



PuzzleMaker Threat Group Attacks Windows Devices

CRITICALITY 

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

The recently patched vulnerabilities in Microsoft Windows and Google Chrome have been used in highly targeted attacks against the enterprise by a threat group called PuzzleMaker.



Threat Details

The PuzzleMaker is successfully leveraging a series of Google Chrome and Windows zero-day flaws. For the initial access, the attacker took advantage of two remote code execution vulnerabilities in the Google Chrome V8 JavaScript engine, known as CVE-2021-21220 and CVE-2021-21224 to gain access to the targeted systems.

After that, the attacker used two different vulnerabilities. One of them is a Windows Kernel vulnerability known as CVE-2021-31955 and the other one is a Windows NTFS privilege escalation vulnerability known as CVE-2021-31956.

Kaspersky says that when these vulnerabilities chained together, it will allow the attacker to run malicious code on the targeted machine. The malicious code includes a module called stager that is responsible for downloading and executing a malware dropper. Then, the dropper installs two executables. One of them will pretend to be a legitimate file, and the other one is a remote shell module that can upload files, create processes and self-destruction.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

PuzzleMaker attacks exploit Windows zero-day, Chrome vulnerabilities. (n.d.). Retrieved from ZDNet: <https://www.zdnet.com/article/puzzlemaker-attacks-exploit-windows-chrome-zero-day-vulnerabilities/>

PuzzleMaker attacks with Chrome zero-day exploit chain. (n.d.). Retrieved from Securelist English Global securelistcom: <https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/>

Windows 10 targeted by PuzzleMaker hackers using Chrome zero-days. (n.d.). Retrieved from BleepingComputer: <https://www.bleepingcomputer.com/news/security/windows-10-targeted-by-puzzlemaker-hackers-using-chrome-zero-days/>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to follow the below steps to help organizations thwart these attacks:

- Immediately patch the vulnerabilities (CVE-2021-21220 and CVE-2021-21224) by upgrading Google Chrome to the latest version.
- Immediately patch the vulnerabilities (CVE-2021-31955 and CVE-2021-31956) by upgrading Microsoft Windows to the latest version.



Appendix B – Indicators of Compromise

Indicators of Compromise

Malware URLs

media-seoengine[.]com

File names and Hashes

%SYSTEM%\WmiPrvMon.exe

MD5 09A5055DB44FC1C9E3ADD608EFFF038C

SHA-1 BFFA4462901B74DBFBFFAA3A3DB27DAA61211412

SHA-256 982F7C4700C75B81833D5D59AD29147C392B20C760FE36B200B541A0F841C8A9

%SYSTEM%\wmimon.dll

MD5 D6B850C950379D5EE0F254F7164833E8

SHA-1 E63ED3B56A5F9A1EA5C92D3D2444196EA13BE94B

SHA-256 8A17279BA26C8FBE6966EA3300FDEFB1ADAE1B3ED68F76A7FC81413BD8C1A5F6



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.