JumpCloud Intrusion | Attacker Infrastructure Links Compromise to North Korean APT Activity

Tom Hegel

In recent news, the cloud-based IT management service JumpCloud publicly shared details gathered from the investigation into an intrusion on their network. Alongside the updated details, the organization shared a list of associated indicators of compromise (IOCs), noting attribution to an unnamed "sophisticated nation-state sponsored threat actor".

Reviewing the newly released indicators of compromise, we associate the cluster of threat activity to a North Korean state sponsored APT. The IOCs are linked to a wide variety of activity we attribute to DPRK, overall centric to the supply chain targeting approach seen in previous campaigns.

Infrastructure Analysis

Based on the IOCs shared by JumpCloud, we were able to analyze the threat actor's infrastructure. The following list is our starting point:

Domains

alwaysckain.com	canolagroove.com	centos-pkg.org
centos-repos.org	datadog-cloud.com	datadog-graph.com
launchruse.com	nomadpkg.com	nomadpkgs.com
primerosauxiliosperu.com	reggedrobin.com	toyourownbeat.com
zscaler-api.org		

IP Addresses

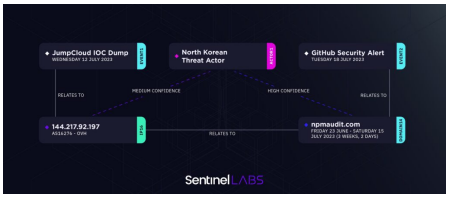
51.254.24.19	185.152.67.39	70.39.103.3
66.187.75.186	104.223.86.8	100.21.104.112
23.95.182.5	78.141.223.50	116.202.251.38
89.44.9.202	192.185.5.189	162.241.248.14
179.43.151.196	45.82.250.186	162.19.3.23
144.217.92.197	23.29.115.171	167.114.188.40
91.234.199.179		

By mapping out this infrastructure, it is possible to show the links between the diverse set of IP addresses and pick up various patterns.

Triggering alerts on `192.185.5[.]189` alone is ill advised, as it's a shared hosting server for many domains and not an indicator of malicious activity by itself. However, `toyourownbeat[.]com` shares an SSL certificate with `skylerhaupt[.]com`, indicating a potential relationship in owner.

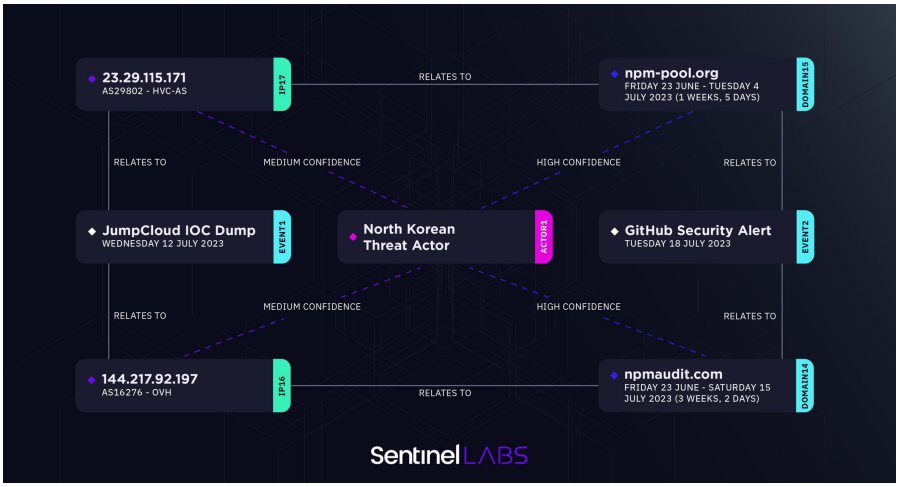
The indicator `144.217.92[.]197` shared by JumpCloud does not host any domains listed, but we can see one similar: `npmaudit[.]com`, which was just recently shared by GitHub associated with an alert of their own. Based on

public details available as of this writing, it's unclear if the GitHub alert originated from the JumpCloud incident or if they are separate efforts by the same attacker.



Infrastructure Map Noting JumpCloud links

Moving on to IP address `23.29.115[.]171`, we can see through PDNS data that the domain `npm-pool[.]org` is related. Notably, this domain is quite similar to the NPM theme of domains shared in the GitHub alert.



Infrastructure Map Noting JumpCloud and GitHub Overlap

While the following is not a strong indicator of attribution alone, it's noteworthy that specific patterns in how the domains are constructed and used follow a similar pattern to other DPRK linked campaigns we track. Indicators with suspected actor association, but unverified as of this writing, include `junknomad[.]com` and `insatageram[.]com` (registered with `jeanettar671belden[@]protonmail[.]com`).

Additional pivots of potential interest can be made through other IPs, including `167.114.188[.]40`, and to a variety of low confidence attacker-associated infrastructure.

Following the profile of the associated infrastructure from both the JumpCloud intrusion and the GitHub security alert, we can expand to further associated threat activity. For example, we can see clear links to other NPM and "package" themed infrastructure we associate with high to medium confidence, as noted in the list below. This list further expands thanks to the findings and blog from Phylum in late June.

```
npmjscloud[.]com
npmcloudjs[.]com
nodepkg[.]com
dadiwarm[.]com
216.189.145[.]247
npmjsregister[.]com
142.44.178[.]222
tradingprice[.]net
bi2price[.]com
```

Trivial pivots from here can be made to similar behaving infrastructure linked to TraderTraitor, as noted by GitHub, plus those of AppleJeus such as Celas Trade Pro via `celasllc[.]com`.

Conclusion

It is evident that North Korean threat actors are continuously adapting and exploring novel methods to infiltrate targeted networks. The JumpCloud intrusion serves as a clear illustration of their inclination towards supply chain targeting, which yields a multitude of potential subsequent intrusions. The DPRK demonstrates a profound understanding of the benefits derived from meticulously selecting high-value targets as a pivot point to conduct supply chain attacks into fruitful networks.