OneLaunch and Threat Response

Mentors: Jennifer Brown, Tammera Campbell, Kevin Broussard, Kahefe Fatima

Intern: Robin Simpson

What is One Launch and PUPs

A Potentially Unwanted Program (PUP), or Potentially Unwanted Application (PUA), is a program that a user may perceive as unwanted. It is used to describe applications that are not malicious by nature but may be annoying or undesirable.

These programs often come bundled with other software and are installed on a system due to the user not noticing or deselecting optional checkboxes during the installation process. PUPs can include software such as adware, spyware, or unwanted toolbars.

While PUPs are usually not harmful or dangerous in the same way that malware is, they can compromise user privacy, slow down your computer, clutter up your system with unwanted files or changes, and generally degrade the user experience.

OneLaunch is classified as a PUP; it is an insecure web browser that can pose a risk to Lab security and systems.

How is OneLaunch detected on Crowdstrike

1. **Behavior Analysis**: CrowdStrike's Falcon uses behavioral analysis to detect abnormal activity, such as the activity that might be associated with a PUP. When a program starts performing actions that are outside the norm, Falcon flags it for further investigation.
2. **Machine Learning**: Falcon incorporates machine learning algorithms to analyze files and detect potential threats. These algorithms are trained on vast datasets, allowing them to recognize and block PUPs based on their characteristics.
3. **Signature-Based Detection**: While less effective against new, unknown threats, signature-based detection can still be useful in identifying known PUPs. Falcon would compare the signatures of files on the system to a database of known threat signatures to identify matches.
4. **Cloud-Based Threat Intelligence**: CrowdStrike's Threat Graph collects and analyzes data from millions of endpoints around the world, giving it a broad view of the threat landscape. This can help in identifying PUPs and other threats based on data from other systems.
5. **Indicators of Attack (IoAs)**: CrowdStrike uses IoAs to detect threats, including PUPs. Rather than waiting for a signature or known malicious behavior, IoAs can help to identify a threat based on the preliminary steps it takes, before the actual damage has been done.
6. **Sandboxing**: Falcon uses sandboxing technology to run and analyze suspicious programs in an isolated environment, preventing them from causing harm to the actual system.

The Protocol in removing PUPs at Berkeley Lab

Workflow preview

- New endpoint detection
  - IF Tactic is equal to Malware
    - AND Technique is equal to PUP
    - AND Severity is equal to Low
    - AND Image file name matches *chromium.exe
    - AND Sensor platform is equal to Windows
  - Remove OneLaunch V2
    - Add comment to endpoint detection
      - Assign endpoint detection to user
        - Set endpoint detection status
          - Send email

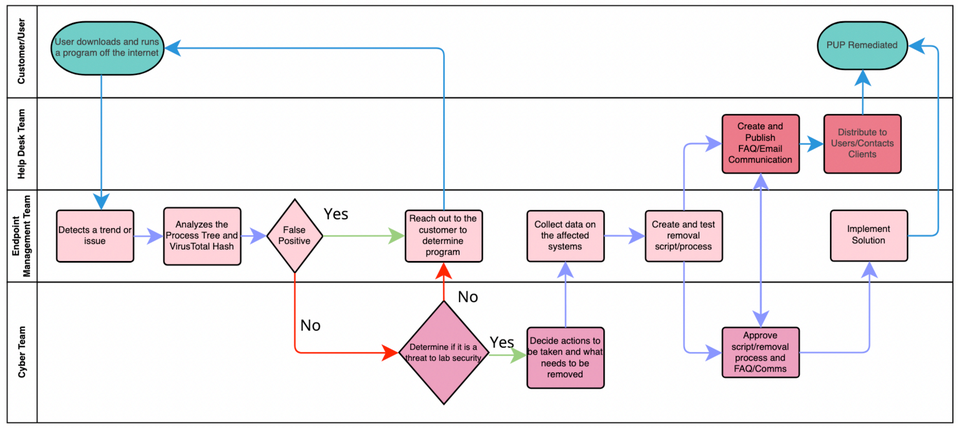
Based on the threat of the program, actions taken by Cyber team could range from quarantining system, to rebuilding the system where you send computer in, receive a loaner until repair

Endpoint creates a ticket for the detection with necessary information and recipients

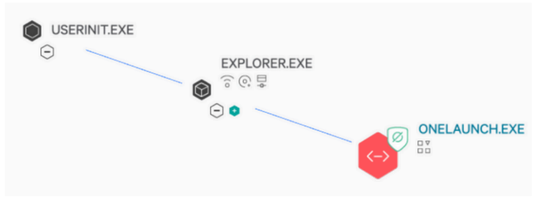
Script removal process depends on its prevalence

Simultaneously, the workflow emphasizes clear and timely communication. This involves creating and distributing communications to inform relevant parties about the threat and the steps being taken to address it.

This enhances workplace security by ensuring a proactive, thorough, and systematic approach to cybersecurity, which is crucial in today's digital age.



How it looks on the Crowdstrike Dashboard



Process History/Tree of a User's Actions

ACTION TAKEN	Process killed
SEVERITY	High
OBJECTIVE	Keep Access
TACTIC & TECHNIQUE	Persistence via Registry Run Keys / Startup Folder
TECHNIQUE ID	T1547.001
IOA NAME	RegistryPersistEdit
IOA DESCRIPTION	A process made a suspicious change to the registry that might indicate a malicious persistence mechanism. Investigate the registry key.

Sample Email Response to OneLaunch Detection

Dear End User,

CrowdStrike detected the installation of One Launch on your system with:

- Hostname: {{Hostname}}
- Last Username: {{Last username}}

This software is categorized as a "Browser Helper" and may not be helpful as you think, see FAQ article Protect Your Browser Against Browser Hijackers. We will be removing this from your computer using CrowdStrike and request your support in learning more about this subject and avoid having your information hijacked.

For more information on CrowdStrike see our FAQ articles below:

CrowdStrike Falcon Information
CrowdStrike Falcon FAQ
CrowdStrike Falcon and Privacy
Install/Uninstall CrowdStrike Falcon

If you have any further questions or require support, reply to this email and a service ticket will be generated.

Sincerely,
IT User Support
go.lbl.gov/ITChat

Beware of phishing attempts! To verify the legitimacy of this email, please contact the IT Help Desk at go.lbl.gov/ITChat.

Effects on Lab Security

- Next Gen AV
- No more scanning of systems
- Uses AI and Machine Learning
- RTR (Real Time Response) and Isolation capabilities can potentially stop threats before they get to LBLNet
- Detected things that Sophos was missing

As of July 2023, Crowdstrike removed 27 OneLaunch instances and hundreds of PUPs/Malware.

The current multilayered in-depth process and protocol ensures safety towards lab and employee data.

Acknowledgements

This research was supported in part by the **U.S. Department of Energy** (DOE), **Omni Technology Alliance Internship Program**. The program is championed by the DOE's **Office of Chief Information Officer** (OCIO) and represents a partnership with the leadership of the **Office of Economic Impact and Diversity**, the **Office of Science, the Office of Nuclear Energy**, and the **National Nuclear Security Agency**. The program is administered by the **Oak Ridge Institute for Science and Education**.