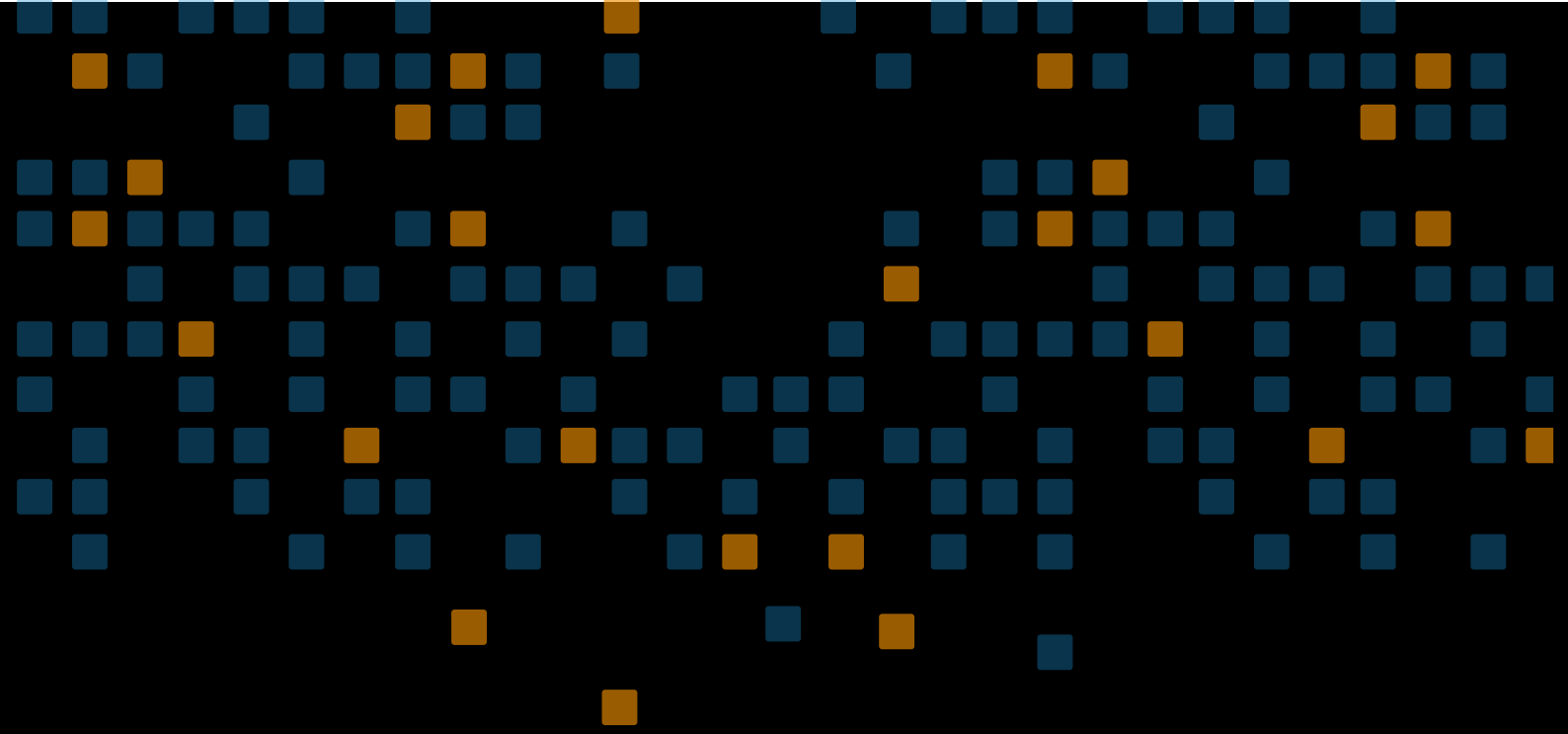

# THREAT INSIGHTS REPORT

OCTOBER-2020

## THREAT LANDSCAPE

Welcome to the October 2020 edition of the HP-Bromium Threat Insights Report. The report reviews notable malware trends identified by HP Sure Click from the third quarter (1 July to 30 September) of 2020, so that security teams are equiped with the knowledge to combat emerging threats and defend their environments.

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

## NOTABLE THREATS

### Emotet Spam Campaigns Focus on Japanese and Australian Organisations

Q3 of 2020 saw a large and sustained increase in malicious spam campaigns distributing **Emotet** malware (Figure 1), particularly at the end of August. The number of Emotet samples isolated by HP Sure Click increased by over 1,200% in Q3 compared to Q2. Emotet spam activity had been intermittent since March 2020. The pattern of Emotet spam since 2018 suggests that we are likely to see weekly spam runs until early 2021.

Despite its origins as a banking Trojan, since 2017 Emotet has more often been used as a loader to provide access to compromised systems to other threat groups.[1] So far in 2020 we have seen secondary **TrickBot** and **QakBot** infections deployed through Emotet.[2] Notably, Emotet infections are often a precursor to human-operated ransomware attacks.[3] Threat actors have been observed using the access to compromised systems to perform reconnaissance of victim networks before deploying ransomware families such as **Ryuk**.[4]

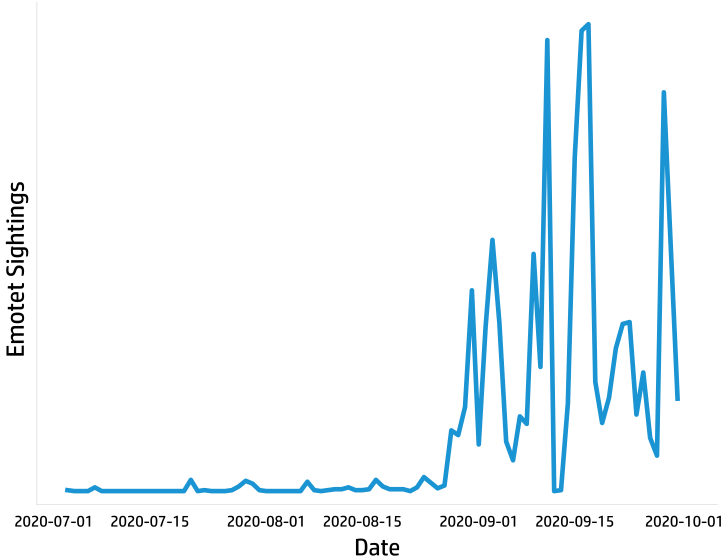


**Figure 1 - Emotet samples isolated by HP Sure Click in Q3 2020.**

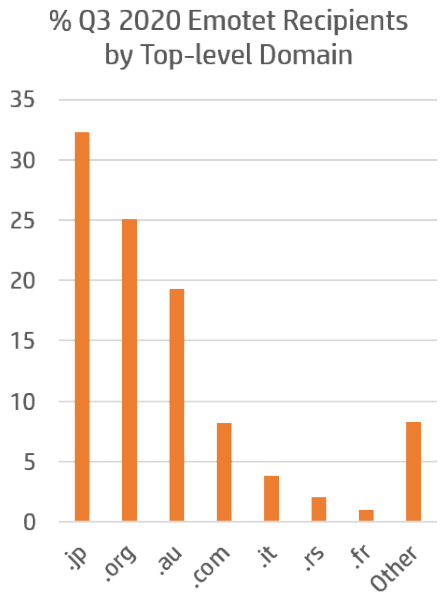


**Figure 2 - Emotet spam recipients by top-level domain from HP Sure Click Q3 2020 telemetry.**

Japanese and Australian organisations were most affected by the resurgent Emotet spam activity in Q3 2020. An analysis of HP Sure Click telemetry found that 32% of samples were sent to domains that used the .jp country code top-level domain (ccTLD), while nearly 20% of recipients used the .au ccTLD (Figure 2). Organisations rather than personal addresses were targeted, with a quarter of Emotet spam sent to .org domains. The targeting of organisations is consistent with the objective of Emotet's operators to broker access to compromised systems to ransomware actors, since they are more likely to hold valuable data.

Emotet gains inital access to Microsoft Windows systems by tricking users into running a malicious

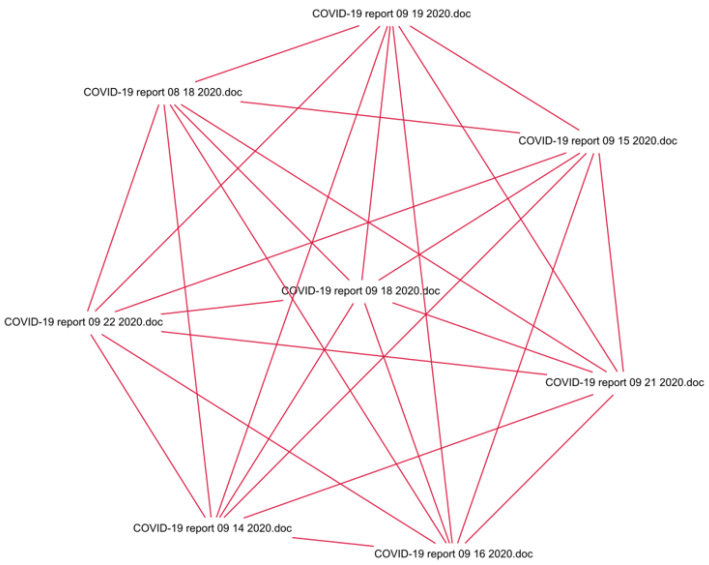


**Figure 3 - Filename similarity graph showing Emotet COVID-19 lures.**

Word document that is attached or linked to in an email. We found that most of the Emotet emails used thread hijacking to make them appear legitimate to the recipient. Thread hijacking is a technique where the mailbox of a user on a system that has been compromised by Emotet is exfiltrated to the malware's command and control (C2) servers.[5] Using this data, Emotet will reply to email threads with the malicious attachment or hyperlink. The technique is effective because the email appears to be from a sender that the recipient knows, albeit from a different sender address.

Emotet's operators have automated the naming of the Word documents by using templates. In Q3 2020, we identified templates in nine languages, including English, French, German, Greek, Hindi, Italian, Japanese, Spanish and Vietnamese. 55% of the files were named generically and contained no identifiable keywords. The remaining lures purported to be invoices, purchase orders and contracts (18%), forms and messages (14%), amendment notifications (11%), and COVID-19 reports (2%). The widespread use of thread hijacking means that Emotet's operators will probably continue to prefer generic names since they are more likely to match the topic of the hijacked thread. In August and September 2020, we also found Emotet documents that had been incorrectly named, likely due to a bug in the system used to generate the documents. For example in Figure 4, the string "{RCPT.DOMAIN-1-UP}" is normally replaced with the domain of the recipient and each "_br_" string is supposed to be replaced with a keyword, random letter or number.

## Top Malware Types and Exploited Vulnerabilities

In Q3 2020, Trojans remained the top type of malware isolated by HP Sure Click (Figure 5). Although Trojans were the most numerous, this masks the prevelance of ransomware attacks since an initial compromise by some families of Trojan may lead to the deployment of ransomware. Despite being patched in 2018, CVE-2017-11882 remains the most popular vulnerability to exploit (Figure 7). Its prevalence in the wild indicates that threat actors are successfully compromising systems using this exploit, which suggests that there are many unpatched versions of Office still being used.

## Droppers on the Rise

In July 2020, we detected an unusual spam campaign delivering TrickBot banking malware where the payloads were embedded in Word attachments (Figure 6). This marked a change from the delivery mechanism usually favoured by TrickBot's operators where a downloader retrieves and executes the payload from a remote server. Starting on 16 September, we detected a much larger campaign involving embedded TrickBot payloads.

```
_br__br_ZMG _br__br__br__br__br_.doc
_br__br__br_1SY _br__br__br__br__br_.doc
_br__br__br_2020_09 _br__br__br__br__br_.doc
_br__br__br_2020_09_24 _br__br__br_.doc
_br__br__br_2020_09_24 _br__br__br__br__br_.doc
_br__br__br_2020_09_24 _br__br__br__br__br_.doc
_br__br__br_MU78PHG _br__br__br__br_.doc
_br__br__br__br_09_25_br__br_.doc
_br__br__br__br_2020.09.21 _br__br__br__br_.doc
_br__br__br__br_2020.09.29 _br__br__br_.doc
_br__br__br__br_2020_09_21 _br__br__br__br_.doc
_br__br__br__br_RG8U5PB _br__br_.doc
_br__br__br__br_T11N0 _br__br__br__br__br_.doc
_br__br__br__br__br_.doc
_br__br__br__br__br_09_21_br__br_.doc
_br__br__br__br__br_2020_09 _br__br_.doc
_br__br__br__br__br__br_.doc
_br__br__br__br__br__br_.doc
_br__br__br__br__br__br_.doc
_br__br__br__br__br__br_.doc
_br__br__br__br__br__br__br_.doc
_br__br__br__br__br__br__br_.doc
_br__br__br__br__br__br__br__br_.doc
documento-967270-agosto_2020-{RCPT.DOMAIN-1-UP}.doc
documento-967270-agosto_2020-{RCPT.DOMAIN-1-UP}.doc
thông tin_br__br__br__br_.doc
{_REGEX_ sept. 2020.doc
{_REGEX_ sept. 2020.doc
{_REGEX_ septiembre 20.doc
```

**Figure 4 - Examples of Emotet documents from Q3 2020 whose filenames were not correctly generated.**

September's campaign was notable for its low detection rates. The HP-Bromium threat research team published an article and indicators of compromise (IOCs) relating to these campaigns, discussing the costs and benefits of emdedding payloads into a single stage of malware and the factors making downloaders less attractive to attackers.[6]

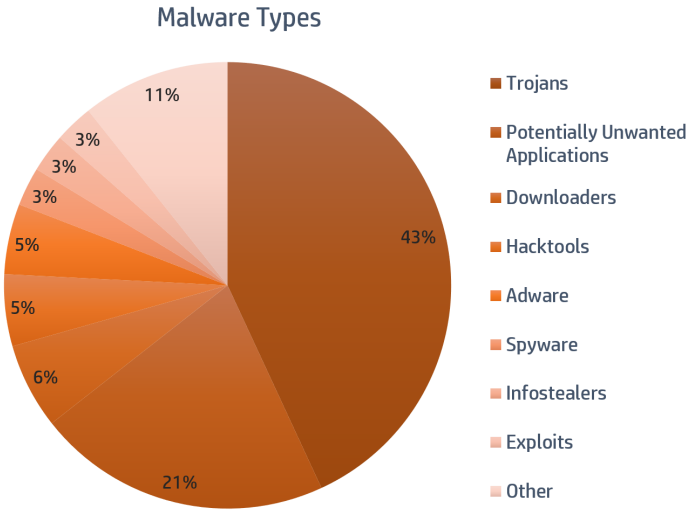


**Figure 5 - Top malware types isolated by HP Sure Click in Q3 2020.**

## Disruption of TrickBot's Command and Control Infrastructure

Ahead of the United States (US) elections in November, US Cyber Command temporaily disrupted TrickBot's C2 infrastructure.[7] On 22 September, systems infected with TrickBot received a configuration file instructing them to connect to a local loopback address (127.0.0.1) that is not routable over the Internet.[8] Separately, Microsoft and a group of industry and telecommunications providers successfully disabled TrickBot C2 servers located in the US after being granted a court order.[9] The disruption effort, which is ongoing, aims to limit TrickBot-linked ransomware attacks that could disrupt the election. Notably, in 2019 TrickBot was used to compromise US municipal governments including two Florida cities, Riviera Beach and Lake City, who paid ransoms totalling $1.1 million (USD) after Ryuk ransomware was deployed on their networks.[10]

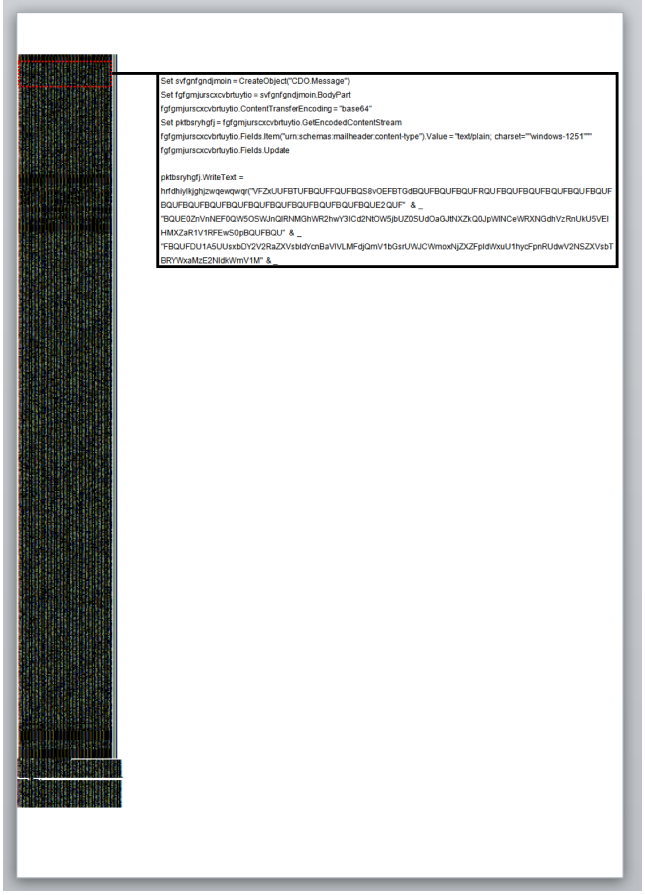


**Figure 6 - VBScript containing an encoded TrickBot payload hidden in a Word document dropper from September 2020.**

## Ongoing Ransomware Attacks

Ransomware attacks remain a significant threat to organisations. In August, Coveware reported that the average ransom payment rose by 60% to $178,254 compared to Q1 of 2020.[11] Several factors are likely driving this increase. First, threat actors are moving away from untargeted ransomware attacks that use pre-determined demands. Instead, we increasingly see criminals choosing victim organisations based on their size and revenue to maximise potential payments. Within underground forums and marketplaces, access brokers often advertise these characteristics about the organisations they have breached to appeal to ransomware operators seeking to do "business". Second, the growing number of ransomware families since November 2019 that exfiltrate victim data prior to encryption as an extortion tactic has ramped up the pressure on victims to pay. Many ransomware families have data breach blogs associated with them, where victim data is published if the ransom is not paid. In addition to losing access to their data, victims must also consider the reputational damage if confidential data is publicly disclosed.

## NOTABLE TECHNIQUES

### Encrypting Word Documents to Evade Detection

Threat actors are continually experimenting with ways to improve their chances of successfully compromising systems. Despite the size of TrickBot campaign in September 2020, the Word document droppers were effective at evading detection. 70% of the samples were identified as malicious by four or fewer scanning engines, and several files received zero detections (Figure 9).[6]

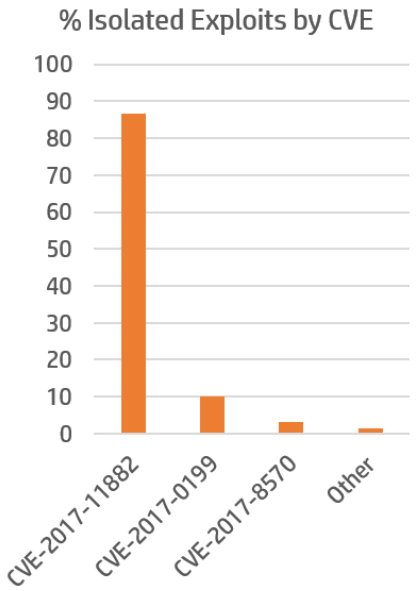


Figure 7 - Top exploits isolated by HP Sure Click in Q3 2020.

The low detection rates were primarily due to the documents being encrypted using Microsoft Word's "Encrypt with Password" feature. In this case, the documents' content and extended metadata were encrypted using AES in CBC mode with a 256-bit key. The emails containing the malicious attachments referenced the password so that recipients would be able to decrypt and open them. The most common passwords we found in this campaign were five characters long (e.g. "DLW16"), matching the regular expression ***[A-Z]{3}\d{2}***. Without the password, static and behavioural engines are unable to inspect the contents of the files. This technique also slows down retrospective investigations if the document password is not known. Since HP Sure Click captures a behavioural trace of activity when files are opened, this enables investigators to quickly obtain IOCs and the understand the capabilities and intent of malware involving encrypted files (Figure 8).

| Time from triggering event | Process | Details |
|---|---|---|
| 00:00:00.000 | 3340 WINWORD.EXE | ACTION: PROC_LOADIMAGE<br>SOURCE PATH: \Windows\explorer.exe<br>TARGET PATH: \Windows\explorer.exe |
| 00:00:00.000 | 3340 WINWORD.EXE | ACTION: PROC_CREATE_DROPLOADED<br>SOURCE PATH: \PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\WINWORD.EXE<br>TARGET PATH: \Windows\explorer.exe<br>DESCRIPTION: Dropped and Executed<br>`explorer c:\programdata\objStreamUTF8NoBOM.Vbe` |
| +00:00:00.672 | 4640 explorer.exe | ACTION: PROC_LOADIMAGE<br>SOURCE PATH: \Windows\System32\wscript.exe<br>TARGET PATH: \Windows\System32\wscript.exe |
| +00:00:00.687 | 4640 explorer.exe | ACTION: PROC_CREATE<br>SOURCE PATH: \Windows\explorer.exe<br>TARGET PATH: \Windows\System32\wscript.exe<br>DESCRIPTION: Invoked<br>`"C:\Windows\System32\WScript.exe" "C:\programdata\objStreamUTF8NoBOM.Vbe"` |
| +00:00:40.984 | 4792 regsvr32.exe | ACTION: PROC_LOADIMAGE<br>FILE SIZE: 311296<br>SHA-256: 7fee0f3adb6bb5a3ed22ad960709a87893e2512d099f6c8c39946097d9a4122b<br>SOURCE PATH: \UTF8NoBOM\APSLVDFB.dll<br>TARGET PATH: \UTF8NoBOM\APSLVDFB.dll |
| +00:00:41.844 | 4800 regsvr32.exe | ACTION: PROC_LOADIMAGE<br>FILE SIZE: 311296<br>SHA-256: 7fee0f3adb6bb5a3ed22ad960709a87893e2512d099f6c8c39946097d9a4122b<br>SOURCE PATH: \UTF8NoBOM\APSLVDFB.dll<br>TARGET PATH: \UTF8NoBOM\APSLVDFB.dll |

Figure 8 - HP Sure Click Enterprise behavioural trace showing an isolated TrickBot payload being executed by regsvr32.exe after a user opened a dropper document.

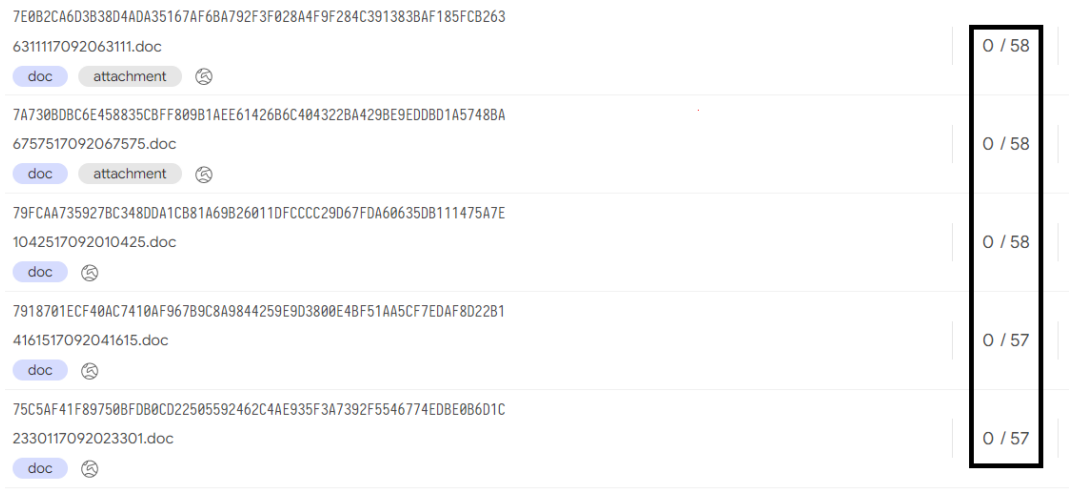


Figure 9 - Low detection rates of TrickBot dropper documents on VirusTotal, September 2020.

## ACTIONABLE INTELLIGENCE

### HP Sure Click Enterprise Recommendations

HP Sure Click Enterprise customers are always protected 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.

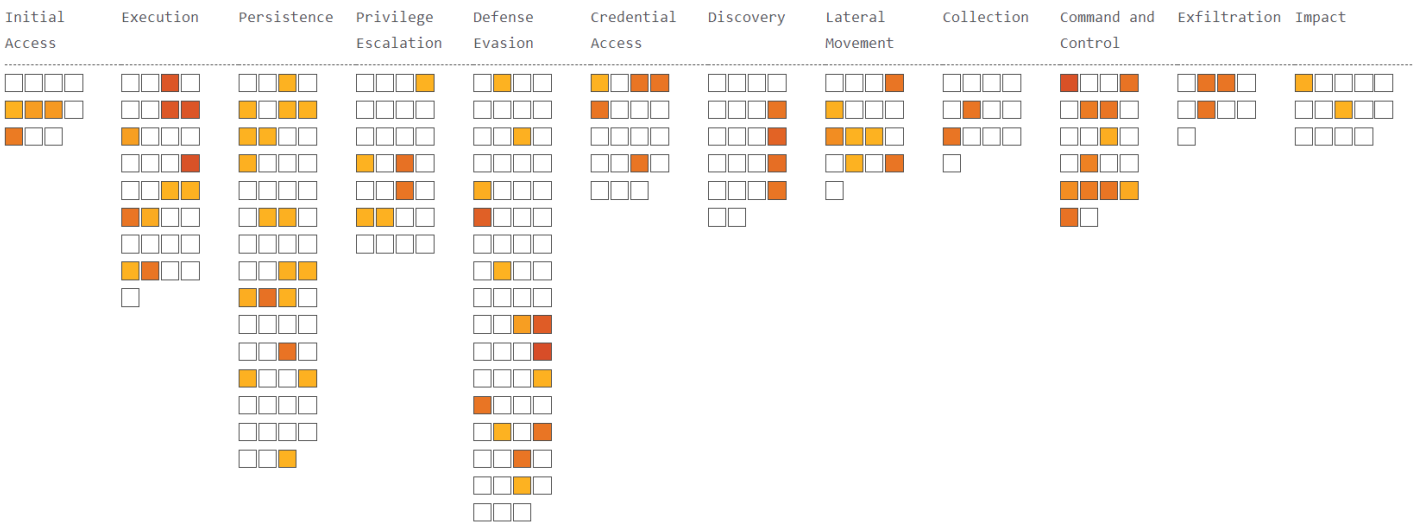


Figure 10 - MITRE ATT&CK heatmap showing the range of techniques used by threats isolated Q3 2020.[12]

## General Security Recommendations

Network defenders should consider implementing an email content filtering policy to reduce the risk of compromise by encrypted attachments containing malware. In June 2020, the Australian Cyber Security Centre published updated guidance on mitigating malicious emails.[13] These recommendations include implementing DMARC, safelisting attachments based on file types your organisation would expect to receive and blocking encrypted attachments.

## Signatures

The TrickBot dropper documents in the September 2020 campaign contained distinctive file artefacts that made it possible to detect them statically using a YARA rule. Specifically, the attackers modified two bytes in each document, likely as a way to avoid hash-based detection. We have published the rule below.

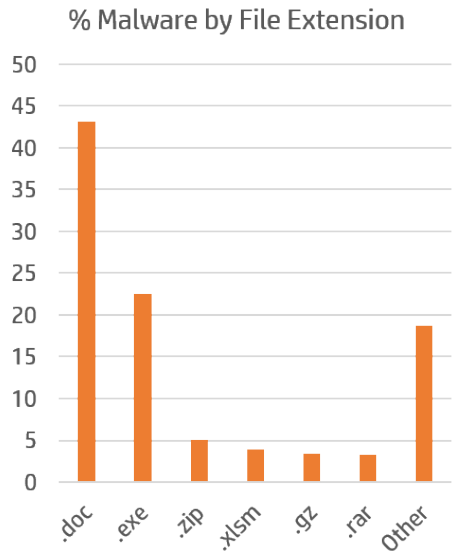


**Figure 11 - Top malware file extensions isolated by HP Sure Click in Q3 2020.**

```
rule trickbot_maldoc_embedded_dll_september_2020 {
   meta:
      author = "HP-Bromium Threat Research"
      date = "2020-10-03"
      sharing = "TLP:WHITE"

   strings:
      $magic = { D0 CF 11 E0 A1 B1 1A E1 }
      $s1 = "EncryptedPackage" wide
      $s2 = "{FF9A3F03-56EF-4613-BDD5-5A41C1D07246}" wide
      $s3 = { FF FF FF FF FF FF FF FF FF FF ( 90 90 | 10 10 | E2 E2 | 17 17 ) FF FF FF FF FF FF FF FF FF FF }

   condition:
      $magic at 0 and
      all of ($s*) and
      (filesize > 500KB and filesize < 1000KB)
}
```

## 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.[14] 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.[15] [16]

- 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.[17]

## 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.

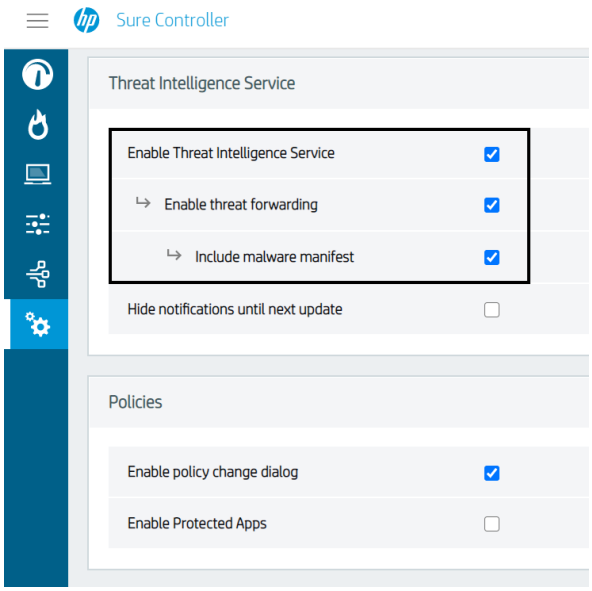


**Figure 12 - Recommended threat forwarding settings in HP Sure Controller.**

## REFERENCES

[1] https://www.bromium.com/wp-content/uploads/2019/07/Bromium-Emotet-Technical-Analysis-Report.pdf
[2] https://www.bleepingcomputer.com/news/security/emotet-botnet-is-now-heavily-spreading-qakbot-malware/
[3] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
[4] https://www.ncsc.gov.uk/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf
[5] https://www.kryptoslogic.com/blog/2019/04/emotet-scales-use-of-stolen-email-content-for-context-aware-phishing/
[6] https://threatresearch.ext.hp.com/detecting-a-stealthy-trickbot-campaign/
[7] https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html
[8] https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/
[9] https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
[10] https://www.bbc.co.uk/news/technology-48770128
[11] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report
[12] https://attack.mitre.org/
[13] https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Malicious%20Email%20Mitigation%20Strategies%20%28June%202020%29.pdf
[14] https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization
[15] https://support.bromium.com/s/topic/0TOU0000000Hz180AC/latest-news?language=en_US&tabset-3dbaf=2
[16] https://my.bromium.com/software-downloads/current
[17] https://threatresearch.ext.hp.com