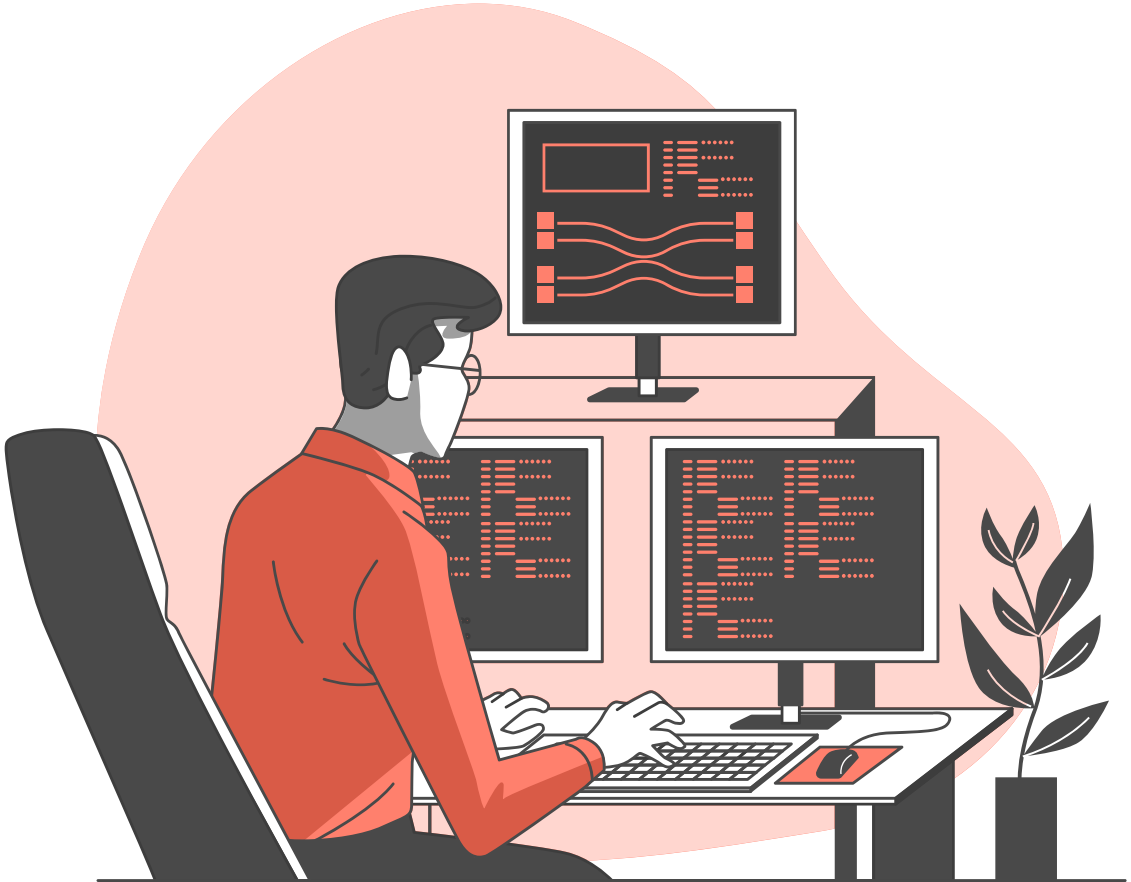
viettel
security



Vietnam Cyber Threat Trends

Vietnam Security Summit 2021

Agenda

01

Numbers

Statistics of Vietnam's cyber threats
by **Viettel Threat Intelligence**

02

Trends

Cyber threat emerging trends
in Vietnam 2021

03

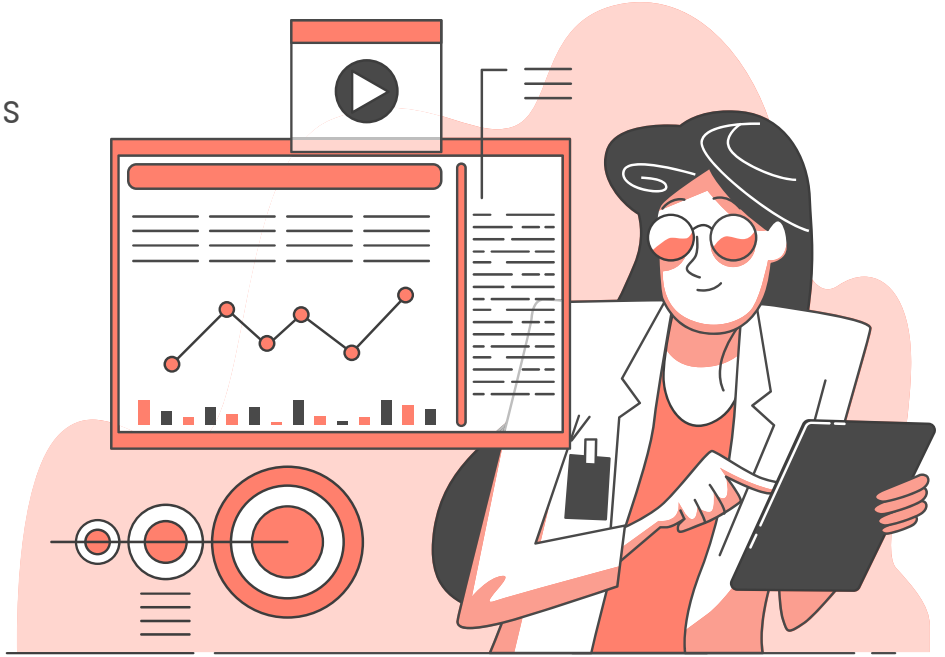
Case Study

Some real-world cases

04

Conclusion

Summary, suggestion



viettel
security

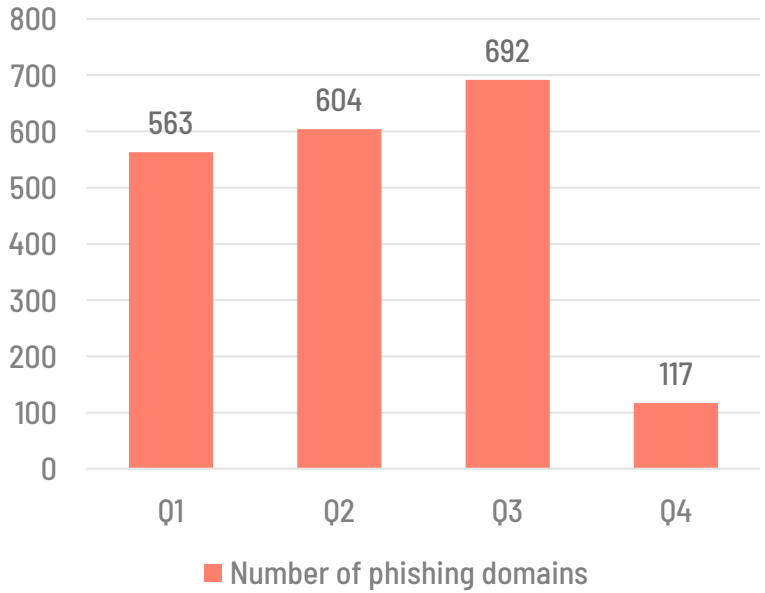
viettel security

01 Numbers

Vietnam Cyber Threat Trends 2021

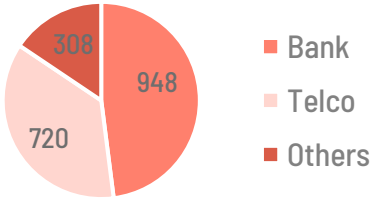
Phishing

Phishing domains / Quarter



1976

Number of phishing domains

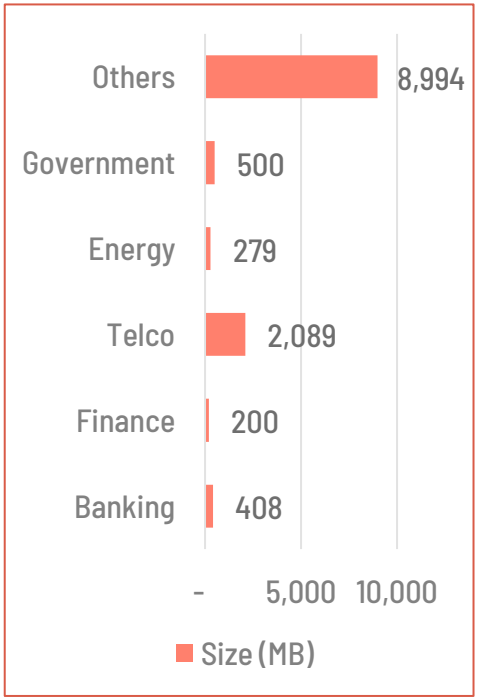


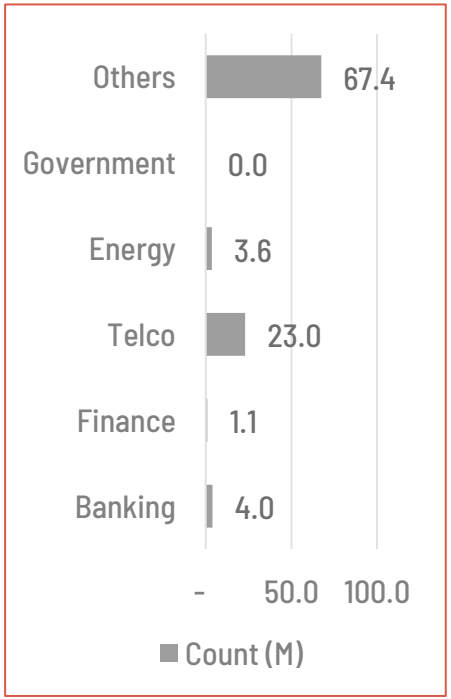
Phishing by industry

Source: Viettel Threat Intelligence (cyberintel.io)

Data Leak

Data Leak by Industry





99M

Total number of leaked data entry

107k

Total number of leaked credentials

Source: Viettel Threat Intelligence (cyberintel.io)

APT Attacks

27 days

Mean time to detect

5 days

Mean time to response

10 days

Mean time to comeback

viettel security

Source: Viettel Threat Intelligence (cyberintel.io)

viettel security

APT Groups

APT32 (Ocean Lotus)

- Origin: Vietnam (suspicious)
- C&C (active): 18
- Targets: companies, organizations in Vietnam

Mustang Panda

- Origin: China
- C&C (active): 33
- Targets: government, political, non-profit organizations

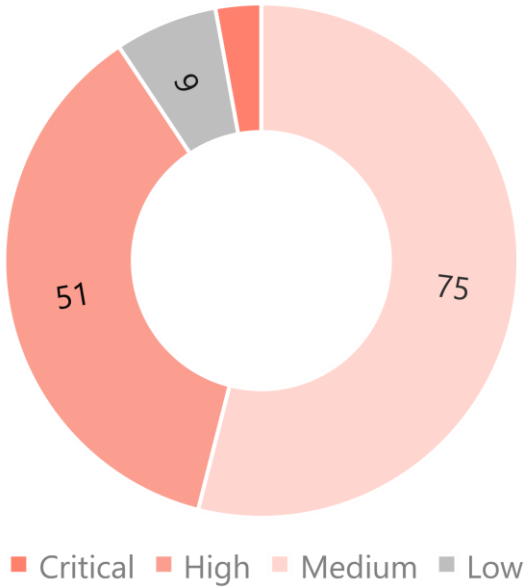
Goblin Panda

- Origin: China
- C&C (active): 12
- Targets: government, military, health, diplomacy, politics

Source: Viettel Threat Intelligence (cyberintel.io)

Vulnerabilities

Number of vulnerabitities



Top impact vulnerabilities

- CVE-2021-22005 (VMware vCenter)
- CVE-2021-1675 (MS Windows Print Spooler)
- CVE-2021-34473 (ProxyShell - MS Exchange)
- CVE-2021-26084 (Atlassian Confluence)
- CVE-2021-40444 (MS Office)

Source: Viettel Threat Intelligence (cyberintel.io)

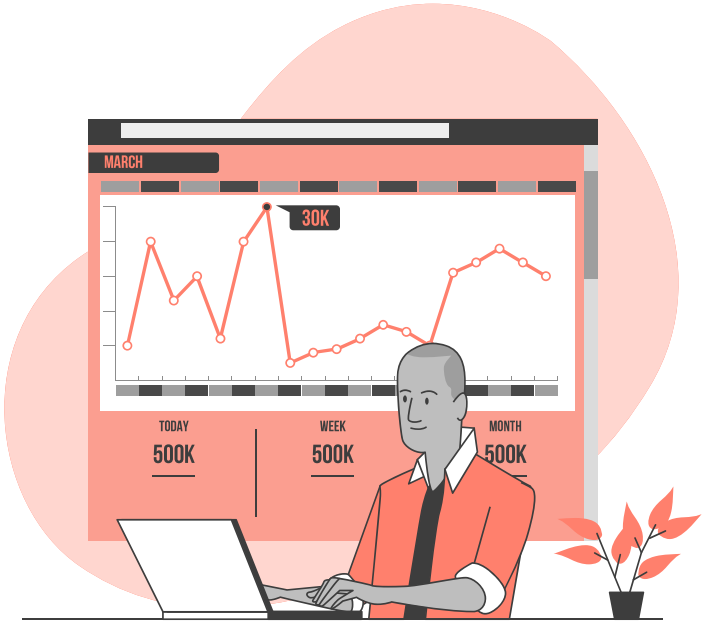
viettel security

viettel security

02
Trends

Vietnam Cyber Threat Trends 2021

Phishing is rising!



A large number of phishing campaigns have been recorded in Vietnam 2021:

- Multiple phishing domains
- Advanced attack techniques (email, sms, call...)
- Big campaigns targeted Vietnam banks

viettel security

Data Leak: Big & Critical!

VCS TI recorded a large amount of leaked data of Vietnam companies on Dark/Deep Web:

- Customer data
- Company's credentials
- Confidential Documents

viettel security

Real-world Exploitation

Many discovered vulnerabilities have been used in cyber attacks against Viet Nam organizations:

- Popular applications (MS Exchange, VMWare vSphere, Confluence, MS Office...)
- From advisories to working exploits
- Mass scan & attacks
- Both botnet & APT

viettel security

APT is still a big problem

Vietnam is still one of the most active regions of targeted attacks

- Multiple industries (government, energy, finance, health, education...)
- Very active cyber espionage
- Dedicated tools, infrastructure
- Multiple purposes (politics, espionage, finance)

viettel security

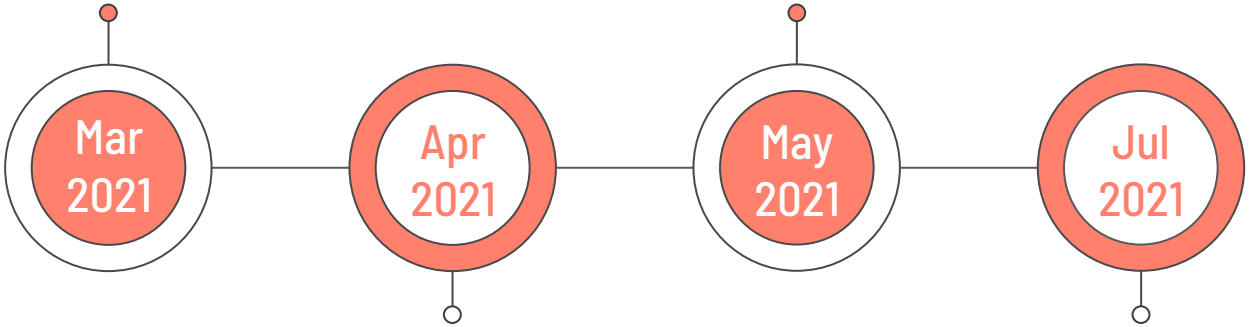
viettel security

03

Case Study

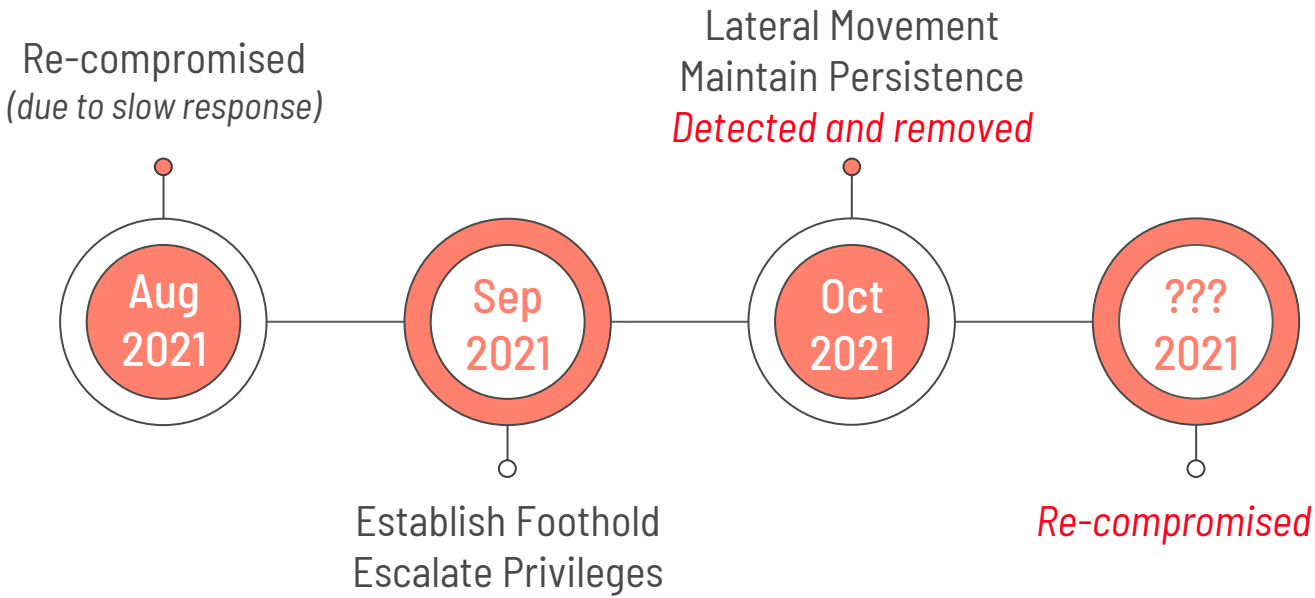
Vietnam Cyber Threat Trends 2021

Goblin Panda: New Campaign!



Source: Viettel Threat Intelligence (cyberintel.io)

Goblin Panda: New Campaign!



Source: Viettel Threat Intelligence (cyberintel.io)

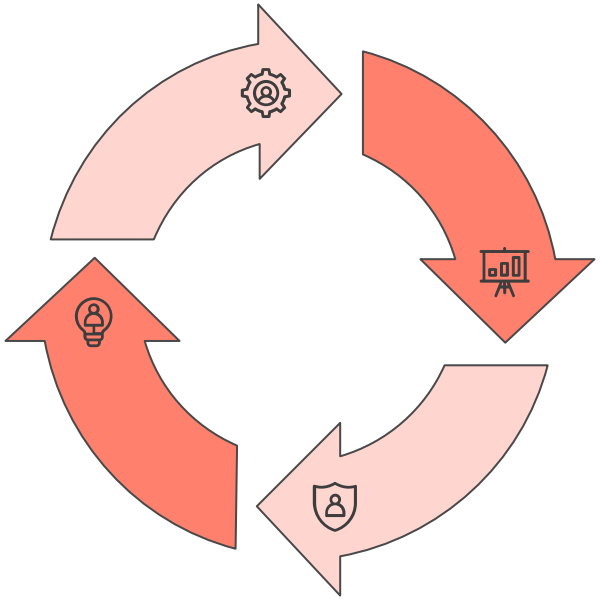
Goblin Panda: New Campaign!

Initial Attack Vector

- MS Exchange Vulnerabilities (ProxyLogon)

Defense Evasion

- Rootkit
- Disable Antivirus



Maintain Persistence

- Compromise Authen Systems
- Compromise Central Management Systems

Credentials Collection

- Exchange Special Module
- Customize Mimikatz

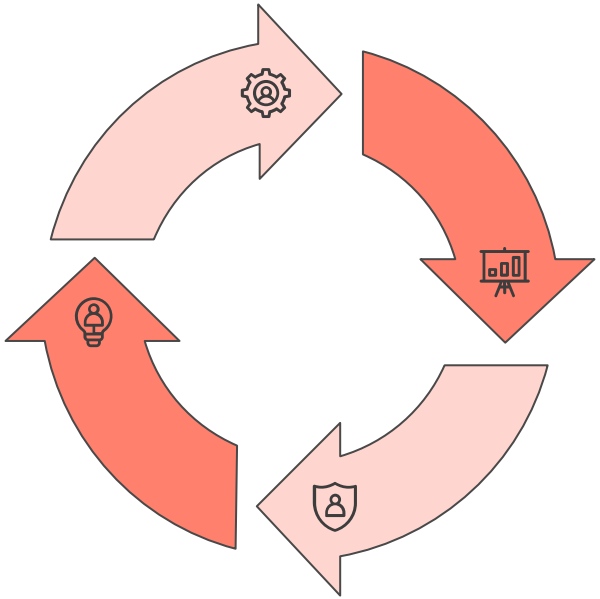
Source: Viettel Threat Intelligence (cyberintel.io)

viettel security

Goblin Panda: New Campaign!

Malware & Tools

- Special Loader
- Newly built
  - May/Jun 2021
  - Aug 2021
- Same code-base from 2015



Infrastructure

- No domain used
- VPS/compromised hosts
  - Viet Nam
  - China
  - Hong Kong
  - South Korea
  - Malaysia

Source: Viettel Threat Intelligence (cyberintel.io)

viettel security

Sophisticated Phishing Campaigns

Campaign 1

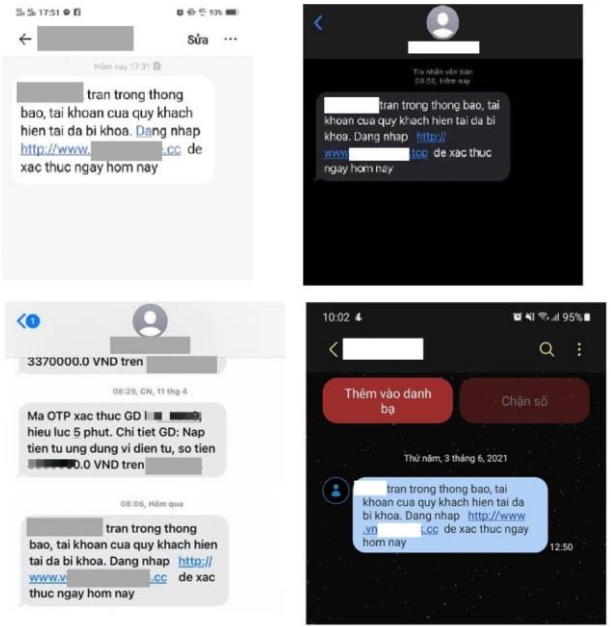
- From Dec 2020
- Target: Vietnamese Bank Users

Campaign 2

- From Mar 2021
- Target: Vietnamese Bank Users

Source: Viettel Threat Intelligence (cyberintel.io)

Sophisticated Phishing Campaigns



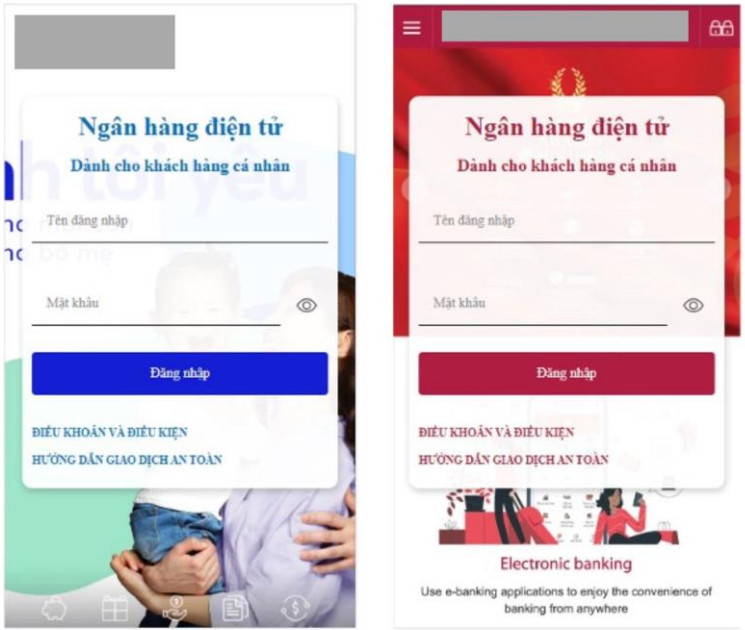
Step 1: Send SMS to victim

- Fake sender: victim's bank
- Content: account lock announcement, lure victim to malicious URL
- How?
  - Fake BTS
  - SMS Fake Sender ID
  - Malicious Application

viettel security

Source: Viettel Threat Intelligence (cyberintel.io)

Sophisticated Phishing Campaigns



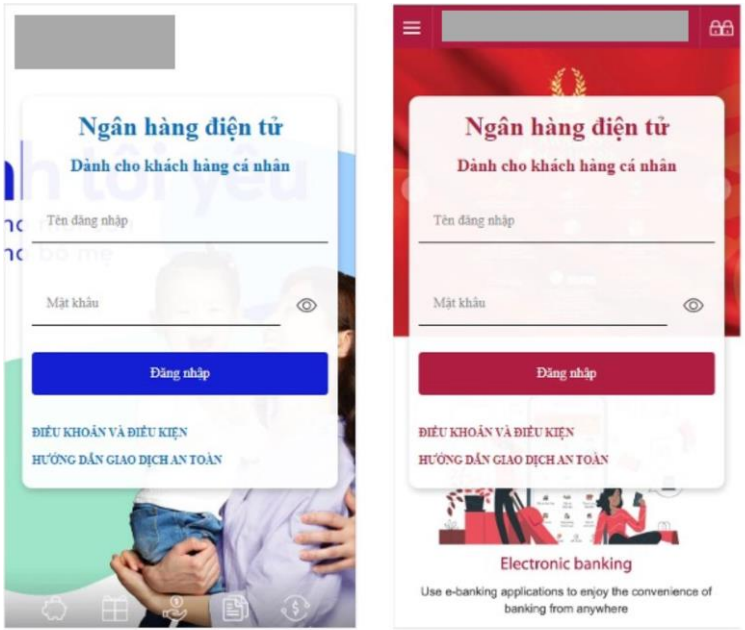
Step 2: Information Steal

- Victim access malicious URL, input personal finance information
- Malicious websites have similar interface to original websites
- Victim information is sent to attacker

viettel security

Source: Viettel Threat Intelligence (cyberintel.io)

Sophisticated Phishing Campaigns



Step 3: OTP Request

- Attacker use victim credential to login to bank systems, request to get OTP

viettel security

Source: Viettel Threat Intelligence (cyberintel.io)

Sophisticated Phishing Campaigns

Step 4: OTP Steal

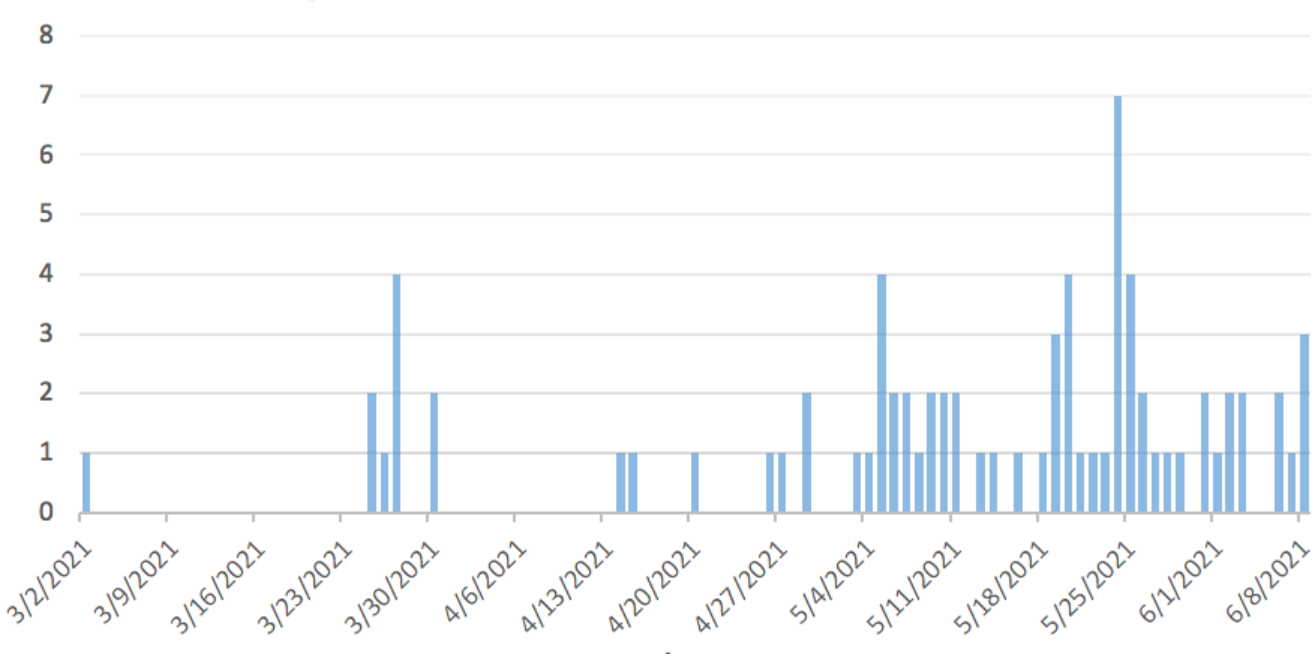
- OTP is sent to victim's phone
- Phishing website redirect to OTP submit form
- Victim submit real OTP
- Attacker now able to do transactions

viettel security

Source: Viettel Threat Intelligence (cyberintel.io)

Sophisticated Phishing Campaigns

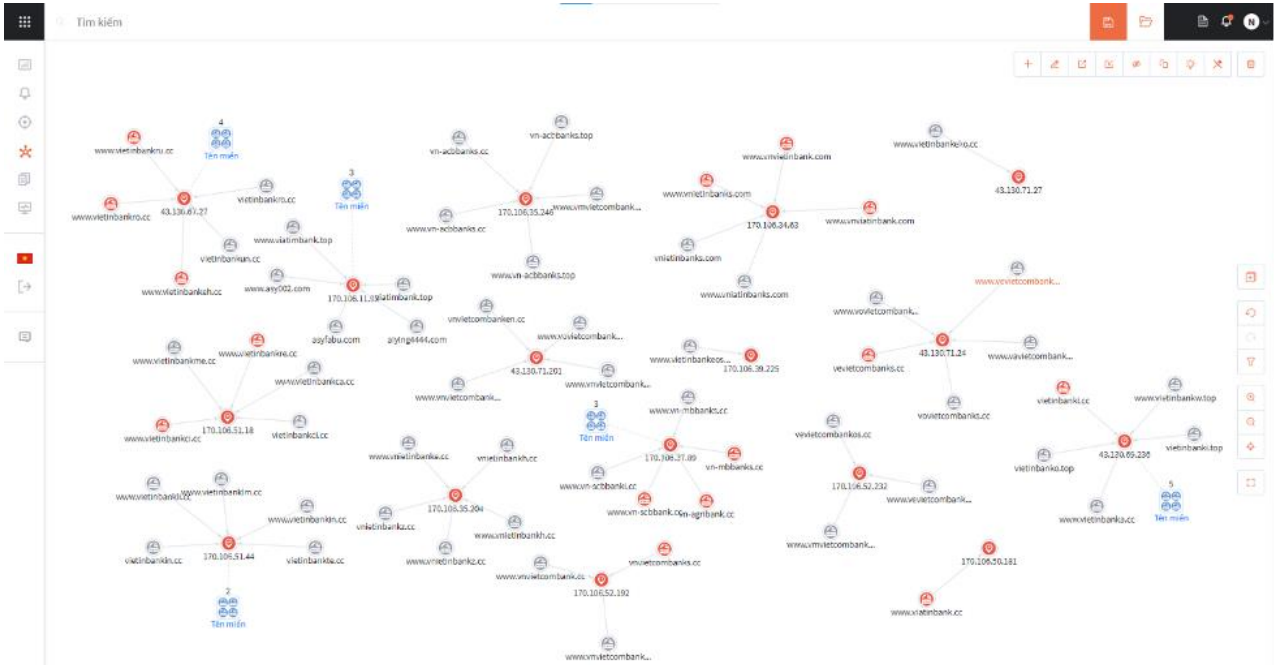
Number of phishing domains by time



Source: *Viettel Threat Intelligence (cyberintel.io)*

Sophisticated Phishing Campaigns

Phishing Infrastructure

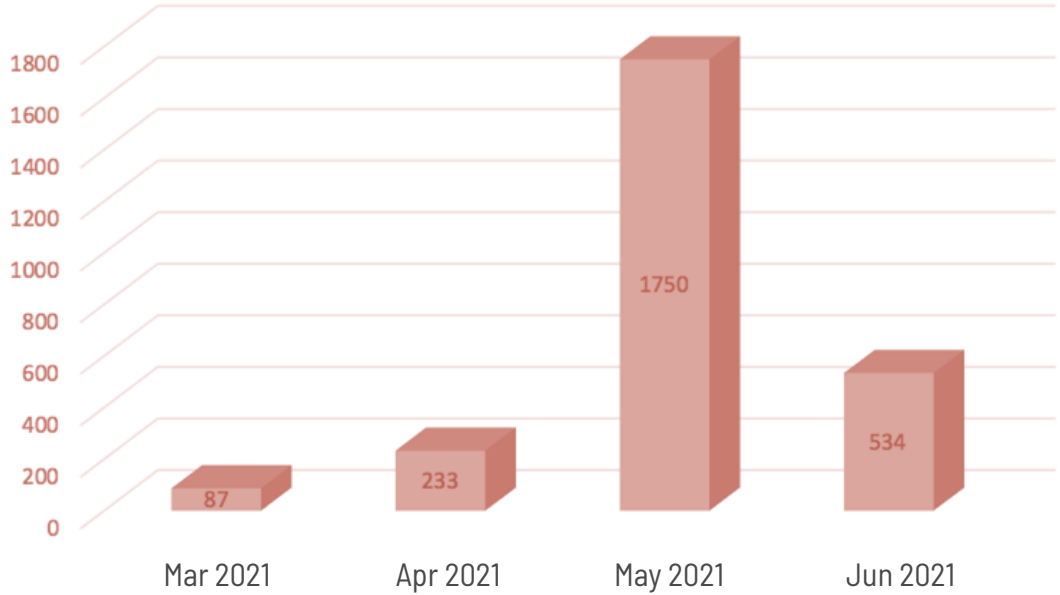


** 18 IPs, 80 domains (maybe more)*

Source: *Viettel Threat Intelligence (cyberintel.io)*

Sophisticated Phishing Campaigns

Connections to phishing infrastructure



Source: Viettel Threat Intelligence (cyberintel.io)

viettel security

04 Conclusion

Vietnam Cyber Threat Trends 2021

Conclusion

The significant increase in number and severity of cyber security threats make organizations to quickly adapt, take effective countermeasures, and pay a much greater attention to information security

viettel security

Conclusion

End users are facing many increasingly sophisticated scams, well organized by cybercriminals, which forces enterprises to have solutions to protect their customers to increase their prestige, credibility and competitiveness of its brand, especially organizations in the banking and finance sector

viettel security

Thanks!

Do you have any questions?

quangtm4@viettel.com.vn
vcs.sales@viettel.com.vn
(+84) 971 360 360
viettelcybersecurity.com

viettel security