

Active North Korean campaign targeting security researchers

blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/

Clement Lecigne

September 7, 2023



Threat Analysis Group

In January 2021, Threat Analysis Group (TAG) publicly disclosed a campaign from government backed actors in North Korea who used 0-day exploits to target security researchers working on vulnerability research and development. Over the past two and a half years, TAG has continued to track and disrupt campaigns from these actors, finding 0-days and protecting online users. Recently, TAG became aware of a new campaign likely from the same actors based on similarities with the previous campaign. TAG is aware of at least one actively exploited 0-day being used to target security researchers in the past several weeks. The vulnerability has been reported to the affected vendor and is in the process of being patched.

While our analysis of this campaign continues, we are providing an early notification of our initial findings to warn the security research community. We hope this post will remind security researchers that they could be targets of government backed attackers and to stay vigilant of security practices.

Security researcher targeting

Similar to the previous campaign TAG reported on, North Korean threat actors used social media sites like X (formerly Twitter) to build rapport with their targets. In one case, they carried on a months-long conversation, attempting to collaborate with a security researcher on topics of mutual interest. After initial contact via X, they moved to an encrypted messaging app such as Signal, WhatsApp or Wire. Once a relationship was developed with a targeted researcher, the threat actors sent a malicious file that contained at least one 0-day in a popular software package.

 image of an actor-controlled X / Twitter profile

Actor-controlled Twitter profile


Upon successful exploitation, the shellcode conducts a series of anti-virtual machine checks and then sends the collected information, along with a screenshot, back to an attacker-controlled command and control domain. The shellcode used in this exploit is constructed in a similar manner to shellcode observed in previous North Korean exploits.

The vulnerability has been reported to the affected vendor and is in the process of being patched. Once patched, we will release additional technical details and analysis of the exploits involved in line with our [disclosure policies](#).

Potential secondary infection vector

In addition to targeting researchers with 0-day exploits, the threat actors also developed a standalone Windows tool that has the stated goal of 'download debugging symbols from Microsoft, Google, Mozilla and Citrix symbol servers for reverse engineers.' The [source code](#) for this tool was first published on GitHub on September 30, 2022, with several updates being released since. On the surface, this tool appears to be a useful utility for quickly and easily downloading symbol information from a number of different sources. [Symbols](#) provide additional information about a binary that can be helpful when debugging software issues or while conducting vulnerability research.

But the tool also has the ability to download and execute arbitrary code from an attacker-controlled domain. If you have downloaded or run this tool, TAG recommends taking precautions to ensure your system is in a known clean state, likely requiring a reinstall of the operating system.

 screenshot of Github repository for GetSymbol

Github repository for GetSymbol

Protecting the community

As part of our efforts to combat serious threat actors, TAG uses the results of our research to improve the safety and security of Google's products. Upon discovery, all identified websites and domains are added to Safe Browsing to protect users from further exploitation. TAG also sends all targeted Gmail and Workspace users government-backed attacker alerts notifying them of the activity and encourages potential targets to enable Enhanced Safe Browsing for Chrome and ensure that all devices are updated.

We are committed to sharing our findings with the security community to raise awareness, and with companies and individuals that might have been targeted by these activities. We hope that improved understanding of tactics and techniques will enhance threat hunting capabilities and lead to stronger user protections across the industry.

Actor controlled sites and accounts

GetSymbol:

- [https://github\[.\]com/dbgsymbol/](https://github[.]com/dbgsymbol/)
- [https://dbgsymbol\[.\]com](https://dbgsymbol[.]com)
- 50869d2a713acf406e160d6cde3b442fafa7cfe1221f936f3f28c4b9650a66e9
- 0eedfd4ab367cc0b6ab804184c315cc9ce2df5062cb2158338818f5fa8c0108e
- 2ee435bdafacfd7c5a9ea7e5f95be9796c4d9f18643ae04dca4510448214c03c
- 5977442321a693717950365446880058cc2585485ea582daa515719c1c21c5bd

C2 IPs/Domains:

- 23.106.215[.]105
- www.blgbeach[.]com

X (formerly Twitter) Accounts

https://twitter.com/Paul091_

Wire Accounts

@paul354

Mastodon Account:

https://infosec.exchange/@paul091_

POSTED IN:

Threat Analysis Group