stores as a way to publish malicious code into mobile devices. Depending on phone operating system architecture, these malicious applications can access contents of SMS messages and retrieve them from mobile devices. Once this information is retrieved, attackers can use it to access victims accounts bypassing SMS authentication.

COMPUTER TROJAN

Malicious code, specifically banking trojans, have been reported, to steal victim's phone number information to then be used for interception.

CELL PHONE SIGNAL INTERCEPTION

There has been numerous vulnerability advisories on SS7 (Signaling System 7). A framework of protocols used for transmitting information in the form of voice and text between phones. Commercial tools for interception are available for purchase as well as tutorials on how to make a homemade "IMSI catcher" also known as fake/rogue cell phone towers. This type of setup allows for interception of voice and text data. This can be in conjunction of stealing user's name and password by other means then intercepting SMS used for two factor authentication.

This type of attack was reported in Germany, where a number of users were victim of financial theft after their accounts were accessed by catching SMS for bank authentication. More recently a wave of attacks against the cryptocoin community using SMS interception was researched by security firm Positive Technologies. In this report researchers were able to effectively intercept SMS messages and access cryptocoin exchange provider.

PORT TO OWN /SOCIAL ENGINEERING

Another vector of attack actively exploited by malicious actors is the porting of phone numbers to reset targeted accounts. Malicious actors will pre-text victims (names, phone numbers, social media, address, etc) then proceed to use that information to port victim's phone numbers into a new SIM card. They then proceed to reset passwords and take over accounts from victims. In some cases malicious actors are using Google voice numbers and calling from foreign countries, or going in person into phone dealers and using social engineering to convince dealer representatives to port phone. Malicious actors have at times followed victim's social media to identify victims inability to react (boarding a plane, time zone, or any event that will keep victim away).

Many victims have landed or woke up in the morning to find a "No signal" message in their phone. Things such as "Port Freeze", account PIN, account secret codes, have been bypassed by malicious actors at times calling over dozens of times until a representative allows the port, or visiting phone dealers. Persistent targeting of cryptocoin owners has been reported. The number of porting attacks related to "dealer" phone porting may indicate a bigger network of complicity in these type of attacks.

SMS CAN BE READ IN DEVICES BEYOND PHONE

Many applications allow reading of SMS text messages in other places besides the phone, including online carrier sites. Examples of that functionality can be seem in Google hangouts and Apple iMessage. This means, for certain victims, criminals do not need to have access to phone or cellphone signal, they can instead either access online site or compromise computer and extract information.

PHONE TOTP APPLICATIONS CAN ALSO BE COMPROMISED

Time-based one time passwords algorithms (TOTP), have been suggested as an alternative to SMS two factor authentication. These applications "compute a one-time password from a shared secret key and the current time". These one time passwords are generated within the phone and makes interception more difficult, however some of these applications have been shown to be "portable" to other phones, so malicious actors have been able to port phones and then install TOTP application, proceeding to compromise account. As of the writing of this advisory only Google Authenticator seems to be the most reliable TOTP application.

MULTI FACTOR AUTHENTICATION PHISHING TOOLS

Phishing is a very powerful attack vector, being currently one of the principal attack vectors against enterprises. The use of misleading messages usually in the form of emails that contain malicious code attached to them, continues to be one of the most used vectors of attacks against enterprises. SMS is primarily used by many enterprises as two factor authentication and to prevent phishing. However, as of the writing of this advisory there are already MFA phishing research tools in the infosec community. It is only logical to expect tools like these into crimeware further decimating the reliability of SMS as authentication form.

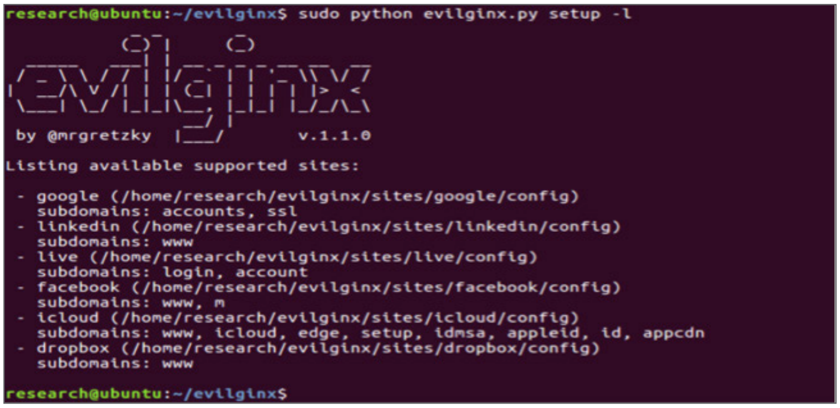
TIME TO MOVE ON FROM SMS FOR AUTHENTICATION

The above indicators clearly expose multiple and significant vulnerabilities in the use of SMS as form of authentication. Such vulnerabilities establish a scenario where reception of SMS cannot be used to prove identity. The National Institute of Standards and Technologies has advised to deprecate the use of SMS for authentication. Such use in enterprises should be deprecated if not eliminated where possible. The number of campaigns at the moment seem to be focusing on financial and cryptocoin community, however it is a matter of time until these type of attacks move to other verticals and industries.

LAB STUDY A MULTI FACTOR AUTHENTICATION PHISHING TOOL (EVILGINX)

As stated above, MFA phishing tools are appearing in the infosec community as proof of concept of the weaknesses of SMS as two factor authentication. Specifically there are at this moment two tools available for this research purpose; MFA Slipstream and Evilginx. What these tools do is basically clone a reputable site, present login page, request login to the actual site in the background, then real site sends code to mobile via SMS, tool mimics real site fields to enter code, then attacker obtains username, passwords and SMS code.

Below a brief proof of concept using Evilginx, to take over a Google sign in page by compromising SMS codes sent back to the user.



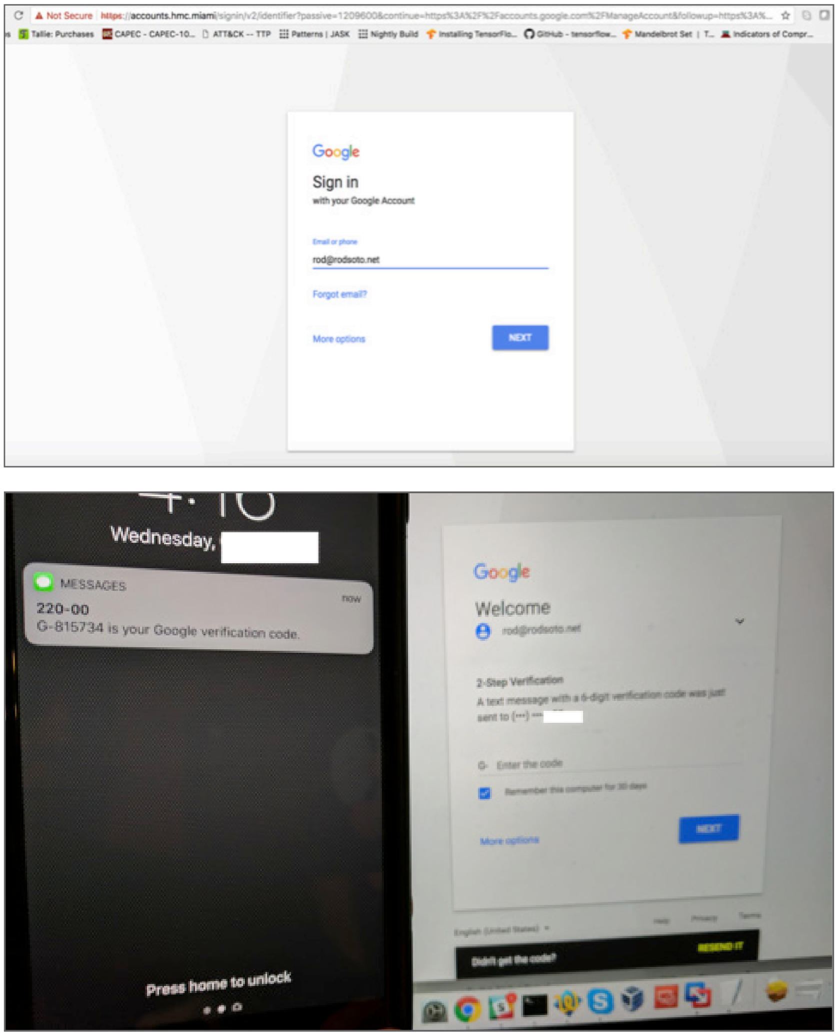
```
research@ubuntu:~/evilginx$ sudo python evilginx.py setup -l
            (_)|     (_)
 ______ ____ _ | | __ _ _ _ __ __ __
/  _ \ \ / /| | |/ _` | | '_ \\ \/ /
|  __/\ V / | | | (_| | | | | |>  <
\___|  \_/  |_|_|\__, |_|_| |_/_/\_\
                  __/ |
 by @mrgretzky   |___/        v.1.1.0

Listing available supported sites:

 - google (/home/research/evilginx/sites/google/config)
   subdomains: accounts, ssl
 - linkedin (/home/research/evilginx/sites/linkedin/config)
   subdomains: www
 - live (/home/research/evilginx/sites/live/config)
   subdomains: login, account
 - facebook (/home/research/evilginx/sites/facebook/config)
   subdomains: www, m
 - icloud (/home/research/evilginx/sites/icloud/config)
   subdomains: www, icloud, edge, setup, idmsa, appleid, id, appcdn
 - dropbox (/home/research/evilginx/sites/dropbox/config)
   subdomains: www

research@ubuntu:~/evilginx$
```

Fig 1 Evilginx MFA phishing tool menu



Not Secure https://accounts.hmc.miami/signin/v2/identifier?passive=1209600&continue=https%3A%2F%2Faccounts.google.com%2FManageAccount&followup=https%3A%...

Google

Sign in

with your Google Account

Email or phone

rod@rodsoto.net

Wednesday, [redacted]

MESSAGES now

220-00

G-815734 is your Google verification code.

Google

Welcome

rod@rodsoto.net

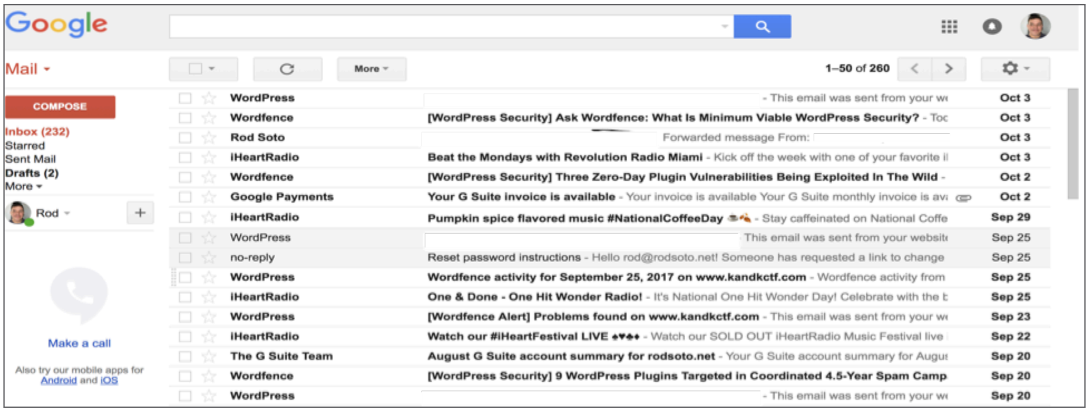
2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) ••• [redacted]

G- Enter the code

☑ Remember this computer for 30 days

Fig 2 phishing page/ 2FA prompt and code



WordPress	- This email was sent from your w	Oct 3
Wordfence	[WordPress Security] Ask Wordfence: What Is Minimum Viable WordPress Security? - Toc	Oct 3
Rod Soto	Forwarded message From:	Oct 3
iHeartRadio	Beat the Mondays with Revolution Radio Miami - Kick off the week with one of your favorite i	Oct 3
Wordfence	[WordPress Security] Three Zero-Day Plugin Vulnerabilities Being Exploited In The Wild -	Oct 2
Google Payments	Your G Suite invoice is available - Your invoice is available Your G Suite monthly invoice is av	Oct 2
iHeartRadio	Pumpkin spice flavored music #NationalCoffeeDay - Stay caffeinated on National Coffe	Sep 29
WordPress	This email was sent from your websit	Sep 25
no-reply	Reset password instructions - Hello rod@rodsoto.net! Someone has requested a link to change	Sep 25
WordPress	Wordfence activity for September 25, 2017 on www.kandkctf.com - Wordfence activity from	Sep 25
iHeartRadio	One & Done - One Hit Wonder Radio! - It's National One Hit Wonder Day! Celebrate with the t	Sep 25
WordPress	[Wordfence Alert] Problems found on www.kandkctf.com - This email was sent from your w	Sep 23
iHeartRadio	Watch our #iHeartFestival LIVE ♠♥♣♦ - Watch our SOLD OUT iHeartRadio Music Festival live	Sep 22
The G Suite Team	August G Suite account summary for rodsoto.net - Your G Suite account summary for Augu	Sep 20
Wordfence	[WordPress Security] 9 WordPress Plugins Targeted in Coordinated 4.5-Year Spam Camp	Sep 20
WordPress	- This email was sent from your w	Sep 20

Fig 3 successful login

It is important to clarify that the above type of attack is based on Phishing as initial attack vector. User must click on link and stay within malicious link entering username, password and code in order for this attack to be successful.

IDENTIFIED MICRO BEHAVIORS OF A MULTI FACTOR AUTHENTICATION PHISHING ATTACK

JASK DETECTION

At JASK we are working on developing models that approach the Phishing vector using Machine Learning. Some of the identified Micro behaviors in this type of attack include:

- Entropy in URI/URL (I.E. Number of dots, special characters, URL crazy)
- Whois (registrar with bad reputation / geolocation / bulletproof hosting)
- URL Shorteners (Tiny URL, bit.ly, etc)
- Spelling errors, passwords/code fields,
- Presence of iframes, javascript, pagerank, source of images, redirects
- Presence of .exe, .pdf, .bat, ps1, ps, .bin, .bat, .jar, .bin, .zip

JASK Trident focuses on detection of micro behaviors in conjunction with entity analytics and behavioral baselining, thus providing a multi contextual approach where these types of attacks can be detected.

MITIGATION

Current state of this type of authentication method exposes enterprises to a higher risk of compromise due to the possibility of the above mentioned attacks. However, there are certain things that can be done to protect users and enterprises. Some of them include:

BURNER PHONE FOR SMS ONLY

Some individuals have resorted to purchase phones with numbers to be used exclusively for SMS authentication, keeping their numbers away from public exposure. This may partially protect from pre-texting.

TOTP—TIME BASED ONE TIME PASSWORD (GOOGLE AUTHENTICATOR)

Many enterprises are turning into google authenticator as second form of authentication. There are also Microsoft Authenticator and Authy among others.

LOCKING FEATURES

Some enterprises are using "locking", "freezing", "delaying" mechanisms in order to give victims enough time to react and claim their accounts, some of these measures such as Coinbase AutoLocking, Apple ID lock, Facebook Extra Security.

DO NOT LINK SMS PHONE WITH MAIN EMAIL ACCOUNT

It creates a single point of failure. Many victims could not communicate with their companies, or services because once attackers obtained SMS they proceeded to change passwords and prevent access from genuine users.

TOKENS

If possible use tokens as well as forms of authentication. Username/Password → TOTP → Token, like a Yubikey for example.

PORT PHONE NUMBER AWAY FROM CARRIERS

As carriers have shown extremely poor levels of security when it comes to preventing phone porting attacks, many users have discovered that porting phone to things such as Google Voice/Fi makes it extremely difficult to malicious actors to port phone numbers.

JASK

ABOUT JASK.AI

JASK monitors networks end to end, surfacing, triaging and mapping the most relevant attacks at unprecedented speed, using advanced AI. Analysts are empowered to make informed decisions faster and with more precision.

www.jask.ai