Noirgate

Cloud Sandboxes for Security Research

@0daySimpson

whoami

- Security Researcher focusing on AI/ML
- Lead Product Security @ Scale AI
- Previously lead DFIR at Segment/Twilio
- 10+ years experience building security tools and platforms

@0daySimpson

Agenda

Project Background

About Noirgate

Demo(s)

Q&A

Background

By Day:

DFIR & Infrastructure Security.

By Night:

Security Research/Bug Bounty Hunting

Background

One evening, my workstation failed while working a high severity incident

Due to limited time, I had to crowdsource our response and rely on cloud based tools instead of rebuilding my workstation.

Although the process took a bit longer than usual, I was impressed with the fact that these tools allowed us to keep running the incident without major downtime.

Background

During this incident, we relied on Google CloudShell, CyberChef, Repl.it and others.

These tools provided a remote computing environment that allowed us to perform analysis without putting ourselves at risk.

Background

Background

What I needed was a Kali style environment, that was isolated, and included tools flexible enough for offensive and defensive use cases.

About Noirgate

Tools

Security

- Offensive
  - msf - Metasploit Framework
  - aterm - Terminal recorder from Paranoids' ASHIRT project
- Defensive
  - Forensics-all - All debian dfir tools (47 forensics tools)
  - OLE Tools - python tools to analyze OLE and MS Office files
  - heatlevel - check current IP reputation

Cloud

- awscli/aws-shell - amazon web services cli
- az - azure cloud cli
- gcloud - google cloud cli
- doctl - digital ocean cli
- kubectl/helm/k9s - kubernetes api client

About Noirgate

- Designed to be cloud hosted
- Network restrictions prevent access to host metadata interfaces
- DNS over TLS protects name resolution
- Torsocks + Privoxy provide anonymity
- Dangerous capabilities removed by cgroups, limits, and least privilege

About Noirgate

Multiple API Endpoints

Security Tools

Cloud Clients

Security Controls

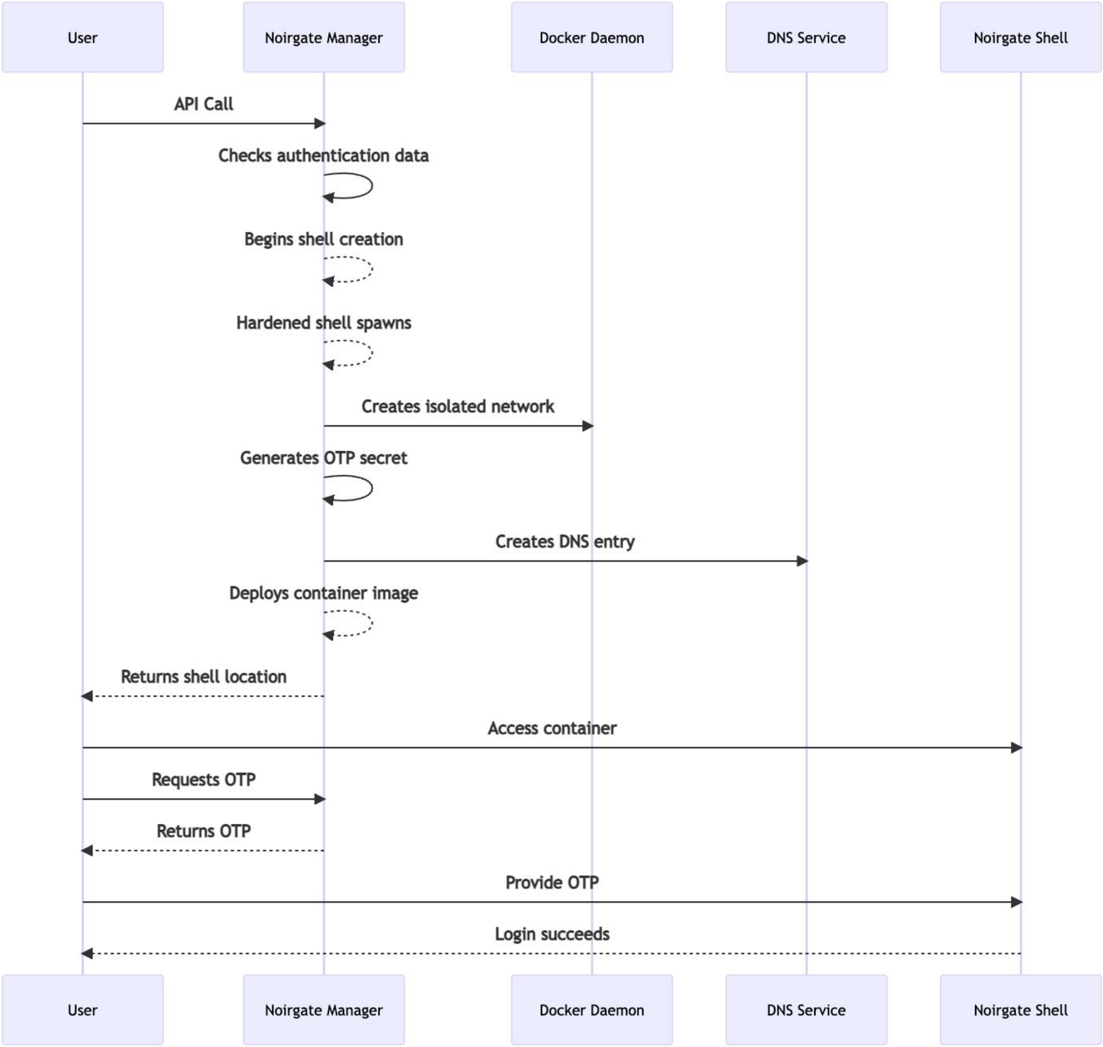
Garbage Collection

TOTP Authentication

About Noirgate

Workflow

Noirgate interfaces with the docker daemon to create isolated environments.



About Noirgate

Noirgate provisions web sandboxes with security tools, cloud clients and layer-7 anonymity. It provides a great way to quickly and easily test findings, or conduct research without having to worry about setting up and maintaining an environment.

About Noirgate

SHELL

Spins up a new sandbox container, creates a TOTP, and binds to a subdomain. Sandboxes have a 30 minute time-to-live

About Noirgate

OTP

Provides the user a one-time-password for their sandbox

About Noirgate

LOOT

Creates a short lived public S3 bucket for quickly sharing and analyzing data

About Noirgate

BYE

Destroys associated sandboxes and loot buckets.

About Noirgate

BYE

Destroys associated sandboxes and loot buckets.

Key Features

SMS API

- Send a text message to manage shells and storage
- AuthN/AuthZ bound to phone number
- Easiest way to get end users up and running quickly

Key Features

ChatOps API

- Use /slash commands to manage shells and storage
- AuthN/AuthZ bound to UserId + platform secret
- Convenient way of using the service while communicating with teammates

Key Features

REST API

- HTTP POST to manage shells and storage
- AuthN/AuthZ bound to an Authorization token + platform secret
- Most extensible way to add Noirgate to your operations

Demo!

Discord Bot

SMS API - Text **HOW** to 1337-561-1337

REST API - https://try.noirgate.shellz.wtf

Self-Host
https://github.com/Shell-Company/noirgate

@0daySimpson

SMS

SMS API - Text **HOW** to 1337-561-1337

REST API - https://try.noirgate.shellz.wtf

Self-Host
https://github.com/Shell-Company/noirgate

Demo Website

SMS API - Text **HOW** to 1337-561-1337

REST API - https://try.noirgate.shellz.wtf

Self-Host
https://github.com/Shell-Company/noirgate

@0daySimpson