

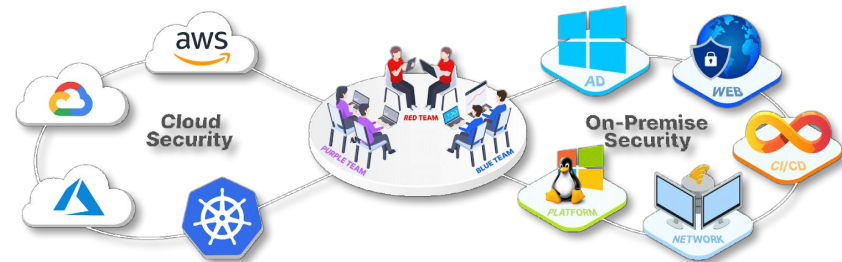


# **ByBit Breach Uncovered: APT-Style Crypto Exploitation in Cloud Environments**

## ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform



### INFINITE LEARNING EXPERIENCE

About Speaker:

**Parth Agrawal**  
(Security Researcher @CWL)

Is a cloud security enthusiast with a keen interest in the intricacies of cloud services offered by AWS, Azure, and GCP. Possessing a comprehensive understanding of these platforms, they are particularly drawn to exploring Red Team methodologies. Interested in Red Team methodologies, focusing on vulnerability testing and detection across external attack surfaces.

# Agenda

- Who the attackers were and what motivated them
- How the attack unfolded — from phishing to data exfiltration
- The cloud exploitation and advanced evasion techniques used
- What security operations could have done to detect or stop this
- And finally, how you can experience this hands-on in a gamified lab on our INFINITY platform.

BYBIT

## Why Bybit Was a Target

1. Massive Funds Under Custody
2. Attractive to North Korean Actors
3. Movement Between Cold and Hot Wallets
4. Possible Human Vulnerabilities:

## Key Growth Highlights of Bybit:

1. User Base
2. Daily Trading Volume
3. Market Position
4. Technology Focus

# Meet the Threat Actor – Lazarus Group

**Lazarus** is a North Korean state-sponsored Advanced Persistent Threat (APT) group, believed to be operating under the Reconnaissance General Bureau (RGB), which is North Korea's primary intelligence agency.

## Notable Attacks:

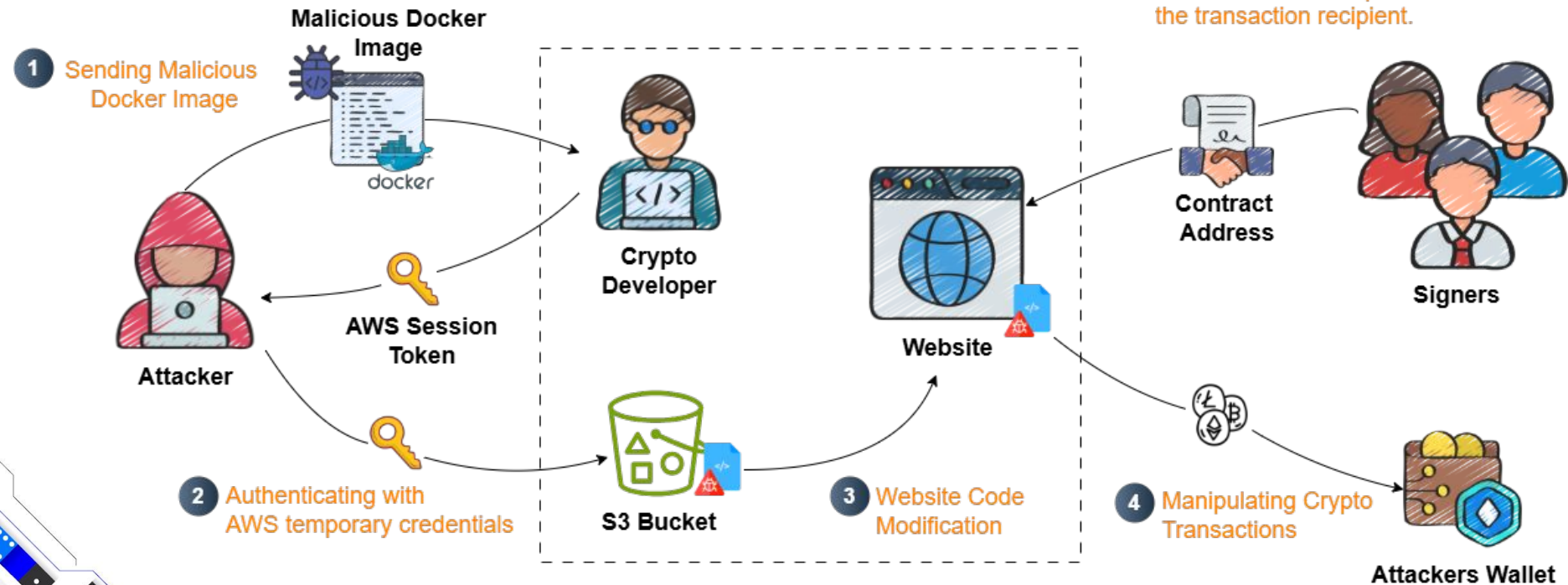
- Sony Pictures Hack (2014)
- Bangladesh Bank Heist (2016)
- WannaCry Ransomware (2017)
- Crypto Exchange Heists (2017–2023)

## Tactics Used by Lazarus in Crypto Exchange Attacks:

- Spear Phishing
- Remote Access Trojans (RATs)
- Cloud Credential Theft
- Lateral Movement
- API Abuse
- Log Tampering

# Crypto exchange heist: by Lazarus Group (DPRK)

The script was altered to include a backdoor and tamper with the transaction recipient.




# Simulation of Crypto Exchange Heist

 **Infinity Learning**




## Crypto exchange heist: by Lazarus Group (DPRK)

As part of Secure-Corp's elite Red Team, your mission is to simulate the Crypto Hack, a real-world-inspired attack where threat actors infiltrated cloud infrastructure to modify legitimate code and drain crypto assets.

 Hard

 Free

 30

 Not Completed



# Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings  
please contact

**support@cyberwarfare.live**

To know more about our offerings, please visit: **<https://cyberwarfare.live>**