

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

SL securelist.com/modern-asia-apt-groups-ttp/111009







APT reports

09 Nov 2023

2 minute read



Authors

-  Nikita Nazarov
-  Expert Kirill Mitrofanov
-  Alexander Kirichenko
-  Vladislav Burtsev
-  Natalya Shornikova
-  Expert Vasily Berdnikov
- Sergey Kireev

Almost every quarter, someone publishes major research focusing on campaigns or incidents that involve Asian APT groups. These campaigns and incidents target various organizations from a multitude of industries. Likewise, the geographic location of victims is not limited to just one region. This type of research normally contains detailed information about the tools used by APT actors, the vulnerabilities that they exploit and sometimes even a specific attribution. Despite the large number of these types of reports, companies often remain unprepared to face these kinds of attackers. With the advanced

tools and techniques used by threat actors today, cybersecurity professionals require not only high-level expertise and extensive experience, but also the infrastructure supplemented by well-organized asset management and vulnerability management processes, network segmentation, fine-tuned audits, and intelligently configured data security tools. In most cases, an unprepared infrastructure is the primary factor enabling Asian APT groups to conduct successful attacks.

In this report, we share the most valuable intelligence that we gathered on Asian APT groups. Over the course of our work, we noticed that these groups attacked the greatest number of countries and industries. Most importantly, our analysis of hundreds of attacks revealed a similar pattern among various groups. They achieve specific objectives at various stages of the Cyber Kill Chain using a common but limited number of techniques encountered by security professionals all over the world. Unfortunately, security teams often have difficulty detecting these attacks in their own infrastructure.

Intended audience of this report

We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups. This report will be the most helpful to the following:

- SOC analysts
- Cyber Threat Intelligence analysts
- Threat Hunting experts
- Digital Forensics (DFIR) experts
- Cybersecurity experts
- Domain administrators
- C-Level executives responsible for cybersecurity at their companies

This material can serve as a library of knowledge on the main approaches used by Asian APT groups when they hack an infrastructure. The report also contains detailed information on the attackers' tactics, techniques and procedures (TTPs) based on the MITRE ATT&CK methodology.

Structure of the report

This report consists of six main sections:

1. Incidents involving Asian APT groups in various regions of the planet

Information on five unique incidents that we detected in different parts of the world. Each incident is a unique case within a specific country and industry, and we provide a description of the actions and TTPs of the perpetrators. At the end of each section, we put together a consolidated table showing a list of TTPs (related to the APT groups that we encountered in these incidents) and their overlapping use in these incidents.

2. Technical details

A detailed description of the individual techniques that we detected in the attacks conducted by Asian APT groups. Each technique contains the following:

- Main description. Technical details on how the specific technique works.
- Examples of procedures. Example implementations of this technique that we detected in attacks by Asian APT groups.
- Data on the approaches employed to detect the described technique, and the EventIDs of events in various monitoring agents used to detect the specific threat.
- SIGMA rules. List of SIGMA rules relevant to this technique. The actual SIGMA rules can be found in the Appendix: SIGMA.

3. Analysis of attacker actions based on the Unified Kill Chain

We used the Unified Kill Chain model to create our own table linked to Asian APT groups, so that we could provide a high-level look at the motivations and behavioral patterns of these actors, and provide data on the possible steps taken by Asian APT groups when they conduct potential attacks.

4. Mitigation

The measures undertaken to mitigate risks associated with the described TTPs.

5. Statistics on attack victims

Consolidated statistics on the victims of Asian APT groups throughout the world and a breakdown by country and industry.

6. Appendix: SIGMA

The SIGMA rules that can help to detect the techniques described in this report.

Download the full version of the Modern Asian APT groups' tactics, techniques and procedures report (English, PDF)

- APT
- Cyber espionage
- Malware Statistics
- Malware Technologies
- Targeted attacks
- TTPs

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

Your email address will not be published. Required fields are marked *
GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm

GReAT Ideas. Green Tea Edition

17 Jun 2020, 1:00pm

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

26 Aug 2020, 2:00pm

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

22 Jul 2020, 2:00pm

GReAT Ideas. Powered by SAS: threat hunting and new techniques

From the same authors



From Caribbean shores to your devices: analyzing Cuba ransomware



The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs



New zero-day vulnerability CVE-2019-0859 in win32k.sys



The fourth horseman: CVE-2019-0797 vulnerability



A simple example of a complex cyberattack

Subscribe to our weekly e-mails

The hottest research right in your inbox

In the same category



HrServ – Previously unknown web shell used in APT attack



A cascade of compromise: unveiling Lazarus' new campaign



How to catch a wild triangle



StripedFly: Perennially flying under the radar



Updated MATA attacks industrial companies in Eastern Europe

•



Kaspersky Threat Intelligence

Boost your incident investigation and threat hunting missions



kaspersky

Reports

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

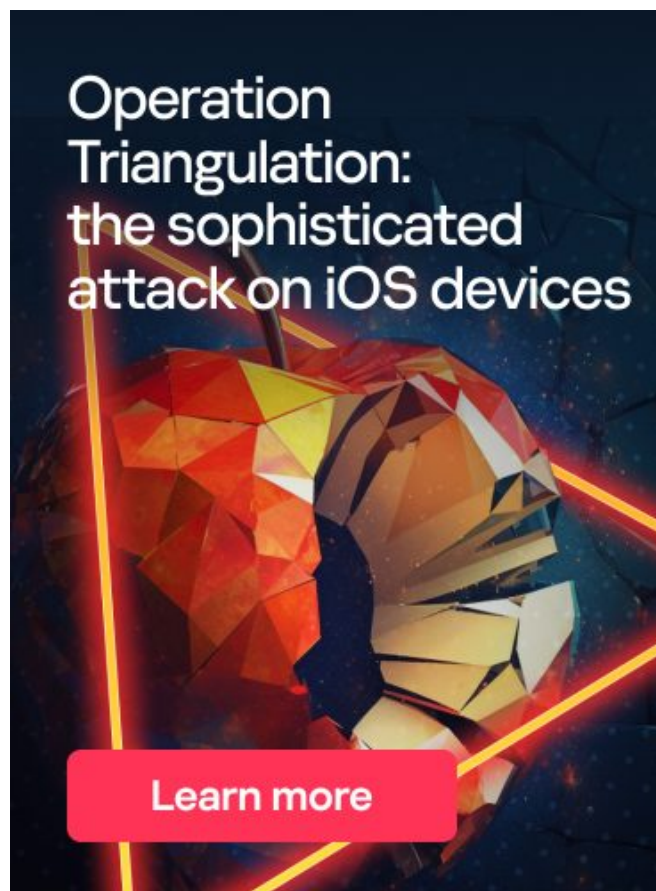
Asian APT groups target various organizations from a multitude of regions and industries. We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups.

A cascade of compromise: unveiling Lazarus' new campaign

We unveil a Lazarus campaign exploiting security company products and examine its intricate connections with other campaigns

How to catch a wild triangle

How Kaspersky researchers obtained all stages of the Operation Triangulation campaign targeting iPhones and iPads, including zero-day exploits, validators, TriangleDB implant and additional modules.



Subscribe to our weekly e-mails

The hottest research right in your inbox

