Phuket
Thailand
August 24-27, 2022

What if.. We Can See Another Dimension of Cyber Attacks?

Seongsu Park, Lead security researcher

kaspersky

Seongsu Park

- Kaspersky, Global Research and Analysis Team
- Lead security researcher
- Tracking targeted attacks focused on APAC
- Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

Who is Kimsuky?

Adversary

Kimsuky(a.k.a Thallium)

Published by Kaspersky in 2013

Behind the KHNP attack in 2014

Victim

- Impacted countries: South Korea, Japan, USA China ..
- Target industries: Government, diplomat, defense, thank-tank, NGO, journalist, defector academic, cryptocurrency, E-commerce

Capability

Phishing

Timely social engineering

Multi-stage infection

Several malware cluster

Infrastructure

Compromised web server

Free web hosting

Commercial hosting service

Private email service

One dimension of Kimsuky group

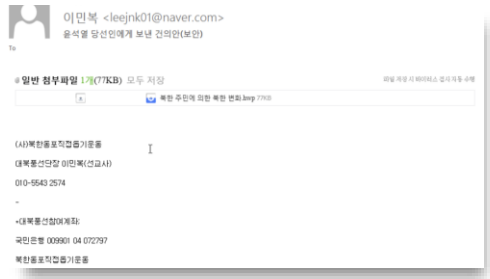
Malware dimension

kaspersky

Initial infection

Spearphishing

Warning of personal email account was compromised

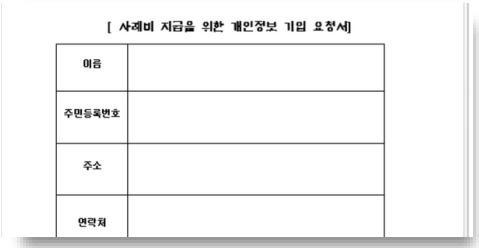


Geopolitical issues/events

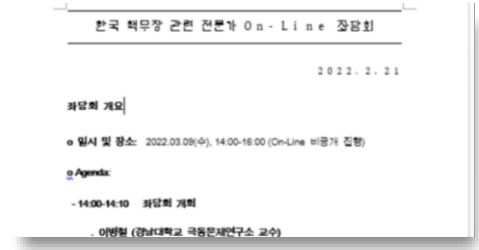
Interested materials to the victims

Malicious document

High-profiled person or job recommendation

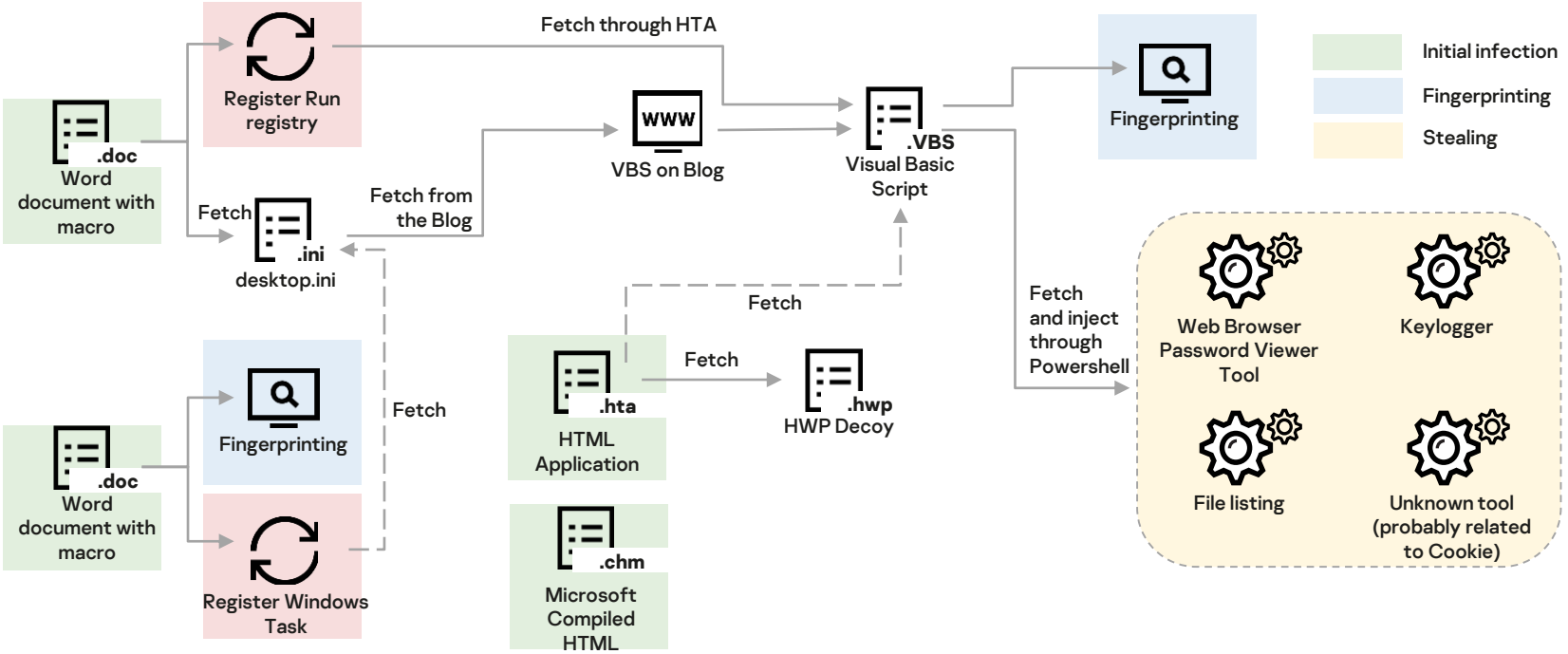


Requset form for honorarium

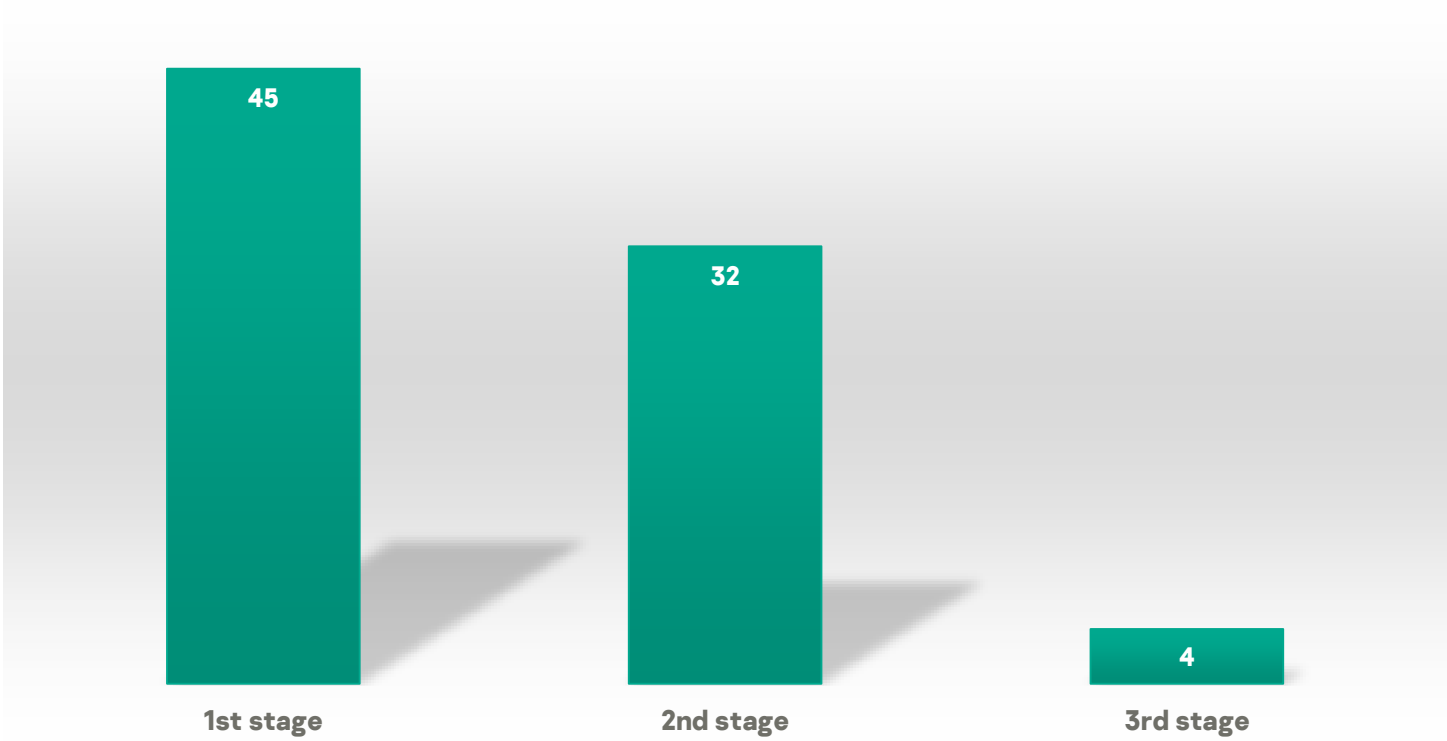


Geopolitical issues/events

Latest attack case: infection scheme

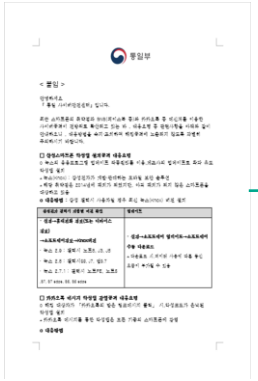


Endeavors of malware author

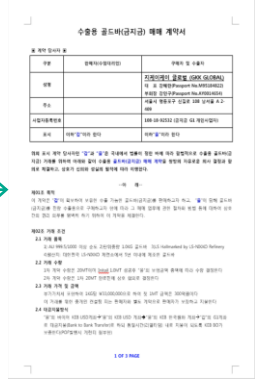


Update cycle of each stage malware

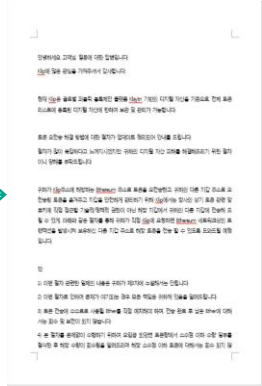
1st stage maldoc



통일부 사이버공격 대응 방법 안내
2021-05-13 7:56:00



1MT 거래조건-20140428 .doc
2021-08-14 2:17:00



[Klip 고객센터]오전송_토큰해결_안내.doc
2021-11-03 7:22:00

Initial infection Word document change at every single attack

2nd stage VBS file

```
Function QProc()
    Set ow_cim = GetObject("winmgmts:\root\cimv2")
    Set plist = ow_cim.ExecQuery("Select * from Win32_Process")
    str_tmp = ""
    For Each ob in plist
        str_tmp = str_tmp & ob.Name & vbTab & vbTab & vbTab & _
                            ob.ProcessID & vbTab & _
                            ob.SessionID & vbNewLine
    Next
    QProc = "++++++++++++ Process List ++++++++++++" & vbNewLine & _
            "Process" & vbTab & vbTab & vbTab & "ProcessID" & vbTab & "SessionID" & vbNewLine & _
            str_tmp & vbNewLine
End Function
```

N-stage payloads are used for a long period

“Hard to fully understand cyber attack only with malware dimension

Hard to acquire full infection chain

Hard to figure out relationship of each component

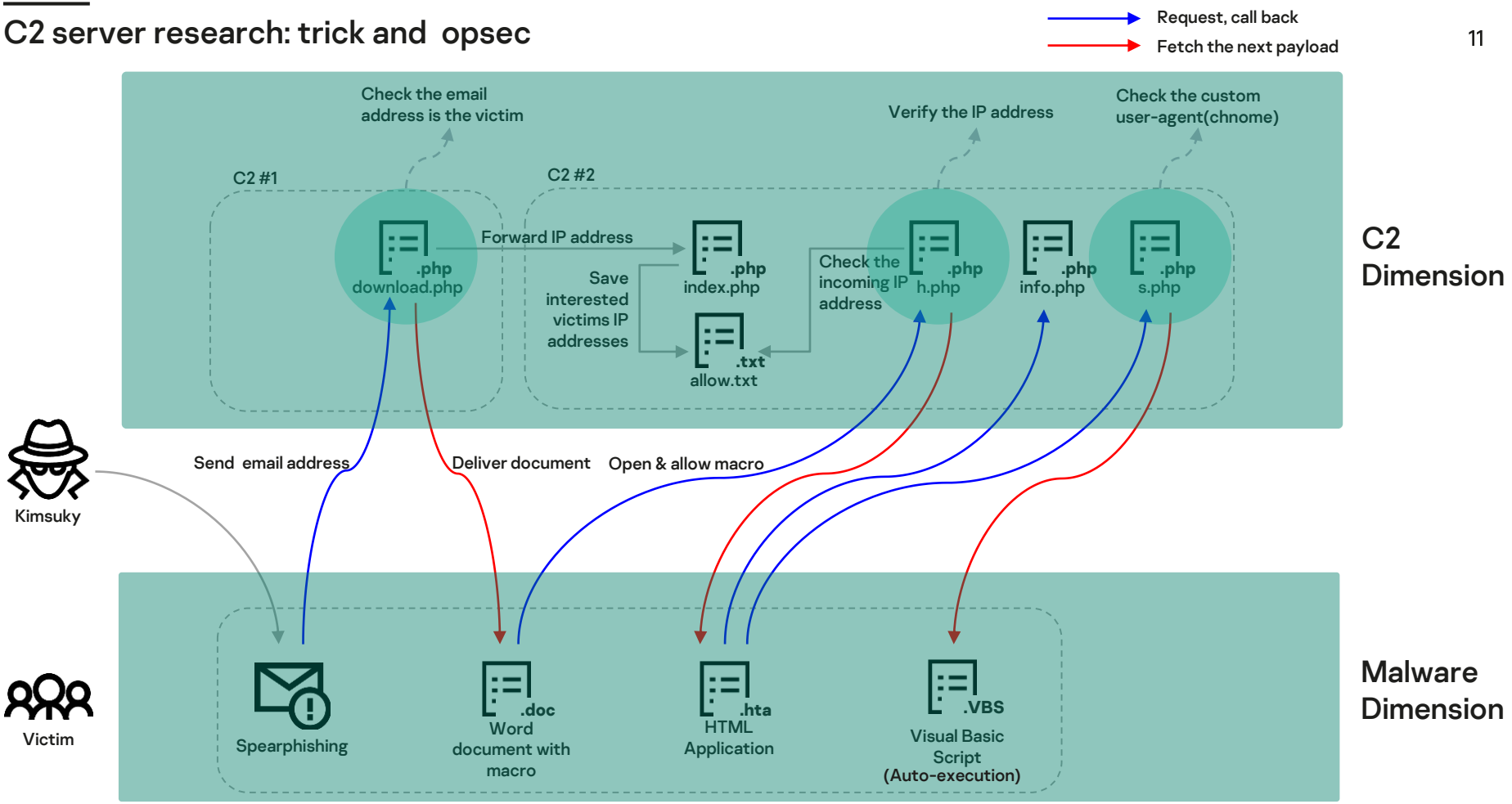
Hard to understand threat actor’s objectives

The other dimension of Kimsuky group

C2 dimension

kaspersky

C2 server research: trick and opsec



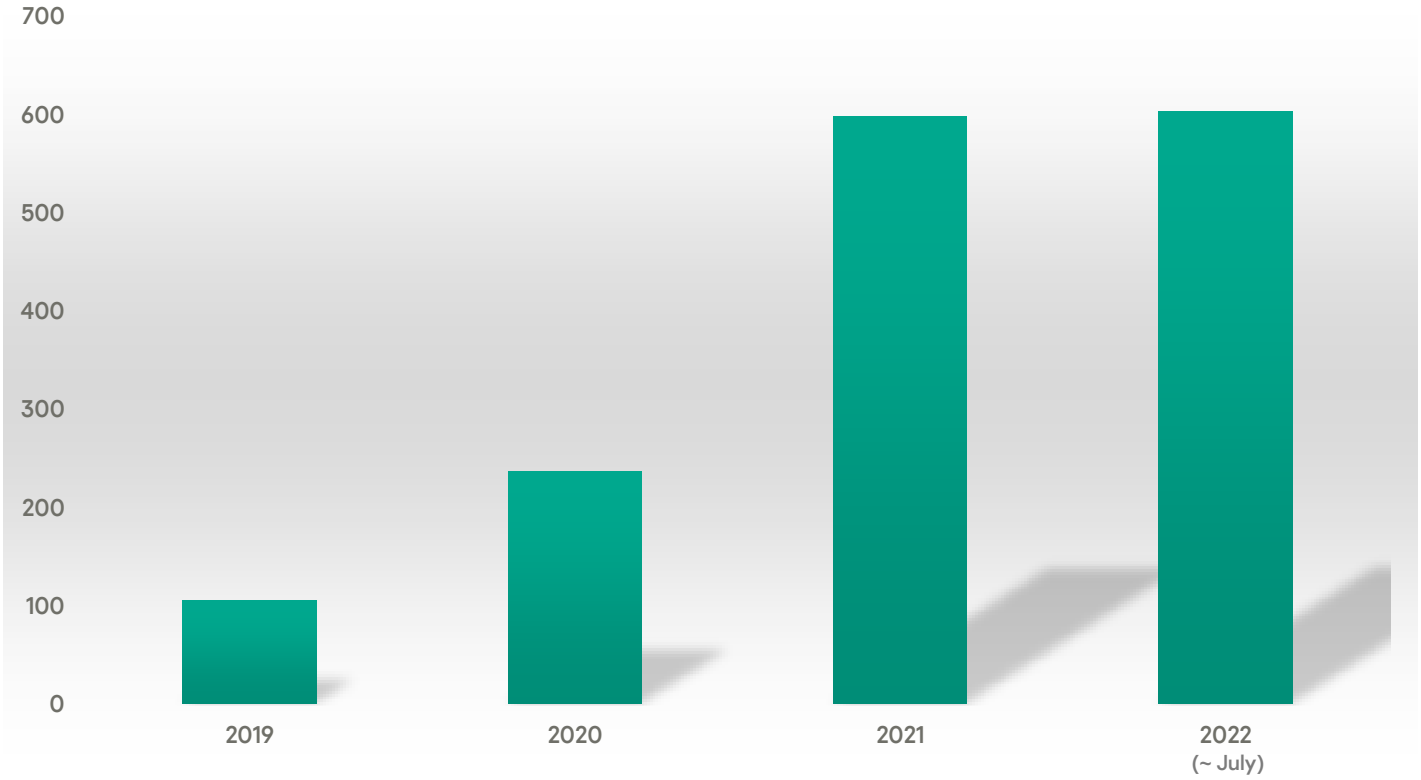
“By researching C2 dimension, we can understand tricks, strategies, and targets

Trick#1: Check the email address and User-agent

Trick #2: Maintain victim’s IP address

Trick #3: Check the pre-defined User-agent

Discovered Kimsuky's C2 servers



Conclusion

Understanding of multidimension

- Emerging cyber threats are complicated
- We should understand multidimension
- Understanding malware and C2

Full-context based defense is the key

- Hit-and-run style defense never works
- Need to understand full-context of threats
- Diversify defense points

Cooperation with other industry

- Each sector has different strength
- Cooperation is essential to understand multidimension of cyber threats

Question?


@unpacker


seongsu.park@kaspersky.com