


Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup

 blogs.jpccert.or.jp/en/2025/03/classifying-lazaruss-subgroup.html



佐々木 勇人 (Hayato Sasaki)

March 25, 2025

Lazarus

-
- Email

***Please note that this article is a translation of the Japanese version published on January 20, 2025, and may not reflect the latest information on threat trends.**

“Lazarus”[1] no longer refer to a single APT group but a collection of many sub-groups. Originally, it referred to a single group or activities by some small groups. I suppose that, as the scale of their activities expanded, the group branched out into multiple units. Now it is realistic to consider that “Lazarus” is no longer an applicable label.

When I start talking about Lazarus’ subgroup-level identification or attribution, many people look skeptical or uninterested. However, this kind of analysis, which may seem overly obsessive, is actually crucial to addressing attacks against the entire Japan, and this blog post explains the reasons.

Characteristics of Lazarus subgroups

There are already a number of labels that refer to activities/campaigns and groups of Lazarus, and the number is growing. In addition, although it is not limited to Lazarus, various security vendors use different names for the same group, subgroup, and malware, making it more difficult to grasp the whole picture. Furthermore, some authors focus on the names of attack groups (or subgroups) in their analysis reports, while others focus on the names of attack campaigns, which makes the terminology even more confusing. There was even a case where a label used as the name of an attack campaign in one report was cited as that of an attack group in another.

*I have organized the labels as follows. Any suggestions or information about the classification are welcome.

Labels for the entire APT activity: Hidden Cobra, TraderTraitor
Labels for individual (or intermittent) campaigns[2]: Operation Dreamjob, Operation In(ter)ception, AppleJeus, Dangerous Password, CryptoCore, SnatchCrypto, Contagious Interview, Operation Jtrack *Dangerous Password and CryptoCore initially appeared as attack group names, but later they are also used as attack campaign names in many cases.
Labels for attack groups (subgroups): TEMP.Hermit, Selective Pisces, Diamond Sleet, Zinc, UNC577, Black Artemis, Labyrinth Chollima, NICKEL ACADEMY APT38, Bluenoroff, Stardust chollima, CryptoMimic, Leery Turtle, Sapphire Sleet, TA444, BlackAlicanto Jade Sleet, UNC4899, Slaw Pisces Gleaming Pisces, Citrine Sleet Andariel, Stonefly, Onyx Sleet, Jumpy Pisces, Silent Chollima Moonstone Sleet (*This may not be a subgroup of Lazarus)
Labels that used to refer to a single attack group and then now used for its successors, related groups, and branched subgroups: Lazarus, Bluenoroff, APT38, Andariel

I have argued[3] in various places that accurate profiling and attribution of APT groups is critical for counter-operations against threat actors. Some people may think that a broad classification is sufficient, rather than more detailed subgrouping. It is true that some of the Lazarus subgroups have the same targets, objectives and TTPs. For example, no matter whether the attacker is Citrine Sleet/UNC4736, Sapphire Sleet/CryptoMimic or Moonstone Sleet, all of which target cryptocurrency, the response strategy may not change significantly. The reasons for identifying threat actors at the subgroup level for Lazarus is further explained later, but there are two characteristics and trends behind this argument, which are unique to Lazarus subgroups and make the grouping of threat actors more difficult:

1. Overlaps in TTPs among multiple subgroups

As many security vendors and analysts have discussed in the past[4], there are overlaps in initial attack vector, C2 infrastructure, and malware among multiple subgroups.

As explained in JPCERT/CC Eyes[5] recently, there have been multiple confirmed attack campaigns in which LinkedIn was used for initial attack vector. In addition, there is a tendency that similar attack methods to be increasingly used, which is explained later.

2. Rise of task force-like groups beyond traditional subgrouping

From 2021 to February 2023, reports and media coverage on a new APT actor called Bureau325 appeared[6]. It is known that this actor shares the same TTPs as multiple known Lazarus subgroups and also uses the same malware as Kimsuky. It is assumed that Bureau325 is a task force-like group or activity which is free from existing group structures[7].

In March 2023, Mandiant published a report on APT43[8]. The activities of the actors described in this report were previously reported as those of Kimsuky or Thallium. However, Mandiant's analysis team has reclassified the group as APT43. The report also notes that APT43 uses the same tools across groups and subgroups, similar to Bureau 325.

Reasons for identification in subgroup level

When identifying APT actors, attention is often paid to attribution, such as identifying the perpetrators, their backgrounds, and attributing responsibility to a specific state, which I believe is the underlying reason why people are not so interested in Lazarus subgroup identification[9]. The following section discusses why detailed identification of subgroups, which are merely virtual distinctions, is necessary in addition to attribution.

Reason 1: To ensure the effects of mid- to long-term damage prevention through security alerts, etc.

For example, in attacks through SNS, such as the case covered on JPCERT/CC Eyes recently, cryptocurrency businesses and defense and aviation industries were targeted, and thus it was possible to focus on alerting such industries. Since attackers usually contact individual engineers at target organizations on SNS, it was effective to alert and share IoCs with organizations in the sector.

On the other hand, objectives, and target sectors/individuals/organizations of subgroups (and related groups) and attack campaigns identified in the second half of 2023 and later are becoming more complex. While most of them target the cryptocurrency sector, there is a wide range of groups, such as those targeting sensitive corporate information, those using ransomware (Moonstone Sleet), and those targeting illegal foreign currency income by IT workers (WageMole attack campaign).

Identifying the target industries and objectives of each subgroup accurately makes it possible to provide information to specific sectors and organizations, which is more effective than issuing alerts. When an alert is issued about an attack that exploits the vulnerability of a specific sector or product, the attacker is also likely to target other sectors or products. However, people may not pay much attention to the alert, thinking that it is irrelevant to them.

Reason 2: Countermeasures/counter operations

The accurate identification of subgroups is also essential for Japan to capture the activities of individual actors over the long term and to conduct accurate threat analysis on what kind of activities are intended by the government agencies behind these Lazarus subgroups[[10].

Active cyber defence will also be important for Japan to conduct counter operations against the activities of APT actors in the future. Behind each subgroup, there should be an organization with formation, rules, and forms of command and control, and the effectiveness of various countermeasures should differ from one another.

Moreover, in addition to the effectiveness, some countermeasures may cause problems under international law[11], and it is extremely important to accurately capture the relationship between the actions and perpetrator of the counterparty and the background entity.

Reason 3: “Message” to the attackers

Many threat analysts are increasingly focusing on subgroup identification. This is partly for counter-tactical reasons, as discussed in Reason 1. However, it is also because the analysts believe that subgroups reflect the actual activities, organizational backgrounds, and resources of the real perpetrators, not just a virtual distinction.

There are only a limited number of cases where disclosing information about threat actors, such as public attribution or publishing analytical reports, influences their activities[12].

However, it is at least possible to make the attacker’s new tactics less likely to succeed or make them obsolete. We do not know to what extent APT actors actually pay attention to such information disclosures since they have rarely been verified so far. In any case, if the information is to be disclosed for the purpose of deterrence, such as in the form of public attribution, accurate subgroup identification and clarification would be a minimum requirement to deliver the message to the target (individual or organizational actors).

Most importantly, it should be noted that disclosure of accurate subgroup identification demonstrates the ability of the defenders and responders.

Case study of subgroups with overlapping tactics: contact targets on SNS and have them download a malicious npm package

As explained in a recent JPCERT/CC Eyes article, several subgroups started to contact individual engineers on LinkedIn or other SNS to have them download a malicious Python or npm package via PyPI or GitHub in their initial phase.

The following is a timeline of the activities of several subgroups that use same or similar tactics.

Relations between Moonstone Sleet and other subgroups

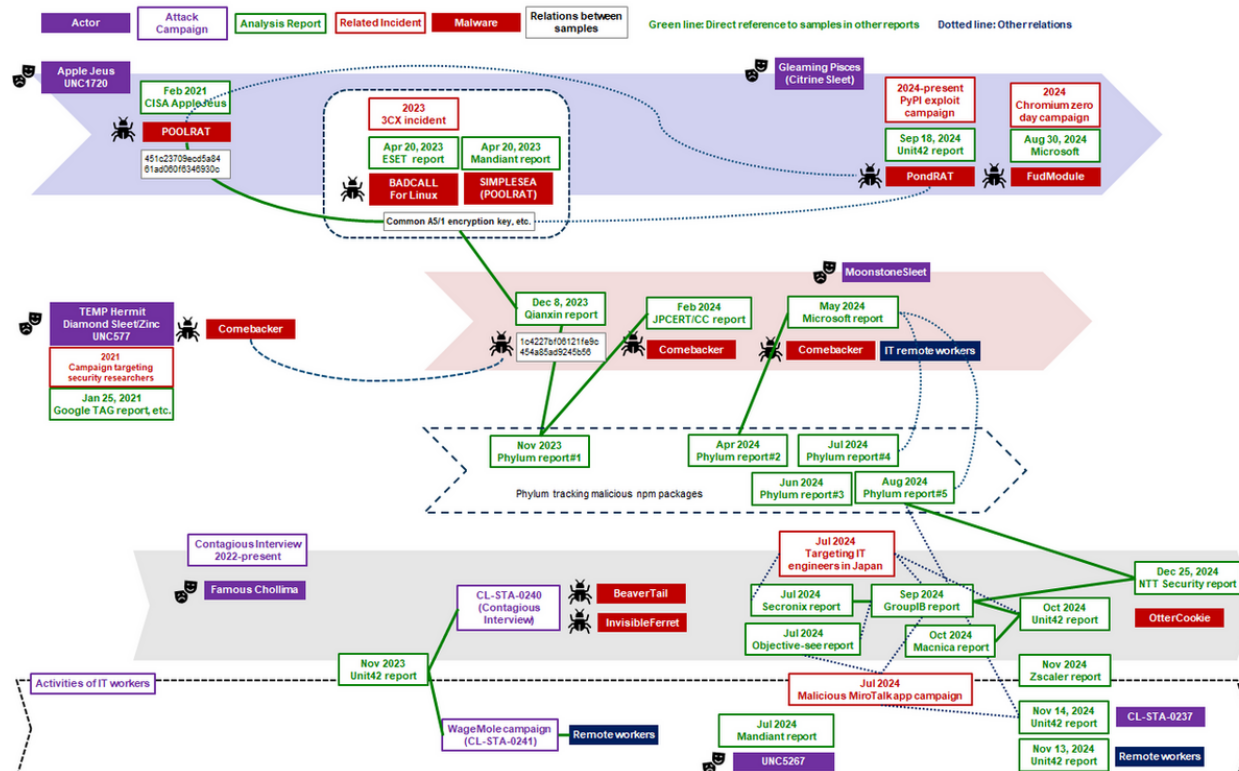


Figure 1: Multiple subgroups that contact their targets on SNS and have them download malicious packages

Moonstone Sleet

Target sectors/objectives: cryptocurrency theft, ransomware attacks, sensitive information in defense industry, etc., illegal income of IT workers

In February 2024, we published a JPCERT/CC Eyes blog article about a case in which this subgroup have their targets to download a malicious Python package via PyPI, and its analysis mentioned that the Comebacker was used[13]. In December 2023, Qianxin reported a similar sample[14], and later in May 2024, Microsoft announced that it was tracking the subgroup under the name Moonstone Sleet[15].

Microsoft says that this subgroup has no direct overlap with the subgroup which performs Contagious Interviews (discussed below), whose TTP is similar[16].

Comebacker was found in a 2021 campaign by TEMP.Hermit (labeled by Mandiant and also classified as UNC577 in the past)/Diamond Sleet (labeled by Microsoft and also classified as Zinc in the past)[17]. However, there is little information on the relations between the attack groups.

Gleaming Pisces (Citrine Sleet)

Relations to previously classified group: actors of Apple Jeus (UNC1720)

Target sectors: cryptocurrency businesses, individuals

Similar to Moonstone Sleet, this subgroup performs initial compromise using PyPI. Unit42 calls the group Gleaming Pisces, and Microsoft refers to it as Citrine Sleet. PondRAT (named by Unit42) used in the PyPI exploit attack campaign in 2024[18] has its origin in PoolRAT (name by Unit42) disclosed by CISA when it issued an alert about AppleJeus attack campaign in February 2021[19], and PoolRAT was also found in the supply chain attack on 3cx in March 2023[20].

These RATs share a common A5/1 encryption key, and it was also found in the previously mentioned Comebacker-like sample reported by Qianxin. In addition, FudModule, reportedly used by TEMP.Hermit/Diamond Sleet, was also found in Citrine Sleet's attack. Microsoft says that there are overlaps between Diamond Sleet and Citrine Sleet in their infrastructure and malware[21].

Contagious Interview (attack campaign)

Target sectors/objectives: cryptocurrency theft, illegal income of IT workers (Associated with Wagemole although it is a separate campaign.)

This attack activity was reported by Macnica in October 2024[22] and by NTT Security in December 2024[23]. The attackers contact IT engineers pretending to request job interviews. It was first reported by Unit42 in November 2023[24], and according to the company, the campaign has been active since 2022.

The attack campaign was allegedly conducted by FAMOUS CHOLLIMA, classified by CrowdStrike, but it remains unclear whether it is a subgroup of Lazarus or another group. In addition, this activity has been associated with Wagemole and CL-STA-0237 (the name used by Unit 42)[25], which are allegedly related to the activities of "IT workers", North Korean IT technical impersonators who work illegally at overseas IT companies to obtain foreign currency[26].

As mentioned earlier, Microsoft currently classifies Moonstone Sleet activity and Contagious Interview as separate activities. Phylum has been tracking the malicious npm packages used in both activities and has published a number of reports[27].

Reference: Summary of relationships among subgroups at the moment

In this article, I have described and compared the Moonstone Sleet activity, Contagious Interview attack campaign, and Gleaming Pisces (Citrine Sleet) activity. They all share the same initial attack vector: contact the target on SNS and then have them download a malicious npm package. The following is a summary of the activities of other Lazarus subgroups and the changes in the classification and the names used by security vendors over time.

I believe that the information will continue to change, with new subgroups emerging and security analysts making reclassifications[28]. In the future, we will try to create a system that captures and organizes such information in a dynamic and flexible manner.

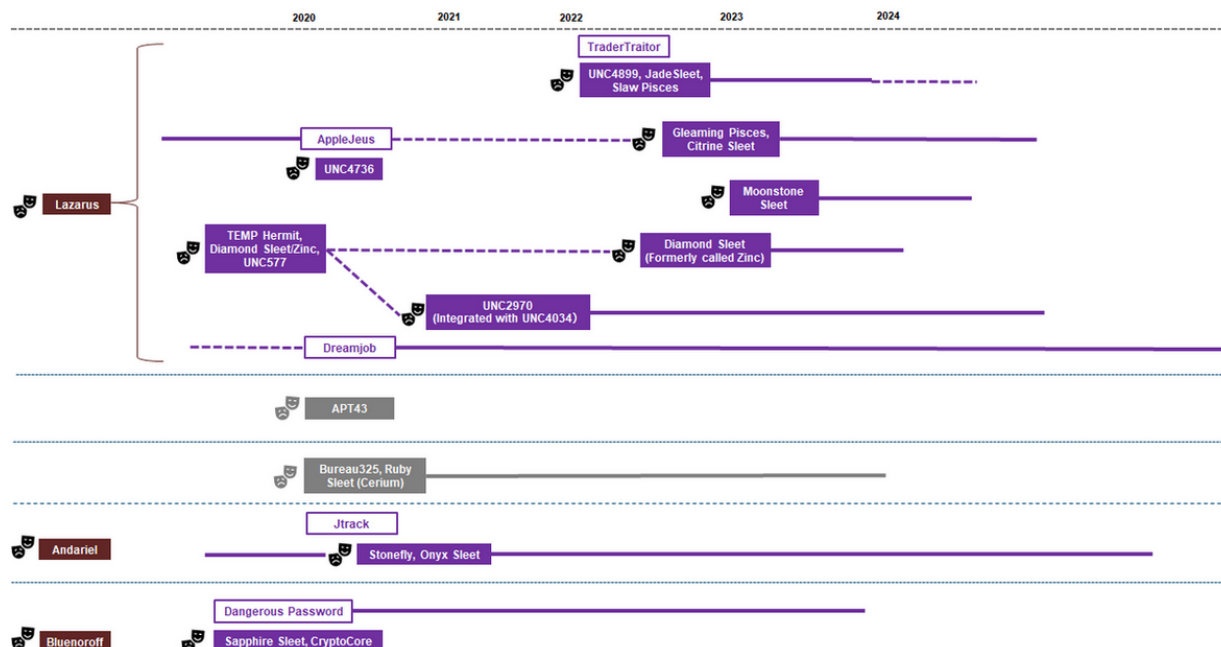


Figure 2: Transition of Lazarus subgroups

In conclusion

The term “attribution” has two concepts. One of them is a strict meaning used in international law and criminal procedure, and the other is traditionally used by the security community. I personally refer to the former as “hard” attribution, which includes the identification of individuals and organizations actually involved as well as the attribution of responsibility, and the latter as “soft” attribution, which covers virtual groupings such as actors/attack groups and profiling.

Even when there is insufficient evidence for “hard” attribution, “soft” attribution may be helpful in issuing appropriate alerts and providing countermeasure information. On the other hand, “hard” attribution is necessary for long-term countermeasures even when it is not feasible for technically timely responses.

There is not enough space here to cover a variety of technical and non-technical issues surrounding attribution, but I believe that “information disclosure” will be a key topic in the future. Disclosure of attribution results is an achievement for analysts in the private sector as well as an important tool for commercial businesses to demonstrate their expertise. While it is difficult for them to visualize the capabilities of products and services, reports of (soft) attribution can easily show their findings, which is important for maintaining the sound growth of the security market.

Meanwhile, attribution is also an achievement for government side. Aside from the arguments over the effectiveness of public attribution[29], it is a valuable opportunity for governments to demonstrate why they collect information on private victim organizations. In addition, as mentioned earlier, it is also a chance to demonstrate the capabilities as a country to their allies and adversaries.

However, in either position, prioritizing achievement and disclosing technically unreliable attribution results bring a number of negative consequences. The effectiveness of information disclosure should also be verified.

Most importantly, it should always be reminded that so-called “threat intelligence,” including attribution results, is not a product created solely by those who release the information. Behind the scenes, victim organizations and analysts involved in on-site response play an extremely important role. Information disclosure influences threat actors, and at the same time, it is also a highly complex activity that affects not only the alerted organizations but also various other parties, including the victim organizations, analysts, and product vendors. Attribution methodology is still in the process of development, and information disclosure involves a number of unresolved issues. I have repeatedly discussed various issues surrounding “information disclosure” in the past[30], and I will continue such discussions along with alerts and analytical reports.

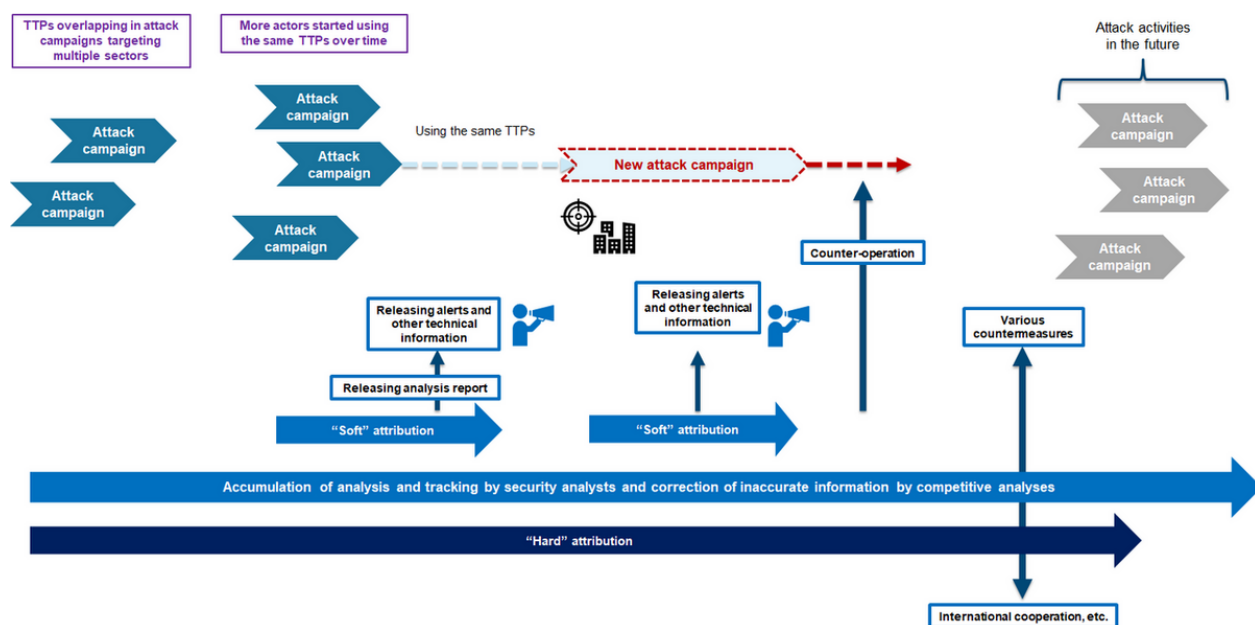


Figure 3: Timing of each attribution

Hayato Sasaki
(Translated by Takumi Nakano)

References

*Please note that the authors and titles are omitted due to the large number of references.

[1] This name first appeared in Operation Blockbuster, a joint analysis report led by Novetta and involving a number of security vendors in 2016. It was initially described as “Lazarus Group.”

[2] Attack campaign: Attack activities conducted against a specific organization or sector for a certain period of time using a specific attack method or infrastructure. (Reference: 2024年3月「攻撃技術情報の取扱い・活用手引き」(サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局(経済産業省、JPCERT/CC)) [Japanese only]

[3] https://jsac.jpCERT.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki_en.pdf, JSAC2024 https://jsac.jpCERT.or.jp/archive/2024/pdf/JSAC2024_2_6_hayato_sasaki_en.pdf, National Institute for Defense Studies (NIDS) Commentary <https://www.nids.mod.go.jp/publication/commentary/pdf/commentary346.pdf> [Japanese only]

[4] These are slightly old reports, but they analyze the organization and overlaps of subgroups based on the clustering of malware clusters. <https://securelist.com/lazarus-threatneedle/100803/>, <https://vblogalhost.com/uploads/VB2021-Park.pdf>

[5] https://blogs.jpCERT.or.jp/en/2025/01/initial_attack_vector.html

[6] <https://cloud.google.com/blog/topics/threat-intelligence/mapping-dprk-groups-to-government/?hl=en>, “Final report of the Panel of Experts submitted pursuant to resolution 2627 (2022)”, https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

[7] CISTECジャーナル2023年5月号 JPCERT/CC 佐々木勇人「2022年度国連北朝鮮制裁委員会報告書から北朝鮮関連のサイバー攻撃動向を読み解く—新たな攻撃グループ登場の背景とその動向について—」 [Japanese only]

[8] <https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage?hl=en>

[9] When I once explained the Lazarus subgroups to a member of an international organization, I was told, “Whatever the subgroups are, they are already attributed (to a certain government) for their illegal activities, and that should be enough.”

[10] Until 2023, such tracking and reporting was conducted at the expert panel of the United Nations Security Council Sanctions Committee on North Korea. The panel collected information like those covered in this article from various security vendor reports and analyzed threats by group and government agencies considered behind such groups. However, as news media reported, the expert panel’s activities ended in FY2023.

[11] Reference: 中谷和弘, 河野桂子, 黒崎将広『サイバー攻撃の国際法 タリン・マニュアル2.0の解説(増補版)』, 中村和彦『越境サイバー侵害行動と国際法—国家実行から読み解く規律の行方—』ほか [Japanese only]

[12] For an explanation on the limitations of the punitive deterrence approach centered on public attribution in the U.S. and the history of the transition to a cost-imposition approach, please refer to the following article of the National Institute for Defense Studies (NIDS) Commentary. 佐々木勇人, 瀬戸崇志『サイバー攻撃対処における攻撃「キャンペーン」概

念と「コスト賦課アプローチ」——近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から』 <https://www.nids.mod.go.jp/publication/commentary/pdf/commentary346.pdf>
[Japanese only]

[13] https://blogs.jpccert.or.jp/en/2024/02/lazarus_pypi.html

[14] <https://ti.qianxin.com/blog/articles/Analysis-of-Suspected-Lazarus-APT-Q-1-Attack-Sample-Targeting-npm-Package-Supply-Chain-EN/>

[15] <https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/>

[16] <https://thehackernews.com/2024/05/microsoft-uncovers-moonstone-sleet-new.html>

[17] <https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/>

[18] <https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/>

[19] <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a>

[20] <https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/>

[21] <https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/>

[22] <https://security.macnica.co.jp/blog/2024/10/-contagious-interview.html>

[23] https://jp.security.ntt/tech_blog/en-contagious-interview-ottercookie

[24] <https://unit42.paloaltonetworks.jp/two-campaigns-by-north-korea-bad-actors-target-job-hunters/>

[25] <https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/>

[26] <https://ofac.treasury.gov/recent-actions/20220516>

[27] <https://blog.phylum.io/crypto-themed-npm-packages-found-delivering-stealthy-malware/>

[28] We mentioned that Mandiant reclassified it as APT43 in March 2023. The activities of this actor were previously often reported and classified as those of Kimsuky and Thallium. However, after years of tracking, it was reanalyzed, reclassified, and then announced as APT43. <https://cloud.google.com/blog/ja/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage>

[29] For the studies based on the argument that deterrence approaches through public attribution and economic sanctions assuming so-called punitive deterrence had little success, refer to the following. Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “Cyber Persistence Theory: Redefining National Security in Cyberspace”, Robert Chesney and Max Smeets Eds, “Deter, Disrupt, or Deceive Assessing Cyber Conflict as an Intelligence Contest”

[30] https://blogs.jpcert.or.jp/ja/2022/04/sharing_and_disclosure.html,
<https://blogs.jpcert.or.jp/ja/2023/05/cost-and-effectiveness-of-alerts.html>,
<https://blogs.jpcert.or.jp/ja/2023/08/incident-disclosure-and-coordination.html>,
<https://blogs.jpcert.or.jp/ja/2023/12/leaks-and-breaking-trust.html>
[Japanese only]

-
- [Email](#)

Author



佐々木 勇人 (Hayato Sasaki)

Threat Analyst. Manager, Early Warning Group, JPCERT/CC. Director of Policy Affairs. Part-time researcher in the Cyber Security Research Division, National Institute for Defense Studies(NIDS) since May 2024.

Was this page helpful?

0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

Related articles

-

Beware of Contacts through LinkedIn: They Target Your Organization's Property, Not Yours

-

New Malicious PyPI Packages used by Lazarus

-

YamaBot Malware Used by Lazarus

-

VSingl malware that obtains C2 server information from GitHub

- ```

v7 = mal_check_count(http_strc->url);
/*(void (__stdcall __)(int, int, int, int __))o_InternetCrackr3A[0]](http_strc->url, v7,
if (v6 == 1)
{
 wsprintfA(
 &v20,
 "Content-Type: multipart/form-data; boundary=%s\r\n",
 (const char *)http_strc->http_bonday_str);
 if (!v20 || !v21)
 {
 if (v20)
 {
 wsprintfA(
 &v22,
 "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
 (const char *)http_strc->http_bonday_str,
 (const char *)http_strc->http_name1,
 (const char *)http_strc->http_body_text);
 }
 else
 {
 wsprintfA(
 &v22,
 "--%s\r\n"
 "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
 "Content-Type: image/png\r\n"
 "\r\n",
 (const char *)http_strc->http_bonday_str,
 (const char *)http_strc->http_name,
 (const char *)http_strc->http_filename);
 }
 }
 else
 {
 wsprintfA(
 &v22,
 "--%s\r\n"
 "Content-Disposition: form-data; name=\"%s\"\r\n"
 "\r\n"
 "%s\r\n"
 "--%s\r\n"
 "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
 "Content-Type: image/png\r\n"
 "\r\n",
 (const char *)http_strc->http_bonday_str,
 (const char *)http_strc->http_name1,
 (const char *)http_strc->http_body_text,
 (const char *)http_strc->http_bonday_str,
 (const char *)http_strc->http_name,
 (const char *)http_strc->http_filename);
 }
 wsprintfA(&v33, "\r\n--%s--\r\n", (const char *)http_strc->http_bonday_str);
 v27 = mal_check_count((int)&v22);
 v28 = mal_check_count((int)&v33);

```

## Lazarus Attack Activities Targeting Japan (VSingle/ValeforBeta)

[Back](#)

[Top](#)

[Next](#)