An Introduction to Continuous Security Testing

Adversary Village Live Stream

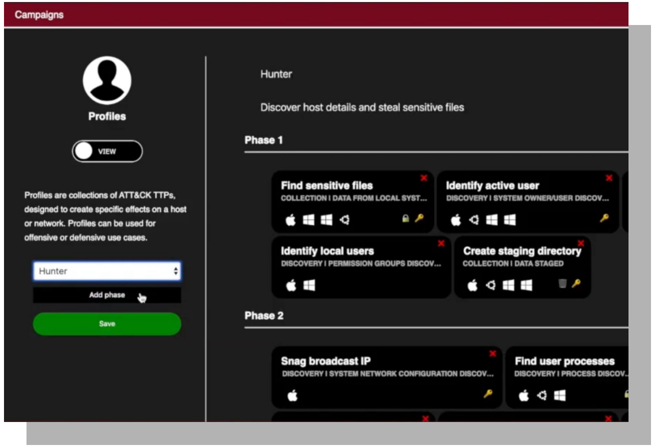
February 28, 2023

David Hunt

[P] | Prelude

preludesecurity.com

Where we’ve come from



Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Hunter

Hunter

Discover host details and steal sensitive files

Phase 1

Find sensitive files
COLLECTION | DATA FROM LOCAL SYST...

Identify active user
DISCOVERY | SYSTEM OWNER/USER DISCOV...

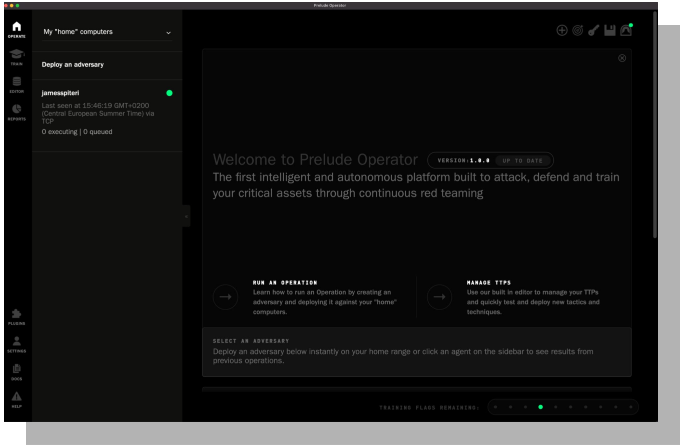
Identify local users
DISCOVERY | PERMISSION GROUPS DISCOV...

Create staging directory
COLLECTION | DATA STAGED

Phase 2

Snag broadcast IP
DISCOVERY | SYSTEM NETWORK CONFIGURATION DISCOV...

Find user processes
DISCOVERY | PROCESS DISCOV...



My "home" computers

jamesspiteri
Last seen at 15:46:19 GMT+0200 (Central European Summer Time) via TCP
0 executing | 0 queued

Welcome to Prelude Operator VERSION:1.0.0 UP TO DATE

The first intelligent and autonomous platform built to attack, defend and train your critical assets through continuous red teaming

RUN AN OPERATION
Learn how to run an Operation by creating an adversary and deploying it against your "home" computers.

MANAGE TTPS
Use our built in editor to manage your TTPs and quickly test and deploy new tactics and techniques.

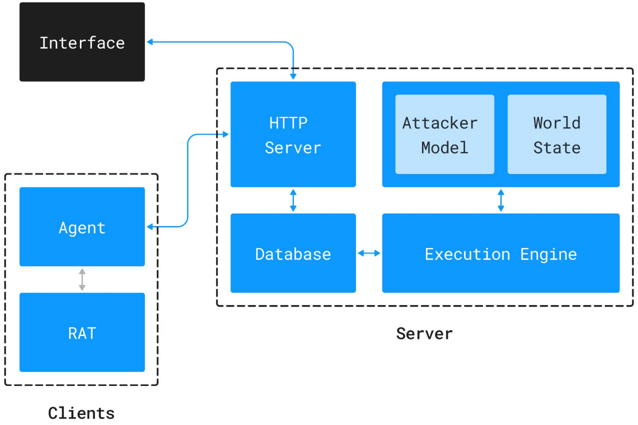
SELECT AN ADVERSARY
Deploy an adversary below instantly on your home range or click an agent on the sidebar to see results from previous operations.

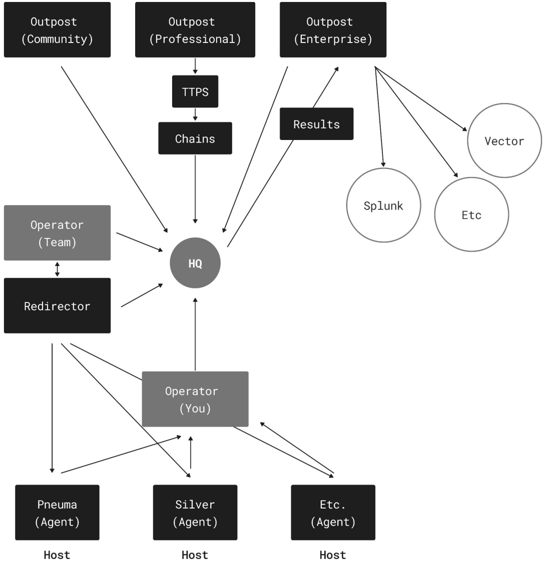
TRAINING FLAGS REMAINING:

CALDERA

[P] Prelude

Where we've come from





CALDERA

[P] | Prelude

TTPs ⤜ Verified Security Tests (VSTs)

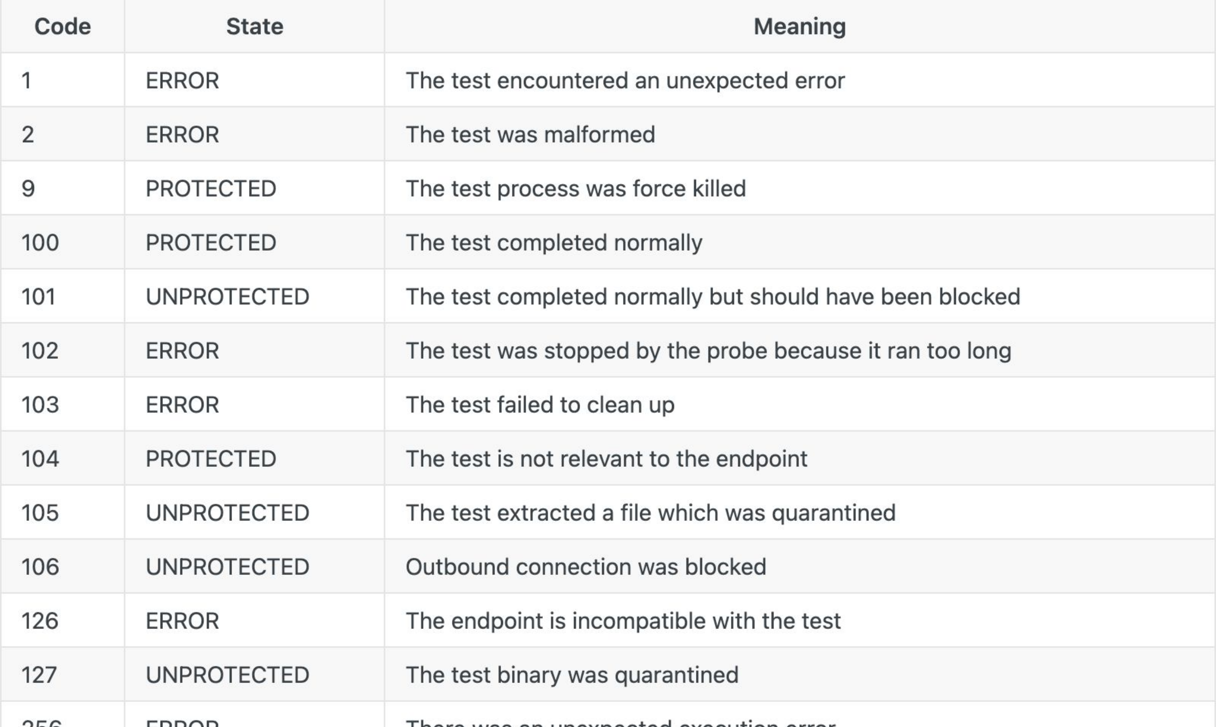
Example of TTP in Operator (and Caldera)

```yaml
id: 4d2c97ed-5464-4a27-9cc4-f76237526aea
name: Discover System Geolocalization
description: Retrieve Geolocalization data based on
the Public IP address retrieved.
metadata:
  authors:
  - w0rk3r
  tags: []
tactic: discovery
technique:
  id: T1614
  name: System Location Discovery
platforms:
  windows:
    psh:
      command: |
        Invoke-RestMethod -UseBasicParsing -Uri
('http://ipinfo.io/'+ (Invoke-WebRequest -
UseBasicParsing -uri
"http://ifconfig.me/ip").Content)
  linux:
    sh:
      command: |-
        wget -qO- http://ifconfig.me/ip | wget -qO-
http://ipinfo.io/$1
```

Verified Security Test (VST)

```go
/*
ID: dd270c6f-a41c-4115-b54d-ff940abd9c27
NAME: What is my IP address?
CREATED: 2023-01-21
*/
package main

import (
    "github.com/preludeorg/test/endpoint"
    "runtime"
)

var supported = map[string][]string{
    "windows": {"powershell.exe", "-c", "Invoke-RestMethod -UseBasicParsing -Uri
('http://ipinfo.io/'+ (Invoke-WebRequest -UseBasicParsing -uri 'http://ifconfig.me/ip').Content)"},
    "darwin":  {"bash", "-c", "wget -qO- http://ifconfig.me/ip | wget -qO- http://ipinfo.io/$1"},
    "linux":   {"bash", "-c", "wget -qO- http://ifconfig.me/ip | wget -qO- http://ipinfo.io/$1"},
}

func test() {
    command := supported[runtime.GOOS]
    response := Endpoint.Shell(command)
    print(response)
    Endpoint.Stop(101)
}

func clean() {
    Endpoint.Stop(100)
}

func main() {
    Endpoint.Start(test, clean)
}
```

Exit Codes That Scale

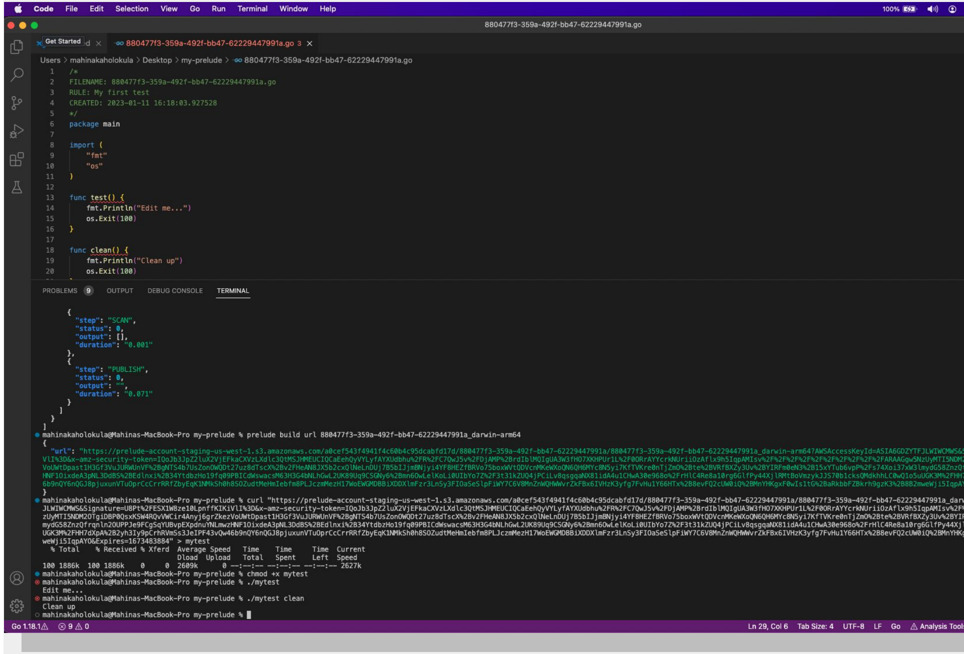


Code	State	Meaning
1	ERROR	The test encountered an unexpected error
2	ERROR	The test was malformed
9	PROTECTED	The test process was force killed
100	PROTECTED	The test completed normally
101	UNPROTECTED	The test completed normally but should have been blocked
102	ERROR	The test was stopped by the probe because it ran too long
103	ERROR	The test failed to clean up
104	PROTECTED	The test is not relevant to the endpoint
105	UNPROTECTED	The test extracted a file which was quarantined
106	UNPROTECTED	Outbound connection was blocked
126	ERROR	The endpoint is incompatible with the test
127	UNPROTECTED	The test binary was quarantined
256	ERROR	There was an unexpected execution error

Authoring Verified Security Tests

Prelude Build: an open source IDE for authoring, testing and verifying security tests for use in production environment.

Visual Studio, CLI


Code
File
Edit
Selection
View
Go
Run
Terminal
Window
Help
100%
880477f3-359a-492f-bb47-62229447991a.go
Get Started
880477f3-359a-492f-bb47-62229447991a.go 3
Users > mahinakaholokula > Desktop > my-prelude > 880477f3-359a-492f-bb47-62229447991a.go
PROBLEMS 9
OUTPUT
DEBUG CONSOLE
TERMINAL
Go 1.18.1⚠
⊗ 9 ⚠ 0
Ln 29, Col 6
Tab Size: 4
UTF-8
LF
Go
⚠ Analysis Tool

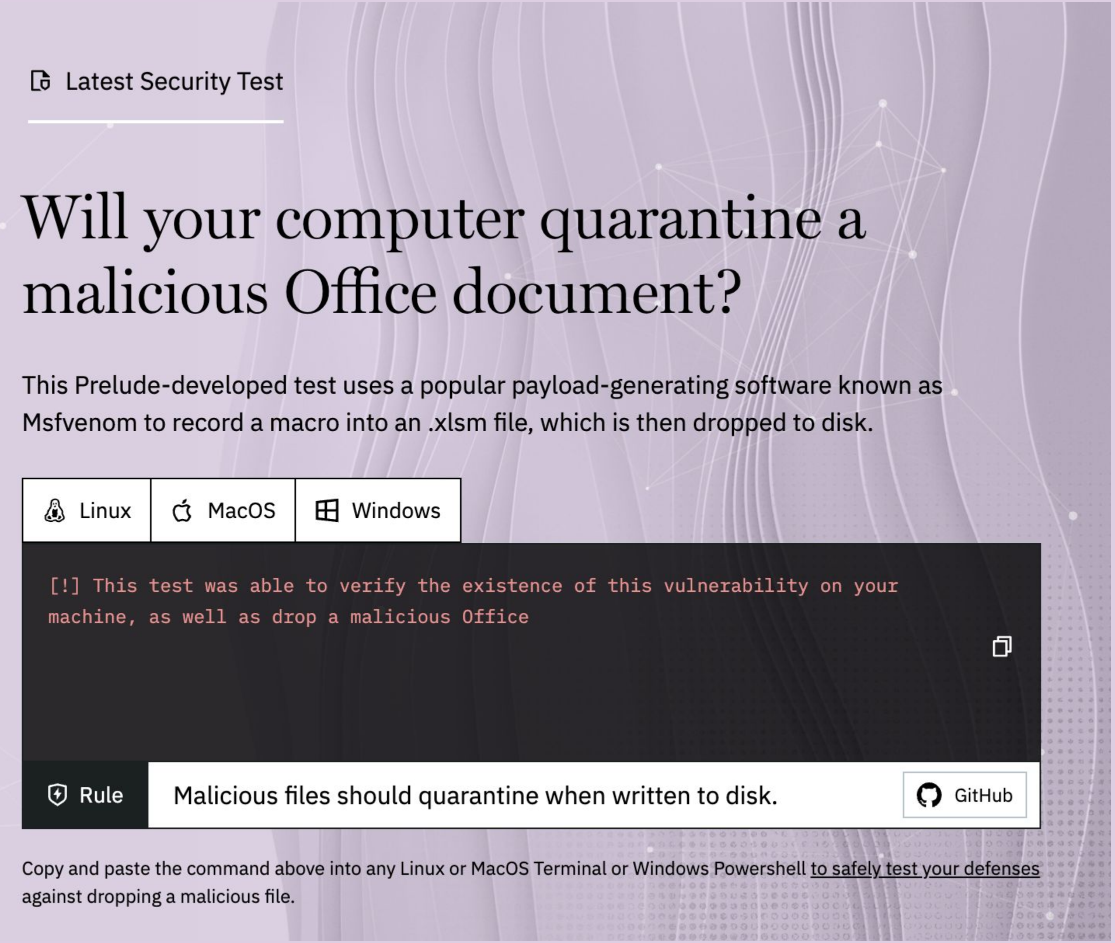
```go
/*
FILENAME: 880477f3-359a-492f-bb47-62229447991a.go
RULE: My first test
CREATED: 2023-01-11 16:18:03.927528
*/
package main

import (
    "fmt"
    "os"
)

func test() {
    fmt.Println("Edit me...")
    os.Exit(100)
}

func clean() {
    fmt.Println("Clean up")
    os.Exit(100)
```

```
      {
        "step": "SCAN",
        "status": 0,
        "output": [],
        "duration": "0.001"
      },
      {
        "step": "PUBLISH",
        "status": 0,
        "output": "",
        "duration": "0.071"
      }
    ]
  }
]
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % prelude build url 880477f3-359a-492f-bb47-62229447991a_darwin-arm64
{
  "url": "https://prelude-account-staging-us-west-1.s3.amazonaws.com/a0cef543f4941f4c60b4c95dcabfd17d/880477f3-359a-492f-bb47-62229447991a/880477f3-359a-492f-bb47-62229447991a_darwin-arm64?AWSAccessKeyId=ASIA6GDZYTFJLWIWCMWS&S
VlI%3D&x-amz-security-token=IQoJb3JpZ2luX2VjEFkaCXVzLXdlc3QtMSJHMEUCIQCaEehQyVYLyfAYXUdbhu%2FR%2FC7QwJ5v%2FDjAMP%2BrdIblMQIgUA3W3fHO7XKHPUr1L%2F0ORrAYYcrkNUriiOzAflx9h5IqpAMIsv%2F%2F%2F%2F%2F%2F%2F%2F%2FARAAGgw5NzUyMTI5NDM2
VoUWtDpast1H3Gf3VuJURWUnVF%2BgNTS4b7UsZonOWQDt27uz8dTscX%2Bv2FHeAN8JX5b2cxQlNeLnDUj7B5bIJjmBNjyi4YF8HEZfBRVo75boxWVtQDVcnMKeWXoQN6QH6MYc8N5yi7KfTVKre0nTjZmO%2Bte%2BVRfBXZy3Uv%2BYIRFm0eN3%2B15xYTub6vpP%2Fs74Xoi37xW3lmydG58ZnzQ
HNF1OixdeA3pNL3DdBS%2BEdlnxi%2B34YtdbzHo19fq09PBICdWswacsM63H3G4bNLhGwL2UK89Uq9CSGNy6%2Bmn6OwLelKoLi0UIbYo7Z%2F3t31kZUQ4jPCiLv8qsgqaNX81idA4u1CHwA30e968o%2FrHlC4Re8a10rg6GlfPy44XjlRMtBoVmzykJJS70b1cksQMdkhhLC0wQ1o5uUGK3M%2FHH
6b9nQY6nQGJ8pjuxunVTuOprCcCrrRRfZbyEqK1NMkSh0h8SOZudtMeHmIebfm8PLJczmMezH17WoEWGMDBBiXDDXlmFzr3LnSy3FIOaSeSlpFiWY7C6V8MnZnWQHWWvrZkFBx6IVHzK3yfg7FvHu1Y66HTx%2B8evFQ2cUW0iQ%2BMnYHKgxF0wIs1tG%2BaRkbbFZBkrh9gzK3%2B8B2mweWji5IqpA
}
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % curl "https://prelude-account-staging-us-west-1.s3.amazonaws.com/a0cef543f4941f4c60b4c95dcabfd17d/880477f3-359a-492f-bb47-62229447991a/880477f3-359a-492f-bb47-62229447991a_darw
JLWIWCMWS&Signature=U8Pt%2FESX1W8ze10LpnffKIKiVlI%3D&x-amz-security-token=IQoJb3JpZ2luX2VjEFkaCXVzLXdlc3QtMSJHMEUCIQCaEehQyVYLyfAYXUdbhu%2FR%2FC7QwJ5v%2FDjAMP%2BrdIblMQIgUA3W3fHO7XKHPUr1L%2F0ORrAYYcrkNUriiOzAflx9h5IqpAMIsv%2F
zUyMTI5NDM2OTgiDBP0QsxKSW4RQvVWCir4Anyj6grZkezVoUWtDpast1H3Gf3VuJURWUnVF%2BgNTS4b7UsZonOWQDt27uz8dTscX%2Bv2FHeAN8JX5b2cxQlNeLnDUj7B5bIJjmBNjyi4YF8HEZfBRVo75boxWVtQDVcnMKeWXoQN6QH6MYc8N5yi7KfTVKre0nTjZmO%2Bte%2BVRfBXZy3Uv%2BYIF
mydG58ZnzQfrqnln2OUPPJe9FCgSqYUBvpEXpdnuYNLmwzHNF1OixdeA3pNL3DdBS%2BEdlnxi%2B34YtdbzHo19fq09PBICdWswacsM63H3G4bNLhGwL2UK89Uq9CSGNy6%2Bmn6OwLelKoLi0UIbYo7Z%2F3t31kZUQ4jPCiLv8qsgqaNX81idA4u1CHwA30e968o%2FrHlC4Re8a10rg6GlfPy44Xjl
UGK3M%2FHH7dXpA%2B2yh3Iy9pCrhRVmSs3JeIPF43vQw46b9nQY6nQGJ8pjuxunVTuOprCcCrrRRfZbyEqK1NMkSh0h8SOZudtMeHmIebfm8PLJczmMezH17WoEWGMDBBiXDDXlmFzr3LnSy3FIOaSeSlpFiWY7C6V8MnZnWQHWWvrZkFBx6IVHzK3yfg7FvHu1Y66HTx%2B8evFQ2cUW0iQ%2BMnYHKg
weWji5IqpAYO&Expires=1673483884" > mytest
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1886k  100 1886k    0     0  2609k      0 --:--:-- --:--:-- --:--:-- 2627k
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % chmod +x mytest
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % ./mytest
Edit me...
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % ./mytest clean
Clean up
mahinakaholokula@Mahinas-MacBook-Pro my-prelude % ▌
```

preludesecurity.com

Running your first VST

Try it now at preludesecurity.com



Will your computer quarantine a malicious Office document?

This Prelude-developed test uses a popular payload-generating software known as Msfvenom to record a macro into an .xlsm file, which is then dropped to disk.

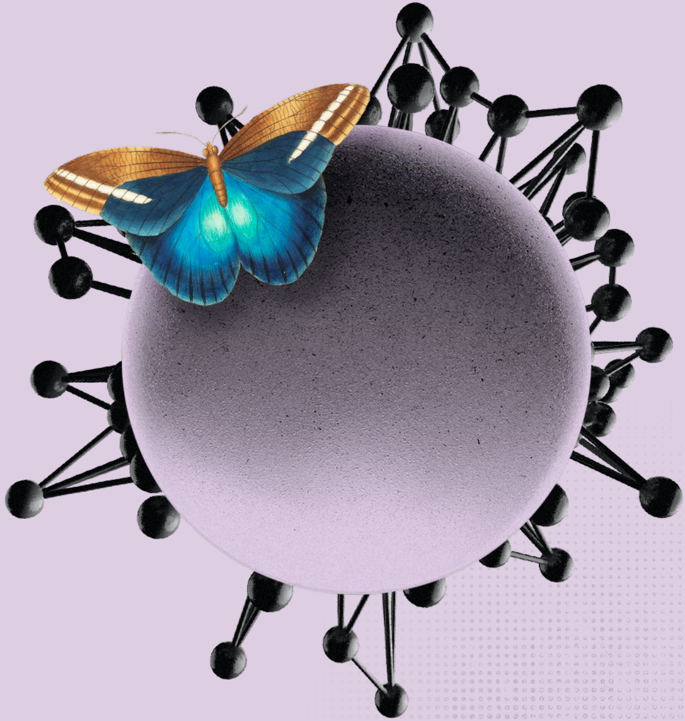
```
[!] This test was able to verify the existence of this vulnerability on your
machine, as well as drop a malicious Office
```

Rule: Malicious files should quarantine when written to disk.

Copy and paste the command above into any Linux or MacOS Terminal or Windows Powershell to safely test your defenses against dropping a malicious file.

[P]

What's happening?



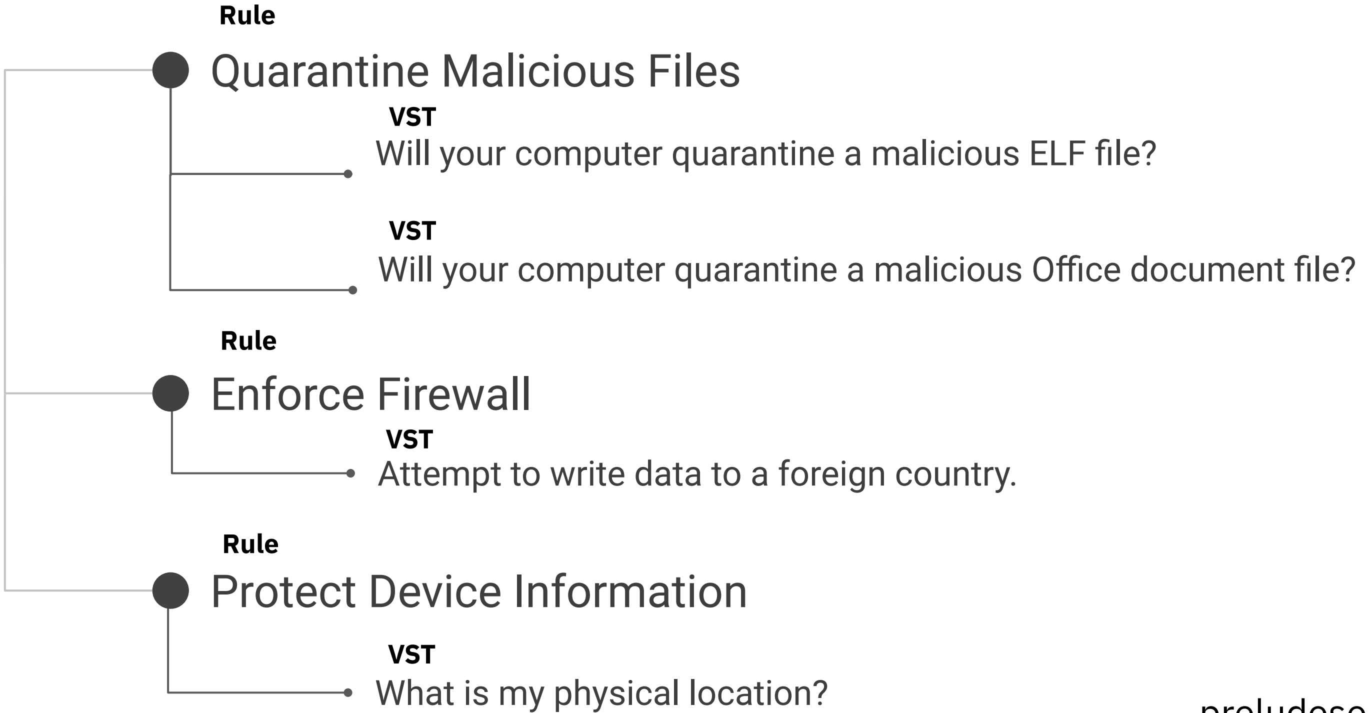
[P]

Probes: Not agents. Not agentless. Agent*ish*.

- Accept, run, and return the results of your VST
- Measured in KBs
- Can run anywhere code runs
- Requires no special privilege

Name	Runtime	Supported (DOS)	Size
Raindrop	PowerShell	windows-x86_64	1kb
Nocturnal	Bash	linux-x86_64, linux-arm64,darwin-x86_64, darwin-arm64	900B
Moonlight	Swift	darwin-x86_64, darwin-arm64	55kb
Hades	Go	windows-x86_64, linux-x86_64, linux-arm64, darwin-x86_64, darwin-arm64	1.4mb

Everybody loves rules



Rule

Quarantine Malicious Files

VST

Will your computer quarantine a malicious ELF file?

VST

Will your computer quarantine a malicious Office document file?

Rule

Enforce Firewall

VST

Attempt to write data to a foreign country.

Rule

Protect Device Information

VST

What is my physical location?

Demo time!

[P]

What we'll do

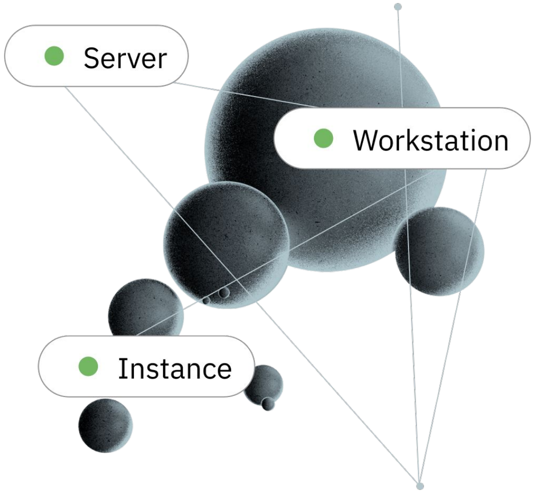
1. Start account
2. Deploy probes
3. Schedule tests
4. View results
5. Explore dashboard

[P]

preludesecurity.com

Getting Started ↴

platform.preludesecurity.com



Resources

Documentation

- Prelude Detect
- Prelude CLI

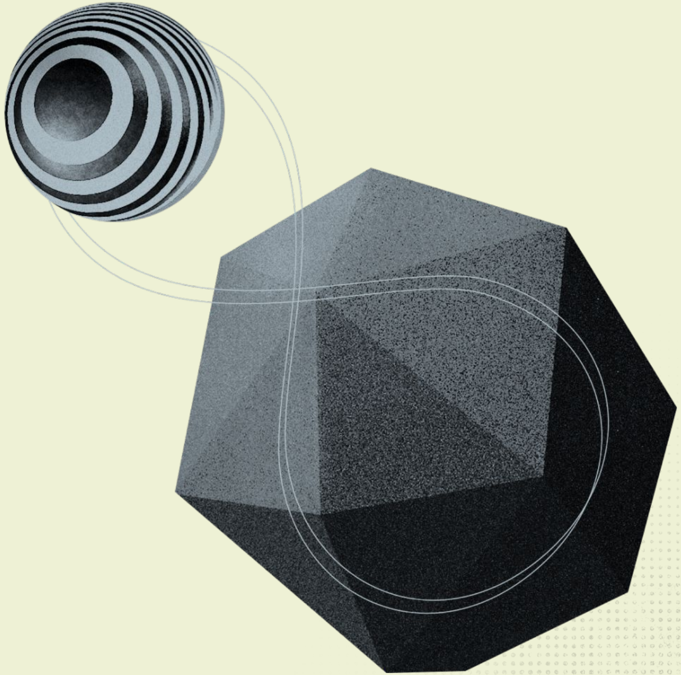
GitHub

- Verified Security Tests (VSTs)
  - Prelude Build
- Probes

Community

- Join our Discord

Thank you!



[P]

preludesecurity.com