Anatomy of a Cyber Attack

Jon Mann

Senior Security Engineer

CISSP, GDSA, GSEC, GSTRT, GCIH, ITIL4

jonmann.nyc

github.com/jonmannn

SANS INSTITUTE

WARBY PARKER

PELOTON

MAVEN

Agenda

- Cyber Kill Chain
- Demonstration
- Mitigations
- Remarks

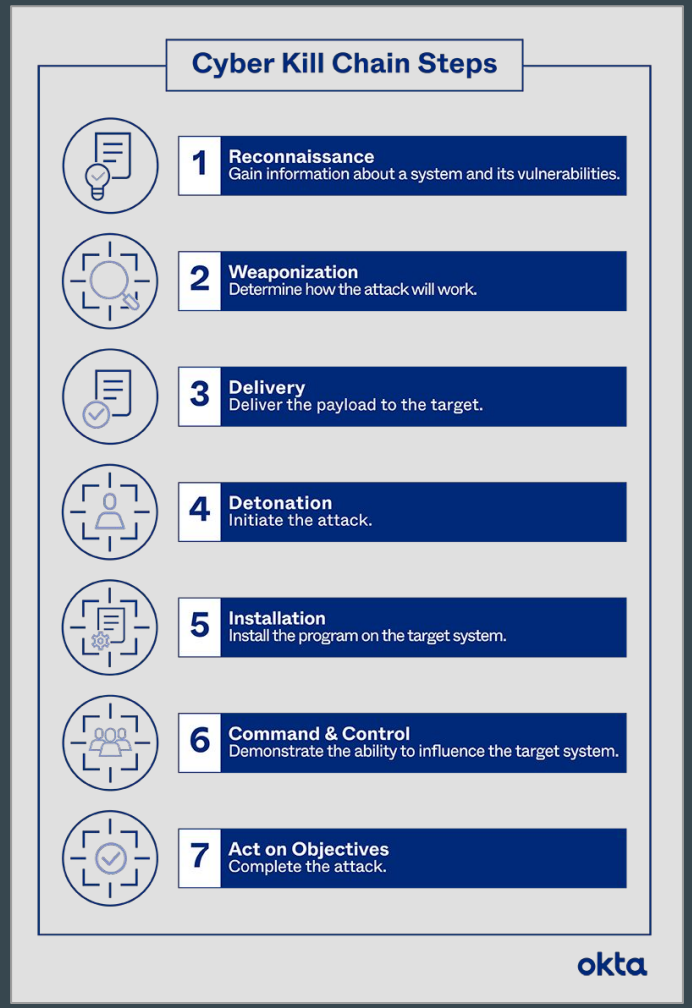
Cyber Kill Chain

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://tmg110.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/wainyman/art/Winston-Smith-pencil-38965327

Reconnaissance

SHODAN | Explore | Downloads | Pricing | hostname:newspeakprinting.com | Account

printersupport.newspeakprinting.com

Regular View | Raw Data

// LAST SEEN: 2024-10-18

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

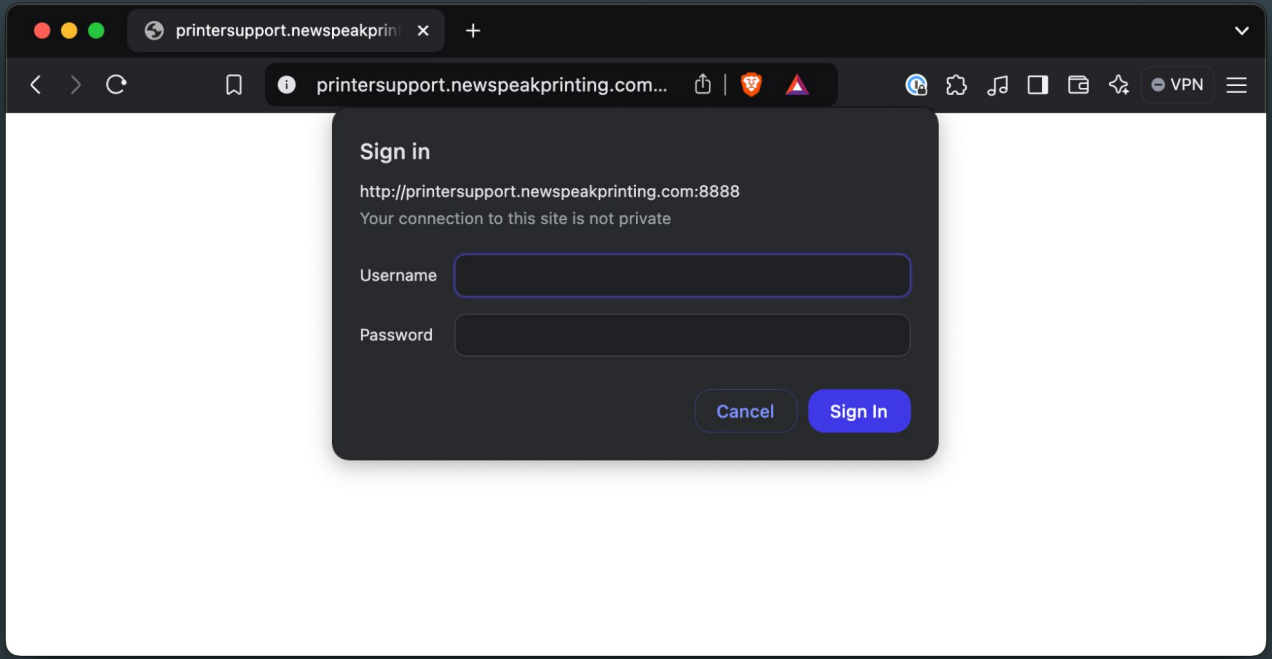
// 8888 / TCP

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

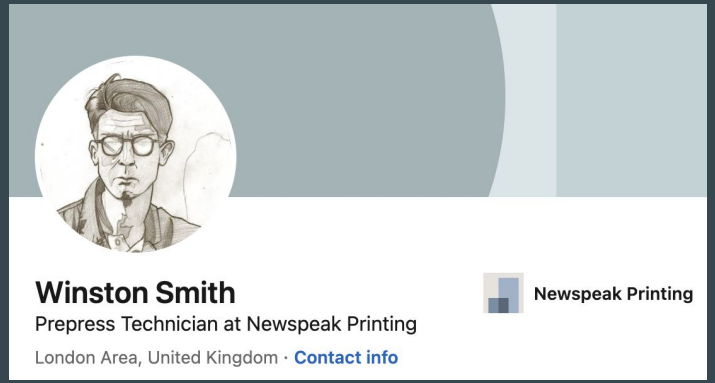
Printer Tester

```
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
```

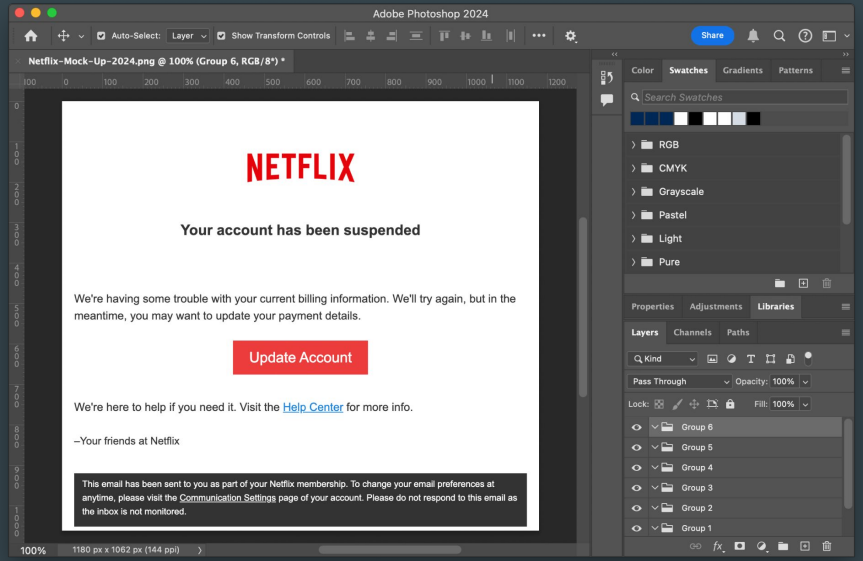
Reconnaissance

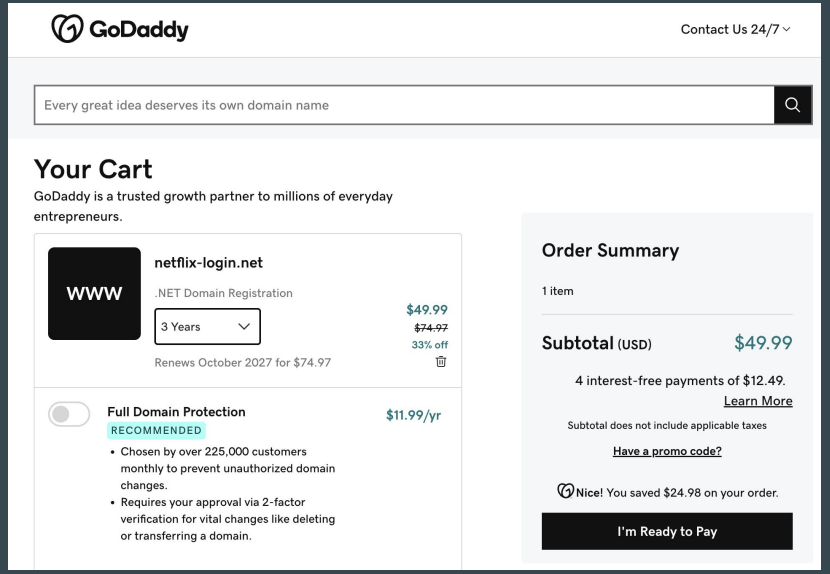


Reconnaissance



Weaponization





Delivery

NETFLIX

Your account has been suspended

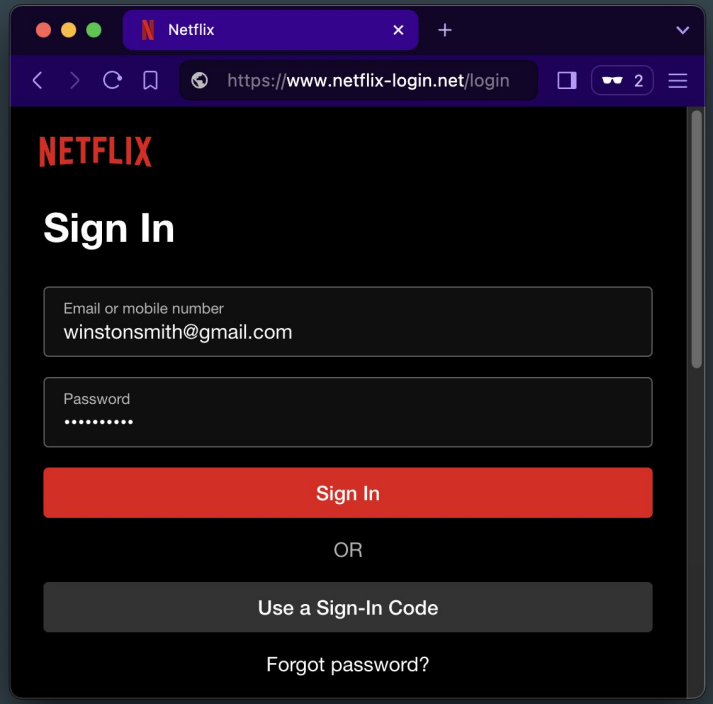
We're having some trouble with your current billing information. We'll try again, but in the meantime, you may want to update your payment details.

Update Account

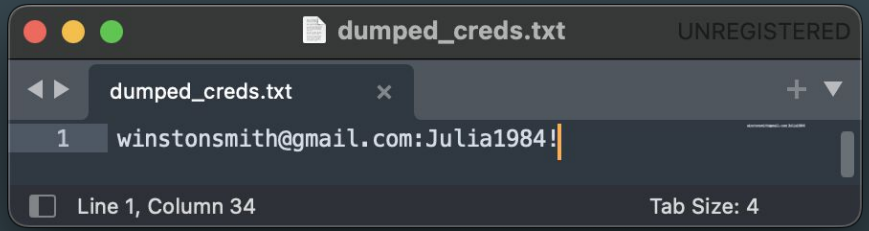
We're here to help if you need it. Visit the Help Center for more info.

–Your friends at Netflix

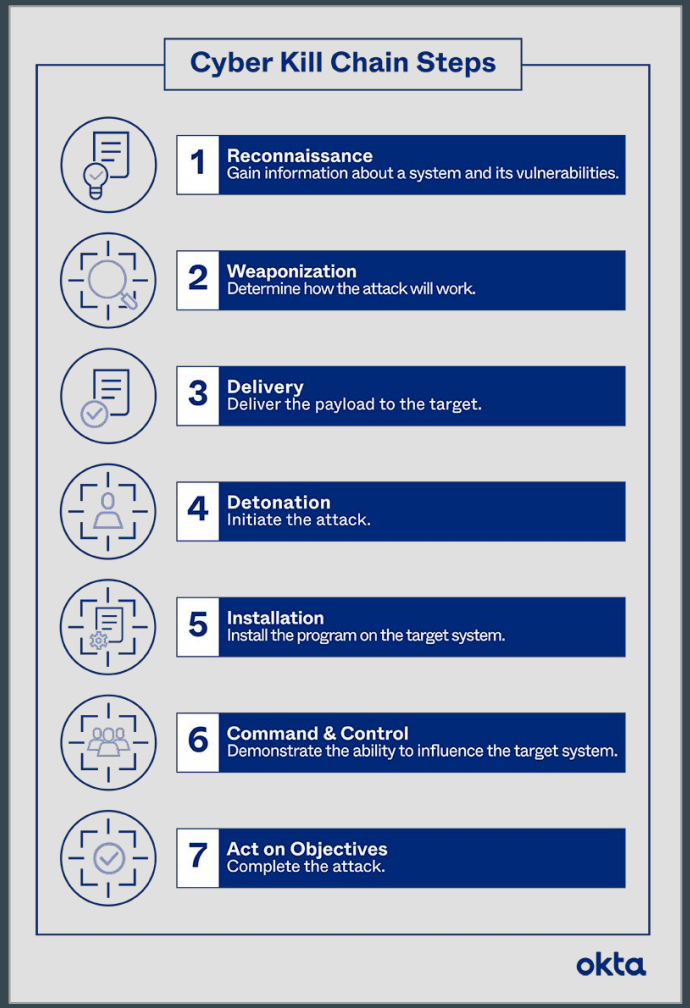
This email has been sent to you as part of your Netflix membership. To change your email preferences at anytime, please visit the Communication Settings page of your account. Please do not respond to this email as the inbox is not monitored.



Delivery


dumped_creds.txt
UNREGISTERED
dumped_creds.txt
1
winstonsmith@gmail.com:Julia1984!
Line 1, Column 34
Tab Size: 4

Exploitation



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

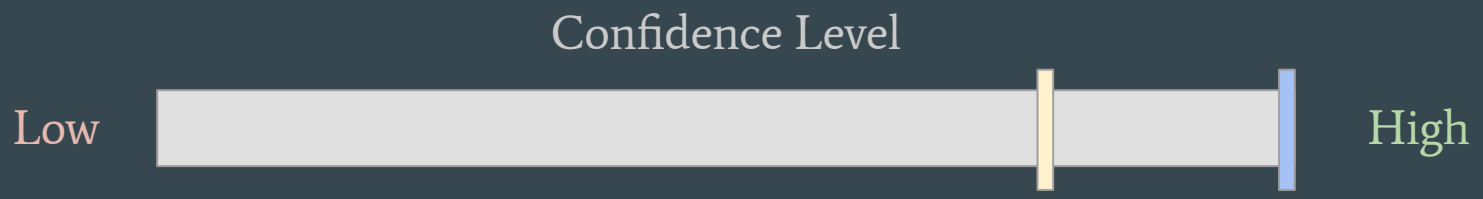
Mitigations

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.



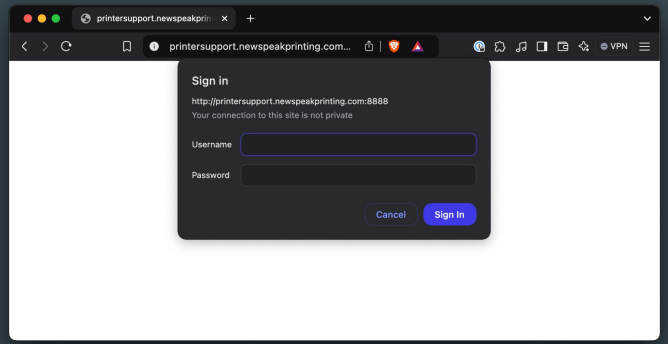
Reconnaissance

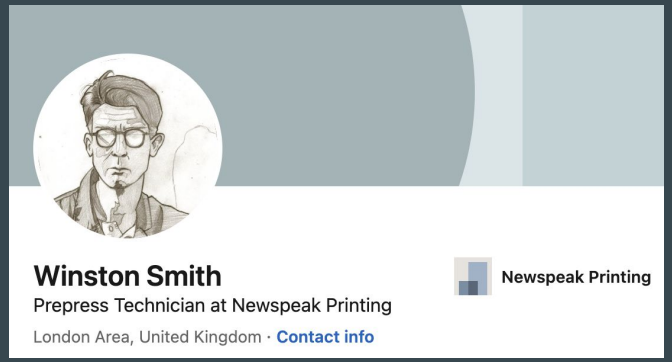
Detection

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

Prevention

- Restrict employees from sharing their employer information.





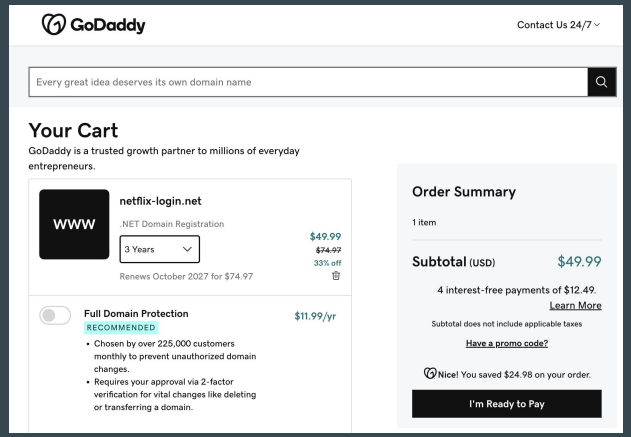
Weaponization

Detection

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

Prevention

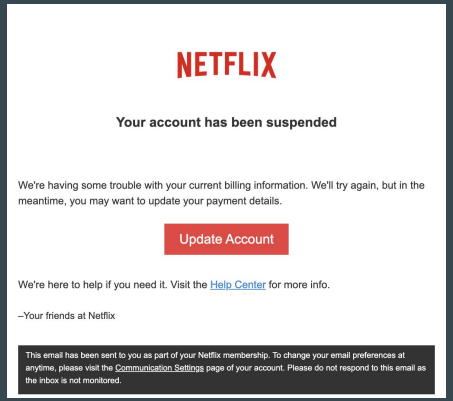
- Purchase “Cousin Domains” to prevent adversaries from doing so.



Delivery

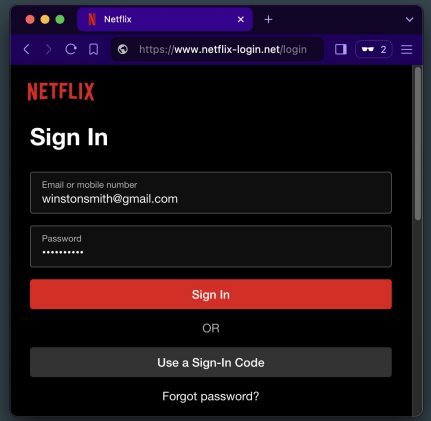
Detection

- 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.



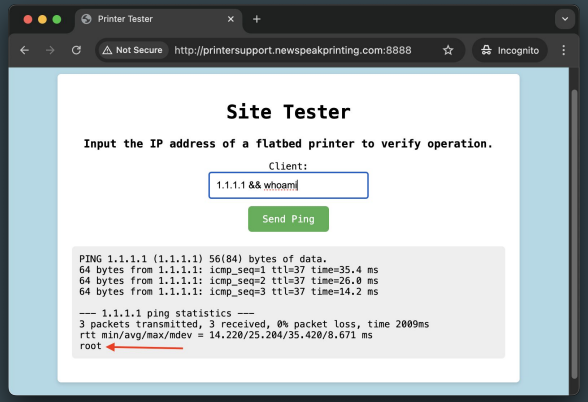
Exploitation

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.



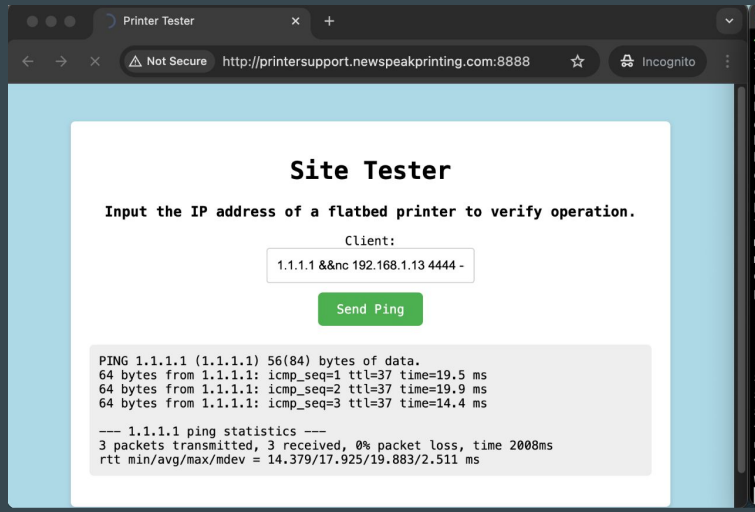
Installation

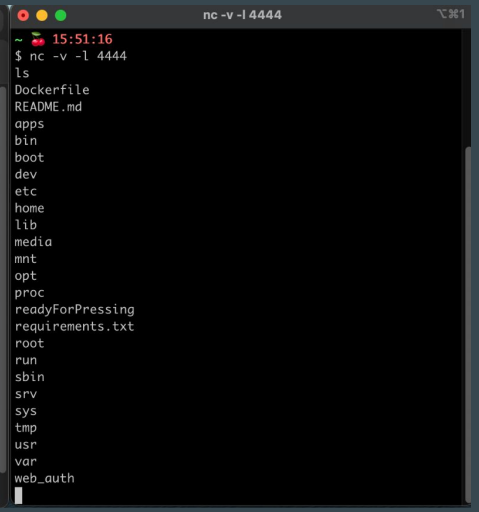
Detection

- 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.

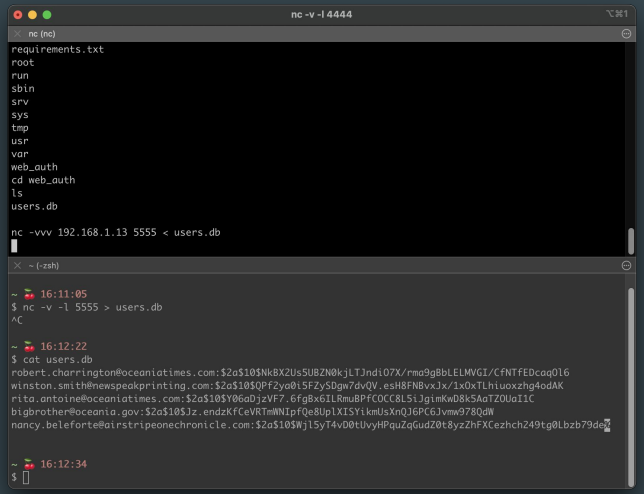
nc -v -l 4444

```
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

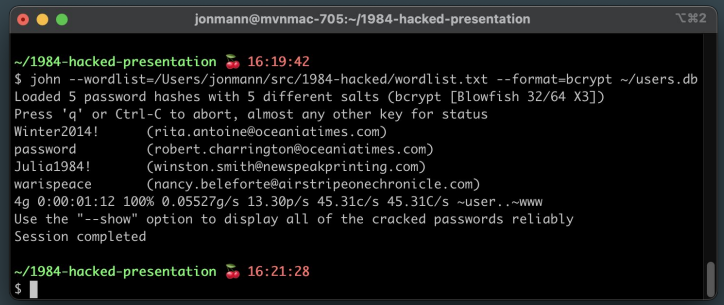
Detection

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



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.



Remarks

Anatomy of a Cyber Attack

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

jonmann.nyc

github.com/jonmannn

Try it yourself!

News Stories