What Red Canary Detects

Red Canary delivers extensive detection across the attacker's kill chain by analyzing endpoint telemetry and detecting threats using multiple techniques and technologies. Below are examples of the threatening behaviors that Red Canary detects.

- **Use of anonymization services**
  Includes use of services such as Tor to mask the source and/or destination of network traffic.

- **Unauthorized access to hidden or administrative shares**
  Access to hidden-but-present shares intended for use by systems administrators. Very commonly leveraged for lateral movement.

- **Specific threat actor campaigns and/or TTP**
  Patterns of behavior and movement associated with specific actors and/or used to achieve specific objectives.

- **Privilege escalation**
  Use of malware or native operating system utilities to escalate from userspace to superuser privileges. Used to gain access to resources not available upon arrival.

- **Placement of exploit kits**
  Use of automated targeting and exploitation kits within an environment for lateral movement with a minimum of external communication or human interaction.

- **Obfuscation of binary names**
  Executable files with misleading extensions. Malware is often disguised as a rich document type, screen saver or another file type/extension other than .exe. This is done to evade simple mail and web content filtering.

- **Network connections to recently registered domains**
  Use of DNS- and registrar-based intelligence to identify systems communicating with external hosts that are globally new or unique.

- **Network connections to known bad domains and IPs**
  Use of comprehensive threat intelligence to identify known bad artifacts within network connection metadata.

- **Misuse of host OS utilities**
  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 shared file systems**
  Placement of malware, auto-execution configuration files and other undesirable items on file systems shared amongst endpoint or network users. Frequently used to propagate malware within an environment.

- **Manipulation of host operating system**
  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.

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

- **Hiding processes from logged-in user**
  Tools and techniques used to evade detection based in human or automated review of running processes.

- **Exploitation of known vulnerabilities**
  Behaviors specific to exploitation of vulnerable software or vulnerable operating system configurations.

- **Exfiltration of data**
  Behaviors or intelligence that indicate movement of data from an endpoint to a suspicious network or media destination.

- **Execution of malware based on signature**
  Files detectable based on threat intelligence or traditional anti-virus signature.

- **Execution of malware based on behavior**
  Processes exhibiting behaviors or having interprocess relationships often observed by malware.

- **Execution of binary flagged by binary analysis**
  Processes associated with a binary that either dynamic or static analysis indicates may be malicious.

- **Execution from abnormal file system locations**
  Includes execution from recycle bin, removable media and a number of similar locations. This technique is used to prevent malware from being found in overt paths by humans or automated systems.

- **Destruction of data**
  Deletion or relocation of data, either for purposes of destruction or random.

- **Delivery of executable files via email**
  Files written by mail clients such as Outlook that either are or contain an executable. Detects probable phishing attacks.

- **Credential stealing**
  The process of accessing sensitive files or protected memory to obtain user credentials. Also the tools used to perform these activities.

- **Addition/Modification of user accounts**
  Use of native operating systems tools to create or manipulate user accounts or groups. This technique is frequently used to maintain access without the use of additional malware.

- **Execution of untrusted binary**
  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.

- **Suspicious network activity**
  Suspicious patterns of network-related activity, including connections to many unique domains and/or IP addresses within a period of time.

- **Abnormal user activity at time**
  User activity on an endpoint that is abnormal based on when the activity occurred as compared to a baseline of the user’s activity.

- **Installation or modification of persistence mechanisms**
  Use of startup folders, autoruns, task scheduling and service registration among others for purposes of gaining, maintaining or altering persistence on an endpoint.

- **Execution of binary with suspicious content**
  Files detectable based on contents of a binary file. Includes YARA and similar inspection mechanisms.

- **Use of dynamic DNS services**
  Dynamic DNS is often used by attackers to avoid stand-out activities such as registration of a new domain name.

- **Disabling of security software and safeguards**
  Includes tampering with, disabling or changing a variety of security safeguards, to include host-based firewalls and others. Does not include tampering related to the Red Canary sensor.

- **Abnormal user activity on endpoint**
  User activity on an endpoint that is abnormal based on which endpoints the activity occurred on as compared to a baseline of the user's activity across the organization.

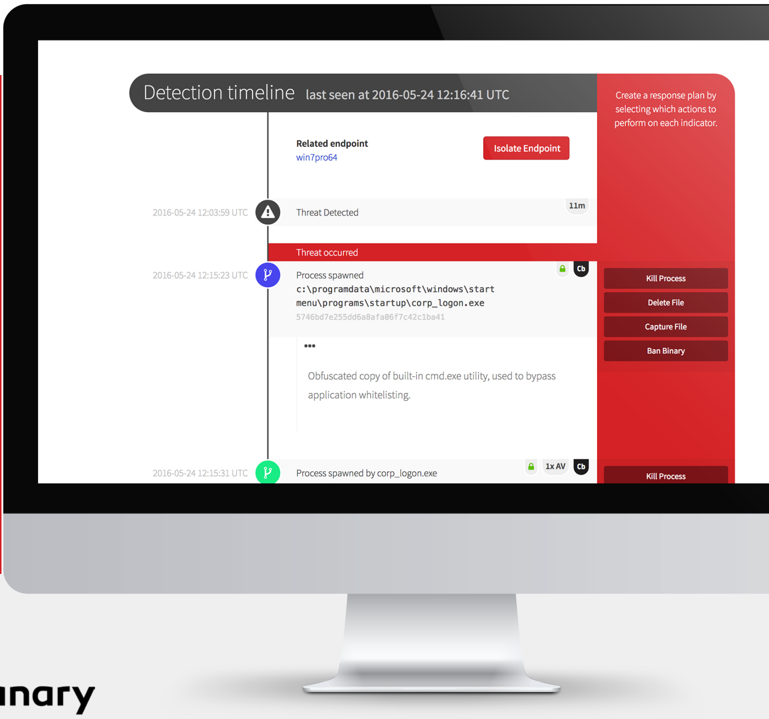
- **Abnormal user activity**
  User activity that is abnormal based on the existence of that user or prevalence across the organization as compared to a baseline of the organization's user activity.

- **Abnormal application by user**
  Use of an application that abnormal for a user compared to a baseline of the user's activity.

- **Sensor tampering**
  Tampering of the Red Canary endpoint sensor as evidenced by activity including attempted injection into the sensor process, modification of the sensor's data store, recorded activity, log files, etc.

About Red Canary

Red Canary helps defenders win against rapidly evolving adversaries. The solution quickly and accurately identifies threats on customers' endpoints ranging from compromised credentials to lateral movement to crimeware. Every threat is investigated by a Red Canary analyst to remove false positives and provide the context required for remediation.



Detection timeline last seen at 2016-05-24 12:16:41 UTC

Create a response plan by selecting which actions to perform on each indicator.

Related endpoint
win7pro64

2016-05-24 12:03:59 UTC Threat Detected 11m

Threat occurred

2016-05-24 12:15:23 UTC Process spawned

```
c:\programdata\microsoft\windows\start
menu\programs\startup\corp_logon.exe
5746bd7e255dd6a8afa06f7c42c1ba41
```

Obfuscated copy of built-in cmd.exe utility, used to bypass application whitelisting.

2016-05-24 12:15:31 UTC Process spawned by corp_logon.exe 1x AV

See how Red Canary can help you secure your endpoints.

www.redcanary.com/demo