
KIMSUKY
AXIAL

A SURVEY ON KIMSUKY: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Kimsuky aka Velvet Chollima, Black Banshee, and ITG16 is a state-sponsored threat group from North Korea that has been active since 2013. They had targeted South Korea and the USA. According to Kaspersky, there are multiple reasons why this campaign is extraordinary in its execution and logistics. It all started when they encountered a somewhat unsophisticated spy program that communicated with its “master” via a public e-mail server. This approach is rather inherent to many amateur virus-writers and these malware attacks are mostly ignored.

II. TARGET SECTORS

This threat actor targets South Korean think tanks, industry, nuclear power operators, and the Ministry of Unification for espionage purposes.

III. METHODS USED

Kimsuky uses various spear-phishing and social engineering methods to obtain Initial Access to victim networks. Spear-phishing—with a malicious attachment embedded in the email—is the most observed Kimsuky tactic.

IV. IOC

MD5

- 637e0c6d18b4238ca3f85bcaec191291
- b3caca978b75badffd965a88e08246b0
- dbedadc1663abff34ea4bdc3a4e03f70
- 3ae894917b1d8e4833688571a0573de4
- 8a85bd84c4d779bf62ff257d1d5ab88b
- d94f7a8e6b5d7fc239690a7e65ec1778
- f1389f2151dc35f05901aba4e5e473c7
- 96280f3f9fd8bdbe60a23fa621b85ab6
- f25c6f40340fcde742018012ea9451e0
- cf264f9bca2f2fbcc2c1e7a4a491afec
- 122c523a383034a5baef2362cad53d57
- 2173bbaea113e0c01722ff8bc2950b28
- 2a0b18fa0887bb014a344dc336ccdc8c
- ffad0446f46d985660ce1337c9d5eaa2
- 81b484d3c5c347dc94e611bae3a636a3
- ab73b1395938c48d62b7eeb5c9f3409d
- 69930320259ea525844d910a58285e15

C2

1. christinadudley[.]com
2. seoulhobi[.]biz
3. kaist-ac [.] Xyz
4. app.veryton[.]ml
5. eastsea.or[.]kr
6. kaist.r-naver[.]com
7. kasse.hdactech[.]info
8. csv.posadadesantiago[.]com
9. wave.posadadesantiago[.]com
10. doc-view[.]work
11. suzuki.]datastore.]pe.]hu
12. app-support[.]work
13. web-line[.]work

AX1AL

V. OPERATIONS

- **2013**
  - Kaspersky had been monitoring a cyber-espionage campaign against South Korean think tanks.
- **2014**
  - The South Korean Government issued a report blaming North Korea for network intrusions that stole data from Korea Hydro and Nuclear Power.
- **2018**
  - March and October: Operation "Baby Coin" and Operation "Mystery Baby" were linked to the attribution of same attack vector and underlying codes.
  - May: ASERT revealed a spear-phishing campaign that has been targeting academic institutions. Dubbed as Operation "Stolen Pencil".
  - November: Unit 42 researchers identified spear phishing emails containing new malware that shares infrastructure with playbooks associated with North Korean campaigns. The spear phishing emails were written to appear as though they were sent from a nuclear security expert who currently works as a consultant for in the U.S. The emails were sent using a public email address with the expert's name and had a subject referencing North Korea's nuclear issues. The emails had a malicious Excel macro document attached, which when executed led to a new Microsoft Visual Basic (VB) script-based malware family which we are dubbing "BabyShark".
- **2019**
  - January: Analysis of Operation Kabar Cobra done by Ahn Labs revealed a spear-phishing email with a malicious attachment was sent to members of the Ministry of Unification press corps. The perpetrators behind the mail and malware are assumed to be the so-called Kimsuky threat group.
  - April: Spear-phishing attack against Koreans who are in the fields of diplomacy, security, reunification and NK/defection organization. Dubbed Operation Stealth Power. Also in same month Operation Smoke Screen was being executed.
  - July: Operation Red Salt was observed by AhnLabs which observed a series of activities suspected as targeted email attacks. Although these attacks did not exploit a new weakness or use a high-level of attack methods, it was highlighted due to its activity of targeting specific personnel of the the South Korean government agencies with the intention of stealing personal information. In the same month, Kimsuky had been targeting retired South Korean diplomats, government, and military officials.
- **2020**
  - February: Kimsuky launching spear-phishing attacks to compromise officials part of the United Nations Security Council. The attacks, disclosed in a UN report last month, have taken place this year and have targeted at least 28 UN officials, including at least 11 individuals representing six countries of the UN Security Council.
  - March: According to a tweet shared by South Korean cyber-security firm IssueMakersLab, a group of North Korean hackers also hid malware inside documents detailing South Korea's response to the COVID-19 epidemic. The documents were boobytrapped with BabyShark, a malware strain previously utilized by a North Korean hacker group known as Kimsuky.

VI. ATTRIBUTIONS

- According to Kaspersky, Strings left by malware author in the compile paths of the malicious samples' bodies suggest the attack has Korean origins. They also have been able to define the IP addresses from which attackers visited their email accounts to control the bots. All those IP addresses turned out to be Chinese areas bordering North Korea. Internet Providers from these areas are believed to provide Internet into North Korea. All this, as well as the fact that the targets are of specific interest to the North Korean government, could suggest that North Korea might be behind this threat actor.

VII. COUNTER OPERATIONS

- On December 27 2019, a U.S. district court unsealed documents detailing work Microsoft has performed to disrupt cyberattacks from a threat group we call Thallium, which is believed to operate from North Korea. This resulted in a court order enabling Microsoft to take control of 50 domains that the group uses to conduct its operations. With this action, the sites can no longer be used to execute attacks.

VIII. REFERENCES

- https://apt.securelist.com/apt/kimsuky
- https://global.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation Kabar Cobra (1).pdf
- https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks#When:14:00:00Z
- https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
- https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/