Jun 10 2023

NETMANAGEIT

Intelligence Report

ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People's Republic of Korea (DPRK)

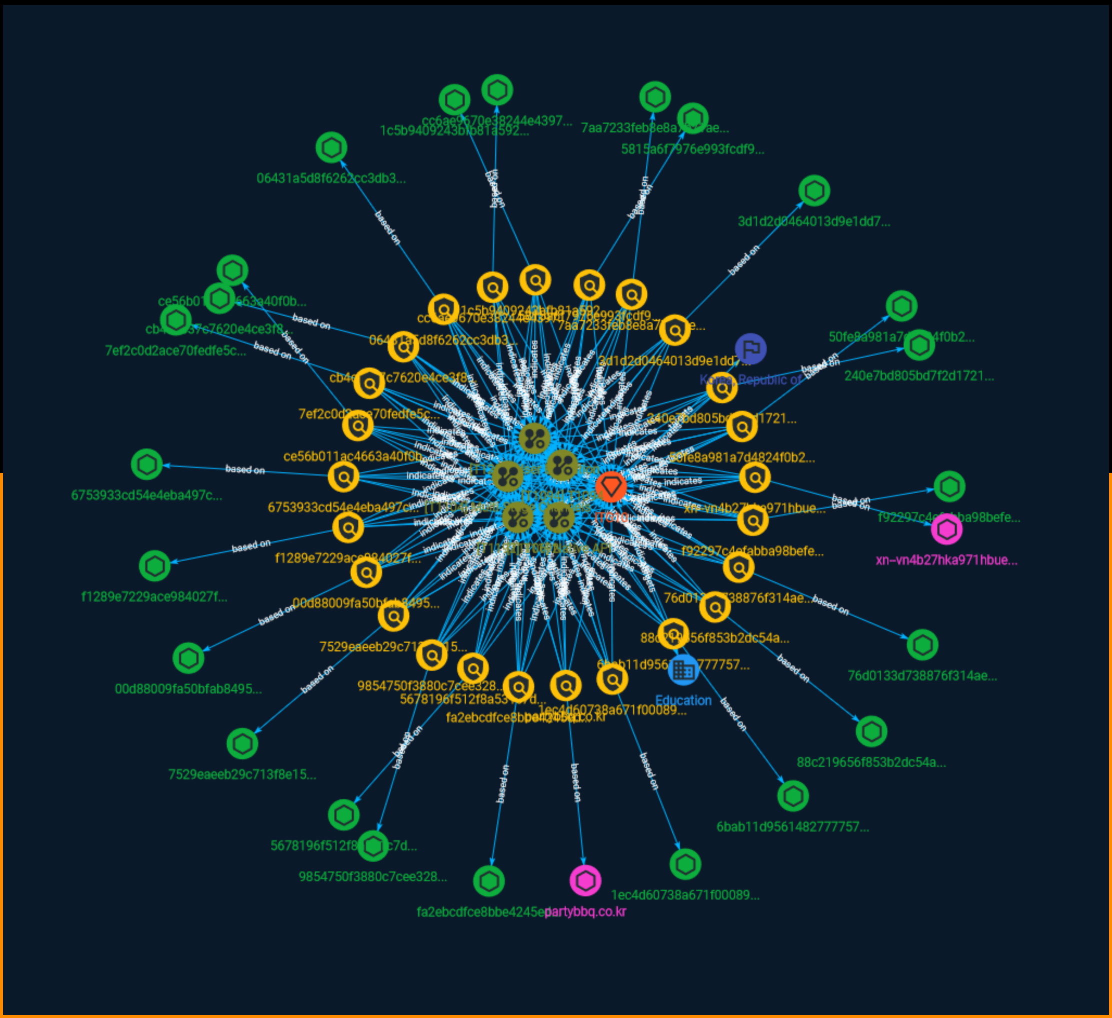

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In late April 2023, uncovered documents that are most likely part of a phishing campaign mimicking credible senders, orchestrated by a group X-Force refers to as ITG10, and aimed at delivering RokRAT malware, similar to what has been observed by others. ITG10's tactics, techniques and procedures (TTPs) overlap with APT37 and ScarCruft. The initial delivery method is conducted via a LNK file, which drops two Windows shortcut files containing obfuscated PowerShell scripts in charge of downloading a second stage RokRAT shellcode. RokRAT can execute remote C2 commands, data exfiltration, file download/upload, and keylogging. The uncovered lure documents suggest ITG10 may be targeting individuals and organizations involved in foreign policy associated with the Korean peninsula.

Confidence

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

15 / 100

Attack-Pattern

Name

T1192

ID

T1192

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

T1094

ID

T1094

Sector

Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Indicator

Name

76d0133d738876f314ae792d0cf949710b66266ba0cebefbd98ce40c64a9b15b

Description

multiple_versions

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '76d0133d738876f314ae792d0cf949710b66266ba0cebefbd98ce40c64a9b15b']

Name

f1289e7229ace984027f29cf8e2dd8fdd19b0c4b488da31ff411ee95305eaecc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f1289e7229ace984027f29cf8e2dd8fdd19b0c4b488da31ff411ee95305eaecc']

Name

7aa7233feb8e8a7b71ae6cdd0ddb8c2b192d4b6e131fed1ade82efdcb8096c57

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'7aa7233feb8e8a7b71ae6cdd0ddb8c2b192d4b6e131fed1ade82efdcb8096c57']

Name

partybbq.co.kr

Pattern Type

stix

Pattern

[domain-name:value = 'partybbq.co.kr']

Name

cb4c7037c7620e4ce3f8f43161b0ec67018c09e71ae4cea3018104153fbed286

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb4c7037c7620e4ce3f8f43161b0ec67018c09e71ae4cea3018104153fbed286']

Name

xn--vn4b27hka971hbue.kr

Pattern Type

stix

Pattern

[domain-name:value = 'xn--vn4b27hka971hbue.kr']

Name

7529eaeeb29c713f8e15827c79001a9227d8bc31c9209bf524a4ff91648a526e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7529eaeeb29c713f8e15827c79001a9227d8bc31c9209bf524a4ff91648a526e']

Name

1c5b9409243bfb81a5924881cc05f63a301a3a7ce214830c7a83aeb2485cc5c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1c5b9409243bfb81a5924881cc05f63a301a3a7ce214830c7a83aeb2485cc5c3']

Name

6bab11d9561482777757f16c069ebef3f1cd6885dbef55306ffde30037a41d48

Description

SLF:Win32/Elenquay.A

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'6bab11d9561482777757f16c069ebef3f1cd6885dbef55306ffde30037a41d48']

Name

ce56b011ac4663a40f0ba606c98c08aaf7caf6a45765aa930258fe2837b12181

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce56b011ac4663a40f0ba606c98c08aaf7caf6a45765aa930258fe2837b12181']

Name

240e7bd805bd7f2d17217dd4cebc03ac37ee60b7fb1264655cfd087749db647a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '240e7bd805bd7f2d17217dd4cebc03ac37ee60b7fb1264655cfd087749db647a']

Name

5678196f512f8a531c7d85af8df4f40c7a5f9c27331b361bb1a1c46d317a77d8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5678196f512f8a531c7d85af8df4f40c7a5f9c27331b361bb1a1c46d317a77d8']

Name

06431a5d8f6262cc3db39d911a920f793fa6c648be94daf789c11cc5514d0c3d

Pattern Type

stix
Pattern
[file:hashes.'SHA-256' = '06431a5d8f6262cc3db39d911a920f793fa6c648be94daf789c11cc5514d0c3d']
Name
f92297c4efabba98befeb992a009462d1aba6f3c3a11210a7c054ff5377f0753
Description
SUSP_LNK_Big_Link_File
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f92297c4efabba98befeb992a009462d1aba6f3c3a11210a7c054ff5377f0753']
Name
00d88009fa50bfab849593291cce20f8b2f2e2cf2428d9728e06c69fced55ed5
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'00d88009fa50bfab849593291cce20f8b2f2e2cf2428d9728e06c69fced55ed5']

Name

5815a6f7976e993fcdf9e024f4667049ec5a921b7b93c8c8c0e5d779c8b72fcc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5815a6f7976e993fcdf9e024f4667049ec5a921b7b93c8c8c0e5d779c8b72fcc']

Name

1ec4d60738a671f00089a86eeba6cb13750bce589e84fd177707718a4cc7d8f1

Description

SLF:Win32/Elenquay.A

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1ec4d60738a671f00089a86eeba6cb13750bce589e84fd177707718a4cc7d8f1']

Name

7ef2c0d2ace70fedfe5cd919ad3959c56e7e9177dcc0ee770a4af7f84da544f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'7ef2c0d2ace70fedfe5cd919ad3959c56e7e9177dcc0ee770a4af7f84da544f1']

Name

50fe8a981a7d4824f0b297f37804b65672ed4484e198e7c324260a34941ddac7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'50fe8a981a7d4824f0b297f37804b65672ed4484e198e7c324260a34941ddac7']

Name

9854750f3880c7cee3281d8c33292ca82d0d288963f0f2771d938c06ccaffaa9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9854750f3880c7cee3281d8c33292ca82d0d288963f0f2771d938c06ccaffaa9']

Name

cc6ae9670e38244e439711b1698f0db3cff000b79bec7f47bc4aa5ab1f6177c0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'cc6ae9670e38244e439711b1698f0db3cff000b79bec7f47bc4aa5ab1f6177c0']

Name

88c219656f853b2dc54ae02d32a716e10c8392ed471d1c813e57de2dc170951e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'88c219656f853b2dc54ae02d32a716e10c8392ed471d1c813e57de2dc170951e']

Name

6753933cd54e4eba497c48d63c7418a8946b4b6c44170105d489d29f1fe11494

Description

SUSP_LNK_Big_Link_File

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6753933cd54e4eba497c48d63c7418a8946b4b6c44170105d489d29f1fe11494']

Name

3d1d2d0464013d9e1dd7611d73176f3a31328a41d6474d5b6d0582ad09d3b17d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d1d2d0464013d9e1dd7611d73176f3a31328a41d6474d5b6d0582ad09d3b17d']

Name

fa2ebcdfce8bbe4245ed77b43d39e22c0c7593ca3f65be3fd0ccdf7ee02130a9

Description

multiple_versions

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = 'fa2ebcdfce8bbe4245ed77b43d39e22c0c7593ca3f65be3fd0ccdf7ee02130a9']

Intrusion-Set

Name
ITG10

Country

Name
Korea, Republic of

Domain-Name

Value
partybbq.co.kr
xn--vn4b27hka971hbue.kr

StixFile

Value
00d88009fa50bfab849593291cce20f8b2f2e2cf2428d9728e06c69fced55ed5
06431a5d8f6262cc3db39d911a920f793fa6c648be94daf789c11cc5514d0c3d
cc6ae9670e38244e439711b1698f0db3cff000b79bec7f47bc4aa5ab1f6177c0
88c219656f853b2dc54ae02d32a716e10c8392ed471d1c813e57de2dc170951e
9854750f3880c7cee3281d8c33292ca82d0d288963f0f2771d938c06ccaffaa9
76d0133d738876f314ae792d0cf949710b66266ba0cebefbd98ce40c64a9b15b
f1289e7229ace984027f29cf8e2dd8fdd19b0c4b488da31ff411ee95305eaecc
ce56b011ac4663a40f0ba606c98c08aaf7caf6a45765aa930258fe2837b12181
cb4c7037c7620e4ce3f8f43161b0ec67018c09e71ae4cea3018104153fbed286
5678196f512f8a531c7d85af8df4f40c7a5f9c27331b361bb1a1c46d317a77d8
5815a6f7976e993fcdf9e024f4667049ec5a921b7b93c8c8c0e5d779c8b72fcc
7aa7233feb8e8a7b71ae6cdd0ddb8c2b192d4b6e131fed1ade82efdcb8096c57
6753933cd54e4eba497c48d63c7418a8946b4b6c44170105d489d29f1fe11494

1ec4d60738a671f00089a86eeba6cb13750bce589e84fd177707718a4cc7d8f1
50fe8a981a7d4824f0b297f37804b65672ed4484e198e7c324260a34941ddac7
7529eaeeb29c713f8e15827c79001a9227d8bc31c9209bf524a4ff91648a526e
3d1d2d0464013d9e1dd7611d73176f3a31328a41d6474d5b6d0582ad09d3b17d
7ef2c0d2ace70fedfe5cd919ad3959c56e7e9177dcc0ee770a4af7f84da544f1
6bab11d9561482777757f16c069ebef3f1cd6885dbef55306ffde30037a41d48
fa2ebcdfce8bbe4245ed77b43d39e22c0c7593ca3f65be3fd0ccdf7ee02130a9
f92297c4efabba98befeb992a009462d1aba6f3c3a11210a7c054ff5377f0753
240e7bd805bd7f2d17217dd4cebc03ac37ee60b7fb1264655cfd087749db647a
1c5b9409243bfb81a5924881cc05f63a301a3a7ce214830c7a83aeb2485cc5c3

External References

- https://securityintelligence.com/posts/itg10-targeting-south-korean-entities/?c=Threat%20Research
- https://otx.alienvault.com/pulse/6480961ee919e1f6ae47d275