Self Protect Service

University of Calgary, Schulich School of Engineering, Cisco Systems

Authors: Martin Ha, Duan Le, Shubh Sharma, Ayush Chaudhari, Hemish Minhas, Steafen Nicolo Rivera
Department: Electrical & Software Engineering

Introduction

- The number of cyber attacks due to malware on target industries has increased over the last 20 years:
  - 12.4 million computer infections in 2009
  - 812.67 million computer infections in 2018
- Many targeted industries leverage technologies such as Cisco's Secure Endpoint to protect their sensitive files and processes from these types of attacks.
- Malware has evolved to recognize these security products and make attempts to disable or uninstall them.
- Our group decided to help Cisco create a safeguard for their security product and any crucial system files or services from being stopped or removed.
- Cisco Secure Endpoint offers cloud-delivered next-generation antivirus and advanced endpoint detection and response.

Methods

- Self Protect Service is an application that runs in the background where it monitors protected files from open, read, write, and delete operations.
- Written in C/C++ and supports the Ubuntu Linux distribution.
- Integrated with Dropbox to backup protected files on the cloud.
- Token to authorize access provided through an external website.
- Implemented over the course of 5 sprints which included Roadmapping, Implementation, Integration, Testing, and Delivery.
- Ultimately, Self Protect Service will protect Cisco Secure Endpoint product from being stopped or uninstalled due to malicious attacks.

Results

- Self Protect Service is now capable of safeguarding any crucial system files from tampering.
- Protects files from any unauthorized open, read, write and delete commands.
- Prevents malware from stopping or shutting down Cisco Security products.
- Self Protect Service is able to be integrated into Cisco's Secure Endpoint and will be used to prevent malware from accessing sensitive information.

Discussion

- Self Protect Service is ultimately intended to prevent malware from interfering with the Cisco Secure Endpoint product.
- The software effectively prevents malicious software or individuals to tamper with files protected by our product, based on our testing.
- Self Protect Service paired with Cisco Secure Endpoint enables for extensive defense against a plethora of cyber-threats by adding an additional layer of security against stopping Cisco Secure Endpoint.

```
Enter Self Protect service token to continue:
incorrect, attempt 1/5
Enter token: incorrect, attempt 2/5
Enter token: incorrect, attempt 3/5
Enter token: incorrect, attempt 4/5
Enter token: incorrect, attempt 5/5
Permission denied. This window can be safely closed
```

```
Date: March 20, 2023 21:03:47 (epoch: 1679367827)
Action: access
Access status: Blocked
Service status: Active
Protected directories:
-       /opt/self_protect/
Tampering locations:
-       /opt/self_protect/test.txt
----------------------------------------
```

Conclusion

- The functional requirements defined by the sponsor were exceeded.
- Self Protect Service will be acquired by Cisco for further development and integration into their Secure Endpoint product offering.
- This technology gives users the ability to not only protect the essential files utilized by their security software, but also any directory containing files which require the same level of protection.
- The team prioritizes security and are committed to improving the service. Our team welcomes and rewards testers who can identify vulnerabilities in the system.

References

1. https://purplesec.us/resources/cyber-security-statistics/
2. https://www.cisco.com/site/ca/en/products/security/endpoint-security/secure-endpoint

Contact Us
selfprotectservice@gmail.com