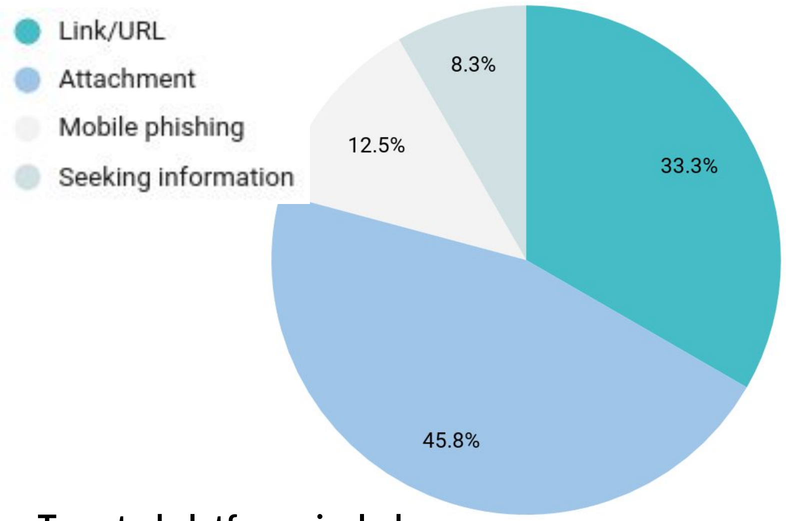
Threat Analysis Summary

Overview

The information presented is the result of phishing and malware that was directly reported to the project team.

- Phishing via link: Phishing email with malicious link in the body to steal your username and password, or download malware.
- Phishing via attachment: Phishing email with malicious attachment which usually downloads malware.
- Phishing via mobile service: Phishing through mobile service like a link or attachment sent in an app
- Phishing for information: Phishing email solely soliciting information

Results



Targeted platforms include:

Gmail
Naver
Daum

KakaoTalk
Threema
SMS

Our Impact?

Threat analysis allows us to expand protections against malicious activity across communities' and sectors in two ways:

1) Reporting to platform providers who then block and hunt for malicious activity on their systems (e.g. Google, Naver, etc.)

2) Sharing tactics increases collective awareness, which makes us able to react more quickly to prevent or deal with infections.

- Identified **486 malicious domains**
- Identified **85 IP addresses**
- Identified **114 malicious links/URLs** delivering malware and info to adversary

The Mitigations?

Use an Antivirus: Catch malware and viruses before they compromise you.

Update your Software: Software developers work hard to fix vulnerabilities, leverage this by updating regularly!

Authenticate your Contacts: Do you really know who you're talking to? Verify and authenticate new contacts.

Threat Sharing: Make everyone stronger. Share and learn about new threats in your community.

User Training: Adversaries change and we have to keep up. Continue to learn the adversary's techniques and how to protect yourself.

Last Updated: September 2020