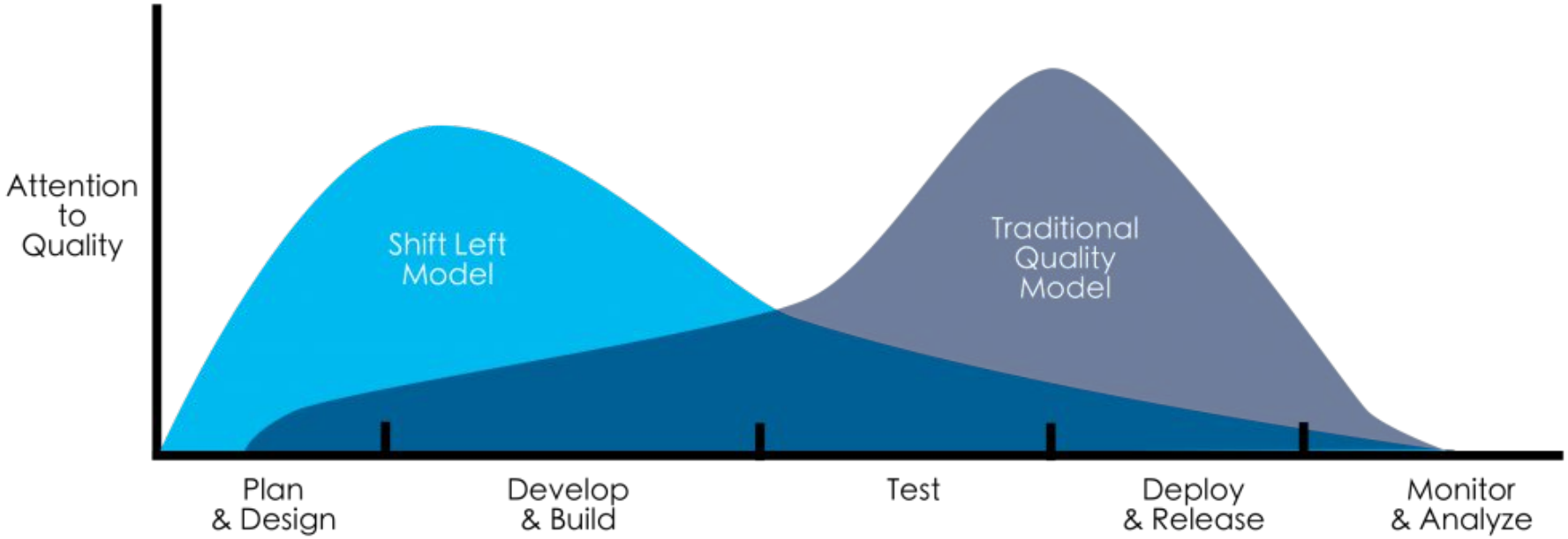
Automating Almost All Application Security Things with CI/CD

Even Honeypots!

Mick Douglas and Andy Douglas

Link to slides+resources at end!

Where is application security?


Attention to Quality
Shift Left Model
Traditional Quality Model
Plan & Design
Develop & Build
Test
Deploy & Release
Monitor & Analyze


Development
Continuous Integration
Continuous Delivery or Deployment

Development → Continuous Integration → Continuous Delivery or Deployment

H ua-parser-js@0.7.5 - Regular Expres...

SECURITY ISSUES - 3

- app.js - 2 issues
  - H Timing Attack
  - H Cross-Site Scripting attack
- server.js - 1 issue
  - H Path Transversal Vulnerability

CODE ISSUES - 1

- standalone.js - 2 issues
  - M Using component state to comput ...
  - M http (used in require) is an insecure...
- Header.js - 1 issue
  - H Unsanitized input flows from the H...
- Code.js - 1 issue
  - L Testing a collection size for >= 0 wi...
- contentScript.js - 1 issue
  - H Setting targetOrigin to "*" in postM...
- standalone.js - 1 issue
  - L Signature mismatch: the implement...

```
8   const mime = require('mime');
9
10  function sendFile(filename, response) {
11    response.setHeader('Content-Type', mime.lookup(filenam
12    response.writeHead(200);
13 3  const fileStream = createReadStream(filename);
14    fileStream.pipe(response);
15    fileStream.on('finish', response.end);
16  }
17
18  function createHTTP2Server(benchmark) {
19    const server = http2Server.createServer({}, (request,
20 2    const filename = join(
21        __dirname,
22        'benchmarks',
23        benchmark,
24 1      request.url
25      ).replace(/\?.*/g, '');
26
27      if (existsSync(filename) && statSync(filename).isFil
28        sendFile(filename, response);
29      } else {
30        const indexHtmlPath = join(filename, 'index.html')
31
32        if (existsSync(indexHtmlPath)) {
33          sendFile(indexHtmlPath, response);
34        } else {
35          response.writeHead(404);
36          response.end();
```

Code flow

1	scripts/bench/**server.js**	line #24
2	scripts/bench/**server.js**	**line 20**
3	scripts/bench/**server.js**	line 13

External example fixes

This issue was fixed by 708 projects. Here are 3 example fixes.

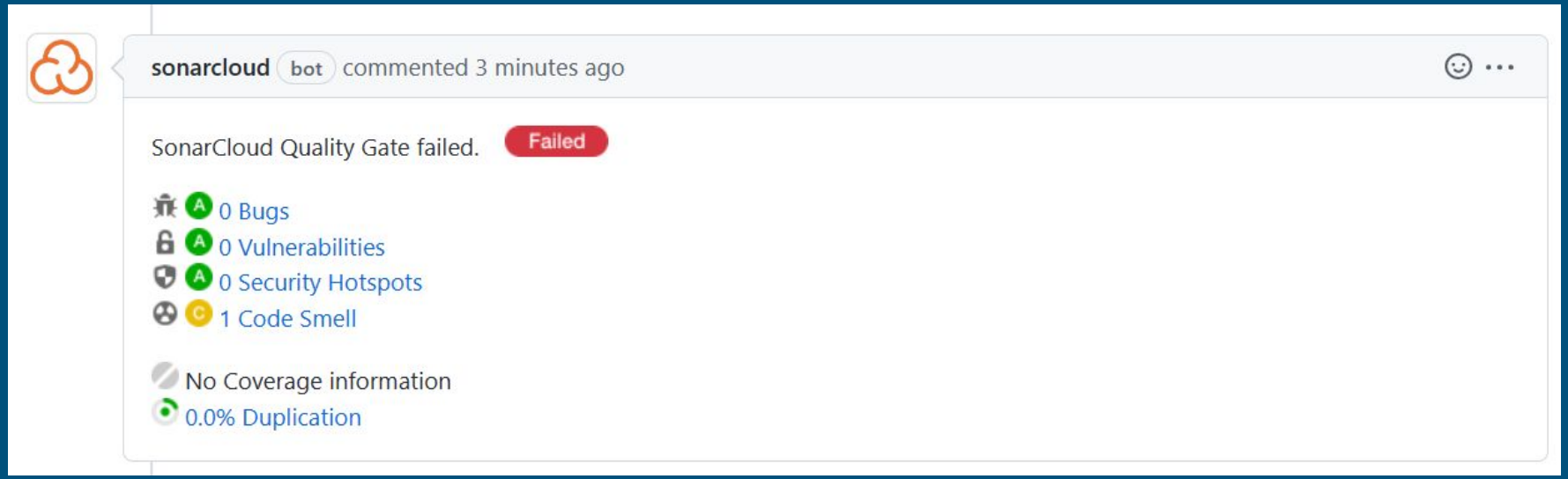
georgi/grant 1/3

```
  }
- function static_file(route, p, req, res) {
-   var uri = url.parse(req.url).pathname;
+ function dump_static_file(route, p, req, res) {
+   var uri = url.parse(this.req.url).pathname;
    var filename = path.join(process.cwd(), 'public', uri);
    fs.exists(filename, function(exists) {
      if(!exists) {
    var fileStream = fs.createReadStream(filename);
-   fileStream.pipe(res);
+   fileStream.pipe(this.res);
  });
```

Share issue | Ignore issue | Feedback

⊗ 0 ⚠ 12 ⓘ 8 Go Live Found 0 variables


Development
Continuous Integration
Continuous Delivery or Deployment


sonarcloud bot commented 3 minutes ago
SonarCloud Quality Gate failed.
Failed
0 Bugs
0 Vulnerabilities
0 Security Hotspots
1 Code Smell
No Coverage information
0.0% Duplication

Development → Continuous Integration → Continuous Delivery or Deployment

Windows PowerShell

```
PS C:\Users\AndyDouglas> docker run --rm -t --network host owasp/zap2docker-stable:2.12.0
zap-baseline.py -t http://localhost:3000 -s
```

The hardest thing in the world is to change the minds of people who keep saying, ‘But we’ve always done it this way.’ These are days of fast changes and if we don’t change with them, we can get hurt or lost.

- Grace M. Hopper

2022 IBM report:
Average time to detect data breach is 287 days

https://www.ibm.com/reports/data-breach

Active Defense

Automate Application Security with CI/CD

Part 1: Static and Dynamic Scans for prevention

Part 2: Active Defense for detection

Goal: Actionable Security Improvement

Hi, my name is Andy Douglas

- Long-time CodeMash attendee, first-time speaking
- Full Stack Web Dev/Engineer > Architect > Engineering Manager
- Security…meh

Hi, my name is Mick Douglas

- First time CodeMash attendee
- Passionate about security
- Infosec Innovations, SANS Principle Instructor, IANS Research Faculty

Part 1: Static and Dynamic Scans for prevention

Static Application Security Testing (SAST)

File Edit Selection View Go Run Terminal Help — source - Visual Studio Code

SNYK

DEPENDENCIES - 1 manifest file

- package.json - 7 vulnerabilities
  - H ajv@6.12.2 - Prototype Pollution
  - M bunyan@1.8.12 - Remote Code Exec...
  - H node-forge@0.7.6 - Prototype Pollu...
  - L dist-perf@2.2.1 - Denial of Service...
  - H ua-parser-js@0.7.5 - Regular Expres...

SECURITY ISSUES - 3

- app.js - 2 issues
  - H Timing Attack
  - H Cross-Site Scripting attack
- server.js - 1 issue
  - H Path Transversal Vulnerability

CODE ISSUES -

- standalone.
  - M Using co ate to comput ...
  - M http (us) is an insecure...
- Header.js -
  - H Unsaniti ws from the H...
- Code.js - 1 i
  - L Testing a size for >= 0 wi...
- contentScri
  - H Setting t to "*" in postM...
- standalone.js - 1 issue
  - L Signature mismatch: the implement...

server.js

```
1  'use strict';
2
3  const http2Server = require('http2');
4  const httpServer = require('http-server');
5  const {existsSync, st re
6  const {join} = requi
7  const argv = require( st )(process.argv.sli 2));
8  const mime = require( ;
9
10 function sendFile(fil response) {
11   response.setHeader t-Type', mime.lookup(filenam
12   response.writeHead
13 3 const fileStream = eadStream(filename);
14   fileStream.pipe(re
15   fileStream.on('fin sponse.end);
16 }
17
18 function createHTTP2Se (benchmark) {
19   const server = http2Server.createServer({}, (request,
20 2   const filename = join(
21       __dirname,
22       'benchmarks',
23       benchmark,
24 1     request.url
25     ).replace(/\?
26
27     if (existsSync(filename) && statSync(filena ).isFil
28       sendFile(filename, response);
29     } else {
30       const indexHtmlPath = join(filename, 'index.html')
31
32       if (existsSync(indexHtmlPath)) {
33         sendFile(indexHtmlPath, response);
34       } else {
35         response.writeHead(404);
36         response.end();
```

Path Traversal Code Vulnerability

H HIGH SEVERITY

Vulnerabilty | CWE-24 | Score: 950

Unsanitized input **flows** [:20, :24] from the **request URL** [:24] and is used as a path in **fs.createReadStream** [:13] . This may result in a Path Traversal vulnerability and allow an attacker to read arbitrary files.

Code flow

1	scripts/bench/**server.js**	line #24
2	scripts/bench/**server.js**	**line 20**
3	scripts/bench/**server.js**	line 13

External example fixes

This issue was fixed by 708 projects. Here are 3 example fixes.

georgi/grant 1/3

```
  }
- function static_file(route, p, req, res) {
-   var uri = url.parse(req.url).pathname;
+ function dump_static_file(route, p, req, res) {
+   var uri = url.parse(this.req.url).pathname;
    var filename = path.join(process.cwd(), 'public', uri);
    fs.exists(filename, function(exists) {
      if(!exists) {
    var fileStream = fs.createReadStream(filename);
-   fileStream.pipe(res);
+   fileStream.pipe(this.res);
  });
```

Share issue | Ignore issue | Feedback

⊗ 0 ⚠ 12 ⓘ 8 — Go Live — Found 0 variables

sonarcloud

My Projects My Issues Explore

website

PUBLIC

Cincinnati-Caledonian-Pipes-Drums-Band > website > main

Summary Issues Security Hotspots Measures Code ivity

Overview

Main Branch

9.4k Lines of Code

Last analysis 34 seconds ago fea57210

Quality Gate

sonarcloud bot commented 3 minutes ago

SonarCloud Quality Gate failed. Failed

0 Bugs

0 Vulnerabilities

0 Security Hotspots

1 Code Smell

No Coverage information

0.0% Duplication

SAST Strengths

SAST Weaknesses

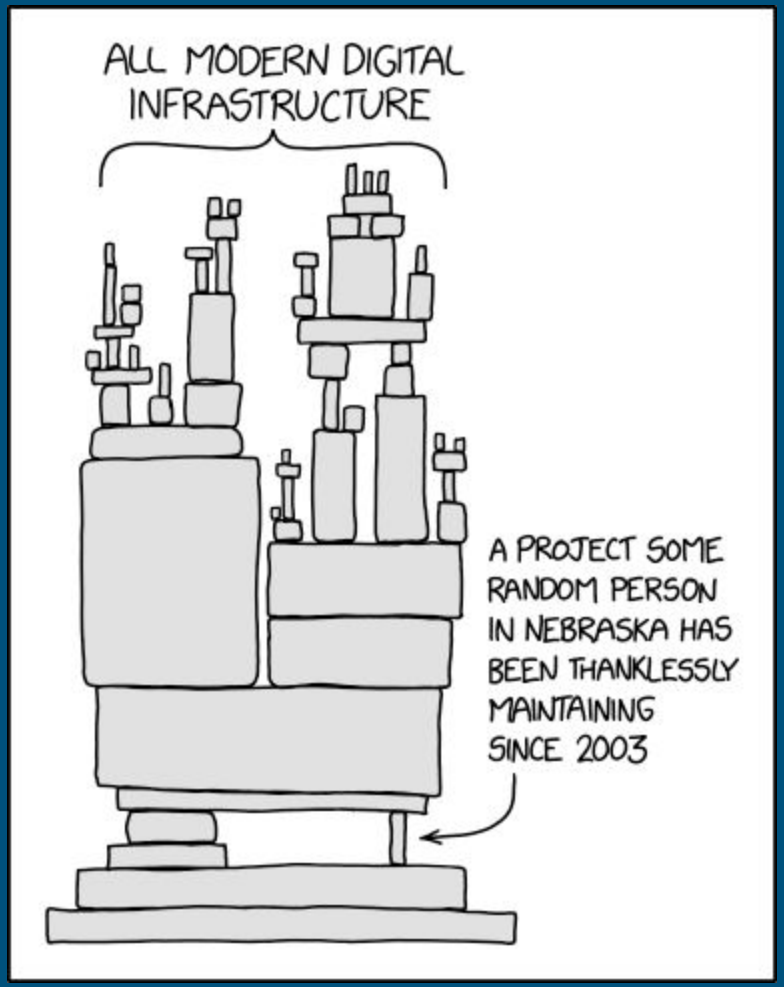
Recommendation:

Integrate SAST w/ IDE + CI

Popular Tools: Snyk, Checkmarx, SonarQube/SonarCloud

Software Composition Analysis (SCA)

npm , Maven, NuGet, pip, etc.


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Recommendation:

SCA: CI or scheduled

Popular Tools: Dependabot, Prisma Cloud, Snyk, Xray

Dynamic Application Security Testing (DAST)


Merge into main
CI build runs
(hopefully with SAST)
CD build runs
to deploy to env X
Smoke tests
and DAST

DAST Strengths

DAST Weaknesses

DAST Demo: ZAP

```yaml
on: [push]

jobs:
  zap_scan:
    runs-on: ubuntu-latest
    name: Scan the webapplication
    steps:
      - name: Checkout
        uses: actions/checkout@v2
        with:
          ref: master
      - name: ZAP Scan
        uses: zaproxy/action-baseline@v0.7.0
        with:
          token: ${{ secrets.GITHUB_TOKEN }}
          docker_name: 'owasp/zap2docker-stable'
          target: 'https://www.zaproxy.org'
          rules_file_name: '.zap/rules.tsv'
          cmd_options: '-a'
```

Recommendation:

DAST: CD and/or scheduled

Popular Tools: ZAP, StackHawk, Burp Suite, Astra Pentest, etc.

Part 2: Active Defense for detection

Part 2: Active Defense ~~for detection~~ FTW!!

Traditional Defense == Passive

Traditional Defense == KNOWN

Active Defense == Passive & Active

Still need to do “basics”

Once you're OK...

Shift focus/effort to higher reward

Honey Pots!

Attackers have predictable paths

TTPs

MITRE ATT&CK matrix

MITRE | ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

Reconnaissance
10 techniques

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (7)
- Compromise Accounts (3)
- Compromise Infrastructure (7)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (6)
- Stage Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
13 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (16)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (7)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (2)
- Valid Accounts (4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (9)
- Plist File Modification

Credential Access
17 techniques

- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (7)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Discovery
30 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (2)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Active Defence at each phase

MITRE | ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

Recon: Port scanning

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (13 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (17 techniques)	Discovery (30 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Infrastructure	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Establish Accounts (3)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	Build Image on Host	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Obfuscated Files or Information (5)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Obtain Capabilities (6)	Phishing	Native API	Create Account (3)	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Stage Capabilities (6)	Replication Through Removable Media	Scheduled Task/Job (5)	Event Triggered Execution (16)	Event Triggered Execution (16)	Exploitation for Defense Evasion	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise	Shared Modules	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (10)	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	System Services (2)	Implant Internal Image	Process Injection (12)	Hijack Execution Flow (12)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			User Execution (3)	Modify Authentication Process (7)	Scheduled Task/Job (5)	Impair Defenses (9)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Indicator Removal (9)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
				Pre-OS Boot (5)		Indirect Command Execution	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Scheduled Task/Job (5)		Masquerading (7)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Server Software Component (5)		Modify Authentication Process (7)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Traffic Signaling (2)		Modify Cloud Compute Infrastructure (4)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
				Valid Accounts (4)		Modify Registry	Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Web Service (3)		
						Modify System Image (2)	Unsecured Credentials (7)	Peripheral Device Discovery		Video Capture			
						Network Boundary Bridging (1)		Permission Groups Discovery (3)					
						Obfuscated Files or Information (9)		Process Discovery					
						Plist File Modification		Query Registry					
								Remote System Discovery					
								Software Discovery (1)					
								System Information Discovery					
								System Location Discovery (1)					

Honey Port

DEMO: Honey Port

MITRE | ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (13 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (17 techniques)	Discovery (30 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	BITS Jobs	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Ur ... n (3)	Process Injection (12)	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Wi Ma Inst	Scheduled Task/Job	Scheduled Task/Job	Hide Artifacts (10)	Steal Web Session Cookie	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Modify Authentication Process	Modify Authentication Process	Hijack Execution Flow (12)	Unsecured Credentials (7)	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Office Application Startup	Office Application Startup	Impair Defenses (9)		Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
				Pre-OS Boot	Pre-OS Boot	Indicator Removal (9)		Password Policy Discovery		Screen Capture	Web Service (3)		
				Server Software Component (5)	Server Software Component (5)	Indirect Command Execution		Peripheral Device Discovery		Video Capture			
				Traffic Signaling (2)	Traffic Signaling (2)	Masquerading (7)		Permission Groups Discovery (3)					
				Valid Accounts (4)	Valid Accounts (4)	Modify Authentication Process (7)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (9)		System Information Discovery					
						Plist File Modification		System Location Discovery (1)					

Initial Access: Admin login

Honey Admin Login

Demo: Honey Admin Login

MITRE | ATT&CK

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Contribute | Search

Privilege Escalation: Session Token

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (13 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (17 techniques)	Discovery (30 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deploy Container	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture	Cloud Service Discovery		Clipboard Data			Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process						Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception						Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation						Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Hide Artifacts (10)	Network Sniffing	Group Policy Discovery	Use Alternate Authentication Material (4)	Local System	Network Denial of Service (2)		
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Network Service Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	Impair Defenses (9)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	Indicator Removal (9)	Steal or Forge Authentication Certificates	Network Sniffing		Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (6)		Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Proxy (4)		
				Pre-OS Boot (5)		Masquerading (7)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Remote Access Software		
				Scheduled Task/Job (5)		Modify Authentication Process (7)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Screen Capture	Traffic Signaling (2)		
				Server Software Component (5)		Modify Cloud Compute Infrastructure (4)		Process Discovery		Video Capture	Web Service (3)		
				Traffic Signaling (2)		Modify Registry		Query Registry					
				Valid Accounts (4)		Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (9)		System Information Discovery					
						Plist File Modification		System Location Discovery (1)					

Honey Session Tokens

Demo: Honey Session Tokens

Strategy: Post Detection

Watch and learn?

Random error response?

Firewall

QoS

Demo response options

Security != Hard/Expensive

Security as Functional Requirement

Security + CI/CD is good

Challenge - Join Us!

Building a secure-by-default system is a choice.

Building an expensive, insecure, and inefficient one is also a choice.

Choose wisely.

-Mick Douglas

Resources

Presentation and related labs:

- GitHub repo with slides, demos, and labs: →
- OWASP SAST Recommendations
- OWASP SCA Recommendations
- OWASP ZAP
- (YouTube) ZAP Automation in CI/CD
- ModSecurity

Misc related resources:

- *Offensive Countermeasures: The Art of Active Defense* by John Strand

Mick Douglas
https://www.infosecinnovations.com/

Andy Douglas
https://www.linkedin.com/in/andy-douglas-8187557/