Bromium®

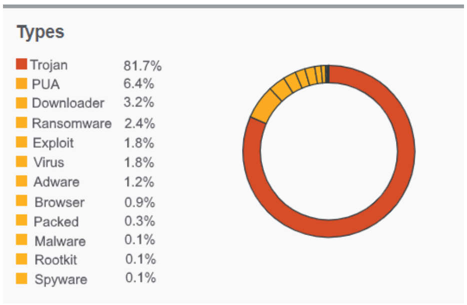
THREAT INSIGHTS REPORT

JULY 2019

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 any potential threats and allowing them to detonate 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 any malware that tries to enter your networks.

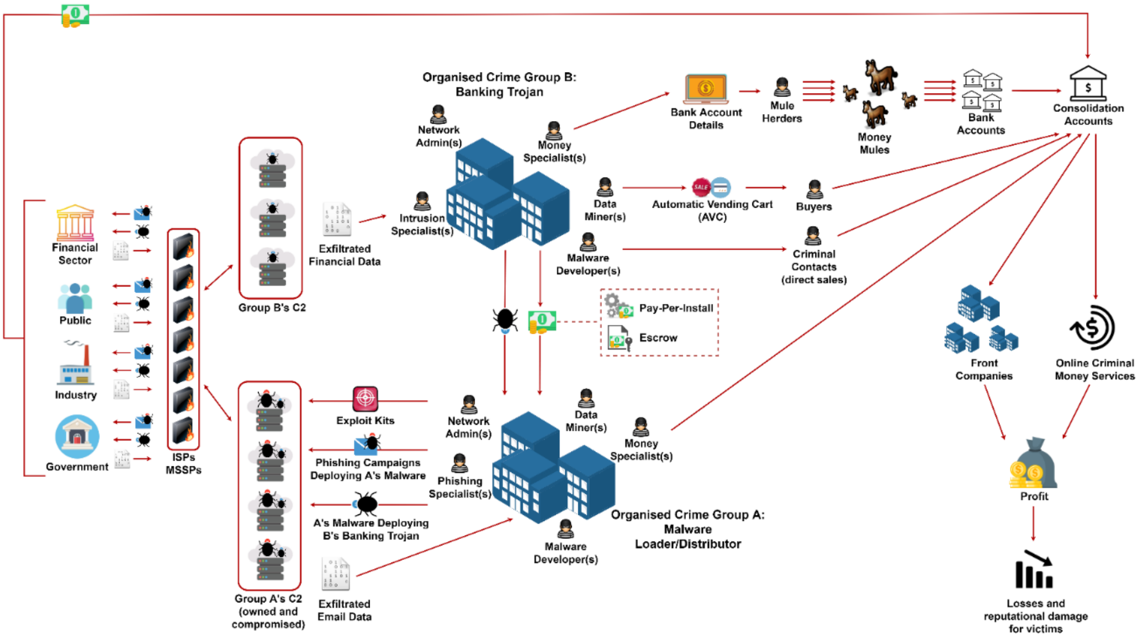


Malware type classifications, June 2019

NOTABLE THREATS

Two Florida cities, Riviera Beach and Lake City, paid ransoms totalling $1.1 million (USD) after their networks were compromised by ransomware. Lake City officials described how they were targeted by a "triple threat", a likely reference to the delivery of Ryuk ransomware by TrickBot following an Emotet infection. These incidents have sharpened focus on the ethical and practical issues of victims paying ransoms to regain access to their data. For Lake City, the cost of the ransom was covered by cyber liability insurance, an increasingly popular type of insurance that mirrors kidnap-and-ransom (K&R) insurance developed in the 1930s. To victims, paying the ransom is an attractive but expedient choice compared to costly and lengthy remediation projects, particularly if no working backups exist. For example, the estimated remediation cost of the LockerGoga ransomware incident that affected Norsk Hydro in March 2019 is $52 million. However, paying ransoms fuels the operations of criminal groups, offers no guarantee that attackers are willing or able to decrypt ransomed files, and may incentivise more ransomware attacks.

Since the start of June 2019, we observed that Emotet phishing campaign activity ceased. The Cryptolaemus group of security researchers found that Emotet's first tier of command and control (C2) infrastructure went offline on 7 June. CenturyLink also published excellent research into the structure of Emotet's C2 infrastructure using network forensics. In our upcoming report we examine the business model of malware distributors such as Emotet, building on previous research into organised criminal groups by the UK's National Cyber Security Centre.

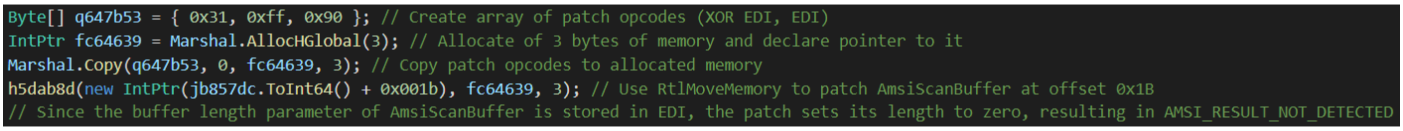


Malware as a Service (MaaS) business model where group A distributes group B's banking Trojan

Historically cryptomining malware has been regarded as a low severity threat, but Bromium Labs analysed Monero cryptomining malware that changes this assessment. The malware was notable for dropping a suite of publicly available post-exploitation tools, including Mimikatz, Smbtouch-Scanner, masscan and ProcDump. The use of these tools suggests that deploying cryptominers was not the only objective of the attacker. The rebound in the value of cryptocurrencies is one reason why cryptojacking attacks have become increasingly attractive to criminals. The value of Monero more than doubled over the first half of 2019, from $46 to $98.

NOTABLE TECHNIQUES

Bromium Labs analysed a malicious Rich Text Format (RTF) file shared by a government customer after it was isolated by Bromium Secure Platform. The file contained a C# class that bypasses the Antimalware Scan Interface (AMSI) in Windows 10. AMSI is an interface standard that allows services and applications such as PowerShell to be scanned by antimalware software installed on a system. The bypass works by patching the AmsiScanBuffer function in memory so that the value of the length parameter is zero, causing AMSI to scan an empty buffer and return a clean result. The RTF file used the PowerShell Add-Type cmdlet to compile the class after it was delivered using .NET Framework tools that were already installed on the host (MITRE ATT&CK IDs: T1500 and T1127). Ultimately the document attempted to deliver Pony, a family of information stealing malware.



```
Byte[] q647b53 = { 0x31, 0xff, 0x90 }; // Create array of patch opcodes (XOR EDI, EDI)
IntPtr fc64639 = Marshal.AllocHGlobal(3); // Allocate of 3 bytes of memory and declare pointer to it
Marshal.Copy(q647b53, 0, fc64639, 3); // Copy patch opcodes to allocated memory
h5dab8d(new IntPtr(jb857dc.ToInt64() + 0x001b), fc64639, 3); // Use RtlMoveMemory to patch AmsiScanBuffer at offset 0x1B
// Since the buffer length parameter of AmsiScanBuffer is stored in EDI, the patch sets its length to zero, resulting in AMSI_RESULT_NOT_DETECTED
```

Annotated AMSI C# bypass observed in June 2019

Bromium Labs examined creative language-checking techniques used by malware to determine if a particular operating system language is being used before downloading a second-stage payload. Instead of checking the system language directly, two separate malware families looked for strings in the output of system commands that are unique to certain language packs.

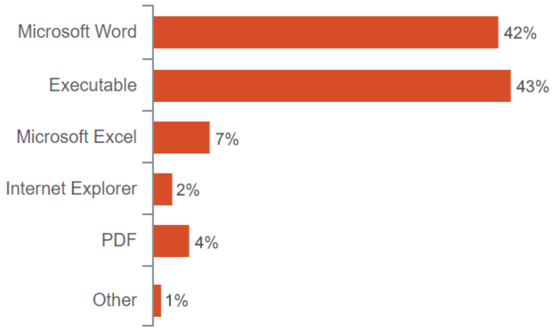
Command	Output	Desired String	OS Language
ping 4.4.4.4 -n 0	“Valeur incorrecte pour l’option -n, plage valide comprise entre 1 et 4294967295.”	l’	French
((Get-WmiObject Win32_OperatingSystem).OSArchitecture -match [char]12499)	“32ビ” “64ビ”	ビ	Japanese

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 June 2019, the most targeted application by malware across Bromium customers were portable executable (PE) files.



Malware by application, June 2019

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.

General Security Recommendations

We recommend reducing your attack surface by enforcing the principle of least privilege on programs that users have access to. Access control features built into Windows such as Windows Defender Application Control (Windows 10, Windows Server 2016 and 2019) and AppLocker (Windows 7 and above) can be used to achieve this. For example, we recommend limiting access to high risk living off the land binaries (LOLBins) only to groups in your Active Directory that need them to perform their role in the organisation. For example, non-developer groups should not have access to build tools that can be abused by malware.

Signatures

The focus of this month’s signatures are methods of detecting language-checking techniques. Below are two OpenIOC signatures for detecting the techniques described in Notable Techniques.

```
<?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="6435ced8-5f43-418b-97d4-6d69a6e78698"
last-modified="2019-07-02T20:44:50" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>language_check_ping</short_description>
  <description>Detects language-checking technique using ping.exe documented here:
https://www.bromium.com/malware-os-language-targeted-attacks/</description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-07-02T18:04:03</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="473c0c7f-f76d-4152-a67c-bdbf1ef76edf">
      <IndicatorItem id="ec6bfbd1-46b6-4ed2-97ea-6d213b0d11ad" condition="is">
        <Context document="ProcessItem" search="ProcessItem/name" type="mir" />
        <Content type="string">ping.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="5d3b54d6-c3af-4aa9-969e-0982a81c20fe">
        <IndicatorItem id="d9fb6a8e-763a-4893-bdcc-c52081674687" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/arguments" type="mir" />
          <Content type="string">-n 0</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

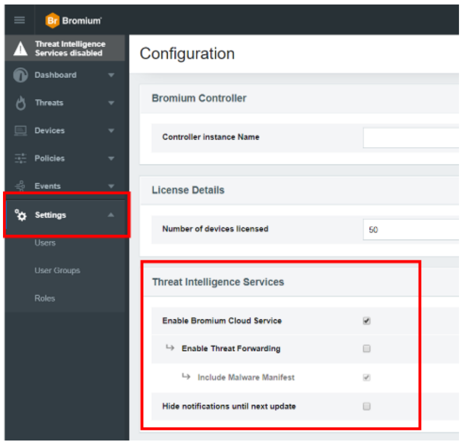
```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="411024cb-350d-4311-b2b7-911cb1adb6ff"
last-modified="2019-07-02T20:44:54" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>language_check_yakes</short_description>
  <description>Detects language-checking technique used by Yakes documented here:
https://www.bromium.com/malware-os-language-targeted-attacks/</description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-07-02T20:40:46</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="7cbf6ebd-ecc6-4ab5-a872-1cbb228dd0bf">
      <IndicatorItem id="7e70c36a-2cdf-4442-a7f0-18e2498b1484" condition="is">
        <Context document="ProcessItem" search="ProcessItem/name" type="mir" />
        <Content type="string">powershell.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="4a6d30f8-06a5-4423-beeb-60af42bb306b">
        <IndicatorItem id="2d22628d-f186-4559-9cb6-eec30656c60b" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/arguments" type="mir" />
          <Content type="string">((Get-WmiObject Win32_OperatingSystem).OSArchitecture
-match</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

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 generate higher fidelity alerts. 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.