ALPHA 7 RESPONSE

 # Secure The Future With Alpha 7 Response

Defend. Detect. Respond.

PROJECT- IRTx

WWW.ALPHA7RESPONSE.COM

Who Are We?

Rachel's Role

As the Project Manager, Rachel oversees the project's progress and ensures that all tasks are completed on time.
Rachel also serves as the Quality Assurance Lead, focusing on maintaining high standards throughout the project, and contributes to Red Team activities.

Pavli's Expertise

Pavli is the Communication Lead, responsible for ensuring clear and effective communication within the team.
Pavli also leads the Blue Team, coordinating efforts to address security challenges.

Adam's Contributions

Adam plays a crucial role in developing the Project Charter and Brief, outlining the project's objectives and scope.
Adam also leads the Red Team and IRTx Review Evaluation, assessing the project's effectiveness in real-world scenarios.

M's Responsibilities

M is the Project Status Lead, providing updates on the project's progress and identifying any potential issues.
M is also part of the Blue Team, contributing to the team's efforts in detecting and responding to security threats.

Overview Of Project

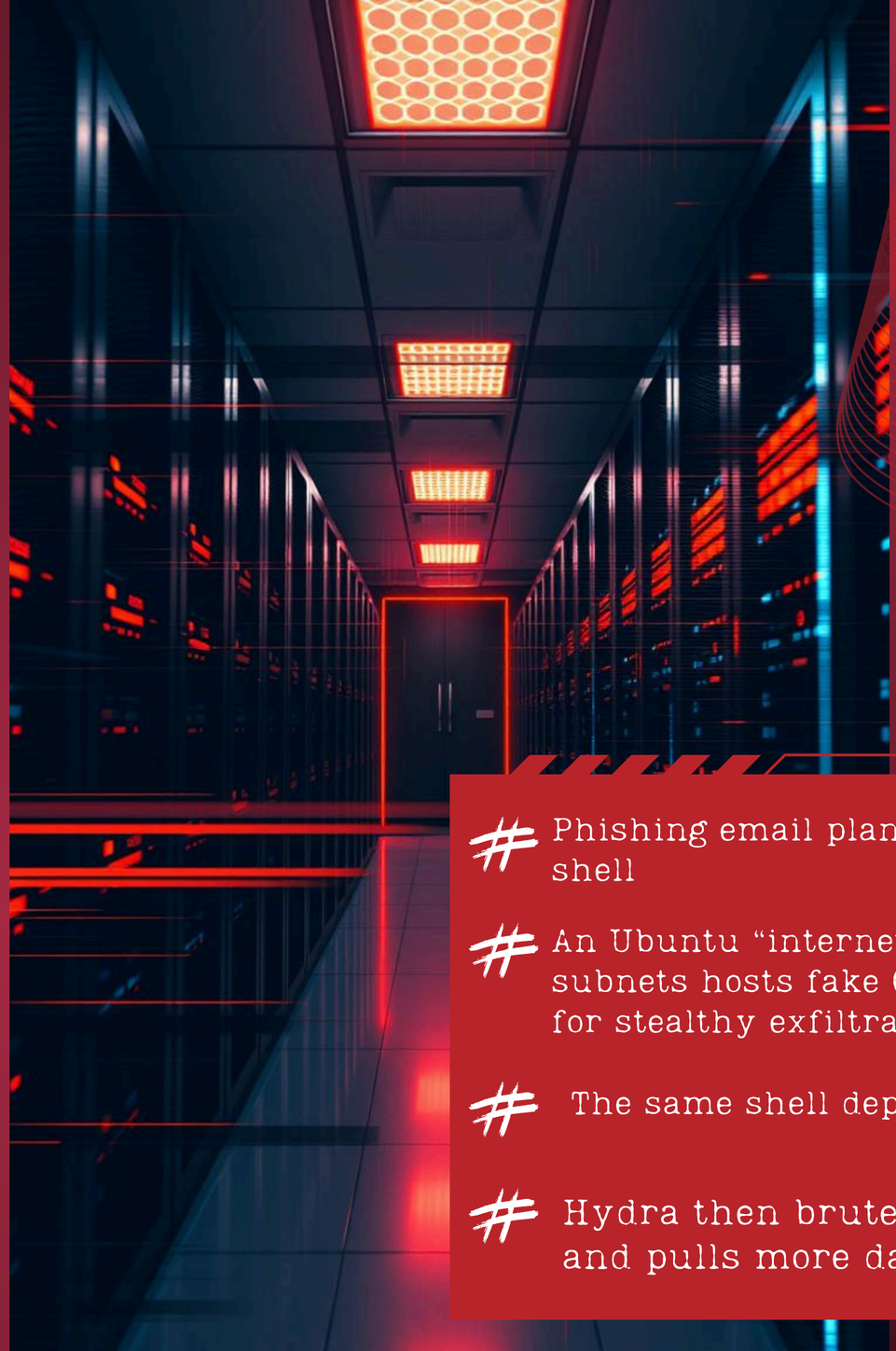
The IRTx project is a three-phase simulation that illustrates how a phishing email can implant a reverse-shell payload, exfiltrate data and keep a covert command-and-control link alive over routine HTTP traffic.

Ubuntu server, placed between attacker and victim VMs on separate subnets, hosts a mock private GitHub repository and Right Point intranet page to emulate internet-facing infrastructure.

Phase 1 covers the initial compromise: the victim runs RightpointV3.exe, data is quietly uploaded and a persistent HTTP reverse shell is established.

Phase 2 leverages that shell for ransomware deployment.

Phase 3 brute-forces SSH with Hydra, obtains root access and extracts further data. Each action is mapped to the Mitre Att&ck Framework and models real-world detection, containment and recovery.

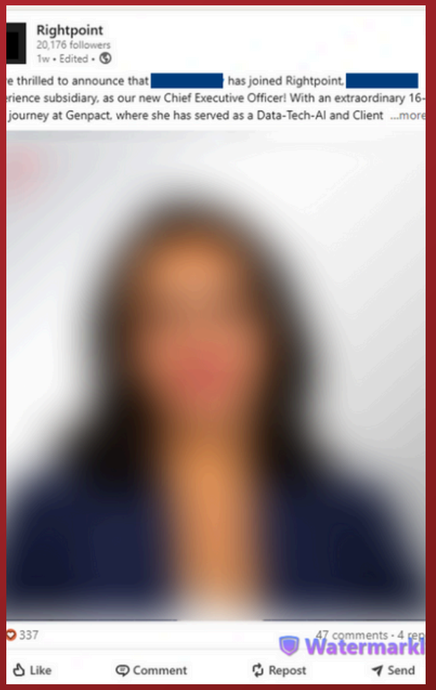


- Phishing email plants a covert HTTP reverse shell
- An Ubuntu “internet” server between isolated subnets hosts fake GitHub and intranet sites for stealthy exfiltration
- The same shell deploys ransomware
- Hydra then brute-forces SSH, gains root and pulls more data

Social Engineering

Subject: URGENT Onboarding Security Update
From: IT Security Department
security@rightpointsec.com
To: Jane Smith@rightpoint.com

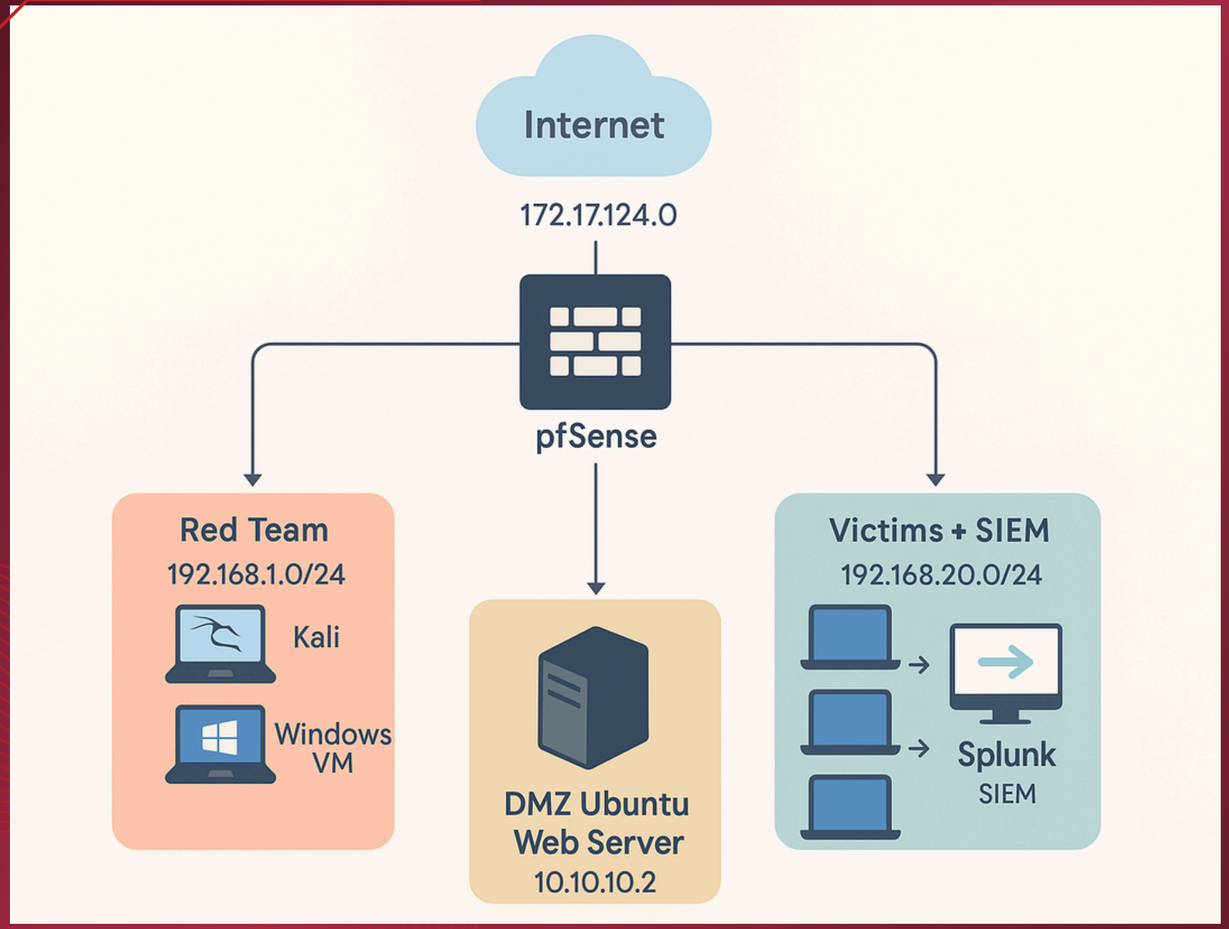
Dear Jane,
Welcome to RightPoint! As part of your system setup and onboarding process, we are finalising the configuration of your user account and workstation security settings.
To ensure your device complies with our internal cybersecurity policies and is fully protected, a critical endpoint security patch must be applied.
This update is part of the standard onboarding procedure for new users and will allow secure access to internal resources, files, and applications.
MANDATORY ACTION REQUIRED:
Please complete the following steps before COB today:
Please visit this secure link to download and run the security update:
http://10.10.10.2/SecurityUpdates/RightPointV3.exe
Once downloaded, right-click the file and select "Run as administrator" to begin the installation.
The patch will install silently in the background. No reboot is required.
Once security update in installed, follow this link to install mandatory anti-ransomware software to protect your machine:
http://10.10.10.2/SecurityUpdates/VictimRansomware.exe
IMPORTANT: Failure to apply this update may result in delays accessing internal systems or a temporary restriction on your account.
If you encounter any issues, please contact the IT Onboarding Desk immediately at helpdesk@rightpointsec.com.
Thank you for your prompt attention, and welcome aboard!
Regards
Adam Baguley
IT Security Department
Right Point



Network Topology

IP Addressing

Kali attack 192.168.1.10/24
Windows Victim 192.168.20.10/24
Ubuntu 10.10.10.2/30



MITRE T1583 - Resource Development

Four VM's will be used to run the attack:

Windows Victim with files located in the Documents and Pictures folders for exfiltration.

A Windows Attacker

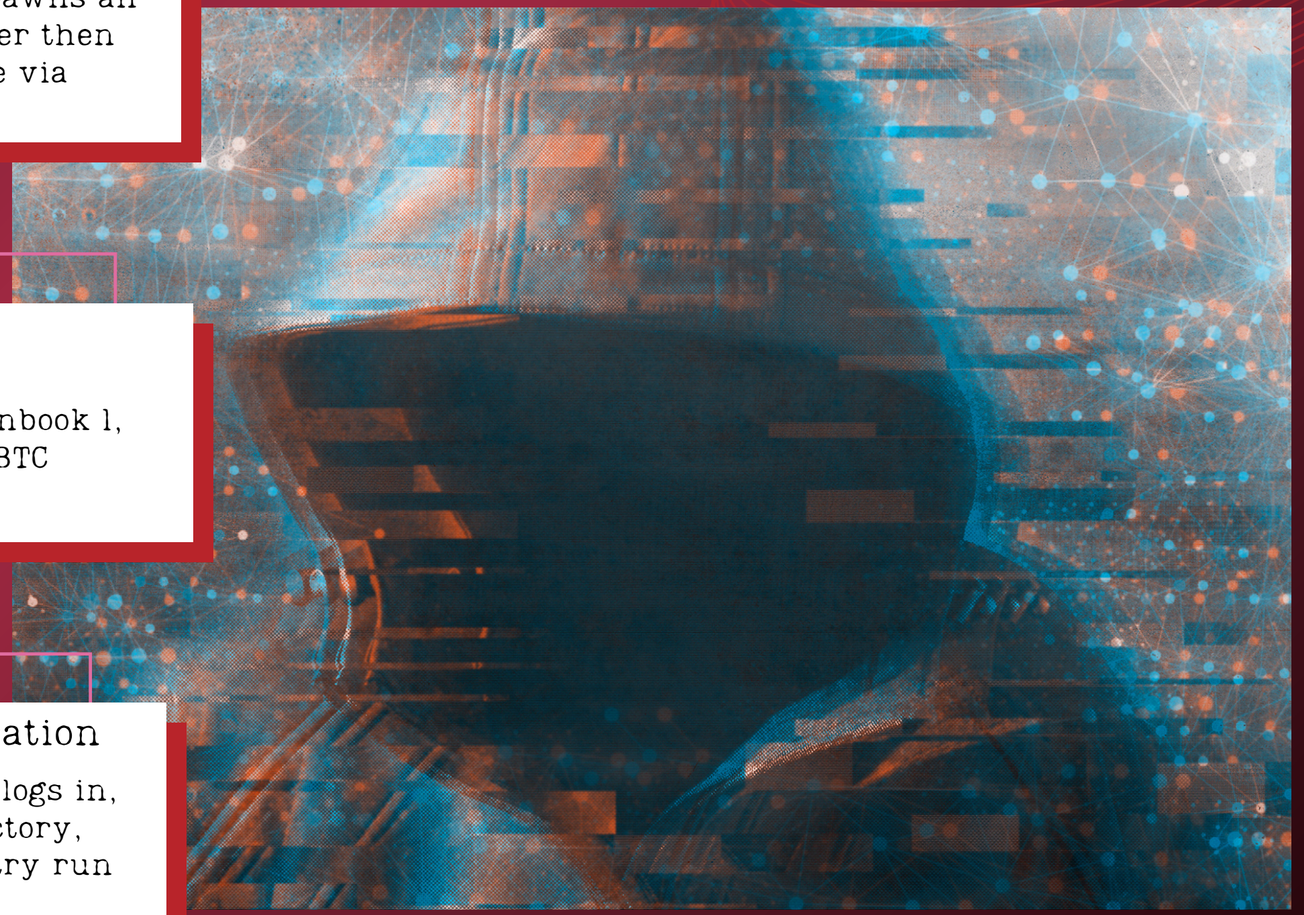
Ubuntu server to host the webpages and cloud storage, acting as the internet.

The Red Run Books

01

Phishing, Reverse Shell, Exfiltration, Persistence

A phishing email delivers RightPointV3.exe, which when run spawns an HTTP reverse shell for covert C2 and file exfiltration; the attacker then gathers host and account details and finally secures persistence via registry run keys.



02

Ransomware

Ransomware is a chained attack approach carrying on from Runbook 1, the payload encrypts files in Documents and Pictures, drops a BTC ransom note on victims desktop.

03

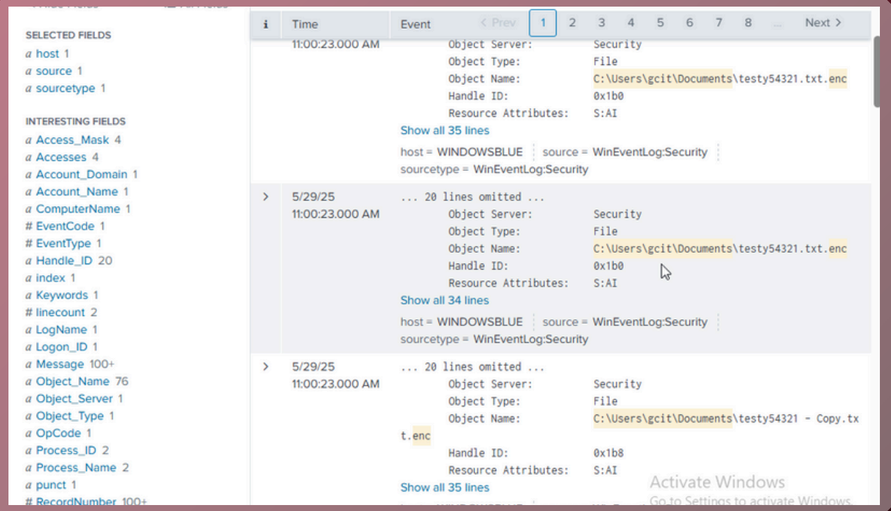
Credential Access, Privilege Escalation, Data Exfiltration

Hydra brute-forces SSH on port 22 (nmap-verified), the attacker logs in, creates a sudo backdoor user, uses SCP to exfiltrate the /var directory, and then removes persistence by deleting the RightPointV3 registry run key.

Blue Team Detection Strategy

A solid Blue Team detection strategy uses Splunk to monitor and analyze logs from virtual machines that simulated attacker's behavior. Custom alerts were configured to detect specific attacker techniques aligned with MITRE ATT&CK framework. Specific alerts were configured. Including:

- User execution of a malicious file - T1204.002
- Persistence via registry run keys - T1547.001
- Command and Control - T1105
- HTTP based communication - T1071.001
- Ransomware execution - T1486



Red Team

Rachel

GOOD

- Realistic attack scenario, allows preparation for real-world attacks.
- Structured and aligned with Mitre Attack Framework

BAD

- Reliance on one method of entry
- Runbook 2 requires the victim to run as administrator

LESSON LEARNT

- From concept to execution takes a vast amount of testing and troubleshooting.
- Could incorporate alternate paths if methods fail.

Adam

GOOD

- Simple reverse shell, evades Windows Defender in some tests.
- Demonstrates how even basic malware can slip past defences
- Demonstrates why Python is a great tool for security professionals.

BAD

- Setup of the infrastructure, websites and Splunk took much longer than planned and required alot of troubleshooting.
- Underestimated time constraints, didn't get to lateral movement.

LESSON LEARNT

- Keep it simple and realistic
- Windows has many built in tools that an attacker can exploit eg. curl, powershell, command prompt.

Blue Team

Pavli

GOOD

- successfully configured custom Splunk alerts
- gained stronger understanding on how real-world attacks align with MITRE ATT&CK

BAD

- spent too much time configuring alerts, Splunk eventually exceeded its memory limits
- time spent recreating alerts rules and dashboards, which delayed threat monitoring and analysis

LESSON LEARNT

- Always shut down virtual machines to prevent Splunk from overloading and flooding the system, thereby exceeding the limit of searches.
- Keeping notes during configuration and setup saves time when rebuilding systems if needed.

M

GOOD

- Using splunk and watching real life alerts
- Working with Windows Security Event IDs

BAD

- Creating alerts for downloading (.exe)files can cause a lot of false positives
- Writing the correct Splunk alert can be an art form -

LESSON LEARNT

- Want to learn Splumk and other SIEM tools better
- How you can spend hours analysing and get yourself down a rabbit hole

#Thank you

support@Alpha7Response

@Alpha7Response

Alpha7 Response

Defend. Detect. Respond.

Secure the Future with Alpha 7 Response