ENEA
AdaptiveMobile Security

CASE STUDY

Combatting Cyber Criminals in Asia

Globe, a major provider of telecommunication services and the largest mobile operator in the Philippines, was targeted by cyber criminals executing an intensive financial SMS phishing campaign. SMS phishing (also known as Smishing) messages were arriving from both international and domestic national operators, with the scammers frequently adapting the messages to avoid detection. Globe urgently needed to protect its near 90 million mobile subscribers. Fortunately, Globe already had in place Enea AdaptiveMobile's Network Protection Platform for Messaging and Signalling Protection, and combined with AdaptiveMobile's industry leading Threat Intelligence Services, they were able to provide highly effective protection for their subscribers and brand.

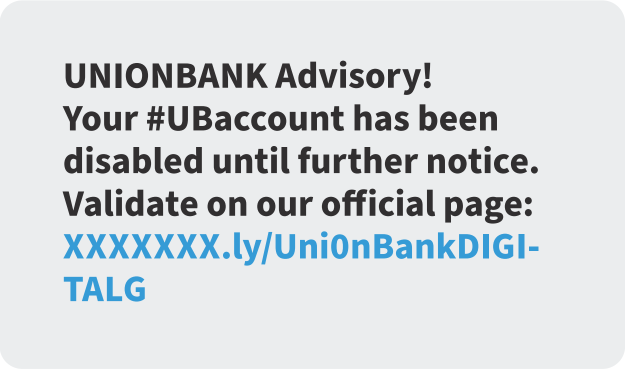
Overview

Situation:	Globe, the largest mobile operator in the Philippines, was targeted by cyber criminals executing an intensive financial SMS phishing campaign.
Solution:	Enea AdaptiveMobile Threat Intelligence Unit (TIU), using the AdaptiveMobile Network Protection Platform (NPP) for Messaging and Signalling Security, applied a blend of security methods.
Success:	With the help of Enea AdaptiveMobile's TIU and NPP, Globe was able to address and control these difficult-to-identify threats, successfully blocking these phishing attacks over the last year.
Impact:	The level of protection afforded by AdaptiveMobile's TIU and NPP to Globe's customers has been critical in keeping them safe over the past year and protecting Globe's leading brand as a secure mobile communications provider.

The success and impact were reinforced by Globe's Chief Information Security Adviser Anton Bonifacio, who described the blocking of malicious messages as a "major step that reflects our commitment to the country's economic recovery by ensuring that the accelerated digital adoption does not expose customers to worsening cyber threats."

The Situation

SMS phishing attacks were coming from both international sources as well as other national operators. Criminals were impersonating real sources, using plausible sender as well as regular local phone numbers, to send SMS phishing messages. Many of these phishing messages resembled real bank messages and most used malicious URLs to entice victims to visit fake bank webpages.



UNIONBANK Advisory!
Your #UBaccount has been disabled until further notice.
Validate on our official page:
XXXXXXX.ly/Uni0nBankDIGI-TALG

Fig 1: AdaptiveMobile’s Mobile Network Protection Platform

AdaptiveMobile’s Threat Intelligence Unit’s analysis of these threats uncovered that they were highly varied and frequently changing, deploying techniques such as Message Metamorphosis and URL Cycling to evade filters.

Spam polymorphism (i.e., changing the attack to avoid detection and blocking) was used extensively for these attacks. We saw techniques ranging from subtly changing key words, adding unnecessary spaces, including special characters, using tokenization, duplicating letters to frustrate word-based fingerprints, to more visible ones such as replacing numbers and punctuation with text. These were all captured and handled by the Enea AdaptiveMobile fingerprinting techniques.

We also observed URL Cycling Detection, where criminal senders dynamically change the URL domain through a large set of temporary sites – which is also used by criminals to avoid detection or blocking of their messages by slow response firewall updates.

In addition to frequently changing the SMS text body and URLs, an additional challenge to dealing with these threats was that the hosts of the attack websites used in that campaign had little in common, i.e., there was no correlation between the host IPs of the URLs being used.

Solution

Understandably, defensive techniques using a limited number of methods would be ineffective given the frequency and extent of changes by the attackers. i.e., no rules could work effectively against this campaign based solely on sender, URL, hosted IP or text body.

Therefore TIU, using the sophisticated and dynamic rules capability of the AdaptiveMobile NPP, developed and then applied a blend of security methods to address and control these attacks.

TIU followed text pattern-based rules to manage the phishing attack campaign, along with other proprietary techniques, to capture the identified phishing messages.

Success

Enea AdaptiveMobile Security TIU along with the NPP Messaging Security platform has now successfully been blocking these phishing attacks over the last year.

From Figure 2 it can be seen that for the first four months, (January to April) the criminals were thwarted, moving away from Globe and targeting other networks.

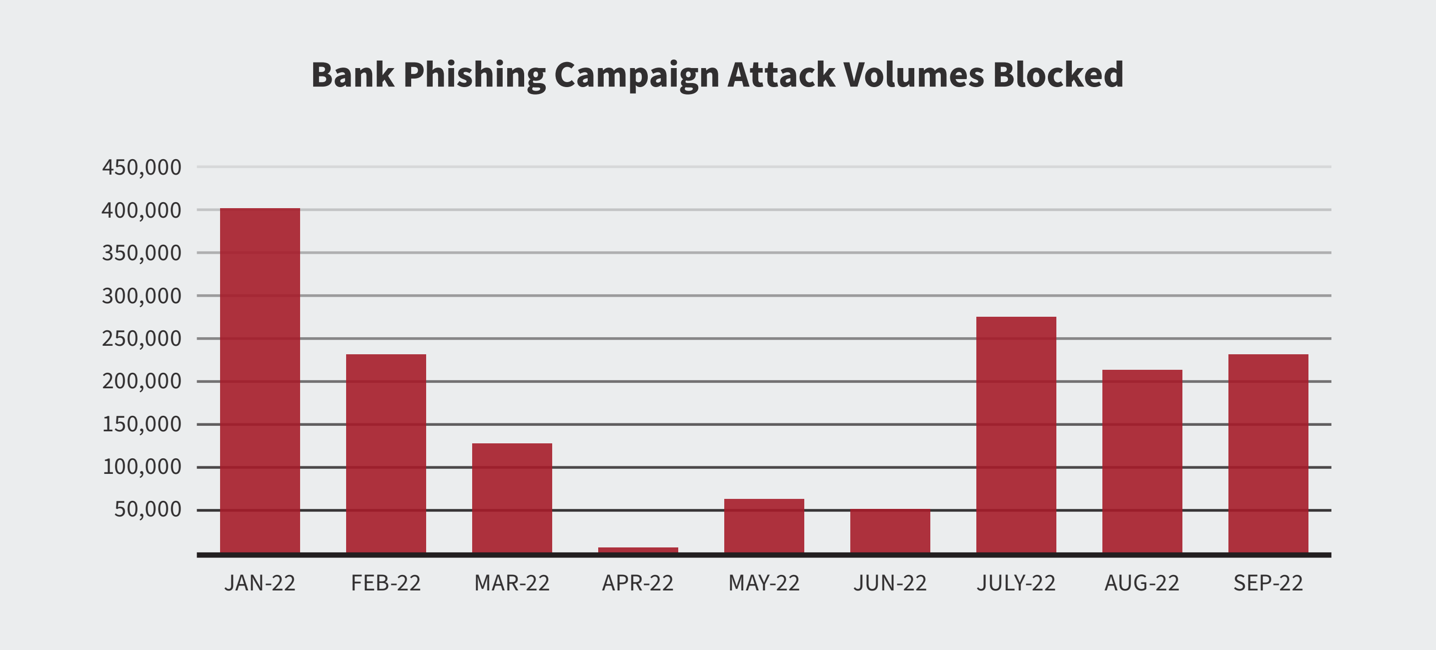


Figure 2: SMS Phishing messages blocked by AdaptiveMobile using text pattern-based rules

However, blocked threat messages increased considerably over the last few months, July to September. This was a result of more frequent updates being taken from Enea AdaptiveMobile's managed Threat Intelligence service, contributing significantly to the effectiveness of the solution and allowing us to keep up our detection and blocking rates even in the face of heightened volume and tactics of attackers.

Impact

Including these phishing attacks with all the other messages AdaptiveMobile NPP are blocking on Globe's network, i.e., other scam campaign messages and grey route messages, it can be seen from the figure below that there has been a significant impact over the past year and that the level of protection afforded by the NPP to Globe's customers has been critical in keeping them safe and protecting Globe's brand and reputation as a secure mobile communications provider.

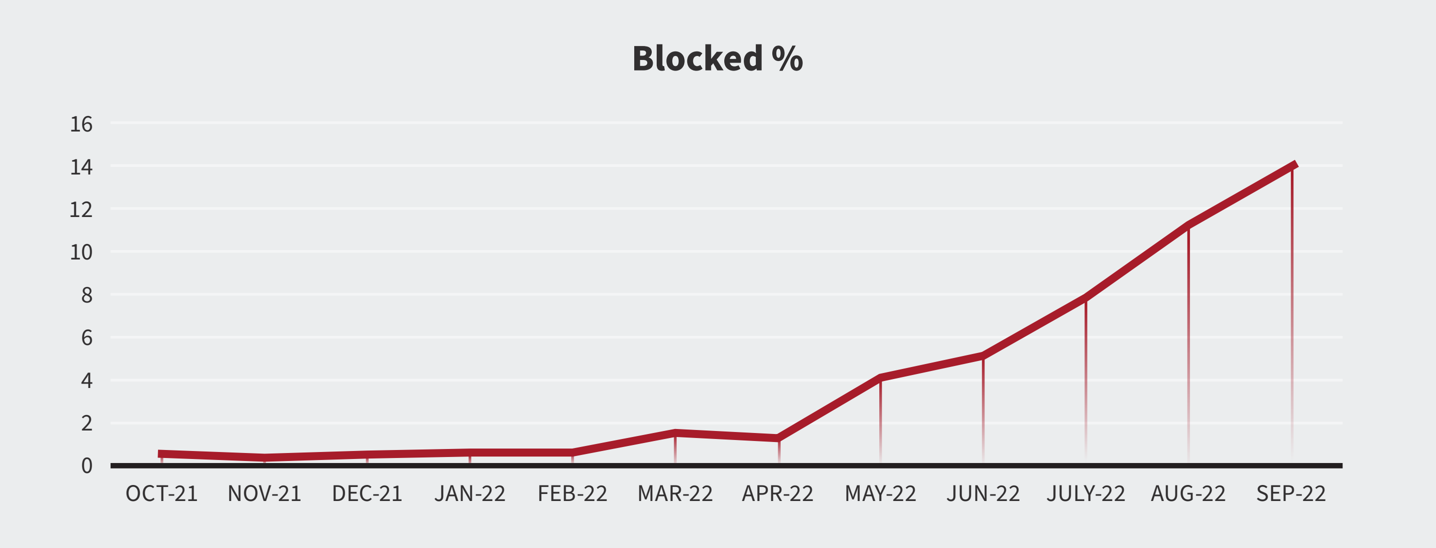


Figure 3: Overall blocked percentage of SMS traffic as a percentage of total SMS traffic on the Globe network.

Anton Bonifacio, Chief Information Security Officer at Globe, commented:

"The protection of our subscribers is at the heart of Globe's cybersecurity strategy. Enea AdaptiveMobile Security understands that, and their strong cybersecurity background and intelligence allow them to go above and beyond in order to protect our network against both signalling and messaging attacks through their Network Protection Platform,"

His team is responsible for the security operations of Globe and its subsidiary companies, looking after security, data privacy, governance and compliance, signalling, as well as operational technology.

Next Steps

Other domestic networks are a major source of spam and phishing messages in the Philippines. Globe's next step was to apply strict rules to messages on this domestic traffic, to target any person-to-person (P2P) messages containing URLs, without impacting commercial application to person messages (A2P).

About Enea AdaptiveMobile Security

Enea AdaptiveMobile Security is a world leader in mobile network security, everyday protecting over 80 Mobile Operators and billions of mobile subscribers and devices globally from fraudsters, criminals and nation states. We have the strongest 5G core network security team, who are designing, planning and building the very best in 5G core network security solutions focussing on threat-intelligence, security heritage and protocol correlation.

Enea AdaptiveMobile Security brings a unique security perspective on real-time mobile network traffic. The global insight provided by our 5G, Signalling and Messaging thought leaders, security specialist teams and Threat Intelligence Unit, combined with our signalling and network protection software that sits at the heart of the network, ensures Enea AdaptiveMobile Security remains at the forefront of the latest advancements in mobile networks and their security, and continues to be the trusted partner of many of the world's largest Mobile Operators.

For more information on how Enea AdaptiveMobile Security can help you protect your communications infrastructure, subscribers and revenues, please contact **sales@adaptivemobile.com**.

Legal Notices

The information contained herein is believed to be accurate and reliable. Adaptive Mobile Security Ltd. accepts no responsibility for its use by any means or in any way whatsoever. Adaptive Mobile Security Ltd. shall not be liable for any expenses, costs or damage that may result from the use of the information contained within this document. The information contained herein is subject to change without notice.

HEAD OFFICE

Ferry House, 48-52 Lower Mount St, Dublin 2.
Contact: sales@adaptivemobile.com
www.adaptivemobile.com

REGIONAL SALES CONTACT NUMBERS

US, Canada, Latin America Sales: +1 972 377 0014
UK Sales: +44 207 049 0421
Middle East Sales: +97144 33 75 83
Africa Sales: +27 87 5502315
Asia Sales: +65 31 58 12 83
European Sales: +353 1 524 9000

REGIONAL OPERATIONAL SUPPORT CONTACT NUMBERS

UK: +44 208 584 0041
Ireland: +353 1 514 3945
India: 000-800-100-7129
US, Canada: +1 877 267 0444
LATAM: +525584211344