THREAT INSIGHTS REPORT

May 2020

Bromium

THREAT LANDSCAPE

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

Bromium Secure Platform is deployed on desktops and laptops, capturing potential threats and allowing them 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 monitor, track and trace malware that tries to enter your networks.

NOTABLE THREATS

COVID-19-themed Threats

In March and April 2020, Bromium Labs observed an increase in threat actors using the COVID-19 pandemic as a lure to infect users. Authors of phishing emails commonly use social engineering techniques to entice targets to open malicious hyperlinks and attachments, for example by appealing to authority, urgency, curiosity, scarcity and current events.[1] COVID-19-themed phishing emails seen over the last two months have included fake purchase orders for ventilators, official notifications from government agencies and safety reports about new treatments for the disease, among others.

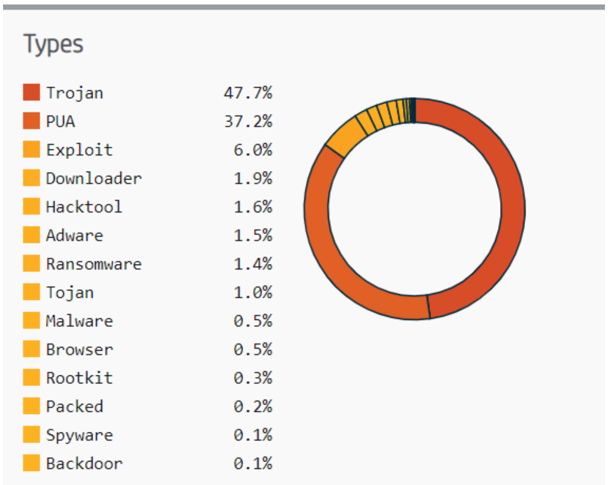
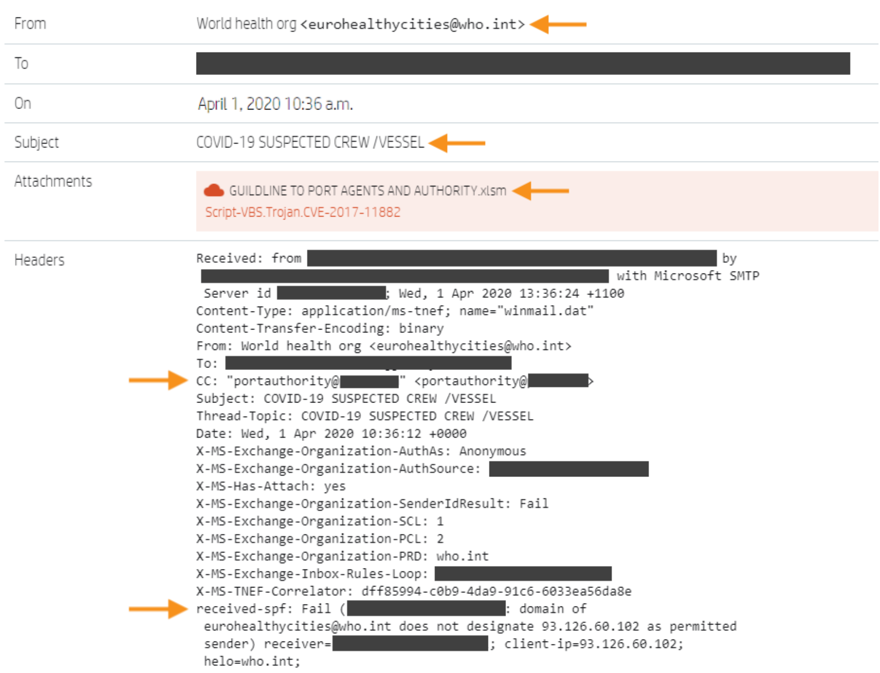


Figure 1 – Malware types isolated in March and April 2020.

Figure 2 shows one of the more interesting examples, where an organisation in the transportation industry was targeted by a phishing campaign delivering Agent Tesla, a commodity keylogger and remote access Trojan (RAT). The messages purported to be official notifications from the World Health Organisation (WHO).



From	World health org <eurohealthycities@who.int>
To	[redacted]
On	April 1, 2020 10:36 a.m.
Subject	COVID-19 SUSPECTED CREW /VESSEL
Attachments	GUILDLINE TO PORT AGENTS AND AUTHORITY.xlsm Script-VBS.Trojan.CVE-2017-11882

Headers

```
Received: from [redacted] by
 [redacted] with Microsoft SMTP
 Server id [redacted]; Wed, 1 Apr 2020 13:36:24 +1100
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: World health org <eurohealthycities@who.int>
To: [redacted]
CC: "portauthority@[redacted]" <portauthority@[redacted]>
Subject: COVID-19 SUSPECTED CREW /VESSEL
Thread-Topic: COVID-19 SUSPECTED CREW /VESSEL
Date: Wed, 1 Apr 2020 10:36:12 +0000
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-AuthSource: [redacted]
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SenderIdResult: Fail
X-MS-Exchange-Organization-SCL: 1
X-MS-Exchange-Organization-PCL: 2
X-MS-Exchange-Organization-PRD: who.int
X-MS-Exchange-Inbox-Rules-Loop: [redacted]
X-MS-TNEF-Correlator: dff85994-c0b9-4da9-91c6-6033ea56da8e
received-spf: Fail ([redacted]: domain of
 eurohealthycities@who.int does not designate 93.126.60.102 as permitted
 sender) receiver=[redacted]; client-ip=93.126.60.102;
 helo=who.int;
```

Figure 2 – Example COVID-19 phishing email viewed in HP Sure Controller.

To make the emails more convincing, the attacker spoofed the sender address to appear to have come from WHO's domain and included a legitimate-sounding email address in the CC field. The targeted organisation's email gateway detected that the sender address was spoofed because a Sender Policy Framework (SPF) authentication check had been configured. Nonetheless, the gateway let the emails through to the recipients' inboxes, where Sure Click isolated them.

The emails contained malicious Excel spreadsheets that downloaded and ran Agent Tesla using two code execution techniques. The first technique was through a Visual Basic for Applications (VBA) Auto Open macro, which relies on the user clicking "Enable Editing" and "Enable Content". The second way the downloader was triggered was by exploiting CVE-2017-11882, a vulnerability in Microsoft Office's Equation Editor present in versions prior to its January 2018 Public Update.[2]

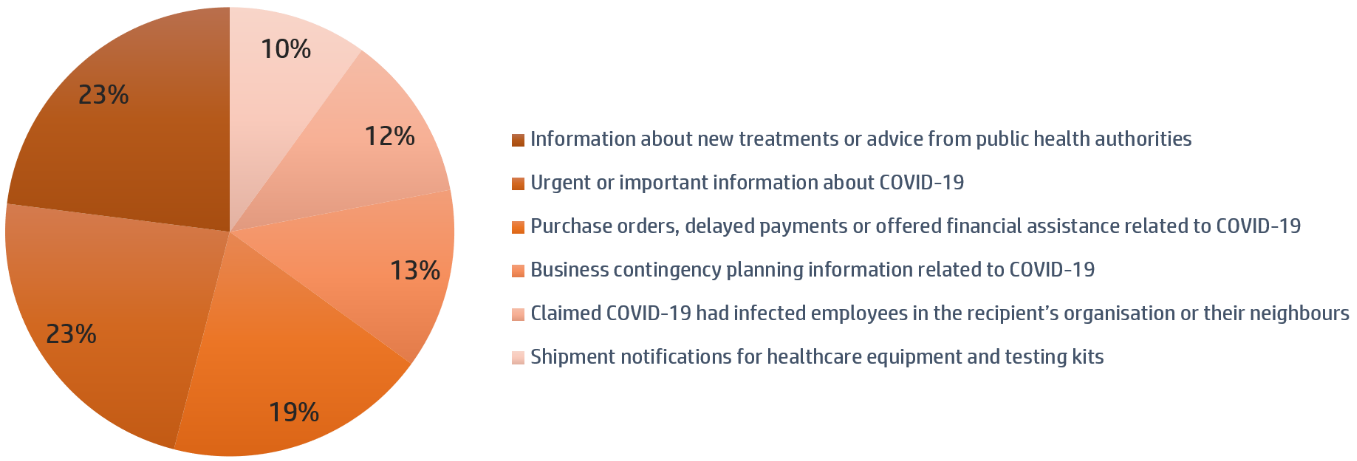
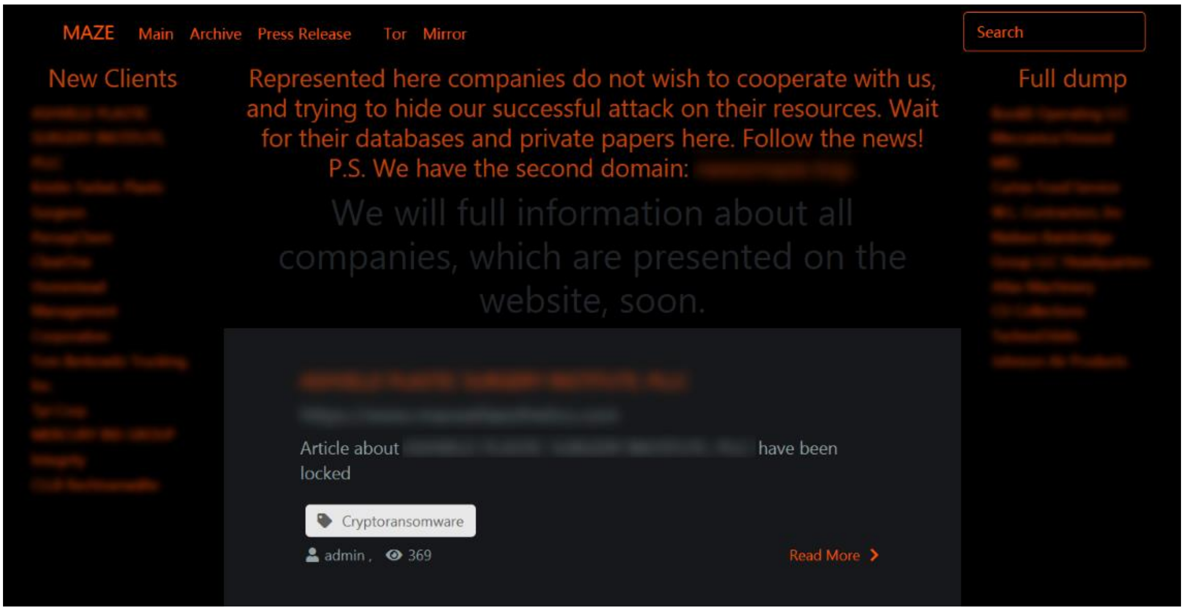


Figure 3 – Email lures used in COVID-19-themed threats isolated by Sure Click in March and April 2020.

Maze Ransomware

On 18 April, the US IT services firm Cognizant announced that their internal systems had been subject to a ransomware infection, causing service disruptions for some customers.[3] The company identified Maze as the ransomware family responsible for the breach. The actors behind Maze are one of the most audacious ransomware crews currently operating. Starting in November 2019, they were the first group to publish stolen victim data as an extortion tactic to pressure organisations into paying ransom demands, a tactic that was subsequently adopted by other malware authors.[4] Its developers keep a close eye on the malware research community and quickly respond to public analysis of their malware. Historical campaigns involving Maze have used a variety of initial access vectors, including stolen remote access service (RAS) credentials, malicious email attachments, and distribution through Fallout and Spelevo exploit kits.[5] The actors also claim to run a website where they release stolen victim data and publish announcements that chastise victims if they are not responsive to negotiating their ransom demands (figure 4).



New Clients

[redacted]

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: [redacted]

We will full information about all companies, which are presented on the website, soon.

Full dump

[redacted]

[redacted]

Article about [redacted] have been locked

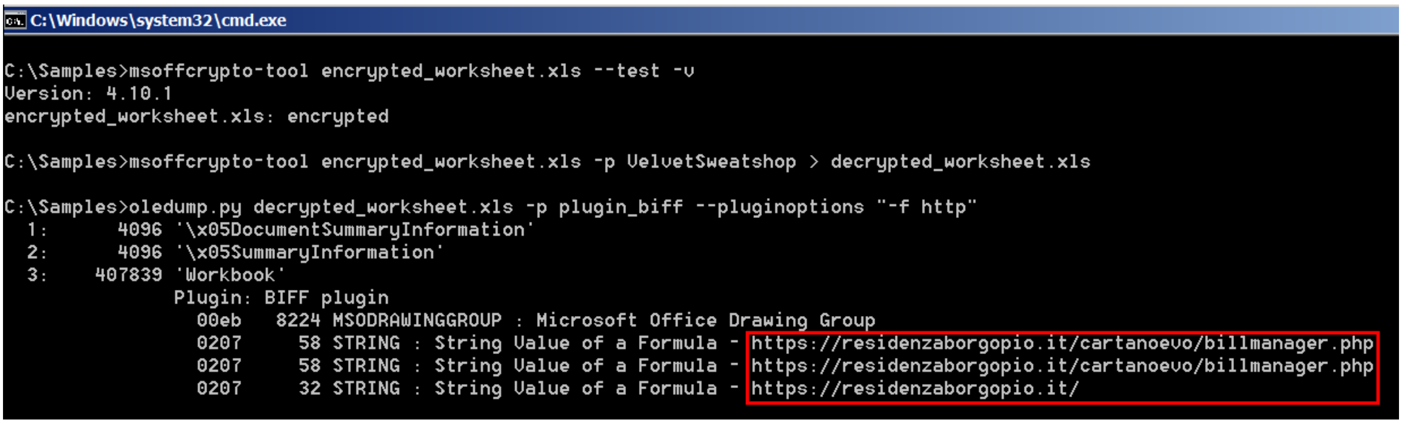
Figure 4 – Website claimed to be run by Maze's operators, May 2020.

NOTABLE TECHNIQUES

Evading Detection using Encrypted Documents and “Default” Passwords

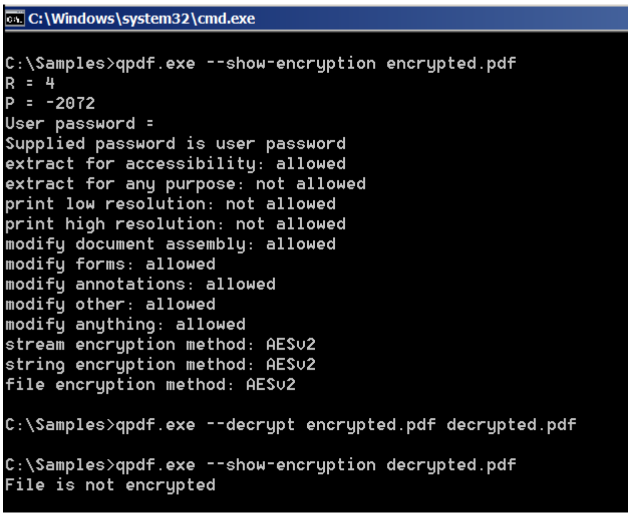
Threat actors often use encrypted documents to bypass static detection. One limitation of this approach is that the attacker needs to communicate the password and instructions on how to decrypt the document to the target, which may raise suspicion. Fortunately for attackers, some document standards contain lesser known or undocumented features that allow encrypted documents to be decrypted without any user interaction beyond opening the file. For example, Microsoft’s Excel Binary File Format (.XLS) allows worksheets to be encrypted. If the key for an encrypted worksheet is set to “VelvetSweatshop”, Excel automatically decrypts the worksheet without prompting the user for a password when the document is opened.[6] Figure 5 demonstrates the decryption of a malicious XLS file from a campaign in April 2020 that distributed Ursnif and QakBot banking Trojans.[7][8]

The Portable Document Format (PDF) specification also allows documents to be password protected through user and owner passwords.[9] If a user password is set to a zero-length key, Adobe Reader automatically decrypts the document without prompting the user when it is opened.[10] The implication of this feature is that an attacker can craft a malicious encrypted PDF file that doesn’t require user interaction to decrypt it when it’s opened, thereby evading static analysis. Figure 6 shows how to identify and decrypt a PDF file encrypted with a blank user password using QPDF.[11]



```
C:\Windows\system32\cmd.exe

C:\Samples>msoffcrypto-tool encrypted_worksheet.xls --test -v
Version: 4.10.1
encrypted_worksheet.xls: encrypted

C:\Samples>msoffcrypto-tool encrypted_worksheet.xls -p VelvetSweatshop > decrypted_worksheet.xls

C:\Samples>oledump.py decrypted_worksheet.xls -p plugin_biff --pluginoptions "-f http"
  1:      4096 '\x05DocumentSummaryInformation'
  2:      4096 '\x05SummaryInformation'
  3:    407839 'Workbook'
               Plugin: BIFF plugin
                 00eb   8224 MSODRAWINGGROUP : Microsoft Office Drawing Group
                 0207     58 STRING : String Value of a Formula - https://residenzaborgopio.it/cartanoevo/billmanager.php
                 0207     58 STRING : String Value of a Formula - https://residenzaborgopio.it/cartanoevo/billmanager.php
                 0207     32 STRING : String Value of a Formula - https://residenzaborgopio.it/
```

Figure 5 – Decryption of a malicious XLS worksheet encrypted using the key “VelvetSweatshop”. The distribution server that hosted the banking Trojans is highlighted in red.



```
C:\Windows\system32\cmd.exe

C:\Samples>qpdf.exe --show-encryption encrypted.pdf
R = 4
P = -2072
User password =
Supplied password is user password
extract for accessibility: allowed
extract for any purpose: not allowed
print low resolution: not allowed
print high resolution: not allowed
modify document assembly: allowed
modify forms: allowed
modify annotations: allowed
modify other: allowed
modify anything: allowed
stream encryption method: AESv2
string encryption method: AESv2
file encryption method: AESv2

C:\Samples>qpdf.exe --decrypt encrypted.pdf decrypted.pdf

C:\Samples>qpdf.exe --show-encryption decrypted.pdf
File is not encrypted
```

Figure 6 – Decryption of a PDF file encrypted using a zero-length password.

ACTIONABLE INTELLIGENCE

Bromium Secure Platform Recommendations

Bromium 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 Bromium Secure Platform software release and to use the Operational and Threat Dashboards in your Bromium Controller to ensure isolation is running correctly on your endpoint devices.

In your Bromium Secure Platform 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 Bromium Support if you need help applying suggested configurations.

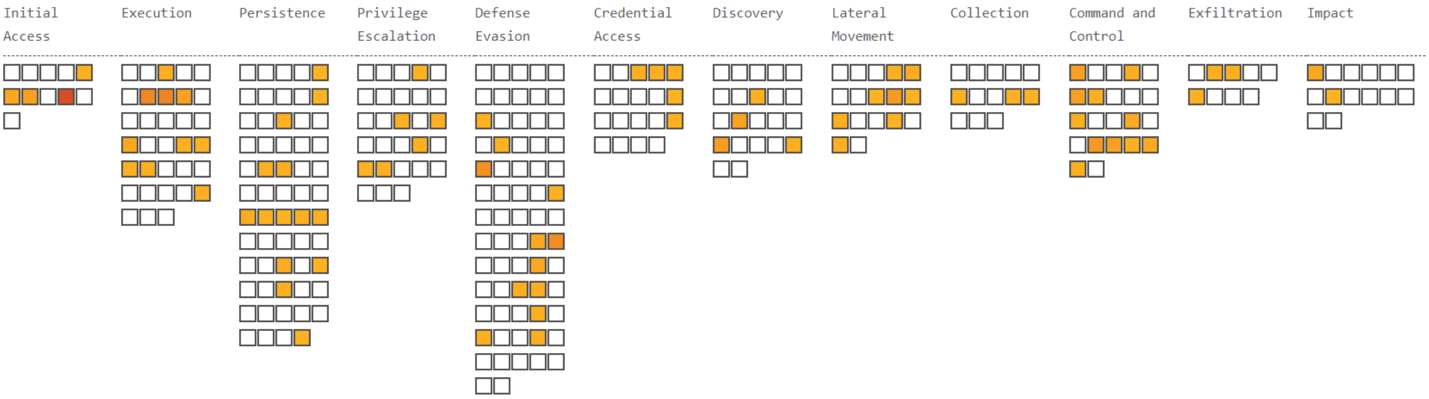


Figure 7 – MITRE ATT&CK heatmap showing the range of techniques used by threats isolated in March and April 2020.

General Security Recommendations

The COVID-19 pandemic has seen a rise in threat actors attempting to exploit home working technologies, such as teleconferencing, RAS and Virtual Private Network (VPN) software. As documented in this month's Notable Threats section, there has also been an increase in COVID-19-themed phishing threats used to distribute malware. In April, the UK's National Cyber Security Centre (NCSC) and US's Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on COVID-19-related threats.[12] Organisations can help reduce their risk by following the guidance set out by the NCSC and CISA, such as securely configuring VPNs and ensuring that software patches are installed in a timely manner.

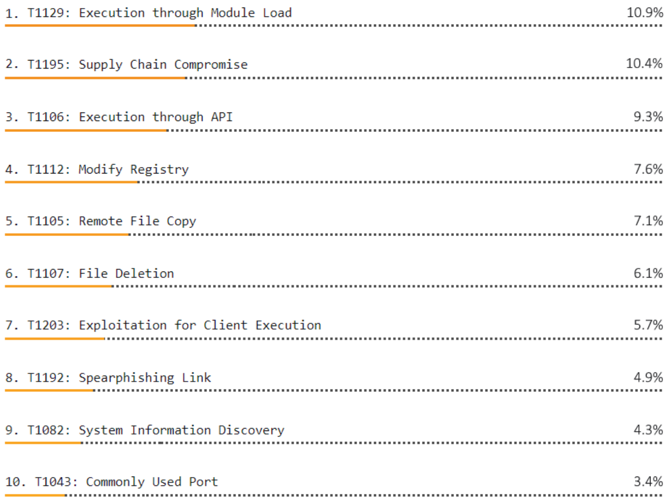


Figure 8 – Top 10 MITRE ATT&CK techniques used by threats isolated in March and April 2020.

Signatures

Bromium Labs have published a YARA rule that security teams can use to hunt for suspicious XLS files containing encrypted worksheets.

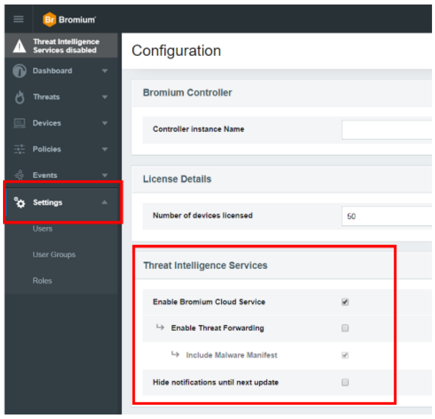
```
rule hunt_xls_encrypted_worksheet {
  meta:
    author = "Bromium Labs"
    date = "2020-04-17"

  strings:
    $magic = {D0 CF 11 E0 A1 B1 1A E1}
    $csp_mscrypto = "Microsoft Enhanced Cryptographic Provider v1.0" wide

  condition:
    $magic at 0 and
    $csp_mscrypto in (0..1000) and
    filesize < 10000KB
}
```

STAY CURRENT

The Bromium Threat Insights Report is made possible by customers who opt in to share their threats on the Bromium Threat Cloud. Alerts that are forwarded to us are analysed by our security experts to reduce false positives and are enriched with information that adds context to each threat. You can also use the threat data collected from isolated malware to protect other critical assets that are not secured by Bromium.

To learn more, review the Knowledge Base article on Threat Sharing. We recommend that customers take the following actions to ensure that they get the most out of their Bromium deployments:

- Enable Bromium Cloud Services and Threat Forwarding. This will keep your endpoints updated with the latest Bromium Rules File (BRF) and make sure we report the latest security incursions to you. Plan to update the Controller with every new release to receive the latest operational and threat intelligence report templates. See the latest release notes and software downloads available on the Customer Portal.
- Update Bromium endpoint software at least twice a year to stay current with emerging attack technique detections added by Bromium Labs.



Configuration

Bromium Controller

Controller instance Name

License Details

Number of devices licensed: 50

Threat Intelligence Services

Enable Bromium Cloud Service ☑

Enable Threat Forwarding □

Include Malware Manifest ☑

Hide notifications until next update □

For the latest threat research, head over to the Bromium Blog, where our researchers regularly dissect new threats and share their findings.

ABOUT THE BROMIUM THREAT INSIGHTS REPORT

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails or chats and downloading files from the web. Bromium Secure Platform protects the enterprise by isolating risky activity into micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. Since the malware is contained, Bromium Secure Platform collects rich forensic data to help our customers harden their entire infrastructure. The Bromium Threat Insights Report addresses key takeaways from the latest reported and analysed threats to ensure that our customers are thoroughly protected.

REFERENCES

[1] https://www.ncsc.gov.uk/guidance/suspicious-email-actions
[2] https://support.office.com/en-gb/article/equation-editor-6eac7d71-3c74-437b-80d3-c7dea24fdf3f
[3] https://news.cognizant.com/2020-04-18-cognizant-security-update
[4] https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/
[5] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze
[6] https://www.mimecast.com/blog/2020/03/velvetsweatshop-microsoft-excel-spreadsheet-encryption-rises-again-to-deliver-limerat-malware/
[7] https://github.com/nolze/msoffcrypto-tool
[8] https://blog.didierstevens.com/programs/oledump-py/
[9] https://en.wikipedia.org/wiki/PDF#Security_and_signatures
[10] https://www.synack.com/blog/decrypting-malicious-pdf-documents-part-one/
[11] http://qpdf.sourceforge.net/
[12] https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf