Mphasis SOC – Information Security News
Date & Time Issued: 30-JUN-2024, 21:30 IST

Title	**MerkSpy: Exploiting CVE-2021-40444 to Infiltrate Systems**
Summary	• FortiGuard Labs recently detected an attack exploiting the CVE-2021-40444 vulnerability in Microsoft Office. This flaw allows attackers to execute malicious code via specially crafted documents. • In this instance, the exploitation led to the deployment of a spyware payload known as "MerkSpy." MerkSpy is designed to clandestinely monitor user activities, capture sensitive information, and establish persistence on compromised systems.
Severity	Medium
Attack Vectors	• The initial vector for this attack is a deceptive Microsoft Word document posing as a job description for a software developer position. • Opening the document triggers the exploitation of CVE-2021-40444, a remote code execution vulnerability within the MSHTML component used by Internet Explorer in Microsoft Office. This vulnerability permits an attacker to execute arbitrary code on a victim's machine without additional user interaction beyond opening the document. The attacker conceals the URL within the "_rels\document.xml" file. It directs to hxxp://45[.]89[.]53[.]46/google/olerender[.]html, downloading an HTML file that sets the stage for the next phase of the attack. • After the successful exploitation, the malicious document initiates the downloaded payload, "olerender.html," from a remote server. This HTML file is strategically crafted, with innocuous script filling the beginning to mask its true intent. The end of the file conceals the shellcode and injection process, which propels the attack forward when executed on the victim's machine. • Once the shellcode is in place, it functions as a downloader, initiating the next phase of the attack. It reaches out to the same remote server to fetch a file, deceptively named "GoogleUpdate." Despite its seemingly innocuous name, "GoogleUpdate" is far from benign. This file harbors the core malicious payload, which is deeply encoded to evade detection by standard security measures. Upon successful download, the shellcode meticulously decodes and prepares this payload for execution. • The extracted payload is protected with VMProtect. Its primary function is seamlessly injecting the MerkSpy spyware into crucial system processes. MerkSpy spyware operates covertly within a system, enabling it to capture sensitive information, monitor user activities, and exfiltrate data to remote servers controlled by malicious actors.
Indicator of Compromise	INDICATOR TYPE: File Hash • 92eb60179d1cf265a9e2094c9a54e025597101b8a78e2a57c19e4681df465e08 • 95a3380f322f352cf7370c5af47f20b26238d96c3ad57b6bc972776cc294389a • 0ffadb53f9624950dea0e07fcffcc31404299230735746ca43d4db05e4d708c6 • dd369262074466ce937b52c0acd75abad112e395f353072ae11e3e888ac132a8 • 569f6cd88806d9db9e92a579dea7a9241352d900f53ff7fe241b0006ba3f0e22 • 6cdc2355cf07a240e78459dd4dd32e26210e22bf5e4a15ea08a984a5d9241067 INDICATOR TYPE: IPs • 45[.]89[.]53[.]46
Recommendations	• Security administrators should block the IoCs on all applicable security solutions post-validation. • Security administrators should make sure that all applications, databases, servers, and network devices are periodically hardened and are adequately configured. • Users should not download suspicious applications or attachments received over the internet and should be vigilant against social engineering and phishing attacks. • Users are recommended to use a unique and strong password at every site with the help of a password manager and use Multi-Factor Authentication (MFA) wherever possible. • Users should not download, accept, or execute files and do not visit websites or follow links provided by unknown or untrusted sources. • Organizations are recommended to have a behavioral detection solution in place to successfully detect the presence of malware payloads. • Keep AV signatures, operating systems, and third-party applications up to date on all systems, mobile devices, and servers. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**

References	• https://www.fortinet.com/blog/threat-research/merkspy-exploiting-cve-2021-40444-to-infiltrate-systems?&web_view=true