ADVERSARY

Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company

TOM HEGEL / AUGUST 7, 2023

By Tom Hegel and Aleksandar Milenkoski

Executive Summary

- SentinelLabs identified an intrusion into the Russian defense industrial base, specifically a missile engineering organization NPO Mashinostroyeniya.
- Our findings identify two instances of North Korea related compromise of sensitive internal IT infrastructure within this same Russian DIB organization, including a specific email server, alongside use of a Windows backdoor dubbed OpenCarrot.
- Our analysis attributes the email server compromise to the ScarCruft threat actor. We also identify the separate use of a Lazarus Group backdoor for compromise of their internal network.
- At this time, we cannot determine the potential nature of the relationship between the two threat actors. We acknowledge a potential sharing relationship between the two DPRK-affiliated threat actors as well as the possibility that tasking deemed this target important enough to assign to multiple independent threat actors.

Background

North Korean threat actors have caught our attention over the past year, providing us with fruitful insight into a variety of campaigns, such as new reconnaissance tools, (multiple) new supply chain intrusions, elusive multi-platform targeting, and new sly social engineering tactics. To add to that list, let's take a look at an intrusion into what might be considered a highly desirable strategic espionage mission – supporting North Korea's contentious missile program.

The Target Organization

While conducting our usual hunting and tracking of suspected-North Korean threat actors, we identified a leaked email collection containing an implant with characteristics related to previously reported DPRK-affiliated threat actor campaigns. A thorough investigation of the email archive revealed a larger intrusion, not fully recognized at the time by the compromised organization.

The victim organization is NPO Mashinostroyeniya (JSC MIC Mashinostroyenia, NPO Mash), a leading Russian manufacturer of missiles and military spacecraft. The organization's parent company is JSC Tactical Missiles Corporation KTRV (Russian: АО «Корпорация Тактическое Ракетное Вооружение», КТРВ). NPO Mashinostroyeniya is a sanctioned entity that possesses highly confidential intellectual property on sensitive missile technology currently in use and under development for the Russian military.

We are highly confident that the emails related to this activity originate from the victim organization. Furthermore, there are no discernible signs of manipulation or technically verifiable inaccuracies present in these emails. It's essential to highlight that the leaked data comprises a substantial volume of emails unrelated to our current research scope. This suggests that the leak was likely accidental or resulted from activity unrelated to the specific intrusion under scrutiny in our investigation. However, this collection provides valuable background context for our understanding of their internal network design, security gaps, and even cases of activity by other attackers.

Example of unrelated email alerts from Russian CERT to NPO Mash

In mid-May 2022, roughly a week prior to Russia vetoing a U.N. resolution to impose new sanctions on North Korea for intercontinental ballistic missile launches that could deliver nuclear weapons, the victim organization internally flagged the intrusion. Internal NPO Mashinostroyeniya emails show IT staff exchanged discussions highlighting questionable communications between specific processes and unknown external infrastructure. The same day, the NPO Mashinostroyeniya staff also identified a suspicious DLL file present in different internal systems. The month following the intrusion, NPO Mashinostroyeniya engaged with their AV solution's support staff to determine why this and other activity was not detected.

Following an examination of the emails and an in-depth investigation into the two separate sets of suspicious activity, we have successfully established a correlation between each cluster of activity and a respective threat actor amounting to a more significant network intrusion than the victim organization realized.

North Korean Overlap

During our investigation, we identified the suspicious file in question to be a version of the OpenCarrot Windows OS backdoor, previously identified by IBM XForce as part of Lazarus group activities. As a feature-rich, configurable, and versatile backdoor, the malware is a strong enabler of the group's operations. With a wide range of supported functionality, OpenCarrot enables full compromise of infected machines, as well as the coordination of multiple infections across a local network. The OpenCarrot variant we analyzed supports proxying C2 communication through the internal network hosts and directly to the external server, which supports the strong possibility of a network-wide compromise.

Additionally, we discovered the suspicious network traffic discussed in emails is the compromise of the business' Linux email server, hosted publicly at `vpk.npomash[.]ru` (`185.24.244[.]11`). At time of discovery, the email server was beaconing outbound to infrastructure we now attribute to the ScarCruft threat actor. ScarCruft is commonly attributed to North Korea's state-sponsored activity, targeting high value individuals and organizations near-globally. The group is also referred to as Inky Squid, APT37, or Group123, and often showcases a variety of technical capabilities for their intrusions. While we are unable to confirm the initial access method and implant running on the email server at time of discovery, we link malware loading tools and techniques involving this set of infrastructure to those seen in previously reported ScarCruft activity using the RokRAT backdoor.

This intrusion gives rare insight into sensitive DPRK cyberespionage campaigns, and an opportunity to expand our understanding of the relationship and goals between various North Korean cyber threat actors. It also highlights a potential rift in relations between Russia and North Korea, considering their growing relationship.

This engagement establishes connections between two distinct DPRK-affiliated threat actors, suggesting the potential for shared resources, infrastructure, implants, or access to victim networks. Moreover, we acknowledge the possibility that the assigned task of an intrusion into NPO Mashinostroyeniya might have warranted targeting by multiple autonomous threat actors due to its perceived significance.

OpenCarrot Backdoor Activity

The OpenCarrot sample we analyzed is implemented as a Windows service DLL file, intended to execute in a persistent manner. In line with typical practices of the Lazarus group, OpenCarrot is subject to continuous, not necessarily incremental, changes. The file has a compilation timestamp of Wednesday, Dec. 01, 2021. Although the timestamp could have been manipulated by the threat actors, given the proximity to the May 2022 suspected intrusion date, it's likely that the timestamp is authentic. Our confidence in this assessment also increases through the infrastructure analysis below.

The OpenCarrot variant we analyzed implements over 25 backdoor commands with a wide range of functionality representative of Lazarus group backdoors. In this case, supported functionality includes:

- Reconnaissance: File and process attribute enumeration, scanning and ICMP-pinging hosts in IP ranges for open TCP ports and availability.
- Filesystem and process manipulation: Process termination, DLL injection, and file deletion, renaming, and timestomping.
- Reconfiguration and connectivity: Managing C2 communications, including terminating existing and establishing new comms channels, changing malware configuration data stored on the filesystem, and proxying network connections.

The OpenCarrot sample displays further characteristics often seen among Lazarus Group malware.

Its backdoor commands are indexed by consecutive integers, a common trait of Lazarus group malware. In addition to integer-indexed commands, the developers implement string-indexed sub-commands.

Backdoor command indexing

Keeping with their typical mode of operations, the malware is intended to execute as a Windows service and exports the `ServiceMain` function.

OpenCarrot implements executable code in a section named `.vlizer` indicating the use of code virtualization for obfuscation. The `.vlizer` section is associated with the Oreans Code Virtualizer code protection platform, a functional subset of Themida. As previously observed in Themida-protected Lazarus group malware, some code segments of the OpenCarrot variant we analyzed are not protected.

As part of its initialization process, OpenCarrot ingests configuration data from a file whose name is composed of the service name in whose context the malware executes and the `dll.mui` extension. The configuration data contains encryption-protected C2 information. The use of configuration files with the `dll.mui` extension is a long-standing theme among Lazarus group malware, mimicking a lesser-known standard Windows file extension used to denote application resources and externalities.

OpenCarrot implements relatively long sleep time periods. To avoid remaining idle for too long whenever the user of the infected machine is active, OpenCarrot implements a mechanism to exit its sleep state earlier than instructed. If the malware is instructed to sleep for 15 seconds or more, it then monitors in 15 second intervals for the insertion of new drives, such as USBs. If such an event occurs, the malware exits its sleep state before the configured sleep time elapses. A variant of this technique has been previously observed in the Pebbledash malware.

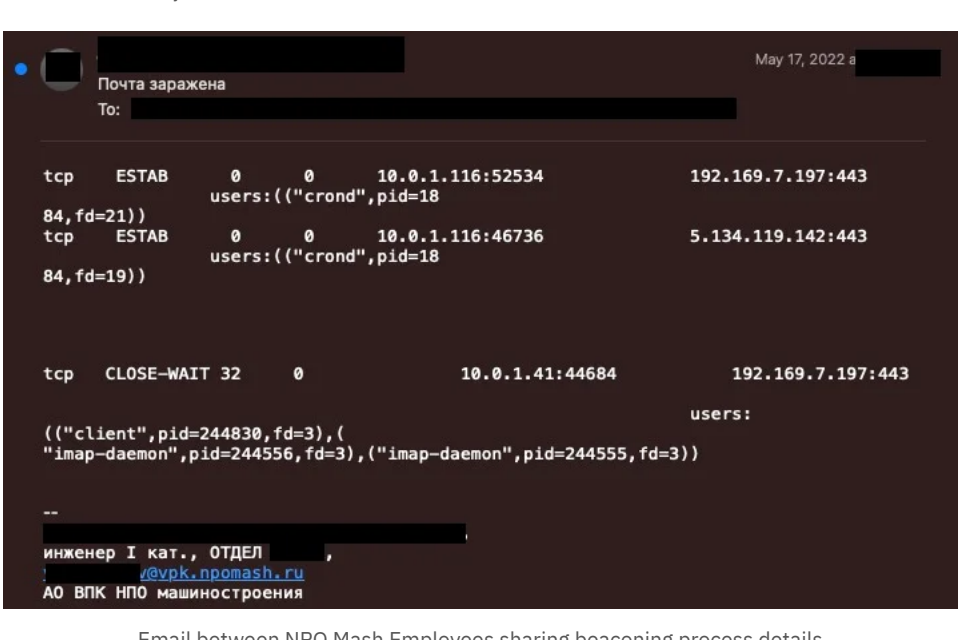
Disk drive monitoring

OpenCarrot's versatility is evident with its support of multiple methods for communicating with C2 servers. The malware dispatches commands for execution based on attacker-provided data originating not only from remote C2 servers, but also from local processes through named pipes and incoming connections to a TCP port on which OpenCarrot listens.

Infrastructure Analysis

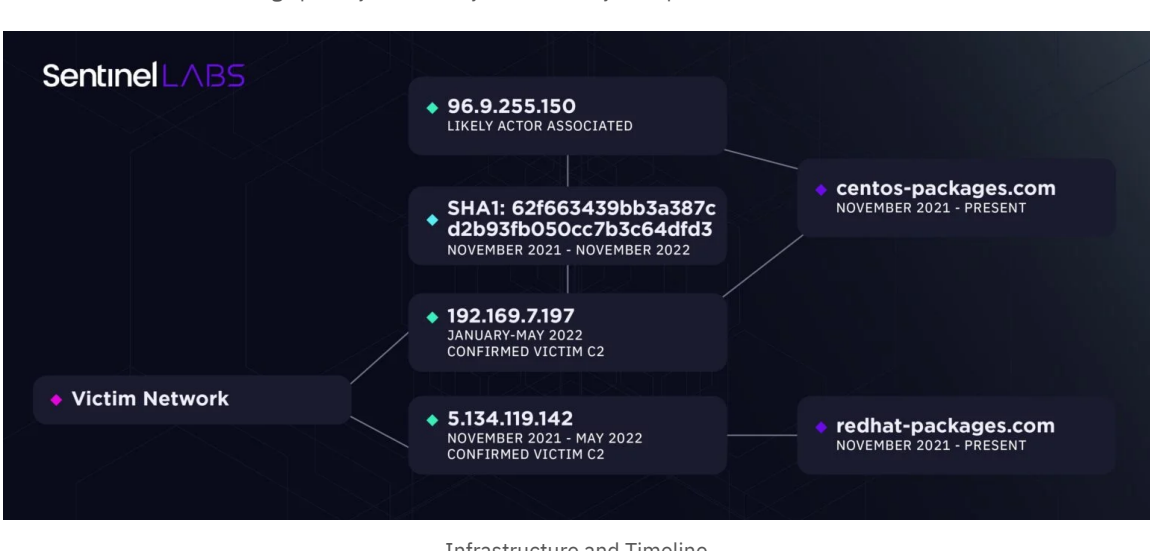
North Korean-nexus of threat actors are known for not maintaining the OPSEC of their campaigns. A characteristic lack of segmentation allows researchers to amass unique insights across a variety of unreported activity. Infrastructure connections in particular often allow us to track the evolution of their campaigns over long periods of time.

We link the NPO Mashinostroyeniya email discussing suspicious networking communication as active C2 communications occurring through `192.169.7[.]197`, and `5.134.119[.]142`. The internal host, the organization's Red Hat email server, was actively compromised and in communication with the attackers malicious infrastructure. A review of all details concludes the threat actor was likely operating on this server for an extensive period of time prior to the internal team's discovery.



Email between NPO Mash Employees sharing beaconing process details

This set of malicious infrastructure was served via CrownCloud (Australia) and OhzCloud (Spain) VPS hosting providers. During the intrusion, the two domains `centos-packages[.]com` and `redhat-packages[.]com` were resolving to those C2 IP addresses. Our assessment is that this particular cluster of infrastructure became active in November 2021, and was immediately paused the same day of NPO Mashinostroyeniya's intrusion discovery in May 2022. This finding may indicate the intrusion was high priority and closely monitored by the operators.

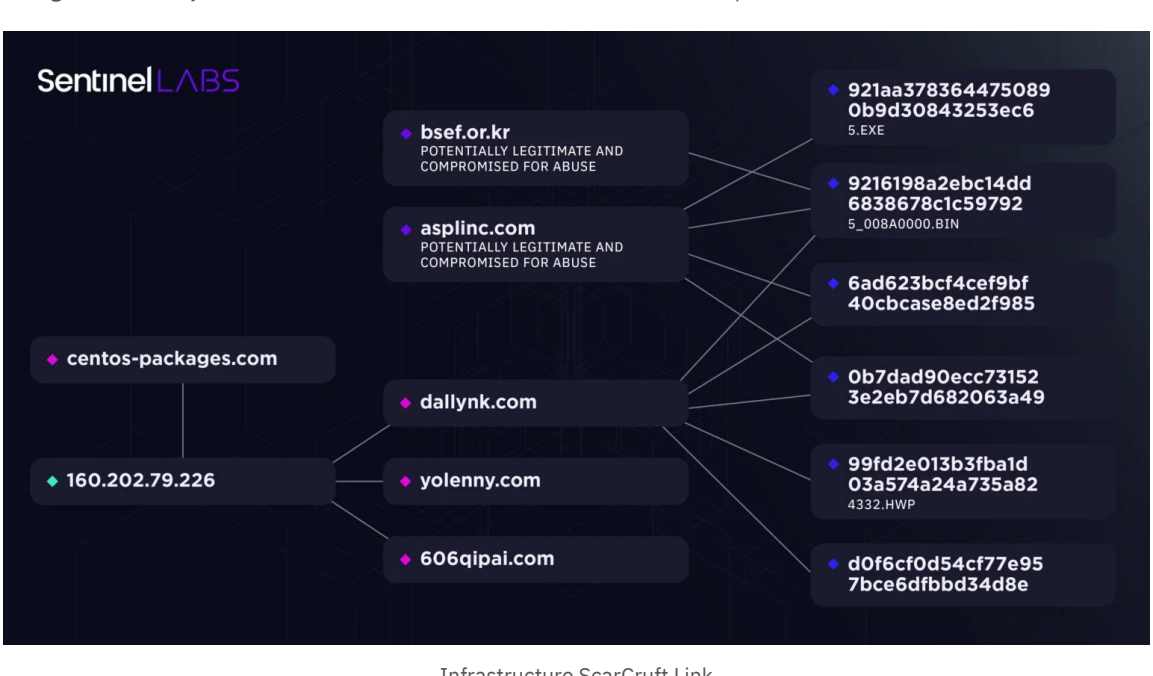


Infrastructure and Timeline

A relationship can be observed between this cluster of activity and a more recent ScarCruft campaign. Following the intrusion operators immediately killing their C2 server when the suspicious traffic was identified by the victim in May 2022, the `centos-packages[.]com` domain use was paused until it began resolving to `160.202.79[.]226` in February 2023. `160.202.79[.]226` is a QuickPacket VPS (US) hosting IP also being shared with the domain `dallynk[.]com` and others used by ScarCruft for malware delivery and C2 initiated through malicious documents.

Further, the domain `dallynk[.]com` follows the theme we've previously reported in which DPRK-associated threat actors impersonate Daily NK, a prominent South Korean online news outlet that provides independent reporting on North Korea.

The collection of activity stemming from the `dallynk[.]com` domain contains malware loading tools and techniques matching those seen in previously reported ScarCruft activity using the RokRAT backdoor. Similarities in server configuration history can also link to lower-confidence BlueNoroff relationships.



Infrastructure ScarCruft Link

While conducting this research, we first publicly identified the link between the JumpCloud intrusion and North Korean threat actors. One detail that immediately struck us was the domain theme similarities, such as `centos-pkg[.]org` / `centos-repos[.]org` (JumpCloud), and `centos-packages[.]com` (NPO Mash). This detail is superficial and not strong enough alone to base direct clustering, but alongside other aforementioned North Korean threat actor connections, it stokes our curiosity for the particulars of the threat actors' infrastructure creation and management procedures.

Lastly, we advise particular care into how this infrastructure is further attributed when reviewed historically. For example, the C2 server IP address `192.169.7[.]197` was used between January and May 2022 by the DPRK linked threat actor; however, that same IP was used by the Arid Viper/Desert Falcon APT in 2020, first reported by Meta Threat Investigators. Arid Viper is associated with Palestinian interests, conducting activity throughout the Middle East. We assess the Arid Viper activity is unrelated to our findings and the overlap of infrastructure is simply an example of commonly reused dubious VPS hosting providers. This further highlights the importance of associating active timeframes with IP-based indicators.

Conclusion

With a high level of confidence, we attribute this intrusion to threat actors independently associated with North Korea. Based on our assessment, this incident stands as a compelling illustration of North Korea's proactive measures to covertly advance their missile development objectives, as evidenced by their direct compromise of a Russian Defense-Industrial Base (DIB) organization.

The convergence of North Korean cyber threat actors represents a profoundly consequential menace warranting comprehensive global monitoring. Operating in unison as a cohesive cluster, these actors consistently undertake a diverse range of campaigns motivated by various factors. In light of these findings, it becomes crucial to address and mitigate this threat with utmost vigilance and strategic response.

Indicators

MD5:
9216198a2ebc14dd68386738c1c59792
6ad6232bcf4cef9bf40cbcae8ed2f985
d0f6cf0d54cf77e957bce6dfbbd34d8e
921aa3783644750890b9d30843253ec6
99fd2e013b3fba1d03a574a24a735a82
0b7dad90ecc731523e2eb7d682063a49
516beb7da7f2a8b85cb170570545da4b

SHA1:
07b494575d548a83f0812ceba6b8d567c7ec86ed
2217c29e5d5ccfcf58d2b6d9f5e250b687948440
246018220a4f4f3d20262b7333caf323e1c77d2e
8b6ffa56ca5bea5b406d6d8d6ef532b4d36d090f
90f52b6d077d508a23214047e680dded320ccf4e
f483c33acf0f2957da14ed422377387d6cb93c4d
f974d22f74b0a105668c72dc100d1d9fcc8c72de

redhat-packages[.]com
centos-packages[.]com
dallynk[.]com
yolenny[.]com
606qipai[.]com
asplinc[.]com
bsef.or[.]kr

192.169.7[.]197
160.202.79[.]226
96.9.255[.]150
5.134.119[.]142

DPRK

TOM HEGEL

Tom Hegel is a Principal Threat Researcher with SentinelOne. He comes from a background of detection and analysis of malicious actors, malware, and global events with an application to the cyber domain. His past research has focused on threats impacting individuals and organizations across the world, primarily targeted attackers.