

# SMASHING SMS CAMPAIGNS

20 September 2019

**CRESTCon Asia 2019**

# AGENDA

- About Me
- Inspiration
- SMS as An Alternative
- TapIt – SMS Phishing Framework
- Conclusion
- Q&A

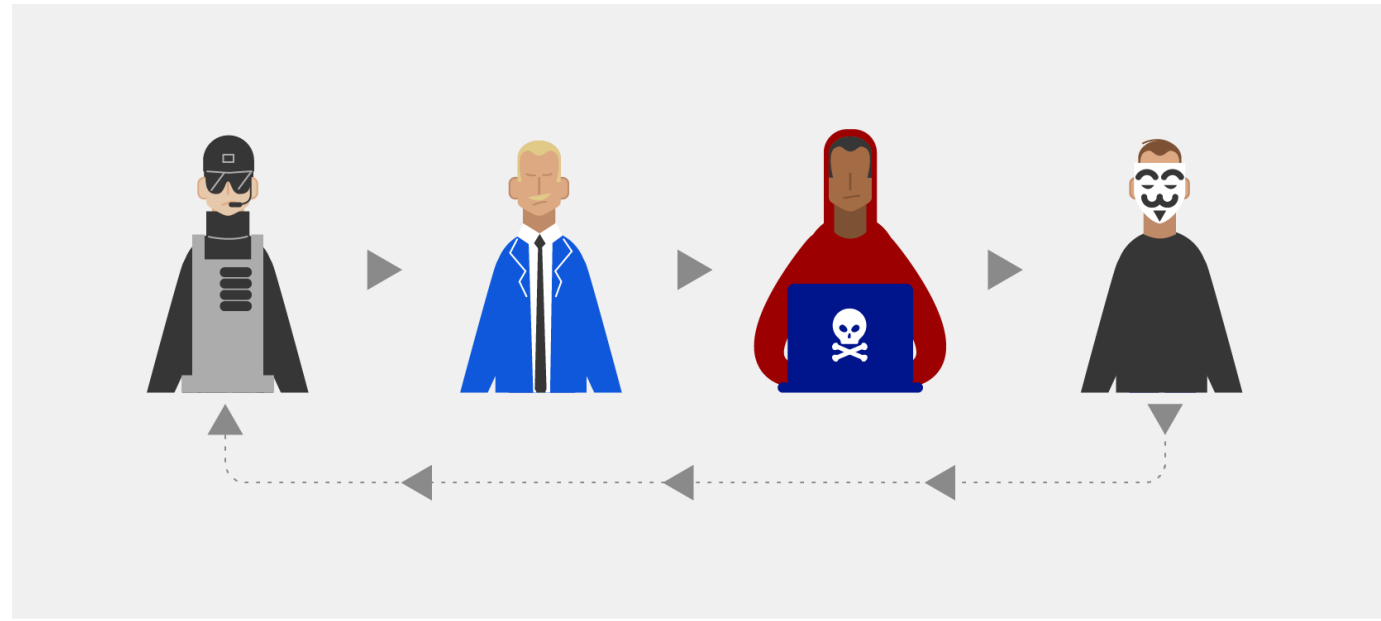
# WHO ARE WE – F-SECURE CONSULTING

- Global cyber-defense consultancy
- Primarily work with Tier-1 Financial Institutions and those with ‘a lot to lose’
- Been doing Red, Blue, and Purple (all the colours of the rainbow) for a long time
- AASE, CBEST, iCAST, TIBER, TAS, STAR, Red Team...
- CSIR, CIR, CCPT - .com. & .gov - gives us visibility of attacks, attackers and compromises across a range of industries and sectors, including nation state attackers.

# WHO AM I?

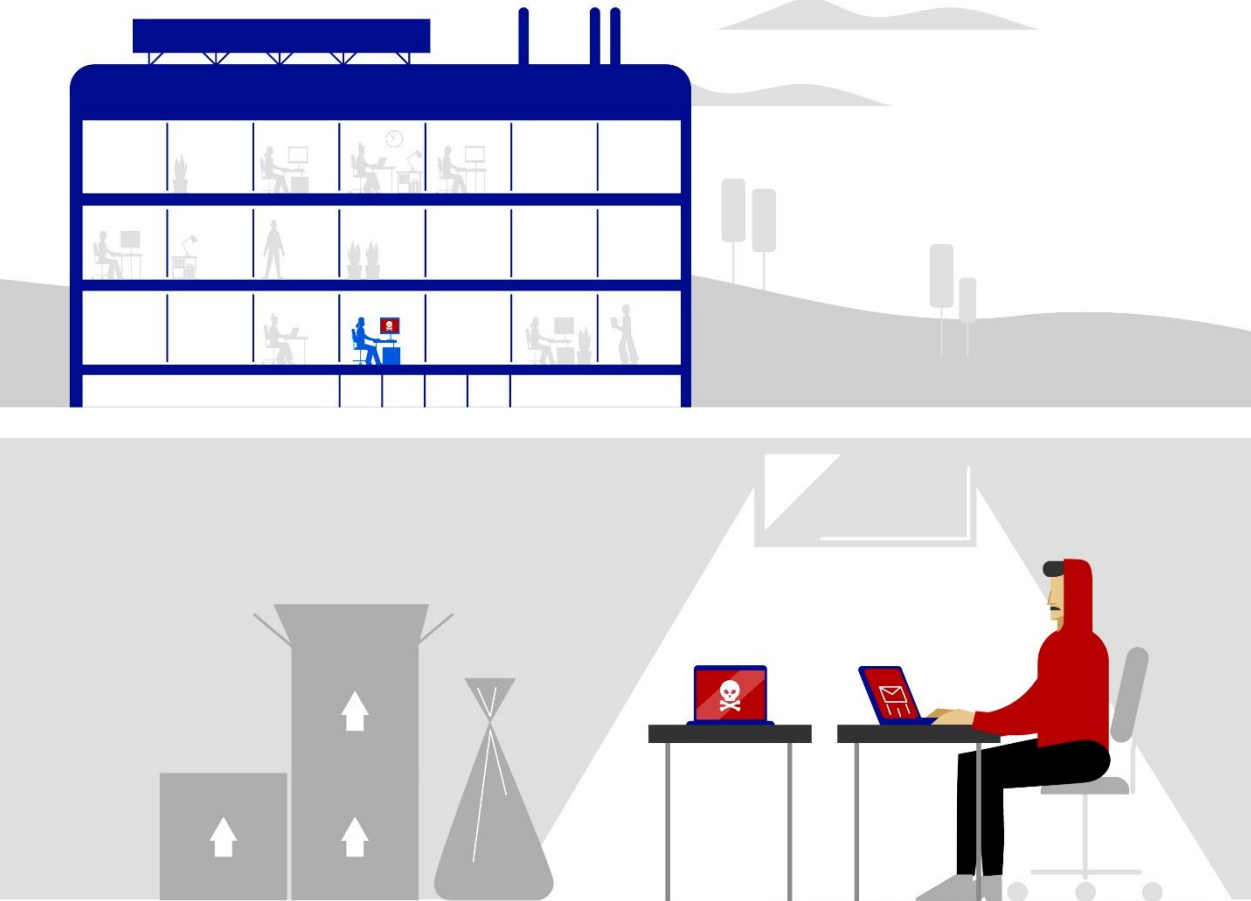
## SAMUEL PUA

- Security Consultant at F-Secure
- Red Team exposure & experience
- Have been developing toolset to aid in red team engagements
- Presented at InfoSec in the City 2019 on red team persistence tooling



# INSPIRATION

# INSPIRATION



- Target: A global financial institution
- Multiple email phishing campaigns were prepared
  - Targeted phishing campaigns for smaller groups (<5 employees)
  - Large-scale phishing campaigns (>50 employees)

# SENDING EMAILS SHOULD BE EASY...RIGHT?

## PRE-SENDING OF EMAILS

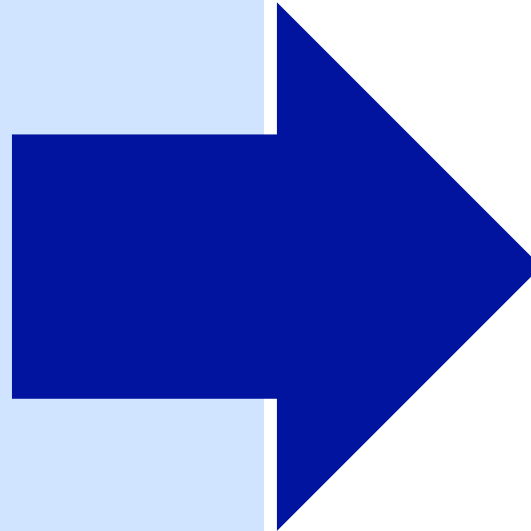
- Infrastructure to be set up

## SENDING OF EMAILS

- Payloads preparation
- Email content preparation
- Metadata management

## POST-SENDING OF EMAILS

- Detection of phishing flagging
- Detection of investigation



## RESULTS

Significant amount of time spent on testing of payloads & emails

Lower ROI

# FOCUS ON EMAIL PHISHING

All

Images

News

Videos


Maps

More

Settings

Tools


About 21,500 results (0.21 seconds)   All news ▼   Past month ▼   Sorted by relevance ▼   Clear



British Gas warns **email scam** is tricking customers into ...

Edinburgh Live - 22 hours ago

British Gas has warning a new email **email scam** is tricking customers into handing over hundreds to fraudsters. British Gas, which is the largest energy and ...



New evasive spear **phishing** attacks bypass **email** security ...

TechTarget - 16 hours ago

Attackers are playing the long game. Their newest **phishing** adaption is a product of monthslong intelligence gathering and social engineering -- and it's already ...



# INCREASING FOCUS ON EMAIL SECURITY

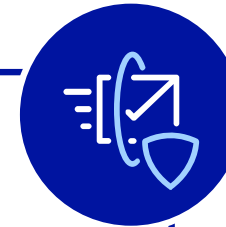
## PEOPLE

- Employees & users are more aware of signs of email phishing
- Return on investment is significantly lower



## PROCESS

- More organisations are aware of the risk of email phishing and have put processes in-place to manage it
- Detection, response processes are in place



## TECHNOLOGY

- More and more detective & preventive systems built around email systems
- SPF, DKIM, spam filters
- Sandbox, email inspection



# WHAT ARE THE OPTIONS?

## CYBER-PHYSICAL ATTACKS

### Pros:

- Difficult to attribute attacks
- Less telemetry on attack source

### Cons:

- Low ROI
- Increased Risk

## VOICE PHISHING

### Pros:

- Ease of creating rapport

### Cons:

- Difficult to conduct large-scale phishing
- Increased complexity to lead to code-execution

## SMS PHISHING

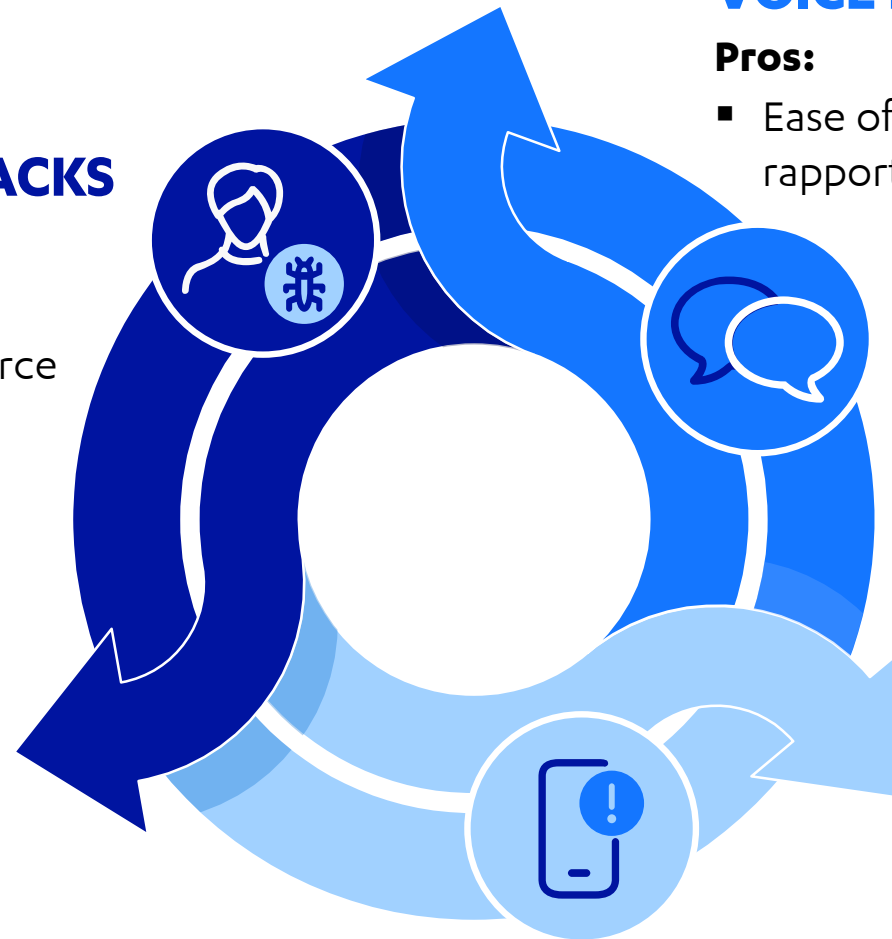
### Pros:

- Ease of conducting large-scale phishing
- Low-cost of execution

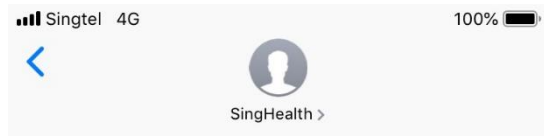
### Cons:

- Target device not on network

*and many others...*



# WHICH OF THESE IS THE REAL MESSAGE?



[sing-health.co/cyber-18](http://sing-health.co/cyber-18)

SAMUEL PUA - your name, IC, address, gender, race, birth date & outpatient dispensed medicines in 2015-18 were accessed but not altered. Mobile no. medical & financial info unaffected. No action needed. We apologise for anxiety caused. For queries [6326-5555](tel:6326-5555) (9am-9pm).



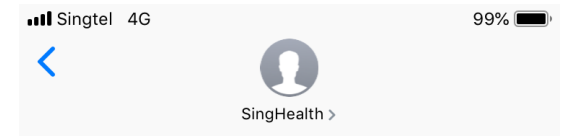
[sing-health.net/cyber-18](http://sing-health.net/cyber-18)

SAMUEL PUA - your name, IC, address, gender, race, birth date & outpatient dispensed medicines in 2015-18 were accessed but not altered. Mobile no. medical & financial info unaffected. No action needed. We apologise for anxiety caused. For queries [6326-5555](tel:6326-5555) (9am-9pm).



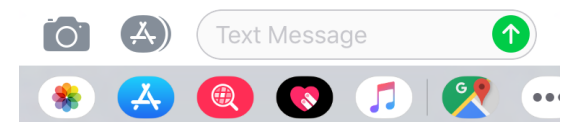
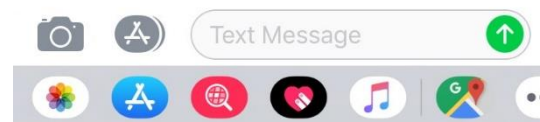
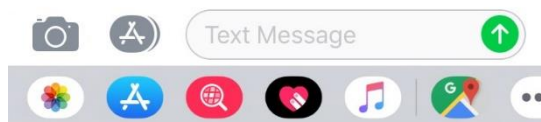
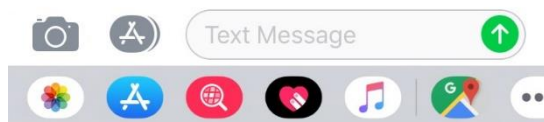
[bit.ly/singhealth-18](http://bit.ly/singhealth-18) SAMUEL

PUA - your name, IC, address, gender, race, birth date & outpatient dispensed medicines in 2015-18 were accessed but not altered. Mobile no. medical & financial info unaffected. No action needed. We apologise for anxiety caused. For queries [6326-5555](tel:6326-5555) (9am-9pm).

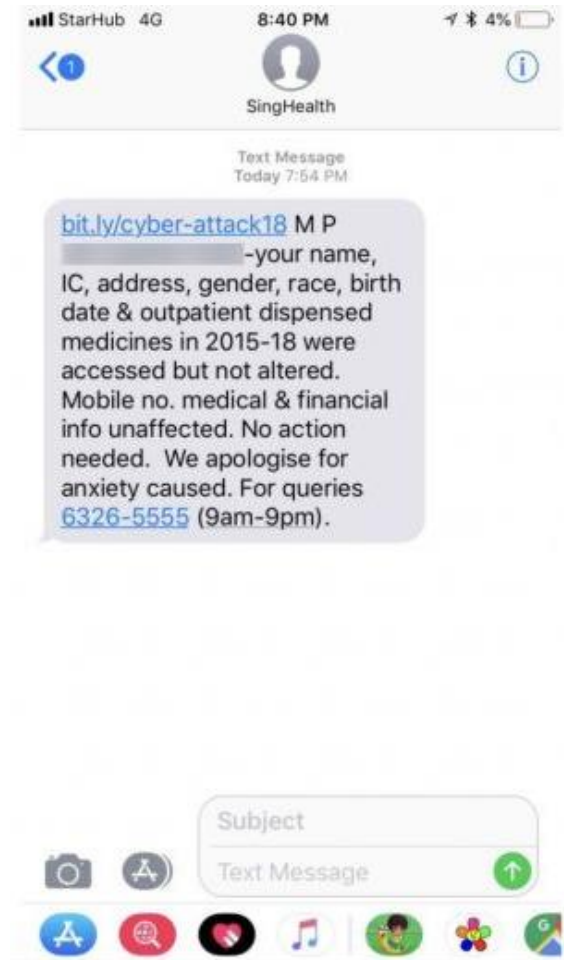


[bit.ly/cyber-attack18](http://bit.ly/cyber-attack18) SAMUEL

PUA - your name, IC, address, gender, race, birth date & outpatient dispensed medicines in 2015-18 were accessed but not altered. Mobile no. medical & financial info unaffected. No action needed. We apologise for anxiety caused. For queries [6326-5555](tel:6326-5555) (9am-9pm).



# REAL MESSAGE



# SMS AS AN ALTERNATIVE

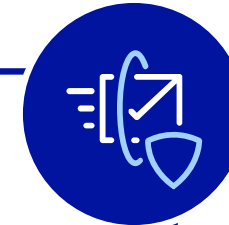
## PEOPLE

- A less used vector, especially for targeting organisations, most users are not wary of SMS as a phishing vector
- Difficult to tell the difference between a real message vs a phishing SMS



## PROCESS

- Few organisations have processes in place to monitor SMS
- No monitor -> No detection -> No response



## TECHNOLOGY

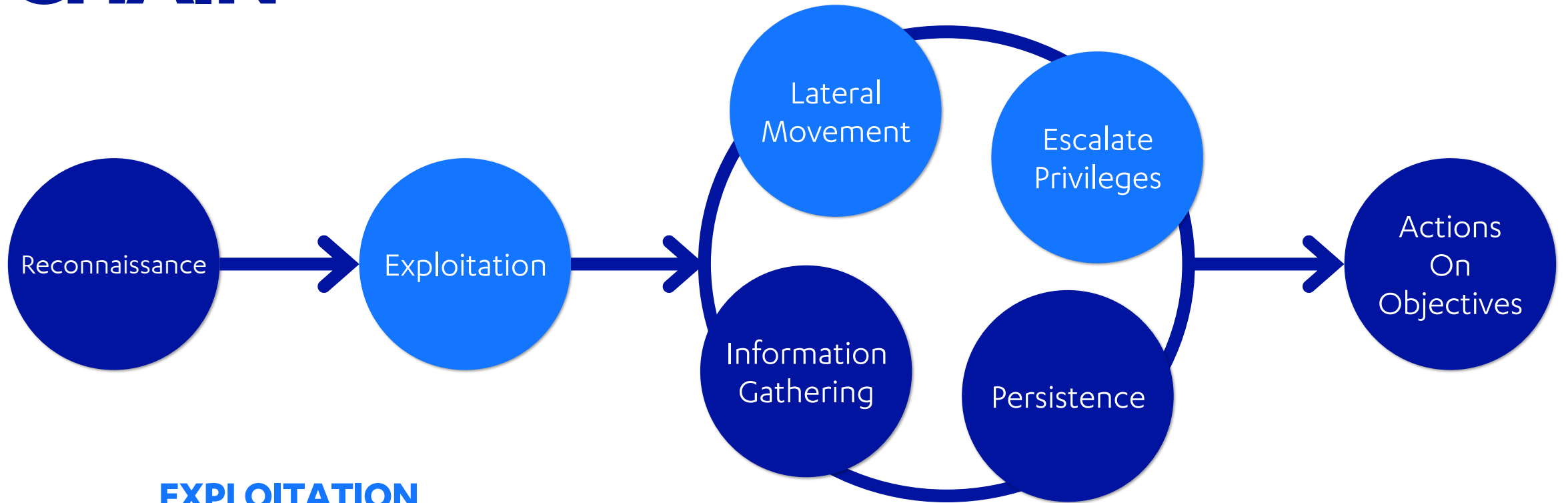
- MDM solutions generally do not monitor content of SMS
- No accessible mechanism to tell real messages from spoofed ones



The background of the slide is a complex network of thin, light blue lines connecting numerous small, dark blue circular nodes. These nodes are scattered across the entire frame, creating a web-like or molecular structure that suggests connectivity and technology.

# **SMS AS AN ALTERNATIVE**

# EFFECTIVENESS OF SMS IN THE KILL CHAIN



## EXPLOITATION

- Pretexting
- Delivery of payload
- Phishing for VPN credentials

## LATERAL MOVEMENT

- Gaining code execution

## ESCALATE PRIVILEGES

- Subverting 2FA in critical systems



# TAPIT – SMS PHISHING FRAMEWORK



# TAPIT – SMS PHISHING FRAMEWORK

- Internally developed application to assist in SMS Phishing within an attack chain
- Specifically aims to create SMS phishing with high ease for the following activities:
  - Pretexting
  - Credentials Harvesting
  - Payload Delivery
  - 2FA Phishing




# **EXAMPLE 1**

# **LATERAL MOVEMENT**

# EXAMPLE 1 – LATERAL MOVEMENT

- You have achieved initial compromise and have beacon on one machine
- You need to move on to more hosts to improve your attack surface
- You have obtained information that HR sends SMS messages to employees using alphanumeric sender ID of “ACME HR”
- You have obtained knowledge that the organisation uses Office 365 for their email and SharePoint
- You have backdoored a MS Word document on the company shared folder

# CREATING SMS TEMPLATE

 TapIt

Campaigns Phonebook Text Templates Web Templates Settings ▾

Log Out

Text Template Name


Text Template

Hi {firstName}. There will be changes to our HR benefits policy from 1 Oct 2019 onwards. Please visit check your email, or visit X:\HR\policy-changes.doc to find out more.

Save Text Template

Delete

# POPULATING VICTIM CONTACTS

 TapIt

Campaigns Phonebook Text Templates Web Templates Settings ▾

Log Out

Phonebook Name


Import Records

[Download file template here.](#)

First Name	Last Name	Alias	Phone Number
Samuel	Pua	Samuel	+6581607352

*Press enter to insert additional record*

# BUILDING SMS PHISHING CAMPAIGN

 TapIt

Campaigns Phonebook Text Templates Web Templates Settings ▾

Log Out

Campaign Name

internal

From Number

ACME HR

Provider

Twilio

Phonebook

Victims: Size 1

Text Template

internal

# MONITORING CAMPAIGNS

T TapIt

Campaigns Phonebook Text Templates Web Templates Settings ▾

Log Out

Start Campaign

Delete

Campaign Name

internal

Campaign Size

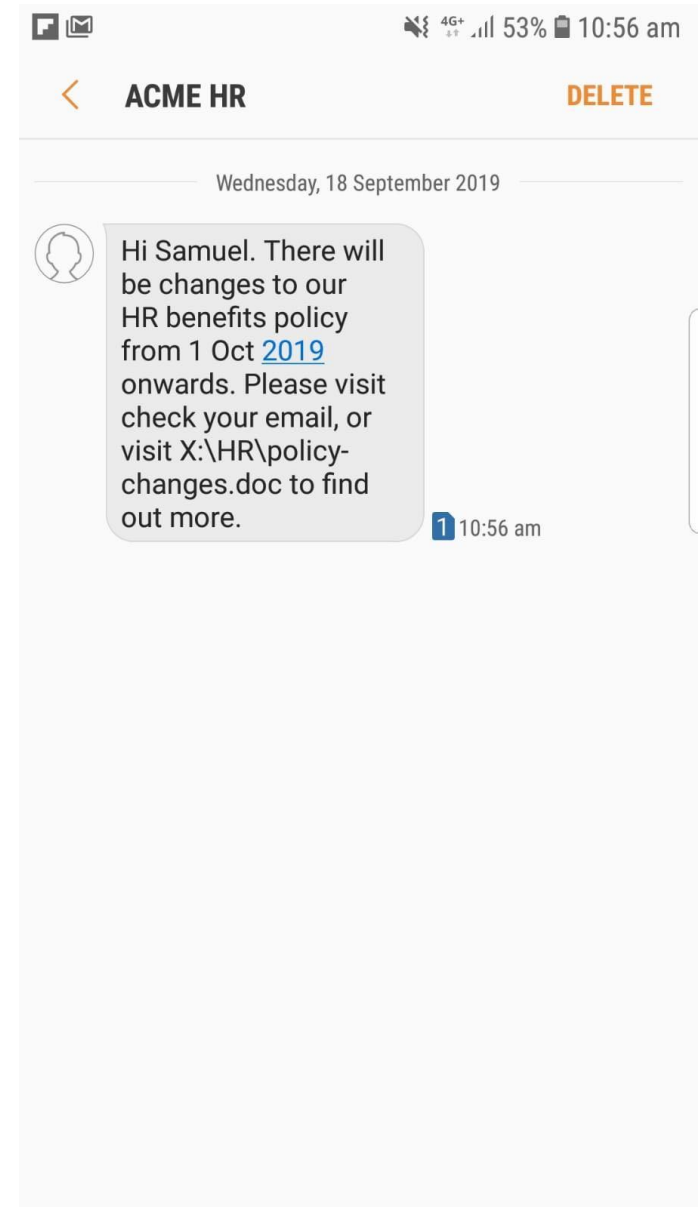
1

Campaign Status

Completed

From	To	Current Status	Web Status	Web Route URL	Time Sent
ACME HR	+6581607352	Delivered			18-Sep-2019

# VICTIM'S POV





# **EXAMPLE 2**

## **2FA PHISHING FOR CITRIX**

# EXAMPLE 2 – 2FA PHISHING

- You have identified a high-value target that gives access to the bank's SWIFT network
- The target is accessible only through a Citrix host
- You have the credentials of a SWIFT user, but the Citrix configuration requires SMS-based 2FA for login
- You have identified the alphanumeric sender ID of the 2FA system as "ACME Citrix"

# CREATING WEB TEMPLATE

T

TapIt

CampaignsPhonebookText TemplatesWeb TemplatesSettings

Log Out

Web Template Name

citrix

Web Template Type

Credentials Harvesting

Placeholder HTML

<!DOCTYPE html>  
<html lang="en"><head>  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Netscaler Gateway 2018</title>  
<!--<link rel="SHORTCUT ICON" href="/vpn/media/NSG\_favicon.ico" type="image/vnd.microsoft.icon">-->  
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">  
<!-- Mobile viewport optimized: i.mn/bslateviewnort

After HTML

<!DOCTYPE html>  
<html lang="en"><head>  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Netscaler Gateway 2018</title>  
<!--<link rel="SHORTCUT ICON" href="/vpn/media/NSG\_favicon.ico" type="image/vnd.microsoft.icon">-->

# BUILDING SMS PHISHING CAMPAIGN

T

TapIt

CampaignsPhonebookText TemplatesWeb TemplatesSettings ▾

Log Out

Campaign Name

2fa

From Number

ACME Citrix

Provider

Twilio

▾

Phonebook

Victims: Size 1

▾

Text Template

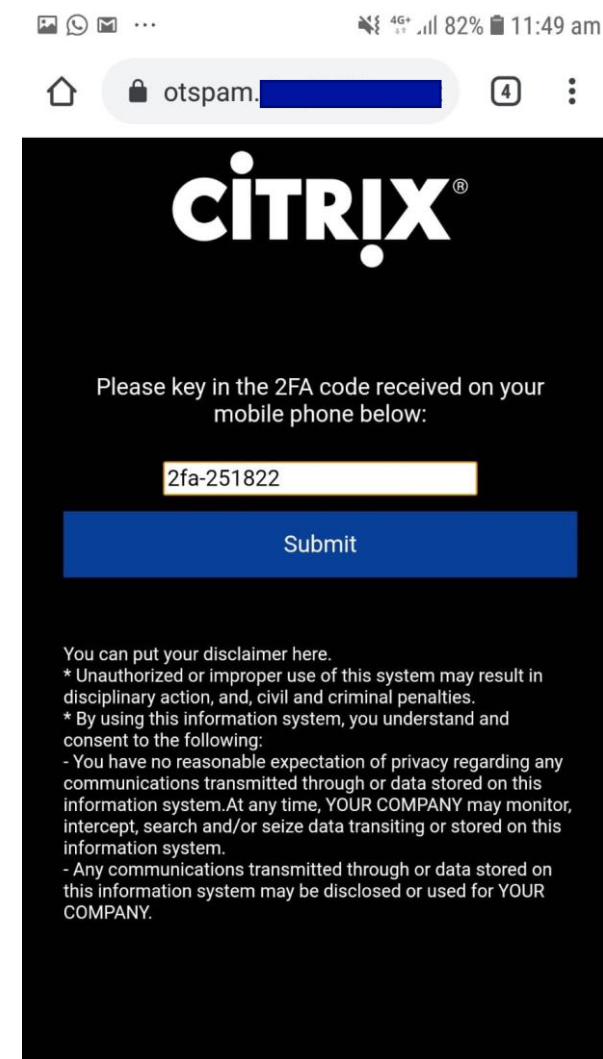
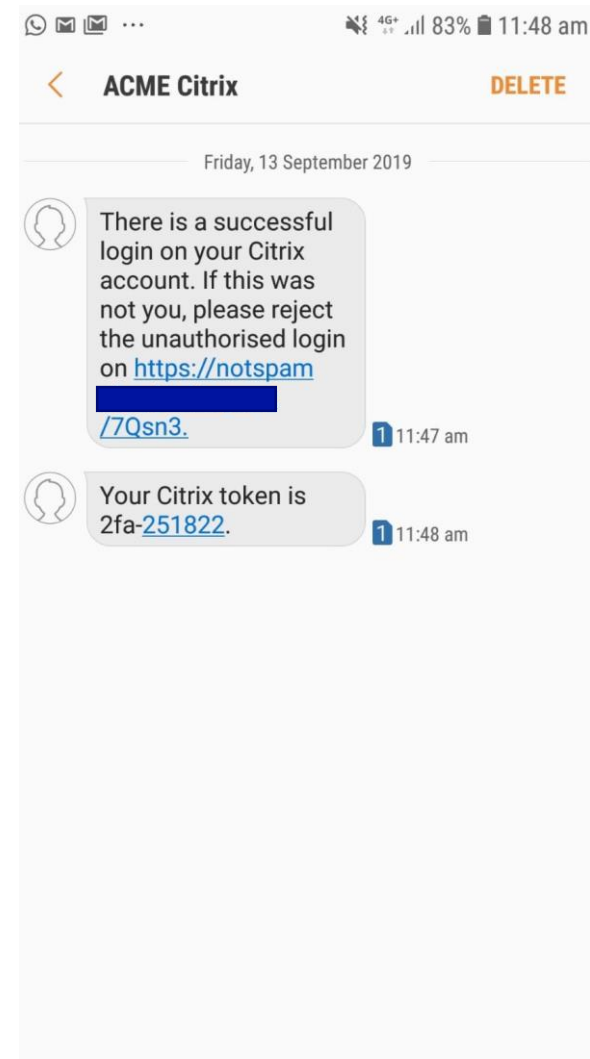
2FA Login

▾

Web Template

▾

# VICTIM'S POV



# HARVESTING CREDENTIALS

T TapIt

Campaigns Phonebook Text Templates Web Templates Settings

Start Campaign Delete

Campaign Name

Office 365

Campaign Size

1

Campaign Status

Completed

From	To	Current Status	Web Status	Web Route	
ACME HR	+6581607352	Delivered	2 visits	https://notspam.[REDACTED]/v9ivA	10-Sep-2019

Opening visits-18.csv

You have chosen to open:  
visits-18.csv  
which is: TXT file (1.2 KB)  
from: blob:

What should Firefox do with this file?  
☒ Open with Notepad++ : a free (GNU) source code editor (d...  
☐ Save File  
☐ Do this automatically for files like this from now on.

OK Cancel



A large commercial airplane is shown from a front-three-quarter perspective inside a spacious hangar. The aircraft's nose, cockpit, and wings are prominent. The hangar has a high ceiling with a complex steel truss structure and large windows. The floor is highly reflective, mirroring the plane and the hangar's interior. A semi-transparent network of white dots and lines is overlaid on the entire image, particularly concentrated around the aircraft's nose and the upper part of the hangar. The word "CONCLUSION" is written in a large, bold, blue sans-serif font across the lower middle of the image.

# CONCLUSION



# CONCLUSION

- Phishing is dead. Long live Phishing!
- Humans are viable as an attack vector in some circumstances
- SMS Phishing can be a useful tool in a social engineer's toolkit





**F-Secure®**