Internet Explorer 0-day exploited by North Korean actor APT37

blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37

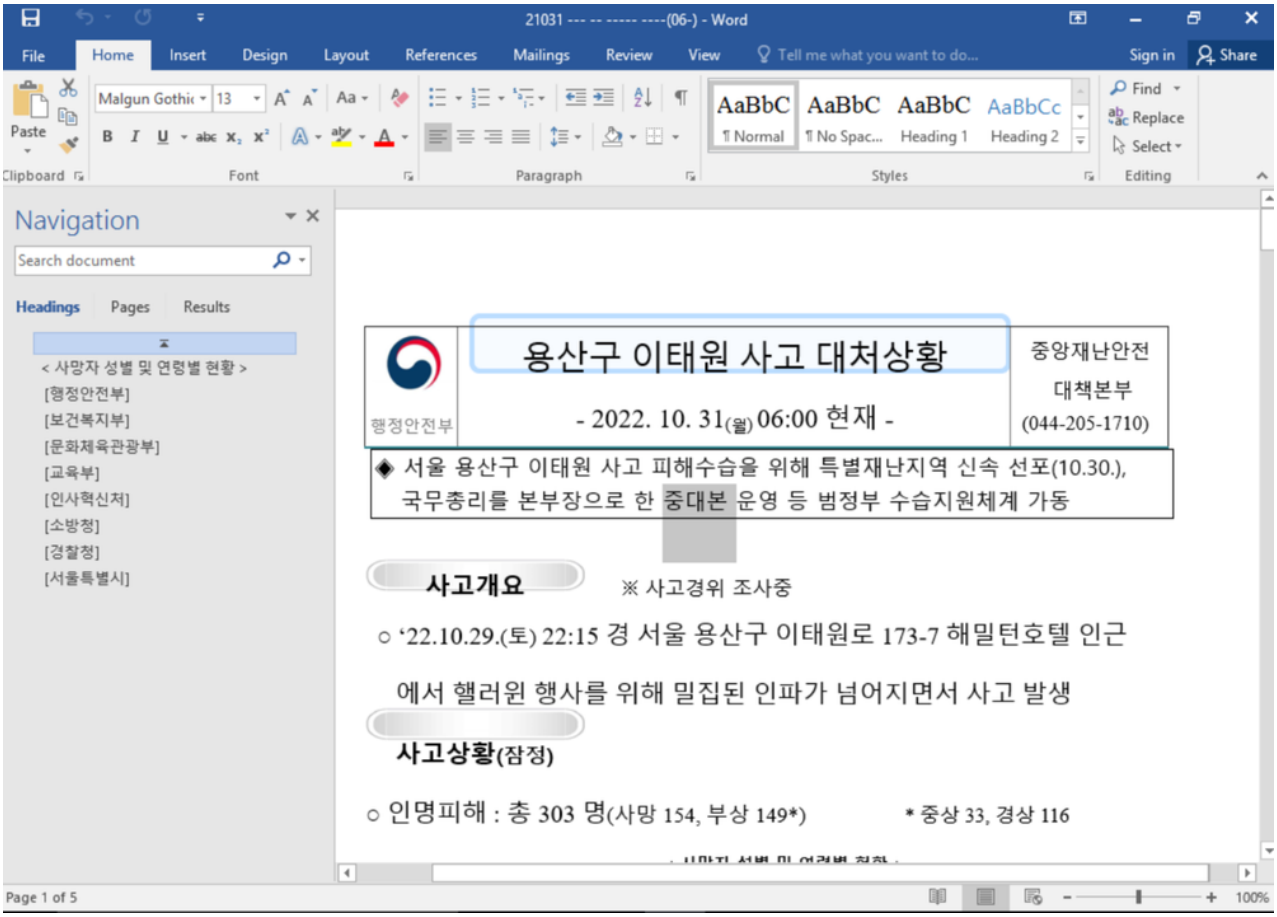
December 7, 2022

To protect our users, Google's Threat Analysis Group (TAG) routinely hunts for 0-day vulnerabilities exploited in-the-wild. This blog will describe a 0-day vulnerability, discovered by TAG in late October 2022, embedded in malicious documents and used to target users in South Korea. We attribute this activity to a group of North Korean government-backed actors known as APT37. These malicious documents exploited an Internet Explorer 0-day vulnerability in the JScript engine, CVE-2022-41128. Our policy is to quickly report vulnerabilities to vendors, and within a few hours of discovering this 0-day, we reported it to Microsoft and patches were released to protect users from these attacks.

This is not the first time APT37 has used Internet Explorer 0-day exploits to target users. The group has historically focused their targeting on South Korean users, North Korean defectors, policy makers, journalists and human rights activists.

Microsoft Office document using tragic news as a lure

On October 31, 2022, multiple submitters from South Korea reported new malware to us by uploading a Microsoft Office document to VirusTotal. The document, titled "221031 Seoul Yongsan Itaewon accident response situation (06:00).docx", references the tragic incident in the neighborhood of Itaewon, in Seoul, South Korea during Halloween celebrations on October 29, 2022. This incident was widely reported on, and the lure takes advantage of widespread public interest in the accident.



The document downloaded a rich text file (RTF) remote template, which in turn fetched remote HTML content. Because Office renders this HTML content using Internet Explorer (IE), this technique has been widely used to distribute IE exploits via Office files since 2017 (e.g. CVE-2017-0199). Delivering IE exploits via this vector has the advantage of not requiring the target to use Internet Explorer as its default browser, nor to chain the exploit with an EPM sandbox escape.

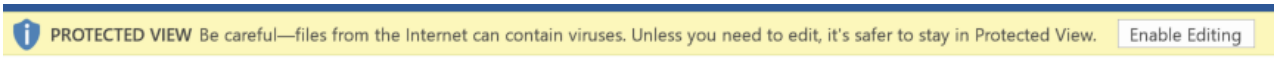
Upon investigation, TAG observed the attackers abused an 0-day vulnerability in the JScript engine of Internet Explorer.

TAG identified Internet Explorer 0-day

The vulnerability resides within "jscript9.dll", the JavaScript engine of Internet Explorer, and can be exploited to execute arbitrary code when rendering an attacker-controlled website. The bug itself is an incorrect JIT optimization issue leading to a type confusion and is very similar to CVE-2021-34480, which was identified by Project Zero and patched in 2021. TAG reported the vulnerability to Microsoft on October 31, 2022, and the label CVE-2022-41128 was assigned on November 3, 2022. The vulnerability was patched on November 8, 2022.

Analysis of the exploit

In a typical delivery scenario, the initial document would have the Mark-of-the-Web applied. This means the user has to disable protected view before the remote RTF template is fetched.



When delivering the remote RTF, the web server sets a unique cookie in the response, which is sent again when the remote HTML content is requested. This likely detects direct HTML exploit code fetches which are not part of a real infection.

The exploit JavaScript also verifies that the cookie is set before launching the exploit. Additionally it reports twice to the C2 server: before launching the exploit and after the exploit succeeds.

TAG also identified other documents likely exploiting the same vulnerability and with similar targeting, which may be part of the same campaign. Further details on those documents can be found in the “Indicators” section below.

The delivered shellcode uses a custom hashing algorithm to resolve Windows APIs. The shellcode erases all traces of exploitation by clearing the Internet Explorer cache and history before downloading the next stage. The next stage is downloaded using the same cookie that was set when the server delivered the remote RTF.

Although we did not recover a final payload for this campaign, we’ve previously observed the same group deliver a variety of implants like ROKRAT, BLUELIGHT, and DOLPHIN. APT37 implants typically abuse legitimate cloud services as a C2 channel and offer capabilities typical of most backdoors.

Additional technical information on the vulnerability, the exploit and the patch, is available in the Root Cause Analysis.

Conclusions

TAG is committed to sharing research to raise awareness on bad actors like APT37 within the security community, and for companies and individuals that may be targeted. By improving understanding of the tactics and techniques of these types of actors, we hope to strengthen protections across the ecosystem. We will also continuously apply these findings to improve the safety and security of our products and continue to effectively combat threats and protect users who rely on our services.

We’d be remiss if we did not acknowledge the quick response and patching of this vulnerability by the Microsoft team.

Indicators of compromise (IOCs)

Initial documents:

- 56ca24b57c4559f834c190d50b0fe89dd4a4040a078ca1f267d0bbc7849e9ed7
- af5fb99d3ff18bc625fb63f792ed7cd955171ab509c2f8e7c7ee44515e09cebf
- 926a947ea2b59d3e9a5a6875b4de2bd071b15260370f4da5e2a60ece3517a32f
- 3bff571823421c013e79cc10793f238f4252f7d7ac91f9ef41435af0a8c09a39
- c49b4d370ad0dcd1e28ee8f525ac8e3c12a34cfcf62ebb733ec74cca59b29f82

Remote RTF template:

08f93351d0d3905bee5b0c2b9215d448abb0d3cf49c0f8b666c46df4fcc007cb

C2:

- word-template[.]net
- openxmlformat[.]org
- ms-office[.]services
- ms-offices[.]com
- template-openxml[.]com

POSTED IN:

Threat Analysis Group