Jun 10 2023

NETMANAGEIT

Intelligence Report

Kimsuky Strikes Again | New Social Engineering Campaign Aims to Steal Credentials and Gather Strategic Intelligence

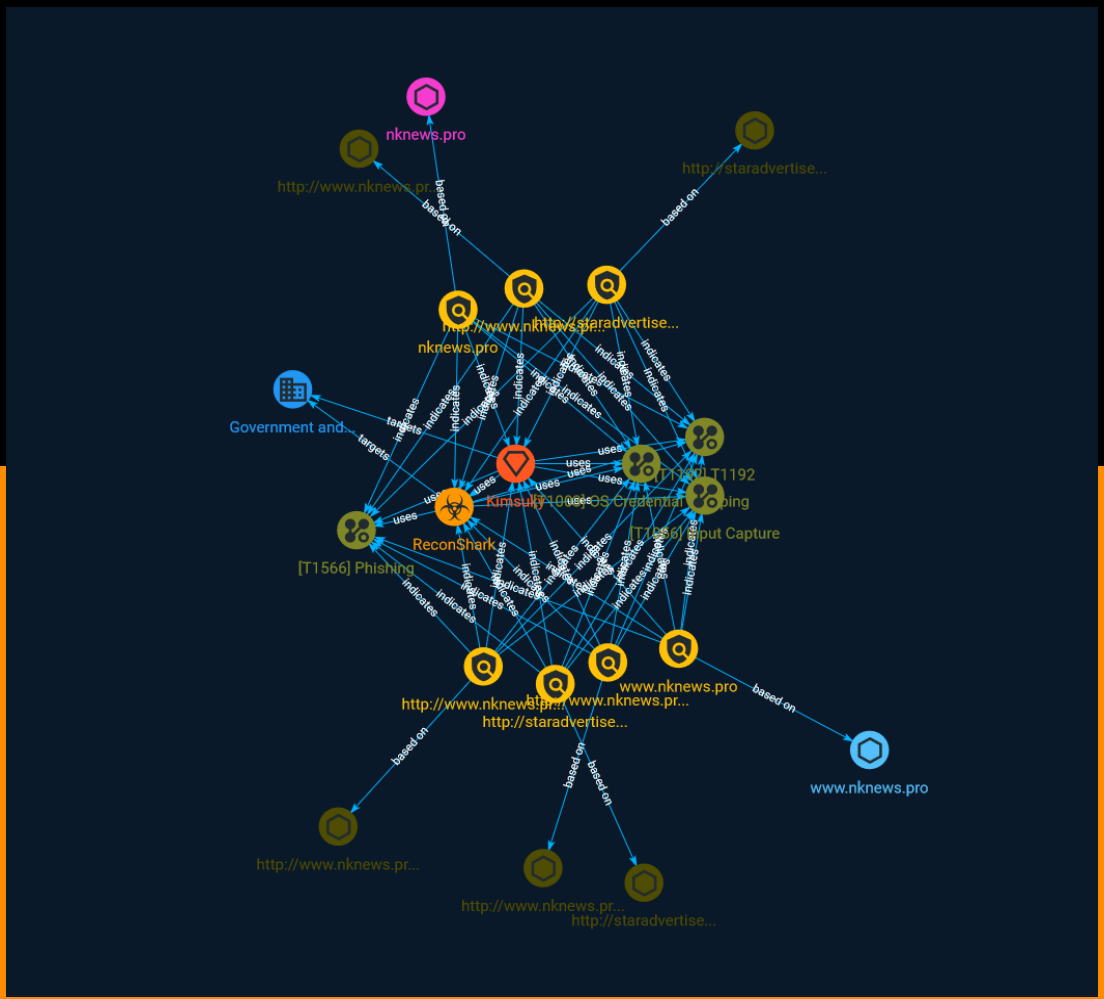

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have been tracking a targeted social engineering campaign against experts in North Korean affairs from the non-government sector. The campaign focuses on theft of email credentials, delivery of reconnaissance malware, and theft of NK News subscription credentials. Based on the used malware, infrastructure, and tactics, they assess with high confidence that the campaign has been orchestrated by the Kimsuky threat actor.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various

different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1192

ID
T1192

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name
http://staradvertiser.store/piece/ca.php
Pattern Type
stix
Pattern
[url:value = 'http://staradvertiser.store/piece/ca.php']
Name
http://www.nknews.pro/ip/register/
Pattern Type
stix
Pattern
[url:value = 'http://www.nknews.pro/ip/register/']
Name
www.nknews.pro

Pattern Type
stix
Pattern
[hostname:value = 'www.nknews.pro']
Name
http://www.nknews.pro/ip/register/login.php
Pattern Type
stix
Pattern
[url:value = 'http://www.nknews.pro/ip/register/login.php']
Name
http://staradvertiser.store/piece/r.php
Pattern Type
stix
Pattern
[url:value = 'http://staradvertiser.store/piece/r.php']
Name
http://www.nknews.pro/config.php

Pattern Type
stix
Pattern
[url:value = 'http://www.nknews.pro/config.php']
Name
nknews.pro
Pattern Type
stix
Pattern
[domain-name:value = 'nknews.pro']

Intrusion-Set

Name

Kimsuky

Description

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

Malware

Name
ReconShark

Domain-Name

Value
nknews.pro

Hostname

Value
www.nknews.pro

Url

Value
http://staradvertiser.store/piece/r.php
http://www.nknews.pro/ip/register/
http://staradvertiser.store/piece/ca.php
http://www.nknews.pro/ip/register/login.php
http://www.nknews.pro/config.php

External References

- https://otx.alienvault.com/pulse/64805aad021906141c79aec0
- https://www.sentinelone.com/labs/kimsuky-new-social-engineering-campaign-aims-to-steal-credentials-and-gather-strategic-intelligence/