Magniber ransomware gang now exploits Internet Explorer flaws in attacks

bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/

Bill Toulas

By
Bill Toulas

- November 11, 2021
- 11:04 AM
- 0

The Magniber ransomware gang is now using two Internet Explorer vulnerabilities and malicious advertisements to infect users and encrypt their devices.

The two Internet Explorer vulnerabilities are tracked as CVE-2021-26411 and CVE-2021-40444, with both having a CVSS v3 severity score of 8.8.

The first one, CVE-2021-26411, was fixed in March 2021 and is a memory corruption flaw triggered by viewing a specially crafted website.

The second flaw, CVE-2021-40444, is a remote code execution in IE's rendering engine triggered by the opening of a malicious document.

Attackers exploited CVE-2021-40444 as a zero-day before Microsoft fixed it in September 2021.

Magniber shifting focus

The Magniber gang is known for its use of vulnerabilities to breach systems and deploy their ransomware.

In August, Magniber was observed exploiting 'PrintNightmare' vulnerabilities to breach Windows servers, which took Microsoft a while to address due to their impact on printing.

The most recent Magniber activity focuses on exploiting Internet Explorer vulnerabilities using malvertising that pushes exploit kits, as confirmed by Tencent Security researchers who identified "fresh" payloads.

One possible explanation for this shift is that Microsoft has largely fixed the 'PrintNightmare' vulnerabilities over the past four months and was heavily covered by the media, pushing admins to deploy security updates.

Another reason why Magniber may have turned to Internet Explorer flaws is that they are relatively easy to trigger, relying solely upon stimulating the recipient's curiosity to open a file or webpage.

It may seem strange to target an old unpopular browser like Internet Explorer. However, StatCounter shows that 1.15% of the global page views are still from IE.

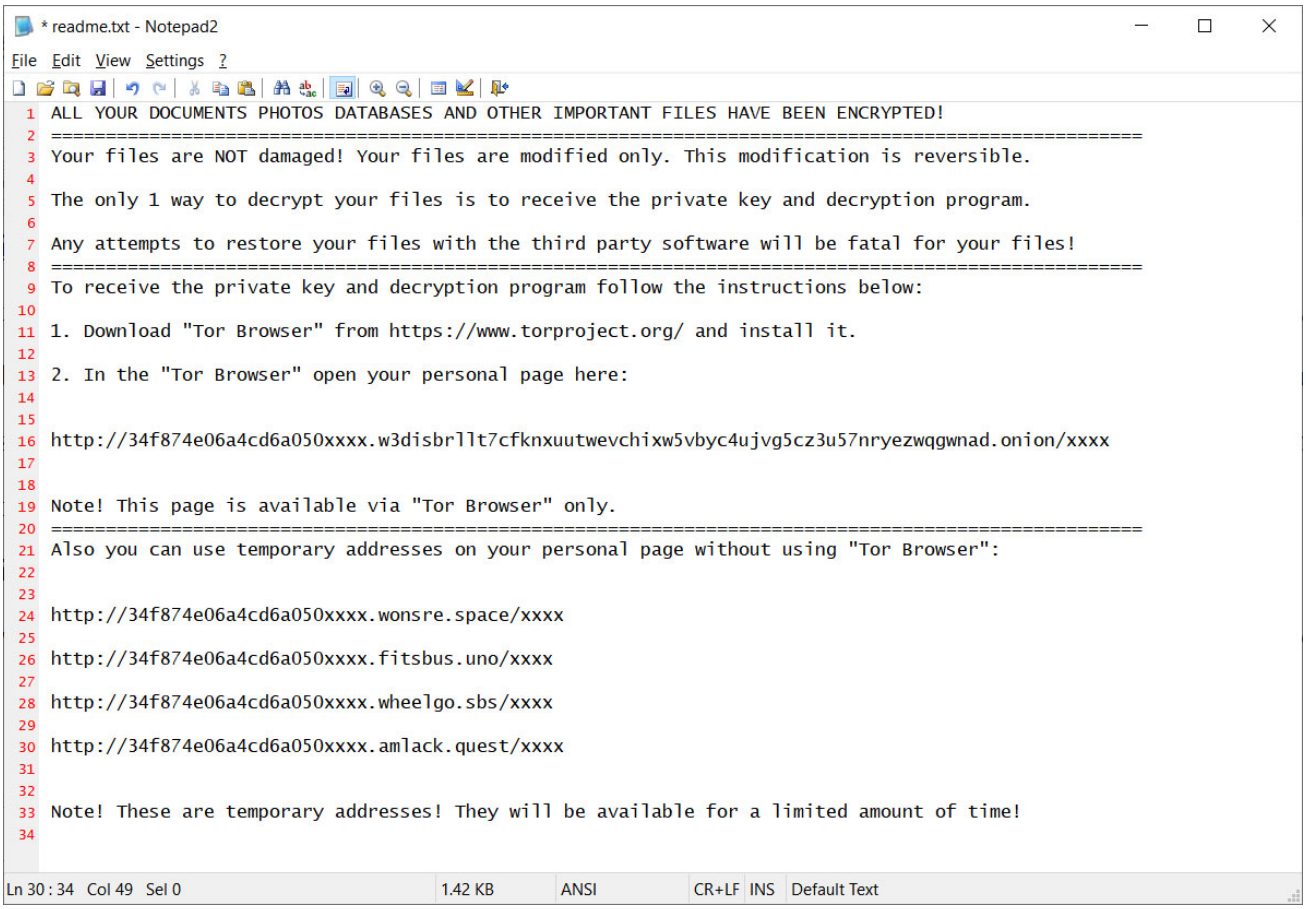
While this is a low percentage, StatCounter tracks over 10 billion page views per month, which equates to 115,000,000 pages views by users of Internet Explorer.

Furthermore, it is much harder to target Firefox and Chromium-based browsers, such as Google Chrome and Microsoft Edge, as they utilize an auto-update mechanism that quickly protects users from known vulnerabilities.

Threat to Asian firms

Magniber started in 2017 as the successor to the Cerber ransomware, and initially, it only infected users from South Korea.

The group then widened their targeting scope and began infecting Chinese (including Taiwan and Hong Kong), Singaporean, and Malaysian systems as well.



Magniber ransom note

This scope has solidified, and today, Magniber is a nuisance almost exclusively for Asian companies and organizations.

Since its launch, the Magniber ransomware has been under very active development, and its payload has been completely rewritten three times.

At this time, it remains uncracked, so there's no decryptor to help you restore any files that have been encrypted with this strain.

Finally, Magniber isn't following the trend of file-stealing and double-extortion, so the damage of their attacks is limited to file encryption.

As such, taking regular backups on secured, isolated systems is a very effective way to deal with this particular threat.

Related Articles:

Darknet market Versus shuts down after hacker leaks security flaw

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Zyxel fixes firewall flaws that could lead to hacked networks

Critical F5 BIG-IP vulnerability exploited to wipe devices

Exploits created for critical F5 BIG-IP flaw, install patch immediately

- CVE-2021-40444
- Exploit
- Internet Explorer
- Magniber
- Ransomware
- Vulnerability

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

You may also like: