THREAT INSIGHTS REPORT

May 2019

Bromium®

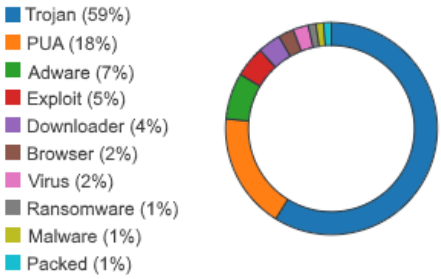
THREAT LANDSCAPE

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

Bromium Secure Platform is deployed on desktops and laptops, capturing any potential threats inside isolated virtual machines and allowing them to detonate. Adding isolation to the endpoint security stack transforms your endpoints into your strongest defense, giving security teams a unique advantage to be able to monitor, track and trace any malware that tries to enter your networks.

NOTABLE THREATS

In recent weeks, Bromium Labs research uncovered malware distribution infrastructure hosted on web servers in an autonomous system located in the United States, called AS53667. The perpetrators used servers to host 10 malware families, sometimes with multiple families on the same servers, and were distributing them through malicious spam campaigns. The malware included banking Trojans, information stealers and ransomware such as **Dridex**, **AZORult** and **GandCrab**. This discovery exposed an Amazon-style fulfilment service used by malware operators.



Malware classifications, April 2019

Campaigns delivering **Ursnif**, a prevalent banking Trojan, are becoming increasingly sophisticated using steganography, COM objects and WMI to bypass security controls. These campaigns are now geo-aware, allowing the Trojan's operators to target specific regions and locales.

Emotet remains one of the most frequent threats we isolate. Find out how this banking Trojan is so effective at establishing a foothold in unprotected networks in parts one and two of our technical breakdown.

NOTABLE TECHNIQUES

The use of scripting languages (MITRE ATT&CK ID: T1064) such as Visual Basic for Application (VBA) macros was the top execution technique we saw in April, but this is far from the only method for launching malicious payloads. We isolated a novel dropper in a malicious Word document that ran an encoded PowerShell command when previewed in Windows Explorer's Preview Pane before the user had even opened the file. By requiring no user interaction to execute the command, the attacker doesn't need to rely on social engineering for the next attack stage to succeed.

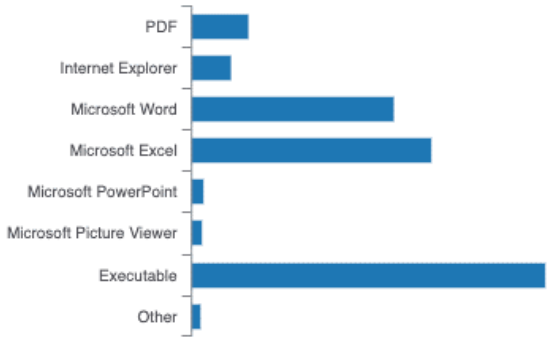
Removable media, such as USB drives, remain an effective vector to spread malware (MITRE ATT&CK ID: T1091). In April, we isolated the execution of malicious shortcut (LNK) files when an infected USB drive was plugged into a protected endpoint. The drive contained **Retadup**, a worm and a Remote Access Trojan (RAT) written in AutoIT and AutoHotKey scripting languages that has keylogger and crypto mining capabilities. The worm propagates by copying itself to all available volumes on the filesystem, including removable media and network shares. When one of the shortcut files is opened, a cmd.exe process is spawned; which then runs an AutoIT or AutoHotkey executable that loads the malicious script.

ACTIONABLE INTELLIGENCE

Bromium Secure Platform Recommendations

Bromium customers are always protected, as malware is isolated from the host PC and cannot spread onto the corporate network. It is always advisable to stay current on software releases (latest release notes) and to use the Operational and Threat Dashboards in your Bromium Controller to ensure isolation is running correctly on your endpoint devices.

Besides executables, the top malware formats that we see across Bromium customers are malicious Microsoft Word and Excel documents that users are either emailed directly or tricked into downloading via their web browser. In your Bromium Secure Platform policy we recommend that untrusted file support for email clients and Microsoft Office protection are enabled (these are enabled by default in our recommended policies). Switching on these settings is a straightforward way to reduce the risk of infection posed by phishing campaigns.



Malware by application, April 2019

There has also been a small increase in Microsoft Office malware delivered in encrypted ZIP files, which is a popular technique to evade email attachment scanning. To mitigate against this technique, we recommend enabling ZIP protection. If you are running version 4.1.5 or later, you will also benefit from significant usability improvements to ZIP workflows inside micro-VMs.

Please contact Bromium Support for assistance in applying the suggested configurations at https://support.bromium.com/.

General Security Recommendations

One of the key findings from our analysis of a collection of US-based web servers found hosting malware was the observation that the payloads were downloaded using VBA macros in Microsoft Office documents distributed in mass phishing campaigns. One of the steps you can take to protect your network is to follow macro security best practice by locking down Microsoft Office's macro settings so that only trusted or signed macros can run. These settings can be enforced through Group Policy using the administrative templates appropriate to the version of Microsoft Office you have deployed. For several years, the Australian Cyber Security Centre has been producing excellent guidance on this topic. Additionally, we've provided an OpenIOC signature to detect file write events of the executables linked to these malicious spam campaigns.

Signatures

OpenIOC (Logic Tree):

```
OR
├ File Name is qwerty2.exe
AND
 └ File Full Path contains \appdata\local\temp\
```

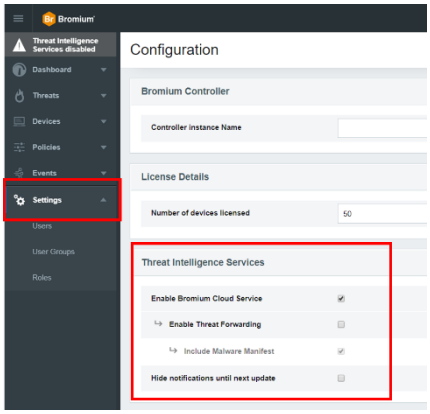
OpenIOC (XML):

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="1f77ee18-7e8f-4d5c-b977-ce1d967483c8"
last-modified="2019-04-15T09:43:09" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>malware_distribution_servers_dropped_exe</short_description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-04-12T14:16:05</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="7e582124-e7eb-4b8b-9c9d-fde09f06017d">
      <IndicatorItem id="2a5647a7-0db6-4241-b2f3-5eb29d5c6c54" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">qwerty2.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="e2bff2a2-0d37-4794-8b9c-366cef9cd0cf">
        <IndicatorItem id="28205128-91fa-4c7a-b589-60bebb577430" condition="contains">
          <Context document="FileItem" search="FileItem/FullPath" type="mir" />
          <Content type="string">\appdata\local\temp\</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

STAY CURRENT

The Bromium 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 analyzed by our security experts to reduce false positives and generate more detailed, higher-fidelity alerts. You can also use the threat data collected from isolating malware in micro-VMs 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 deployments:



- Enable Bromium Cloud Services and Threat Forwarding. This will keep your endpoints updated with the latest Bromium introspection 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.

For the latest threat research check out our Technical blogs, where our researchers dissect novel threats and share how they work.

ABOUT BROMIUM INSIGHTS REPORT

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