ultraviolet

THREAT REPORT:

‘GrimResource’ Used With MSC Files in Phishing Attacks

Services Performed By:
UltraViolet Cyber
Johnathon Moyer
(443) 351-7630
info@uvcyber.com

Published Date:
June 26, 2024

Contents

1 Executive Summary

After Microsoft finally disabled macros by default for files which bear the 'Mark of the Web' (MotW) flag, threat actors adapted by changing their initial infection vector. After initially switching to ISO and ZIP files, to MSI and LNK files, and now to MSC[1] (Management Saved Console) files. MSC files are related to the Microsoft Management Console which is used in the SCCM (System Center Configuration Manager) service. This service is commonly used in enterprise environments. Threat actors have now begun to adopt this readily available resource, as they did with PowerShell and C.

2 Technical Analysis

The overall pattern is still much the same for phishing attacks; a threat actor creates a malicious file, uploads it to a file-sharing platform, usually OneDrive. The threat actor sends out millions of emails to potential victims with prompts to download a file, typically a file made to look like an invoice. This is where things have changed recently. Rather than download a malicious ISO, ZIP, LNK or MSI file, we are seeing MSC files disguised as Word documents.

This newly popularized attack method is what some researchers are dubbing 'GrimResource'[2]. When a user downloads and executes the MSC file, the file can run arbitrary code. The key to this attack is the exploitation of a vulnerability from October 2018 related to the 'apds.dll' library[3]. The MSC file exploits this vulnerability by adding a line of JavaScript code, calls out to the Command and Control (C2) server for instructions, then carries it out on the infected host.

When this file was first uploaded to VirusTotal on June 6, 2024, no security engines flagged the file as malware at that time. As of the time of this writing, eleven out of seventy-eight security engines have currently flagged the initial sample file as a Trojan[7]. So far, these types of attacks have installed Cobalt Strike tools on infected endpoints. We anticipate other payloads will be downloaded as other threat actor groups adopt GrimResource to their toolset.

3 What UltraViolet Cyber is Doing

- We regularly update our Indicators of Compromise (IoC) databases
- Network monitoring tools to alert on traffic to known malicious sites
- Monitoring for commands associated with malicious activity from threat actors

4 What Customers Can Do

- Update user training regarding phishing campaigns to include this new trend
- Ensure endpoint protection applications are kept up to date, including signature databases
- If your organization utilizes MSC files, you may consider testing whether you can restrict the execution of the files from known directories used from approved administrative tools like SCCM. This may be executed from the Applocker Policy within the Group Policy (GPo) tool[6].

5 References

1. (2024, June 26). Kimsuky APT attack discovered using Facebook & MS management console. Genians. Retrieved from https://www.genians.co.kr/blog/threat_intelligence/facebook
2. Desimone, J., Bousseaden, S. GrimResource - Microsoft Management Console for initial access and evasion. Elastic Security Labs. (2024, June 26). Retrieved from http://www.elastic.co/security-labs/grimresource
3. Lokihardt. (2024, June 26). Issue 1598: Microsoft Edge: Sandbox escape. Project-zero. Retrieved from https://bugs.chromium.org/p/project-zero/issues/detail?id=1598&desc=5
4. Peasead. (2024, June 26). GitHub. Retrieved from https://github.com/elastic/labs-releases/tree/main/indicators/grimresource
5. Desimone, J. (2024, June 26). GitHub Gist. Retrieved from https://gist.github.com/joe-desimone/2b0bbee382c9bdfcac53f2349a379fa4
6. (2024, June 26). Administer Software Restriction Policies. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/administer-software-restriction-policies
7. (2024, June 26). VirusTotal. Retrieved from https://www.virustotal.com/gui/file/14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb/detection