Countering threats from North Korea

Mar 24, 2022

4 min read

Share Twitter Facebook Linkedin Mail Copy link A Adam Weidemann Threat Analysis Group Share Twitter Facebook Linkedin Mail Copy link

On February 10, Threat Analysis Group discovered two distinct North Korean government-backed attacker groups exploiting a remote code execution vulnerability in Chrome, CVE-2022-0609. These groups' activity has been publicly tracked as Operation Dream Job and Operation AppleJeus.

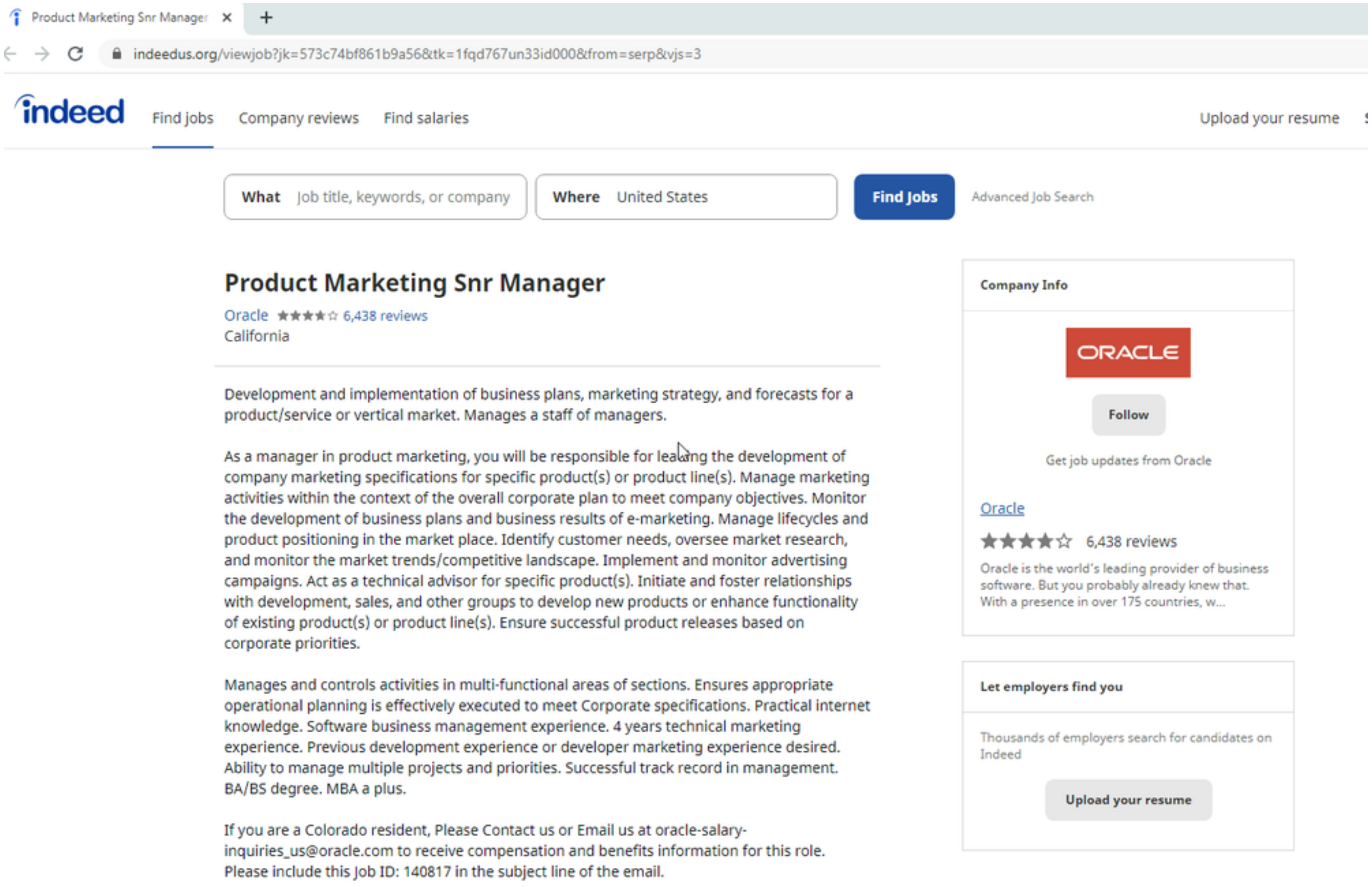
We observed the campaigns targeting U.S. based organizations spanning news media, IT, cryptocurrency and fintech industries. However, other organizations and countries may have been targeted. One of the campaigns has direct infrastructure overlap with a campaign targeting security researchers which we reported on last year. The exploit was patched on February 14, 2022. The earliest evidence we have of this exploit kit being actively deployed is January 4, 2022.

We suspect that these groups work for the same entity with a shared supply chain, hence the use of the same exploit kit, but each operate with a different mission set and deploy different techniques. It is possible that other North Korean government-backed attackers have access to the same exploit kit.

In this blog, we will walk through the observed tactics, techniques and procedures, share relevant IOCs and analyze the exploit kit used by the attackers. In line with our current disclosure policy, we are providing these details 30 days after the patch release.

Campaign targeting news media and IT companies

The campaign, consistent with Operation Dream Job, targeted over 250 individuals working for 10 different news media, domain registrars, web hosting providers and software vendors. The targets received emails claiming to come from recruiters at Disney, Google and Oracle with fake potential job opportunities. The emails contained links spoofing legitimate job hunting websites like Indeed and ZipRecruiter.



indeedus.org/viewjob?jk=573c74bf861b9a56&tk=1fqd767un33id000&from=serp&vjs=3

Product Marketing Snr Manager

Oracle ★★★★☆ 6,438 reviews
California

Development and implementation of business plans, marketing strategy, and forecasts for a product/service or vertical market. Manages a staff of managers.

As a manager in product marketing, you will be responsible for leading the development of company marketing specifications for specific product(s) or product line(s). Manage marketing activities within the context of the overall corporate plan to meet company objectives. Monitor the development of business plans and business results of e-marketing. Manage lifecycles and product positioning in the market place. Identify customer needs, oversee market research, and monitor the market trends/competitive landscape. Implement and monitor advertising campaigns. Act as a technical advisor for specific product(s). Initiate and foster relationships with development, sales, and other groups to develop new products or enhance functionality of existing product(s) or product line(s). Ensure successful product releases based on corporate priorities.

Manages and controls activities in multi-functional areas of sections. Ensures appropriate operational planning is effectively executed to meet Corporate specifications. Practical internet knowledge. Software business management experience. 4 years technical marketing experience. Previous development experience or developer marketing experience desired. Ability to manage multiple projects and priorities. Successful track record in management. BA/BS degree. MBA a plus.

If you are a Colorado resident, Please Contact us or Email us at oracle-salary-inquiries_us@oracle.com to receive compensation and benefits information for this role. Please include this Job ID: 140817 in the subject line of the email.

Oracle
★★★★☆ 6,438 reviews
Oracle is the world's leading provider of business software. But you probably already knew that. With a presence in over 175 countries, w...

Thousands of employers search for candidates on Indeed

Example of spoofed job hunting websites

Victims who clicked on the links would be served a hidden iframe that would trigger the exploit kit.

Attacker-Owned Fake Job Domains:

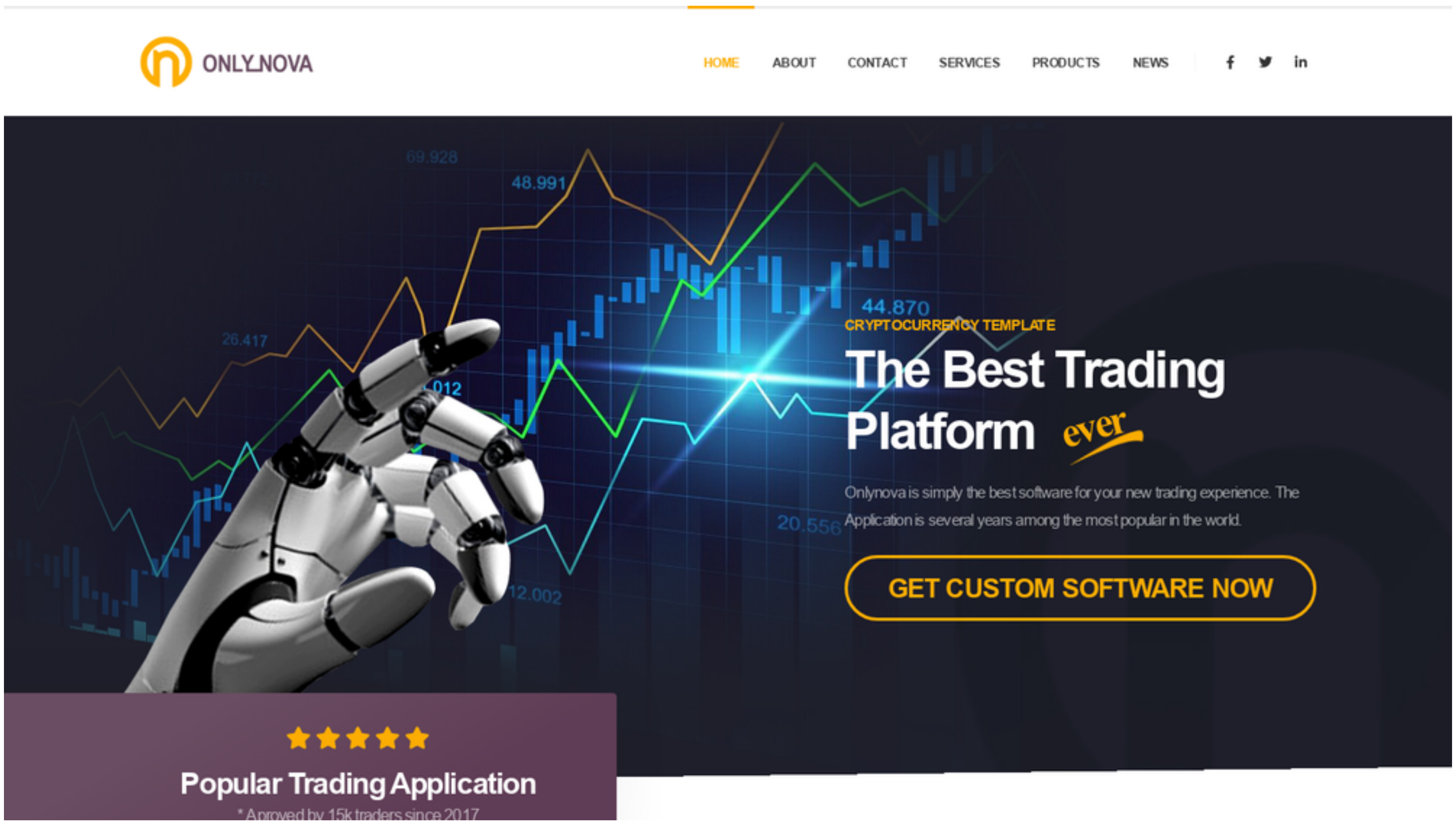
- disneycareers[.]net
- find-dreamjob[.]com
- indeedus[.]org
- varietyjob[.]com
- ziprecruiters[.]org

Exploitation URLs:

- https[:]//colasprint[.]com/about/about.asp (legitimate but compromised website)
- https[:]//varietyjob[.]com/sitemap/sitemap.asp

Campaign targeting cryptocurrency and Fintech organizations

Another North Korean group, whose activity has been publicly tracked as Operation AppleJeus, targeted over 85 users in cryptocurrency and fintech industries leveraging the same exploit kit. This included compromising at least two legitimate fintech company websites and hosting hidden iframes to serve the exploit kit to visitors. In other cases, we observed fake websites —— already set up to distribute trojanized cryptocurrency applications —— hosting iframes and pointing their visitors to the exploit kit.



The Best Trading Platform ever

Onlynova is simply the best software for your new trading experience. The Application is several years among the most popular in the world.

Popular Trading Application

* Aproved by 15k traders since 2017

Attacker-Owned Websites:

- blockchainnews[.]vip
- chainnews-star[.]com
- financialtimes365[.]com
- fireblocks[.]vip
- gatexpiring[.]com
- gbclabs[.]com
- giantblock[.]org
- humingbot[.]io
- onlynova[.]org
- teenbeanjs[.]com

Compromised Websites (Feb 7 - Feb 9):

- www.options-it[.]com
- www.tradingtechnologies[.]com

Exploitation URLs:

- https[:]//financialtimes365[.]com/user/finance.asp
- https[:]//gatexpiring[.]com/gate/index.asp
- https[:]//humingbot[.]io/cdn/js.asp
- https[:]//teenbeanjs[.]com/cloud/javascript.asp

Exploit kit overview

The attackers made use of an exploit kit that contained multiple stages and components in order to exploit targeted users. The attackers placed links to the exploit kit within hidden iframes, which they embedded on both websites they owned as well as some websites they compromised.

The kit initially serves some heavily obfuscated javascript used to fingerprint the target system. This script collected all available client information such as the user-agent, resolution, etc. and then sent it back to the exploitation server. If a set of unknown requirements were met, the client would be served a Chrome RCE exploit and some additional javascript. If the RCE was successful, the javascript would request the next stage referenced within the script as "SBX", a common acronym for Sandbox Escape. We unfortunately were unable to recover any of the stages that followed the initial RCE.

Careful to protect their exploits, the attackers deployed multiple safeguards to make it difficult for security teams to recover any of the stages. These safeguards included:

- Only serving the iframe at specific times, presumably when they knew an intended target would be visiting the site.
- In some email campaigns the targets received links with unique IDs. This was potentially used to enforce a one-time-click policy for each link and allow the exploit kit to only be served once.
- The exploit kit would AES encrypt each stage, including the clients' responses with a session-specific key.
- Additional stages were not served if the previous stage failed.

Although we recovered a Chrome RCE, we also found evidence where the attackers specifically checked for visitors using Safari on MacOS or Firefox (on any OS), and directed them to specific links on known exploitation servers. We did not recover any responses from those URLs.

Example Exploit Kit:

- 03a41d29e3c9763093aca13f1cc8bcc41b201a6839c381aaaccf891204335685

The attackers made multiple attempts to use the exploit days after the vulnerability was patched on February 14, which stresses the importance of applying security updates as they become available.

Protecting Our Users

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

TAG is committed to sharing our findings as a way of raising awareness with the security community, and with companies and individuals that might have been targeted or suffered from these activities. We hope that improved understanding of the tactics and techniques will enhance threat hunting capability and lead to stronger user protections across industry.

POSTED IN: