

New campaign targeting security researchers

 blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

Adam Weidemann

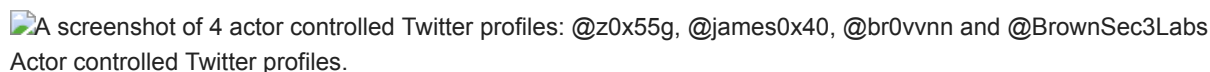
January 25, 2021



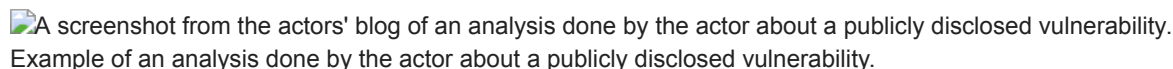
Threat Analysis Group

Over the past several months, the Threat Analysis Group has identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attribute to a government-backed entity based in North Korea, have employed a number of means to target researchers which we will outline below. We hope this post will remind those in the security research community that they are targets to government-backed attackers and should remain vigilant when engaging with individuals they have not previously interacted with.

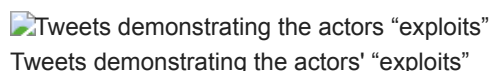
In order to build credibility and connect with security researchers, the actors established a research blog and multiple Twitter profiles to interact with potential targets. They've used these Twitter profiles for posting links to their blog, posting videos of their claimed exploits and for amplifying and retweeting posts from other accounts that they control.

A screenshot of 4 actor controlled Twitter profiles: @z0x55g, @james0x40, @br0vnn and @BrownSec3Labs
Actor controlled Twitter profiles.

Their blog contains write-ups and analysis of vulnerabilities that have been publicly disclosed, including “guest” posts from unwitting legitimate security researchers, likely in an attempt to build additional credibility with other security researchers.

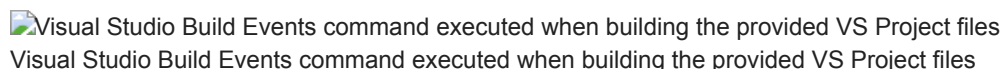
A screenshot from the actors' blog of an analysis done by the actor about a publicly disclosed vulnerability.
Example of an analysis done by the actor about a publicly disclosed vulnerability.

While we are unable to verify the authenticity or the working status of all of the exploits that they have posted videos of, in at least one case, the actors have faked the success of their claimed working exploit. On Jan 14, 2021, the actors shared via Twitter a YouTube video they uploaded that proclaimed to exploit CVE-2021-1647, a recently patched Windows Defender vulnerability. In the video, they purported to show a successful working exploit that spawns a cmd.exe shell, but a careful review of the video shows the exploit is fake. Multiple comments on YouTube identified that the video was faked and that there was not a working exploit demonstrated. After these comments were made, the actors used a second Twitter account (that they control) to retweet the original post and claim that it was “not a fake video.”

Tweets demonstrating the actors' “exploits”
Tweets demonstrating the actors' “exploits”

Security researcher targeting

The actors have been observed targeting specific security researchers by a novel social engineering method. After establishing initial communications, the actors would ask the targeted researcher if they wanted to collaborate on vulnerability research together, and then provide the researcher with a Visual Studio Project. Within the Visual Studio Project would be source code for exploiting the vulnerability, as well as an additional DLL that would be executed through Visual Studio Build Events. The DLL is custom malware that would immediately begin communicating with actor-controlled C2 domains. An example of the VS Build Event can be seen in the image below.

Visual Studio Build Events command executed when building the provided VS Project files
Visual Studio Build Events command executed when building the provided VS Project files

In addition to targeting users via social engineering, we have also observed several cases where researchers have been compromised after visiting the actors' blog. In each of these cases, the researchers have followed a link on Twitter to a write-up hosted on [blog.br0vnn\[.\]jio](https://blog.br0vnn[.]jio), and shortly thereafter, a malicious service was installed on the researcher's system and an in-memory backdoor would begin beaconing to an actor-owned command and control server. At the time of these visits, the victim systems were running fully patched and up-to-date Windows 10 and Chrome browser versions. At this time we're unable to confirm the mechanism of compromise, but we welcome any information others might have. Chrome vulnerabilities, including those being exploited in the wild (ITW), are eligible for reward payout under [Chrome's Vulnerability Reward Program](#). We encourage anyone who discovers a Chrome vulnerability to report that activity via the Chrome VRP submission process.

These actors have used multiple platforms to communicate with potential targets, including Twitter, LinkedIn, Telegram, Discord, Keybase and email. We are providing a list of known accounts and aliases below. If you have communicated with any of these accounts or visited the actors' blog, we suggest you review your systems for the IOCs provided below. To date, we have only seen these actors targeting Windows systems as a part of this campaign.

If you are concerned that you are being targeted, we recommend that you compartmentalize your research activities using separate physical or virtual machines for general web browsing, interacting with others in the research community, accepting files from third parties and your own security research.

Actor controlled sites and accounts

Research Blog

[https://blog.br0vnn\[.\]jio](https://blog.br0vnn[.]jio)

Twitter Accounts

- <https://twitter.com/br0vvnn>
- <https://twitter.com/BrownSec3Labs>
- <https://twitter.com/dev0exp>
- <https://twitter.com/djokovic808>
- <https://twitter.com/henya290>
- <https://twitter.com/james0x40>
- <https://twitter.com/m5t0r>
- <https://twitter.com/mvp4p3r>
- <https://twitter.com/tjrim91>
- <https://twitter.com/z0x55g>

LinkedIn Accounts

- <https://www.linkedin.com/in/billy-brown-a6678b1b8/>
- <https://www.linkedin.com/in/guo-zhang-b152721bb/>
- <https://www.linkedin.com/in/hyungwoo-lee-6985501b9/>
- <https://www.linkedin.com/in/linshuang-li-aa696391bb/>
- <https://www.linkedin.com/in/rimmer-trajan-2806b21bb/>

Keybase

<https://keybase.io/zhangguo>

Telegram

<https://t.me/james50d>

Sample Hashes

- <https://www.virustotal.com/gui/file/4c3499f3cc4a4fdc7e67417e055891c78540282dccc57e37a01167dfe351b244/detection>
(VS Project DLL)
- <https://www.virustotal.com/gui/file/68e6b9d71c727545095ea6376940027b61734af5c710b2985a628131e47c6af7/detection>
(VS Project DLL)
- <https://www.virustotal.com/gui/file/25d8ae4678c37251e7ffbaeddc252ae2530ef23f66e4c856d98ef60f399fa3dc/detection>
(VS Project Dropped DLL)
- <https://www.virustotal.com/gui/file/a75886b016d84c3eaacaf01a3c61e04953a7a3adf38acf77a4a2e3a8f544f855/detection>
(VS Project Dropped DLL)
- <https://www.virustotal.com/gui/file/a4fb20b15efd72f983f0fb3325c0352d8a266a69bb5f6ca2eba0556c3e00bd15/detection>
(Service DLL)

C2 Domains: Attacker-Owned

- [angeldonationblog\[.\]com](http://angeldonationblog[.]com)
- [codevexillum\[.\]org](http://codevexillum[.]org)
- [investbooking\[.\]de](http://investbooking[.]de)
- [krakenfolio\[.\]com](http://krakenfolio[.]com)
- [opsonew3org\[.\]sg](http://opsonew3org[.]sg)
- [transferwiser\[.\]io](http://transferwiser[.]io)
- [transplugin\[.\]io](http://transplugin[.]io)

C2 Domains: Legitimate but Compromised

- [trophylab\[.\]com](http://trophylab[.]com)
- [www.colasprint\[.\]com](http://www.colasprint[.]com)
- [www.dronerc\[.\]jit](http://www.dronerc[.]jit)
- [www.edujikim\[.\]com](http://www.edujikim[.]com)
- [www.fabioluciani\[.\]com](http://www.fabioluciani[.]com)

C2 URLs

- [https://angeldonationblog\[.\]com/image/upload/upload.php](https://angeldonationblog[.]com/image/upload/upload.php)
- [https://codevexillum\[.\]org/image/download/download.asp](https://codevexillum[.]org/image/download/download.asp)
- [https://investbooking\[.\]de/upload/upload.asp](https://investbooking[.]de/upload/upload.asp)

- [https://transplugin\[.\]io/upload/upload.asp](https://transplugin[.]io/upload/upload.asp)
- [https://www.dronerc\[.\]it/forum/uploads/index.php](https://www.dronerc[.]it/forum/uploads/index.php)
- [https://www.dronerc\[.\]it/shop_testbr/Core/upload.php](https://www.dronerc[.]it/shop_testbr/Core/upload.php)
- [https://www.dronerc\[.\]it/shop_testbr/upload/upload.php](https://www.dronerc[.]it/shop_testbr/upload/upload.php)
- [https://www.edujikim\[.\]com/intro/blue/insert.asp](https://www.edujikim[.]com/intro/blue/insert.asp)
- [https://www.fabioluciani\[.\]com/es/include/include.asp](https://www.fabioluciani[.]com/es/include/include.asp)
- [http://trophylab\[.\]com/notice/images/renewal/upload.asp](http://trophylab[.]com/notice/images/renewal/upload.asp)
- [http://www.colasprint\[.\]com/_vti_log/upload.asp](http://www.colasprint[.]com/_vti_log/upload.asp)

Host IOCs

- Registry Keys
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\KernelConfig
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\DriverConfig
 - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSL Update
- File Paths
 - C:\Windows\System32\Nwsapagent.sys
 - C:\Windows\System32\helpsvc.sys
 - C:\ProgramData\USOShared\uso.bin
 - C:\ProgramData\VMware\vmnat-update.bin
 - C:\ProgramData\VirtualBox\update.bin

POSTED IN:

[Threat Analysis Group](#)