VIRUSTOTAL

APT43: An investigation into the North Korean group’s cybercrime operations

THURSDAY, APRIL 20, 2023 | VICENTE DÍAZ | LEAVE A COMMENT

Introduction

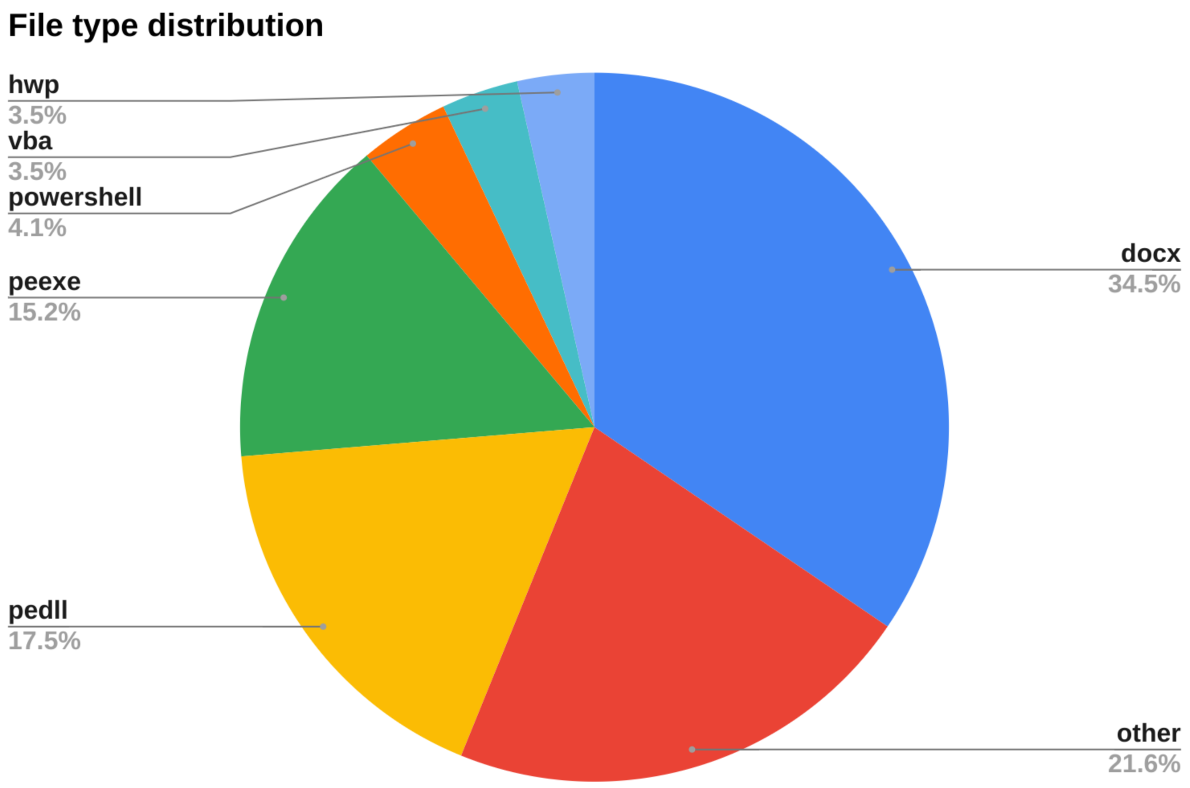
As recently reported by our Mandiant's colleagues, APT43 is a threat actor believed to be associated with North Korea. APT43’s main targets include governmental institutions, research groups, think tanks, business services, and the manufacturing sector, with most victims located in the United States and South Korea. The group uses a variety of techniques and tools to conduct espionage, sabotage, and theft operations, including spear phishing and credential harvesting.

From VirusTotal we wanted to contribute to a better understanding of this actor’s latest activity based on their malware toolset’s telemetry, including geographical distribution, lookups, submissions, file types, detection ratios, and efficacy of crowdsourced YARA rules for the IOCs attributed by Mandiant to this threat actor. All the data provided in this post is also available for VirusTotal users through VT Intelligence. It can be obtained by aggregating Telemetry and Commonalities from a set of IOCs, which you can do using a VT Intelligence search, Collection or Graph.

Malware artifacts

File type distribution

We used Indicators of Compromise (IOCs) attributed to APT43 by Mandiant to collect telemetry on the threat actor's latest activity, resulting in the following file type distribution:



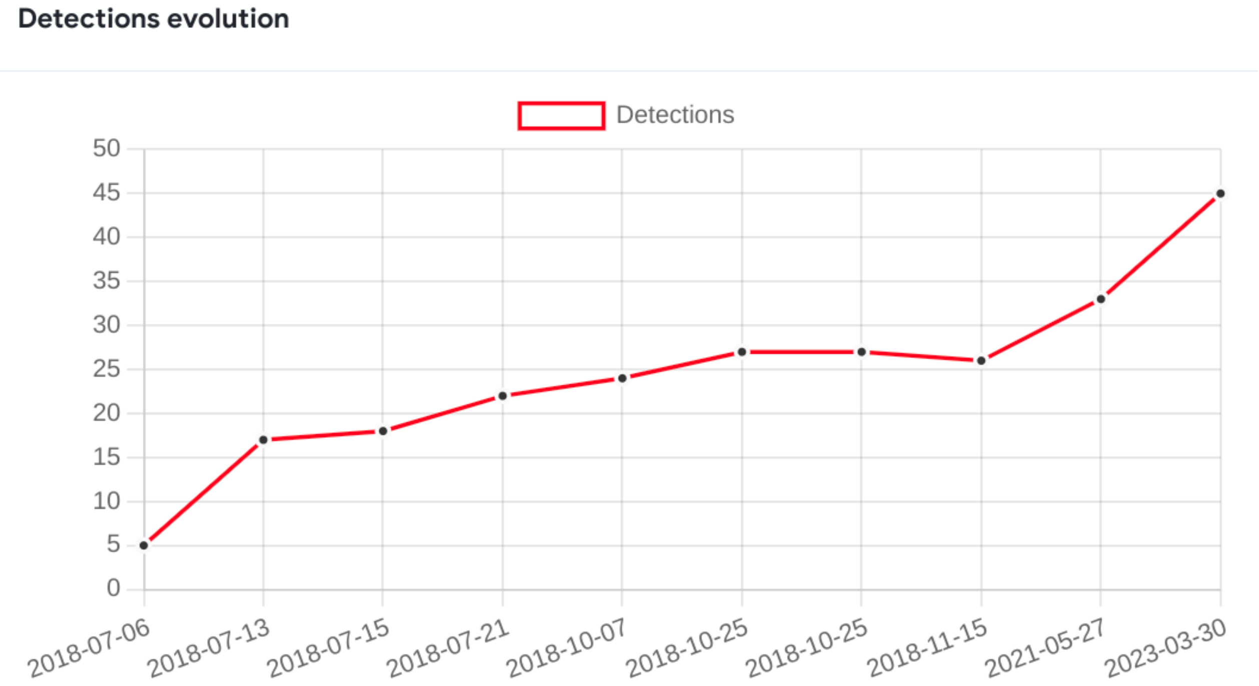
Microsoft Word documents (docx) are the most common file format among the samples we analyzed. This suggests that APT43 relies heavily on Microsoft Word documents as a vector for delivering malicious payloads or exploiting vulnerabilities. We also found that most of these files used macros as their infection technique, while only a few of them exploited the CVE-2017-0199 vulnerability, which allows attackers to run malicious code on target systems by embedding malicious links in the docx file.

The file type distribution also reveals interesting patterns. For example, we can see that there are more pedll files than peexe files, even though both are executable formats. Further analysis of the pedll files revealed that the majority of them used the T1129 MITRE ATT&CK technique, which involves executing malicious payloads via loading shared modules. Another example is that there are more hwp files than doc files, even though both are word processing formats. This may indicate that APT43 targets specific regions or organizations that use Hangul Word Processor (HWP), a popular software in South Korea.

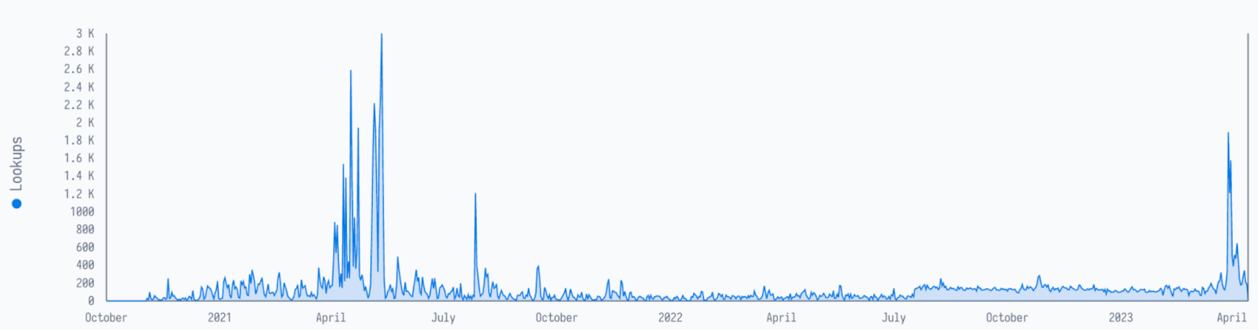
Lookups and submissions timeline

The oldest of the samples we analyzed, a portable executable, was uploaded in July 2018 from the United Kingdom.

The initial submission triggered only five positive detections, but after subsequent submissions from South Korea and Italy, the latest one being on March 30, there are now more than 40 detections. This is an important remark on how typical AV detections evolve protection as new techniques and artifacts are discovered.



For user queries (lookups) now associated with APT43, which speak of the interest of VirusTotal's users on particular samples, there was a peak around April 2021, maybe related to some particular APT43 campaign. The plateau starting July 2022 might be related to security companies monitoring this actor's activity. The very recent peak in April 2023 is most likely related to the publication of APT43, which revamped the interest from security analysts on this actor and related artifacts.



From January to April this year, most of the submissions came from South Korea, and the file type most associated with these submissions was the docx file. For lookups, most of them are from the United States with apk files being the most looked up, followed by docx, text, html, powershell, and peexe.

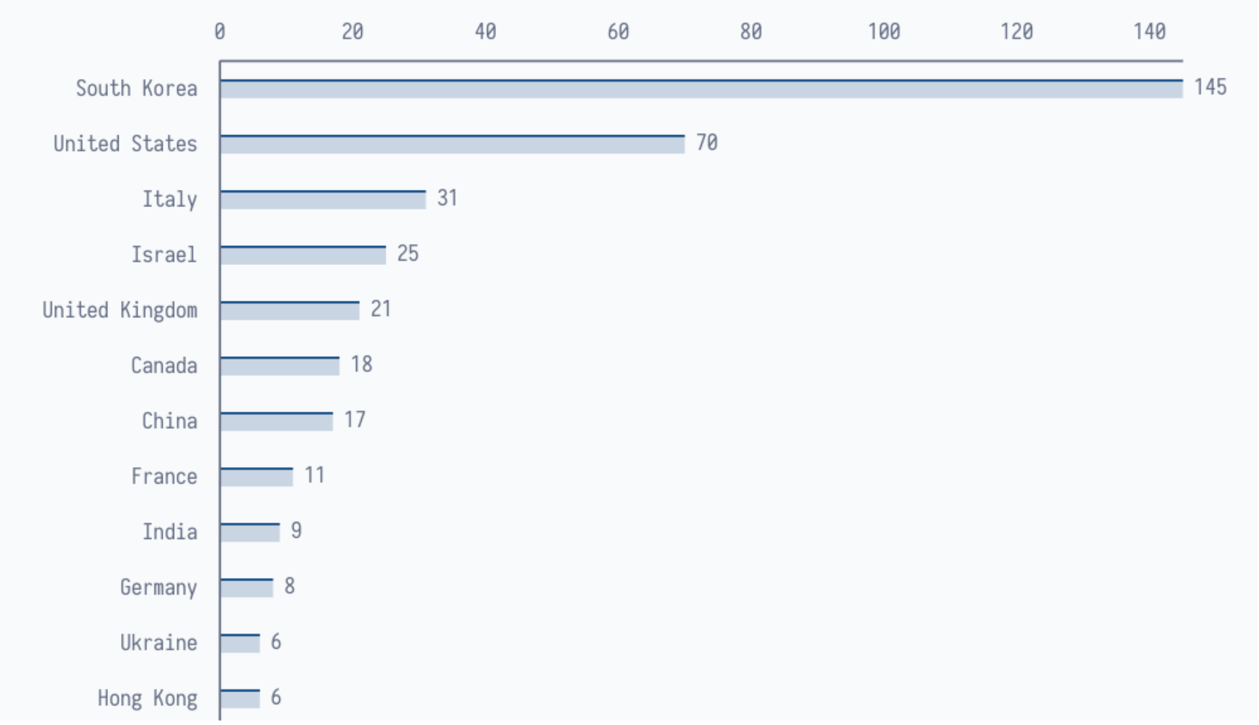
Geographical distribution

File sample submissions and lookups are important indicators of cyber threat activity and awareness. By analyzing the geographical distribution of these activities, we can gain insights into the regions that are most affected by or interested in a particular threat actor or campaign.

According to our telemetry data, the top countries for file sample submission are South Korea, the United States, Italy, Israel, and the United Kingdom.

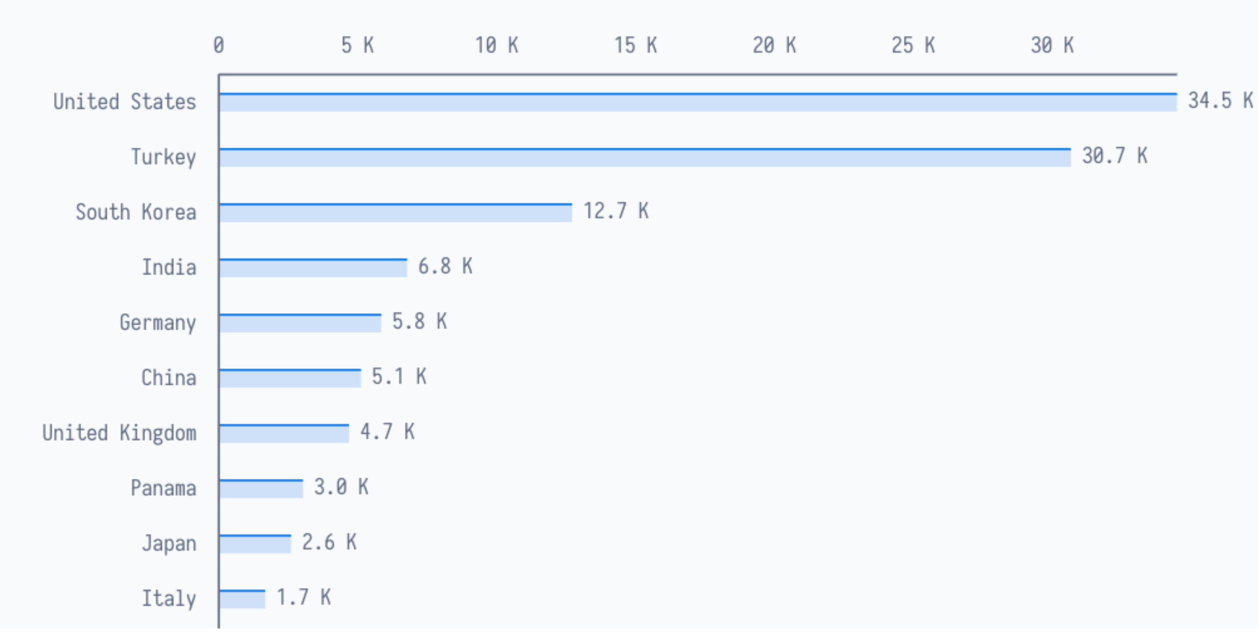
South Korea stands out as the country with the most file sample submissions, accounting for almost half of the total submissions. This is not surprising, given that South Korea is (probably) the primary target of

APT43, as pointed out by Mandiant. Submissions of the identified samples are observed from July 2018 to April 2023.



On the other hand, South Korea ranks third in file sample lookups which is consistent with their leading position in file sample submissions. This is remarkable given South Korea's number of VT submitters, well below top 10 countries.

Interestingly, Turkey stands out as the country with the second highest number of lookups, even if they are not among top submitters. This may suggest that Turkey is either a victim or a conduit of North Korean cyber attacks. Lookups of the identified samples are observed from October 2020 to April 2023.



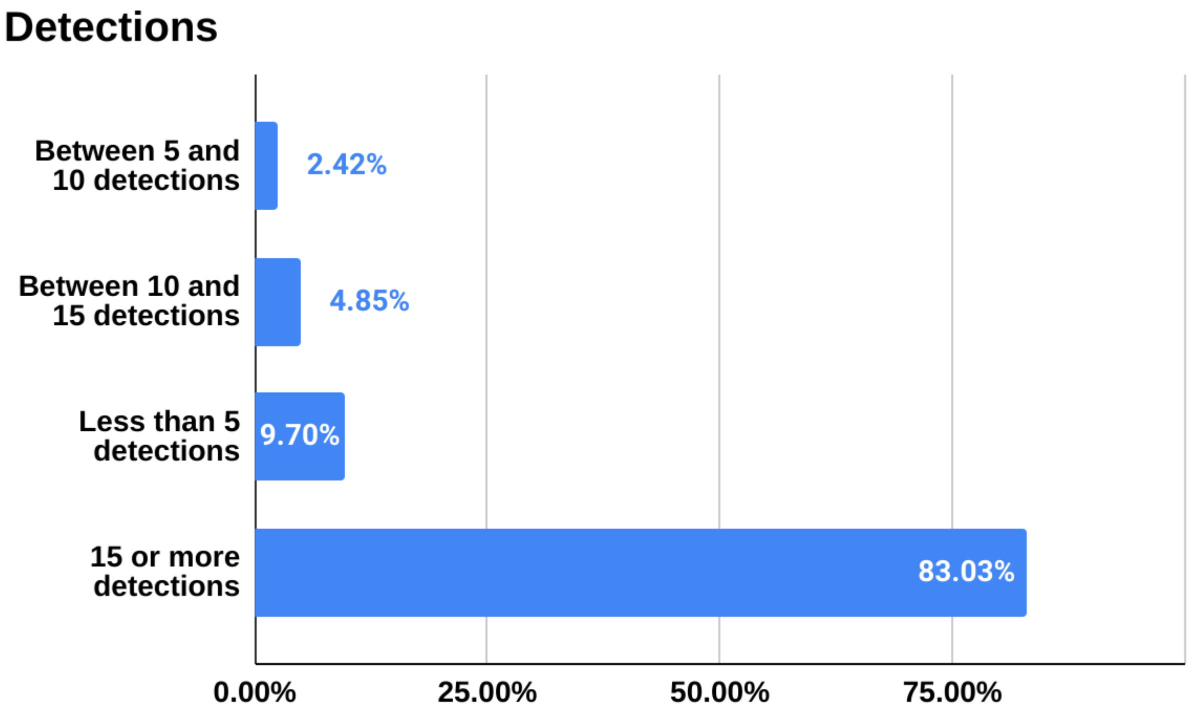
Detections

Analysis from the commonalities tool reveals the most common threat categories as trojan, downloader and dropper. Of the identified samples, 32% of the samples with threat names assigned to them are labeled ‘kimsuky’. Mandiant’s report mentions kimsuky as being used by multiple companies in their public statements on APT43’s activities.

To get a sense of the detection distribution among the samples we analyzed, we divided them into four categories:

- 15 or more detections,
- less than 5 detections,
- between 10 and 15 detections, and
- between 5 and 10 detections.

The most common category was for 15 or more detections, representing 83% of all samples. On the other hand, samples with less than 5 detections came in at 9.7%. The other two categories, between 5 and 10 detections and between 10 and 15 detections, came in at 2.4% and 4.8%, respectively.



MITRE ATT&CK

During our analysis of the samples using the commonalities tool, we observed several MITRE ATT&CK techniques adopted to APT43 to compromise and exfiltrate data from their targets. VirusTotal extracts TTPs from samples by detonating them in different sandboxes and using tools such as CAPA. Among the techniques, the most prevalent ones were:

- T1082: System Information Discovery
- T1083: File and Directory Discovery
- T1129: Execution through Module Load
- T1055: Process Injection
- T1071: Application Layer Protocol

Crowdsourced YARA rules

Of all the samples analyzed, quite a few of them triggered some crowdsourced YARA rules. The YARA rule that detected quite a few of the samples was one created by InQuest Labs, Ruleset: Office_Document_with_VBA_Project. The rule was created to detect any Office document with a VBA project in them. While a VBA project within an Office document is used for automating tasks, it can also be used to perform a range of malicious actions such as stealing sensitive data, installing malware, and modifying or deleting data. It can even be used in phishing attacks where the emails contain attachments with malicious VBA macros. In Mandiant's publication, they point out APT43's use of SPICYTUNA, which is a VBA downloader. This rule could be used as a soft signal.

Another crowdsourced YARA rule that detected a few of the analyzed samples was one by Florian Roth, which detects the Ghost419 RAT used by the Gold Dragon malware: GoldDragon_Ghost419_RAT. Mandiant reports that the malware extracts a payload from a hwp document and writes it to a startup directory resulting in the new file being executed when the current user logs in.

A sample using the Gh0st RAT malware was detected by one of the crowdsourced rules: GhostDragon_Gh0stRAT. The malware is a backdoor written in C++ that communicates via a custom binary protocol over TCP or UDP, as reported by Mandiant.

Collections

Collections are how our users can group different indicators in a shareable set. This has great benefits, such as providing a name and description, external references, attribution, etc. In addition it helps working with large datasets and obtaining commonalities, telemetry and other aggregated data. Other than this, we daily create dozens of collections based on

OSINT security incidents and publications.

During our analysis of the samples, we observed that several of them belonged to two different collections created by AlienVaultOTX: APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations and Analysis of Smoke Screen in APT campaign aimed at Korea and America. For the first collection, we observed that it contained a variety of file types such as pedll, peexe, docx, php, and powershell in that order. The second collection was different, however, as it contained only two file types. We found that the majority of the files were docx files which accounted for over 90% of the samples, and the remaining were peexe files.

Conclusions

This blog post sheds light on the activities of APT43, a threat actor operating on behalf of the North Korean regime. We have used VirusTotal's features to explore the file type and geographical distributions, detections, ATT&CK techniques, collections, and crowdsourced YARA rules related to the threat actor's campaign. We hope that this post has provided some insights into the capabilities and techniques of APT43, and how VirusTotal can help to monitor and investigate such campaigns.

We hope you found this useful, and please reach out to us if you have any suggestions or just want to share feedback.

Happy hunting!