Cyberint

INSIDE A PHISHING SHARING PLATFORM

PHILIPPINE BANKS UNDER ATTACK BY LOCAL THREAT ACTOR GROUPS

Cyberint

Executive Summary

Since the beginning of June 2019 CyberInt unveiled activities of two Philippine threat actor groups, '**PureHackers**' and '**Shinobi Security**', targeting multiple banks in the Philippines. One of the groups' members has developed a unique command and control system (C2) with a phishing collaboration dashboard, used for tracking active phishing sites and its compromised victims' data, which is referred to among the threat actors community as "Fullz"[1].

The Philippine Banks are constantly targeted by Filipino threat actors attempting to steal banks' customers' Fullz - and their credit card details in particular. Phishing is one of the main methods used by these threat actors to achieve the relevant data. The phishing collaboration dashboard was detected early on in its beta phase by CyberInt and analyzed in this report. The platform demonstrates the ongoing effort Filipino threat actors are putting to increase the productivity of their nefarious activities via automation and collaboration processes. CyberInt's direct access to the mentioned system has enabled to provide a unique in-depth view of the way threat actors operate and collaborate. In addition, it has enabled CyberInt to thoroughly map a comprehensive phishing attack 'kill chain' and define the different stages it comprises.

CyberInt is continuing the monitoring and will keep sharing all the relevant information of further 'Pure Hackers' and 'Shinobi Security' activities and the details of additional Fullz and active phishing sites loaded into the system with its customers.

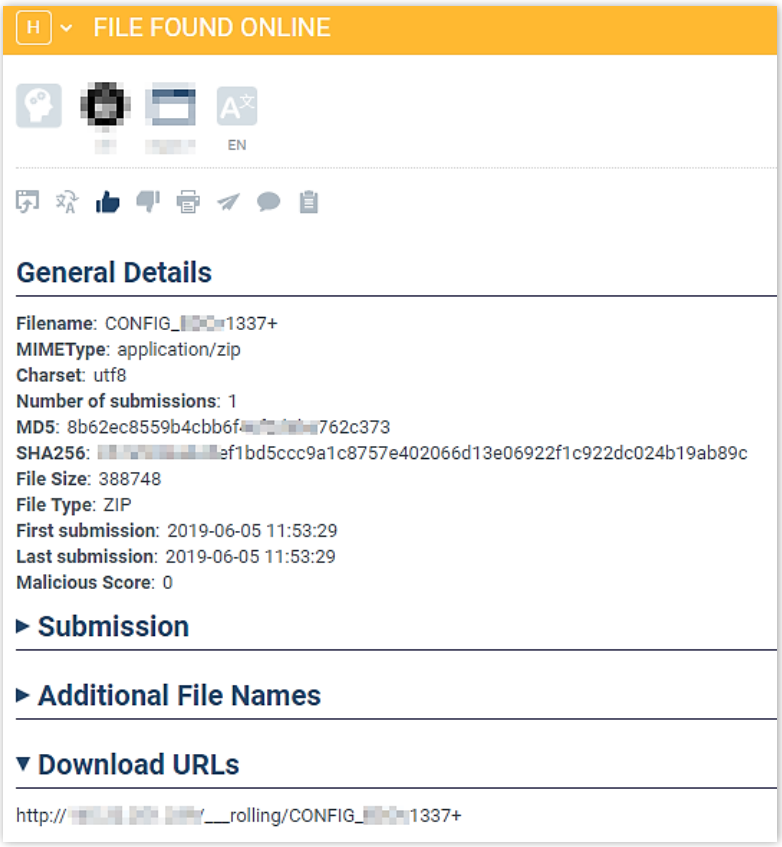
[1] 'Fullz' refers to full packages of individuals' identifying information. This may include full name, billing address, credit card number, expiration date and card security code, birth date, credentials and more.

Cyberint

Argos™ Detection

The initial finding that led to the phishing collaboration dashboard, was a compressed file uploaded to an Anti-virus repository which was flagged by Argos™, CyberInt's proprietary platform. The compressed file (.ZIP file) revealed information which led CyberInt's Threat Intelligence team to a server with open directory, that enabled downloading two password-protected phishing kits targeting two Philippine banks.

The kits were created on May 26, 2019, the same date that a member of the 'PureHackers' and 'Shinobi Security' groups, offered phishing kits for sale on Facebook, targeting the same two Banks. Although some of the files were encrypted, CyberInt was able to affirm they are all being used for phishing purposes. This correlation led CyberInt to further investigate these threat actor groups and continuously monitor their activities.



Suspiciouscompressed.ZIP file detected by Argos™

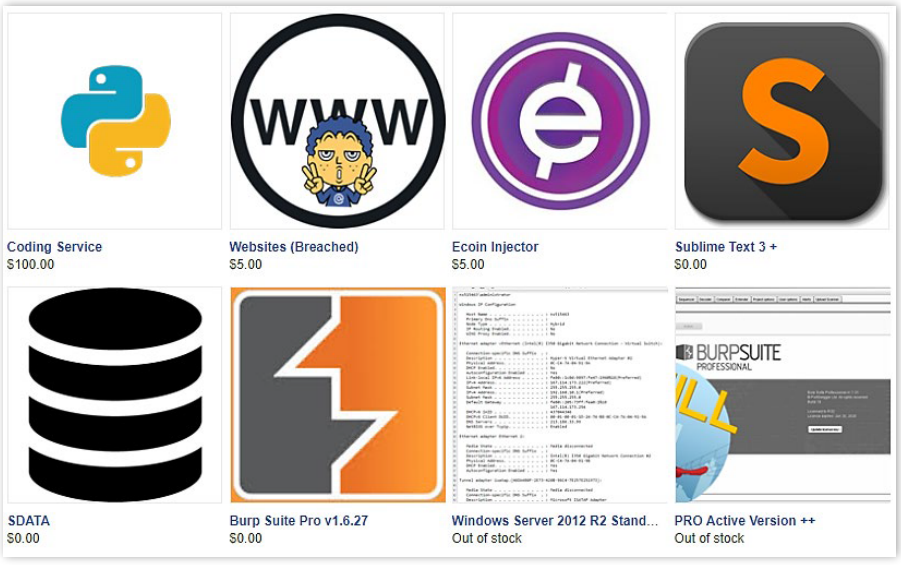
Threat Actor Groups: PureHackers & SHINOBI SECURITY

Following the detection of the mentioned compressed file and phishing kits, CyberInt's Threat Intelligence team further investigated two Philippine Threat Actor groups, whose members are involved in the creation of the Phishing collaboration dashboard: 'PureHackers' and 'SHINOBI SECURITY'.

PureHackers

A Filipino hacking group that has been active since approximately 2014. Originally called PH.RED, later on to PH.R3D, and finally change their name to 'PureHackers #Unleashed -»' on October 12, 2016. They were observed conducting defacements against various known Philippine organizations' websites, as well as phishing attacks against the Philippine banking sector. The group offers for sale compromised servers, coding services, and more. Additional group members based on defacements are: PH.R3D, PH.SOL, KERJ.ATTACKER, Xscyth3, D4rk_ur4n!um, PH.Winsxs, PH.K1LluA, XSilver~, Spade, sm1l3, S4nj1, BSHxS34N, PH.BL4CK, Mafiaboy, PH.XDM8, PH.N, ph.s1L3ntgh0st, xPad3, INTRAVENOUS.PH, Satan666, Imba.PH, PH.3XTR4CT, PH.xR3aper, PH.1nDr4, J4ck Skel3t0n, NewbieXHacker, Mng.Carl<3, ph.MasKARra, Mang Kepweng/DarKLorD.PH, Skywr4th.

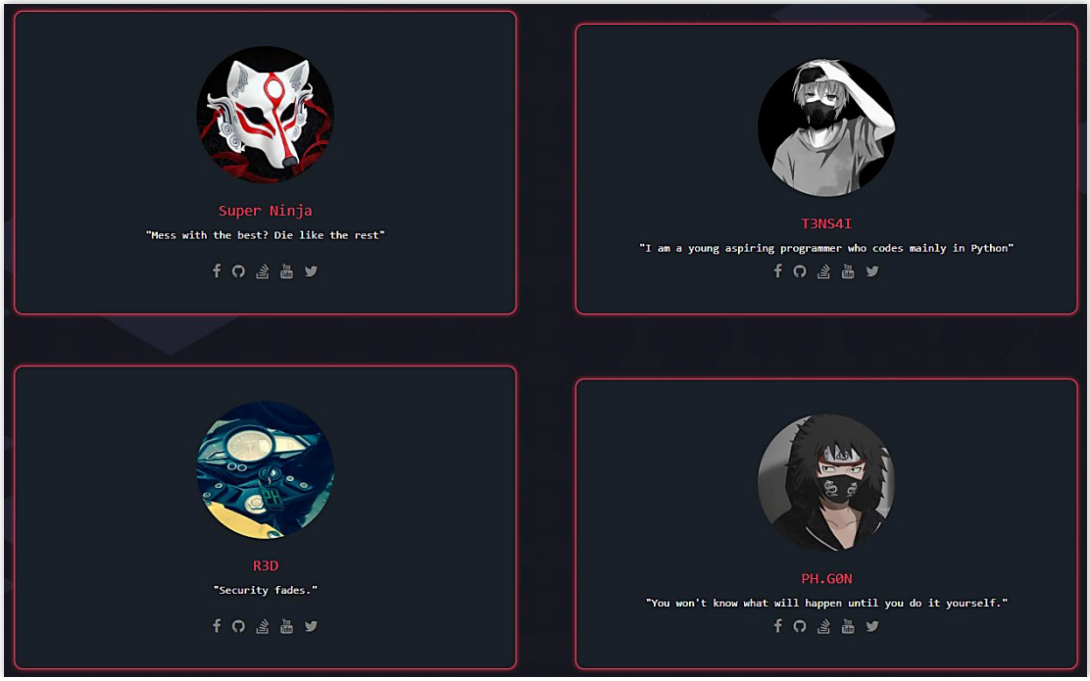
PureHackers team members as seen on one of the defacements



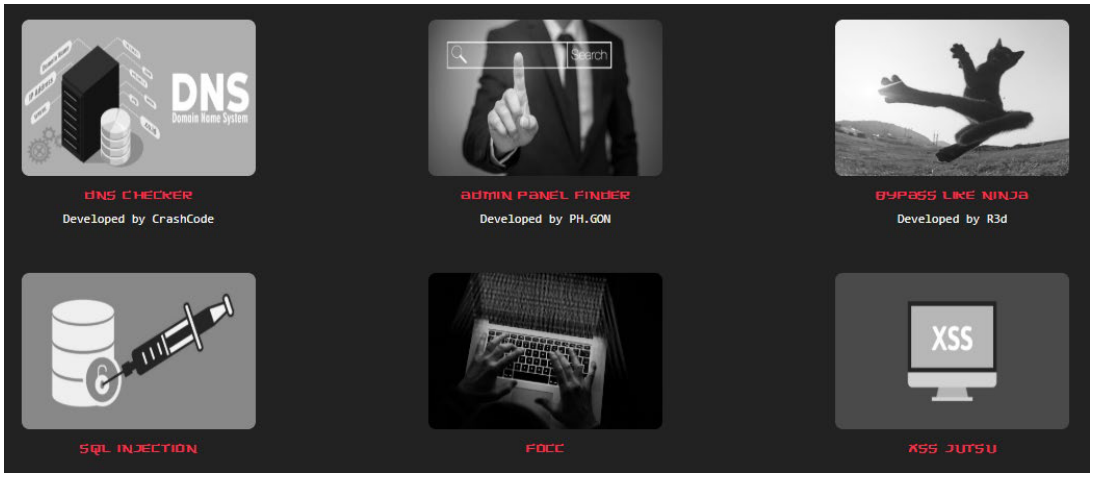
Services and products offered for sale on PureHackers's social media

SHINOBI SECURITY (aka ShinobiSec)

A Filipino hacking group that presents itself as a security firm, which offers security services such as penetration testing and code review and different tools (DNS checker, admin panel finder, SQL Injection tool, and more). The main group members are: Super Ninja, T3NS4I, R3D and PH.G0N.



SHINOBI SECURITY Threat Actors



Offered tools developed and sold by SHINOBY SECURITY

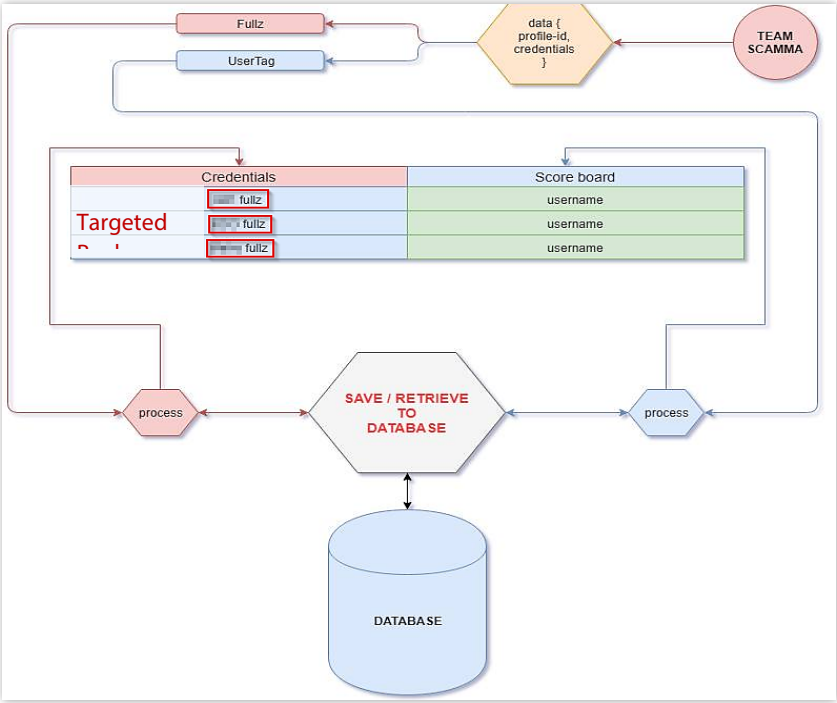
Both threat actor groups present online different hacking skills and appear to be targeting multiple financial institutions in the Philippines, mainly via the phishing attack vector. Many of the groups' members participate in the activities of both groups.

Phishing Collaboration Dashboard | Platform Overview

During the threat actor groups monitoring, CyberInt Threat Intelligence team detected a phishing collaboration dashboard developed by threat actors who are members of the groups 'Shinobi Security' and 'PureHackers'. The platform stores and tracks automatically loaded details of banking customers Fullz and Phishing sites' URL.

As for now, the platform appears to be under a testing phase and is not yet fully operational. As referred by one of the threat actors, the platform is currently at "beta stage".

Below is an architecture diagram shared by a threat actor who developed the platform:



The Systems Schema, posted on Facebook by one of the Threat Actors

CyberInt has been able to get access to the system and obtain all the Fullz and phishing websites URL's it is currently monitoring. During the time of CyberInt's user connection to the platform the following data was retrieved:

- **59 Fullz details**: Full packages of data on 59 compromised victims who are customers of several Philippine banks, including - full name, billing address, credit card number, expiration date, card security code, date of birth, email credentials, and more.
- **67 phishing sites URLs:** Targeting various Philippine banks. It should be noted some of the phishing URL's were inactive, or under construction during the time of the investigation.

CyberInt was able to extract Fullz and phishing sites and report them to our customers.

Executive Summary

Since the beginning of June 2019 CyberInt unveiled activities of two Philippine threat actor groups, '**PureHackers**' and '**Shinobi Security**', targeting multiple banks in the Philippines. One of the groups' members has developed a unique command and control system (C2) with a phishing collaboration dashboard, used for tracking active phishing sites and its compromised victims' data, which is referred to among the threat actors community as "Fullz"[1].

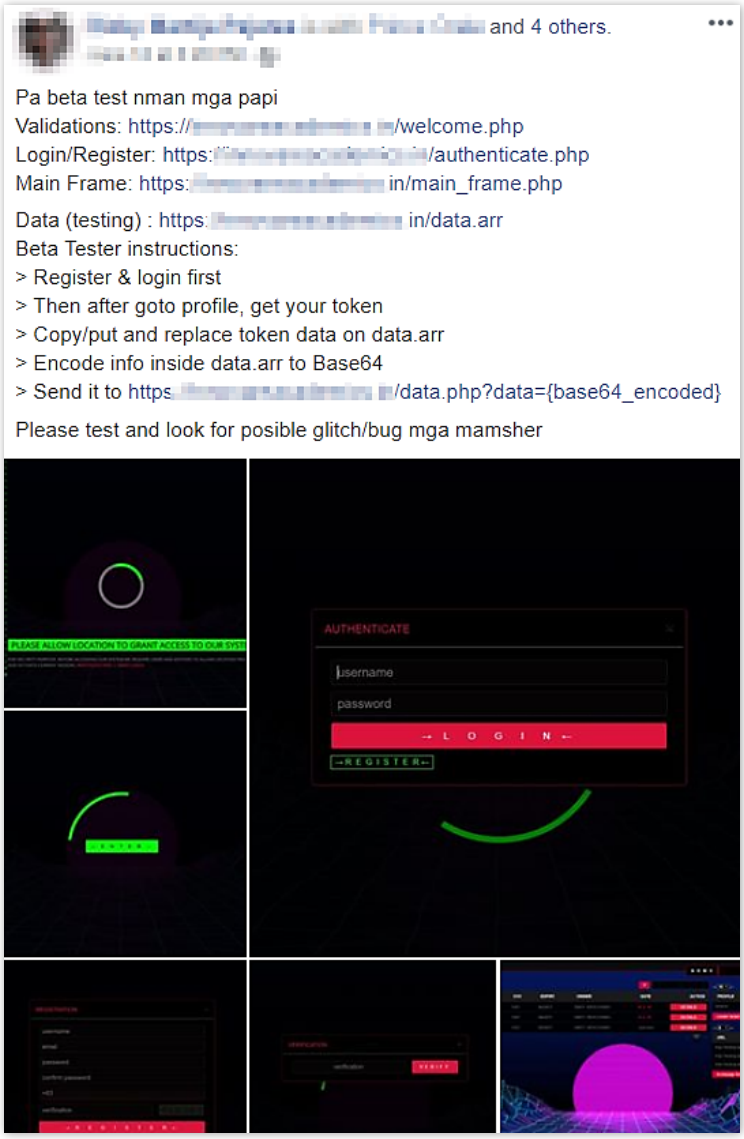
The Philippine Banks are constantly targeted by Filipino threat actors attempting to steal banks' customers' Fullz - and their credit card details in particular. Phishing is one of the main methods used by these threat actors to achieve the relevant data. The phishing collaboration dashboard was detected early on in its beta phase by CyberInt and analyzed in this report. The platform demonstrates the ongoing effort Filipino threat actors are putting to increase the productivity of their nefarious activities via automation and collaboration processes. CyberInt's direct access to the mentioned system has enabled to provide a unique in-depth view of the way threat actors operate and collaborate. In addition, it has enabled CyberInt to thoroughly map a comprehensive phishing attack 'kill chain' and define the different stages it comprises.

CyberInt is continuing the monitoring and will keep sharing all the relevant information of further 'Pure Hackers' and 'Shinobi Security' activities and the details of additional Fullz and active phishing sites loaded into the system with its customers.

[1] 'Fullz' refers to full packages of individuals' identifying information. This may include full name, billing address, credit card number, expiration date and card security code, birth date, credentials and more.

Logging into the System

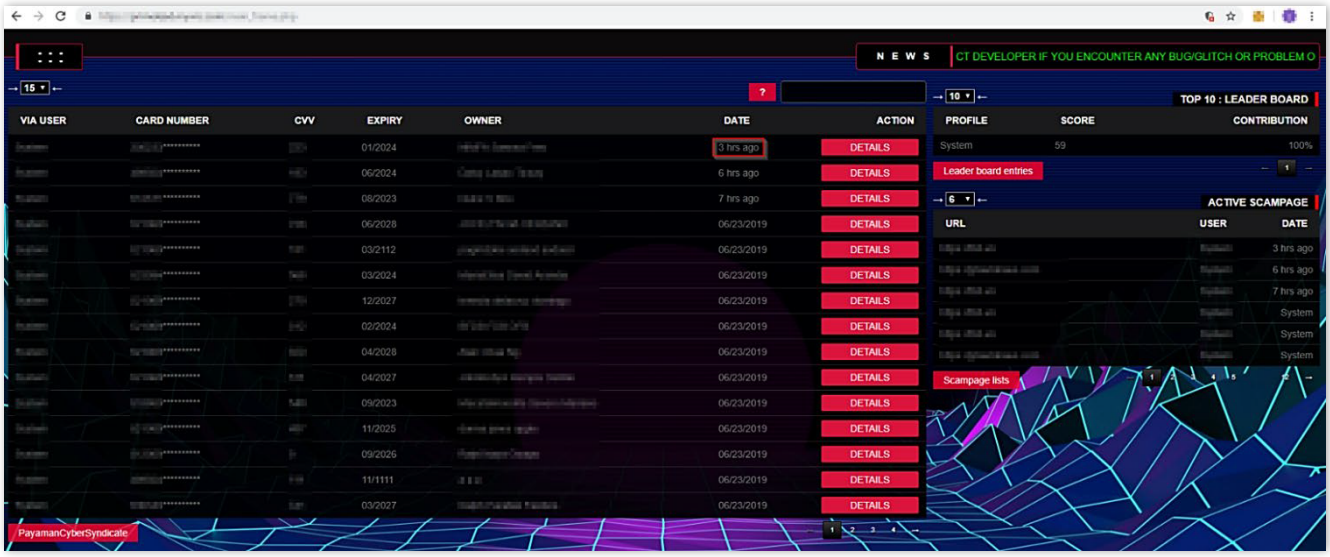
Based on a threat actor's Facebook post with a detailed description on the login process to the phishing collaboration platform. CyberInt's Threat Intelligence team was able to validate this process and obtain access to the system.



Description of the login process into the system

The Platform Features and Capabilities

Upon logging into the system, the user will be presented with a dashboard screen to the control panel, that reflects the status of all the Fullz collected and possibly active phishing websites URL's it is tracking. The control panel enables multiple threat actors to coordinate and collaborate their phishing attacks activities. Typically, phishing kits are deployed on compromised servers and the compromised users data is emailed to a mailbox commonly hosted on a webmail provider. The platform may enhance this capability



The systems' control panel

by allowing multiple members to view and even have rankings to compare against each other. This can motivate the threat actors to lunch even more phishing attacks, to win the 'game of fame'.

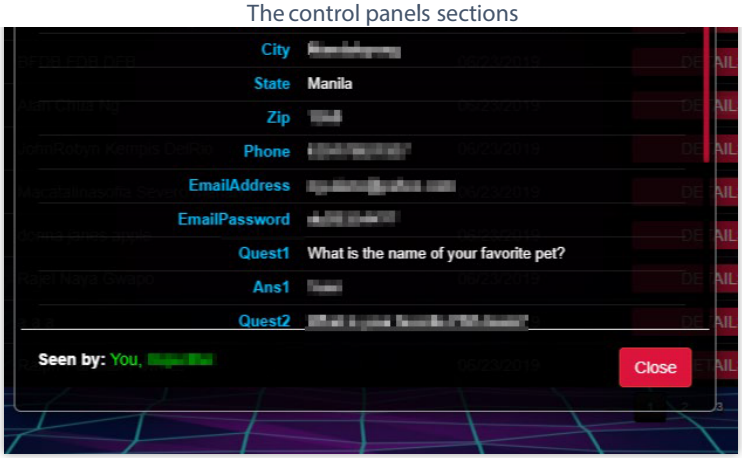
The platform appears to be automatically updated, based on the most recent phishing activity that obtained the Fullz. There is a correlation between the time/date of the stolen Fullz, and the phishing site which was used for obtaining them. Once a victim provides his information to a phishing site (refers on the platform as "scampage"), the details of his Fullz will be sent to the tracking system, alongside the site's information. The Threat Actor who contributed these Fullz to the system will be presented on the 'Leader board', with the percentage of his contribution, out of the overall amount of Fullz in the system.

The dashboard's screen is divided into four sections (as numbered in the image below):

1. **Welcome Users**: The logged in user section, where he can update his account details.
2. **Top 10: Leader Board**: Classification in percentage of the contribution a specific user made, out of the overall Fullz loaded into the system.
3. **Active Scampage**: Tracking of the phishing sites that are currently used as part of the attack.

4. **PayamanCyberSyndicate**: The most recently obtained Fullz details, loaded automatically into the system.

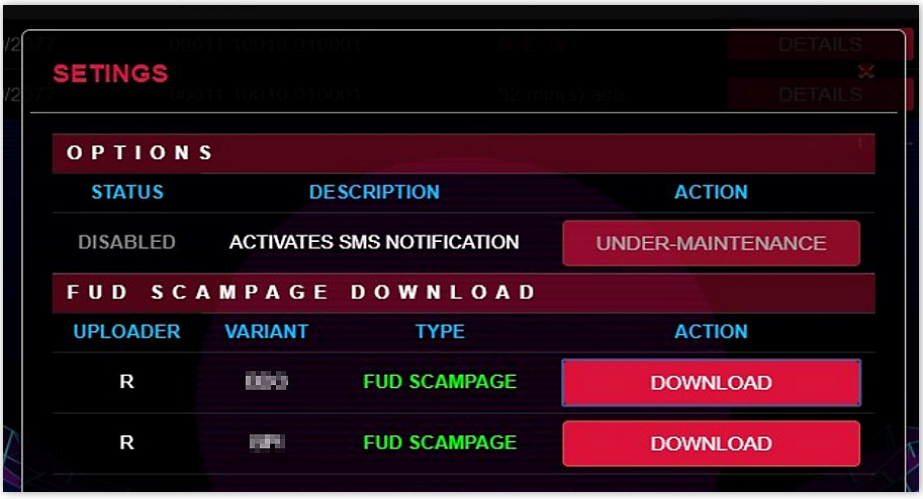
The control panels sections



Stolen Fullz details as presented in the system (obfuscated)

Upon clicking on the "Details" button in the Fullz section (4), the user can view the entire details of a specific set of Fullz.

The user also has an option to download the phishing kits connected to the platform. CyberInt was able to download all phishing kits observed in the platform.

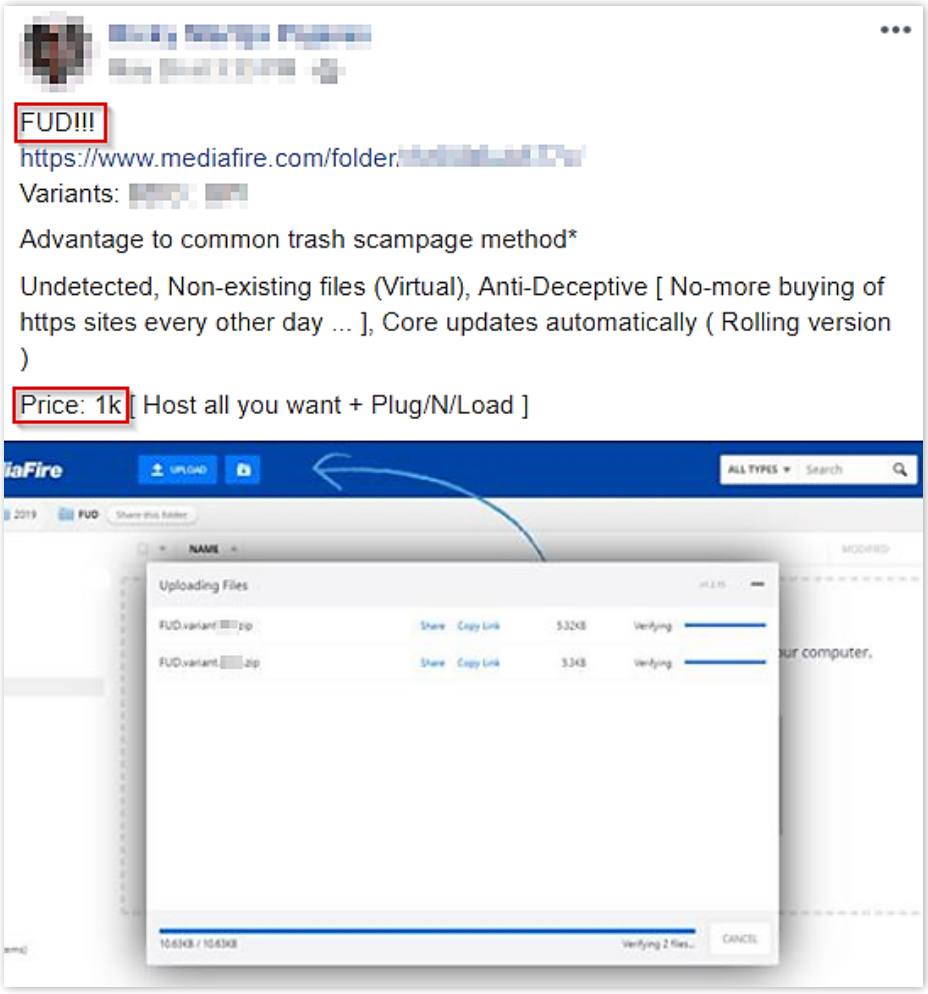


Interface for downloading phishing kits

"Fully UnDetectable" Phishing Attack

Fully Undetectable (also referred as 'FUD') phishing kits are used by many Threat Actors on binary payloads or scripts for obfuscation purposes. This method is preferred and promoted by threat actors who claim that this kind of packaging makes the phishing kit undetectable by Anti-Virus engines. However, the undetectability claim will only be valid for a short period after the FUD-based phishing sites go live, since those may get flagged by Google, web security gateways or some other detection solution.

The threat actor sells on social media the FUD-based phishing kits including sharing proof-of-concept videos demonstrating how a phishing site based on above-mentioned kit successfully avoid of getting



FUD Phishing Kits offered for sale byone of the threat actors

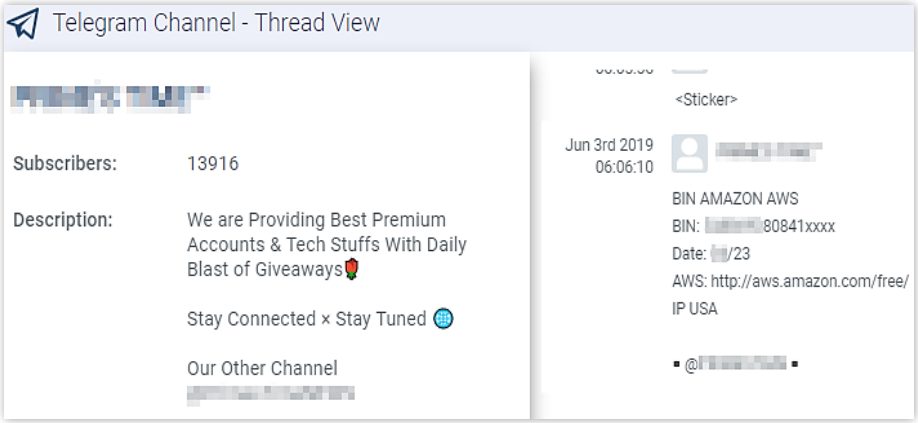
flagged by internet browsers such as Google and FireFox.

The Fullz are Leveraged for Monetization

After the Fullz are obtained from successfully compromised victims of the phishing attacks, a bunch of the Fullz will presumably be leaked by the threat actors to promote themselves and their reputations. Others would be used by the threat actors for personal needs such as purchasing goods or services. However, most of the obtained Fullz will be offered for sale on social media, Deep-web forums and direct messaging applications such as Telegram.

A significant portion of the accounts are offered for sale on Facebook, mainly Facebook pages that are managed by the threat actors. Below are two examples of Fullz being sold online: The first, a Filipino threat actor group offering Philippine banks' fullz for sale. The second, Philippine banks credit cards are offered

Philippine Banks' Fullz offered for Sale on Facebook



Credit cards offered for sale on a Telegram Channel monitored by Argos™

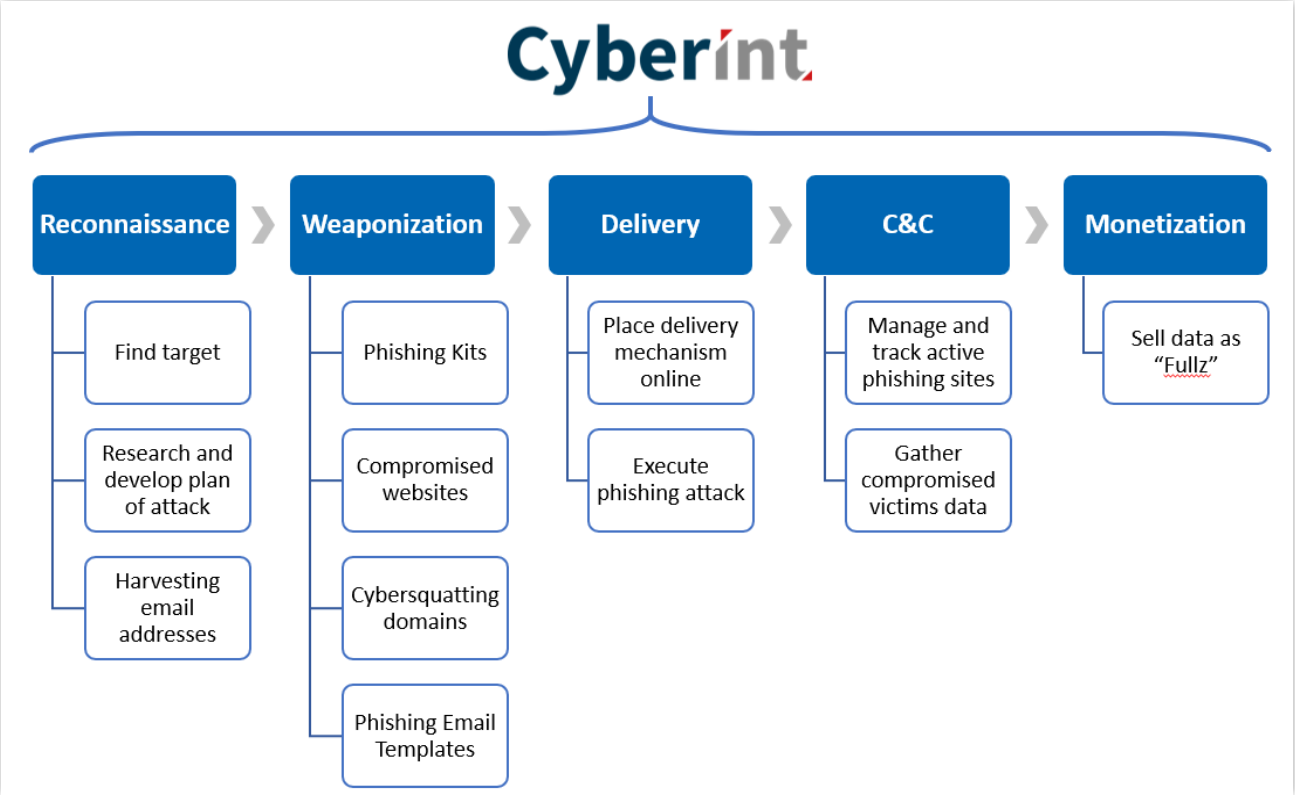
for sale on a threat actors Telegram channel monitored by Argos™.

Selling the Fullz is the last step in the attack kill chain, operated by the threat actors. CyberInt is constantly monitoring and detecting various activities that are occurring in different stages of this lifecycle. Gaining direct access to the phishing collaboration dashboard has enabled to thoroughly map the entire process, and define the different stages it comprises:

1. **Reconnaissance**. The threat actors map the different targets, Philippine banks, and gather the relevant information needed for the execution of a phishing campaign.
2. **Weaponization**. Creation of the needed infrastructure components needed for the campaign, such as phishing kits, phishing email templates and compromising websites or purchase of cybersquatting domains to host and distribute the attack. The platform analyzed in this report has a major contribution to the threat actors weaponization as it allows collaboration and will assist in the attack delivery.
3. **Attack Delivery**. Place delivery mechanism online and lunch the phishing attack – phishing emails will be sent to potential victims.
4. **Command and Control**. compromised victims data will be collected from the phishing sites and send automatically to the phishing collaboration platform or a webmail account. The system tracks the

status of each phishing site, provides threat actors an overview of multiple campaigns that are executed simultaneously and stores the Fullz data.

5. **Monetization**. Fullz are offered for sale online by the threat actors (social media, deep-web forums, direct messaging).



CyberInt Successfullymonitored the wholephishingattack kill chain

Recommendations

The Phishing collaboration platform detected by CyberInt and analyzed in this report enables multiple threat actors coordinate their phishing campaigns and operate in an organized manner.

CyberInt's Threat Intelligence team has been able to get access to the system and obtain all the Fullz data and phishing websites' URL's it was tracking. The direct access to the platform provided CyberInt with valuable insights on the whole phishing attack kill chain and define the different stages it comprises.

As for now, the system is automatically updated constantly, with additional Fullz data collected from multiple active various phishing sites targeting mainly the banking sector in the Philippines. CyberInt will continue to monitor activities of 'PureHackers', 'Shinobi Security' and other Philippine threat actor groups on behalf of its customers.