From Zero to Sixty

The Story of North Korea’s Rapid Ascent to Becoming a Global Cyber Superpower

Josh Burgess
Global Technical Lead Threat Advisor

Jason Rivera
Director: Strategic Threat Advisory group

SPEAKER BACKGROUND

JASON RIVERA
DIRECTOR: STRATEGIC THREAT ADVISORY GROUP

ARMY | GOVERNMENT | INTELLIGENCE | CONSULTING

- **14+ years** innovating at the intersection of security operations & technology
- **US Government**: Former Intelligence Officer/Captain in the U.S. Army; assignments with National Security Agency (NSA), U.S. Cyber Command (USCYBERCOM); served in combat tours overseas
- **Private Sector**: Built threat intelligence programs for large fortune 500 companies and us government agencies
- **Education**: Masters, Security Studies from Georgetown University, and Economics from the University Of Oklahoma
- **Public Speaking**: RSA Conference, Gartner Conference, NATO Conference On Cyber Conflict; InfoSecWorld Conference & Expo

Jason(dot)Rivera@CrowdStrike.com

+1-571-417-0494

SPEAKER BACKGROUND

JOSH BURGESS
LEAD GLOBAL TECHNICAL THREAT ADVISOR

USAF | GOVERNMENT | FINANCE | INDUSTRY

JOSH BURGESS HAS MORE THAN A DECADE OF CYBER THREAT ANALYSIS & MITIGATION EXPERIENCE SERVING IN MULTIPLE POSITIONS INCLUDING IN THE INTELLIGENCE COMMUNITY, THE DEPARTMENT OF DEFENSE, AS WELL AS THE FINANCIAL SECTOR. IN A MAJORITY OF HIS ROLES HE HAS SERVED AS THE TECHNICAL LEAD THREAT INTELLIGENCE OFFICER FOR A LARGE SOC TO ADVISE THEM OF THE LATEST THREATS AND ENSURE A SOUND SECURITY POSTURE. HIS MAIN ROLE IN HIS CURRENT POSITION AT CROWDSTRIKE IS TO SUPPORT CUSTOMERS BY APPLYING HIS EXPERIENCE IN ACTIONING BOTH SHORT-TERM TACTICAL AS WELL AS LONG-TERM STRATEGIC INTELLIGENCE DATA AND REPORTING

✉ JOSH(dot)BURGESS@CROWDSTRIKE.COM

📱 +1-571-432-7004

AGENDA

EXECUTIVE SUMMARY

PHASE 1: MILITARY-FOCUSED TARGETING

PHASE 2: CURRENCY GENERATION OPERATIONS

PHASE 3: DUAL-FOCUSED OPERATIONS

CONCLUSION

EXECUTIVE SUMMARY

NORTH KOREA'S PATH TO BECOMING A GLOBAL CYBER SUPERPOWER

Military-Focused Targeting

Early 2000s – 2014 characterized primarily by military-focused targeting.

Currency Generation Operations

Late 2015 – early 2018 geared more so towards currency generation attacks (fraud, ransomware, SWIFT banking system attacks, etc.)

Dual-Focused Operations

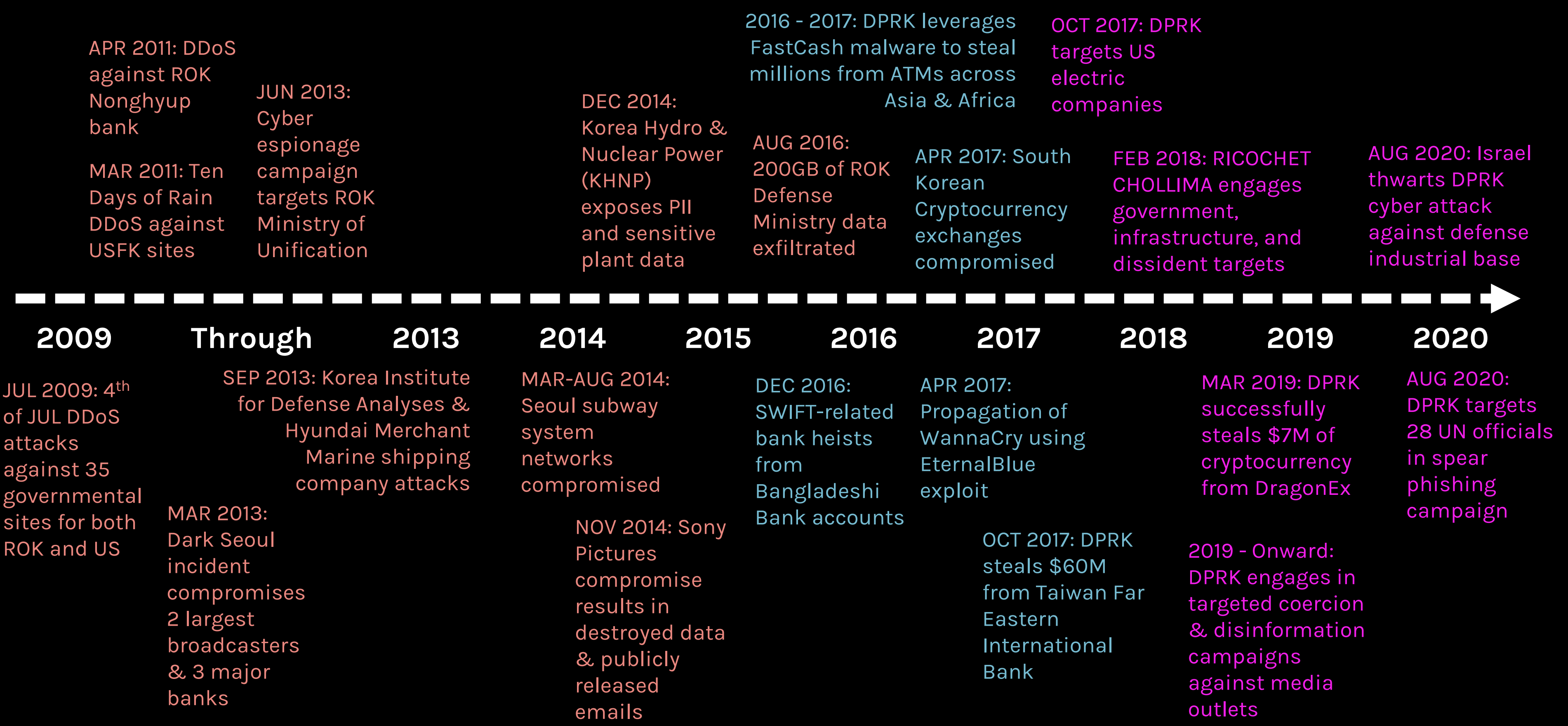
Early 2018 onwards marks a shift towards dual-focused ops engaging both economic expansion targets & gov targets

A BRIEF HISTORY IN REVIEW

Military-Focused Targeting

Currency Generation Operations

Dual-Focused Operations



2009

JUL 2009: 4th of JUL DDoS attacks against 35 governmental sites for both ROK and US

Through

MAR 2011: Ten Days of Rain DDoS against USFK sites

APR 2011: DDoS against ROK Nonghyup bank

MAR 2013: Dark Seoul incident compromises 2 largest broadcasters & 3 major banks

JUN 2013: Cyber espionage campaign targets ROK Ministry of Unification

SEP 2013: Korea Institute for Defense Analyses & Hyundai Merchant Marine shipping company attacks

2013

2014

MAR-AUG 2014: Seoul subway system networks compromised

NOV 2014: Sony Pictures compromise results in destroyed data & publicly released emails

DEC 2014: Korea Hydro & Nuclear Power (KHNP) exposes PII and sensitive plant data

2015

2016

2016 - 2017: DPRK leverages FastCash malware to steal millions from ATMs across Asia & Africa

AUG 2016: 200GB of ROK Defense Ministry data exfiltrated

DEC 2016: SWIFT-related bank heists from Bangladeshi Bank accounts

2017

APR 2017: South Korean Cryptocurrency exchanges compromised

APR 2017: Propagation of WannaCry using EternalBlue exploit

OCT 2017: DPRK targets US electric companies

OCT 2017: DPRK steals $60M from Taiwan Far Eastern International Bank

2018

FEB 2018: RICOCHET CHOLLIMA engages government, infrastructure, and dissident targets

2019

MAR 2019: DPRK successfully steals $7M of cryptocurrency from DragonEx

2019 - Onward: DPRK engages in targeted coercion & disinformation campaigns against media outlets

2020

AUG 2020: Israel thwarts DPRK cyber attack against defense industrial base

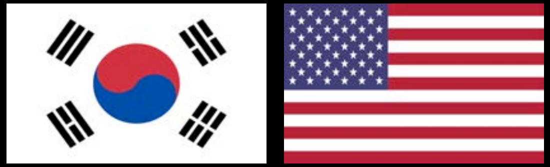
AUG 2020: DPRK targets 28 UN officials in spear phishing campaign

PHASE 1: MILITARY-FOCUSED TARGETING

PHASE 1: MILITARY FOCUSED TARGETING

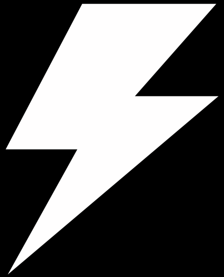
The Personas

In the beginning, North Korea sought to avoid attribution by leveraging aliases in the course of their attacks



Military Targeting of the USA/ROK

Multiple DDoS and data theft operations performed against US and ROK military targets in order to promote national security objectives



Power Projection

Projecting capabilities internationally to demonstrate force to include commercial targets with a symbolic nexus to adversarial entities

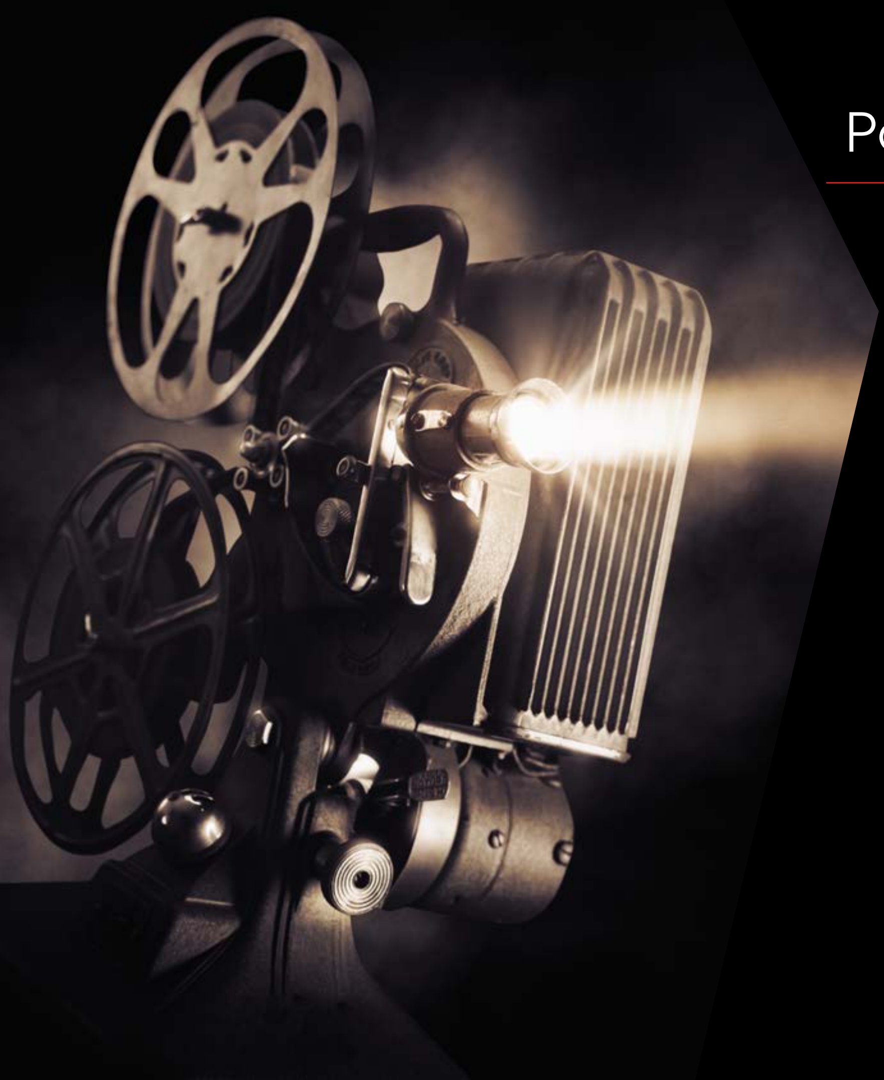
Military-Focused Targeting | **Currency Generation Operations** | **Dual-Focused Operations**

Personas

- Independence Day and 10 Days of Rain
  - Initially no misdirection but also not outright admission
- DarkSeoul
  - Whois Team with references to Roman foot soldiers
- Operation HighAnonymous
  - Riding the popularity of Anon campaigns
- Guardians of Peace
  - Imagery overlap with Whois with all hands on deck
- WhoAmI
  - Bending hacktivist front with straight up monetary extortion

Military Targeting Of South Korea

- Memory of Independence day 4 July 2009
  - Dozer botnets target RoK government and Banking as well as .gov, .mil, and .com
- 10 Days of Rain attacks
  - KoreDoS used to create botnet then a MBR wiper
  - Searched for files specific to RoK systems
- Dark.Seoul Operation
  - Whois wipers used against Media, ATMs and networks at Shinhan and NongHyup banks hit hardest
    - Windows and Linux wipers
- Operation High Anonymous
  - KoreHigh malware used in Gov and media targeting
  - Changes password to Highanon2013 but the malware was coded in with legit credentials
- Kimusky attack on KHNP
  - Kimusky malware used Extensive recon before encryption
  - 5,986 phishing attacks, sent in e-mails to 3,571 KHNP leaked 10,799 employees



Power Project Operations

- SONY Attack
- Retribution for *The Interview*
- Released employee information and future motion pictures
- Ties to multiple DPRK families of malware including
  - BRAMBUL with ties to Independence Day
  - KorHigh used HighAnon
  - MACKTRUCK used to target defense and Financials
  - NESTEGG also used in Financials

Malware Demo: Dozer

Because Sometimes You Want to Break Stuff

PHASE 2: CURRENCY GENERATION OPERATIONS

PHASE 2: CURRENCY GENERATION OPERATIONS

SWIFT Targeting

Targeting the SWIFT banking system, which is the international banking messaging system, to engage in global fraud

ATM Jackpotting

Leveraging malware capabilities such as FastCash to engage banking entities throughout Asia and Africa

Ransomware (WannaCry) Operations

Leveraging ransomware in order to target corporate entities and fulfill financial objectives

Military-Focused Targeting

Currency Generation Operations

Dual-Focused Operations

Swift Targeting

- 19 Total attacks observed in 18 countries
- Attempts to steal over 2 Billion USD across all financial targeting
- Deep knowledge of target systems well before the hack was performed
- Specialized one off malware
  - Modify output of FoxIT PDF reader to hide transactions
- Wipers deployed behind the attack
  - Highly modular malware framework with wipers to delete evidence

ATM Jackpotting (Operation FASTCash)

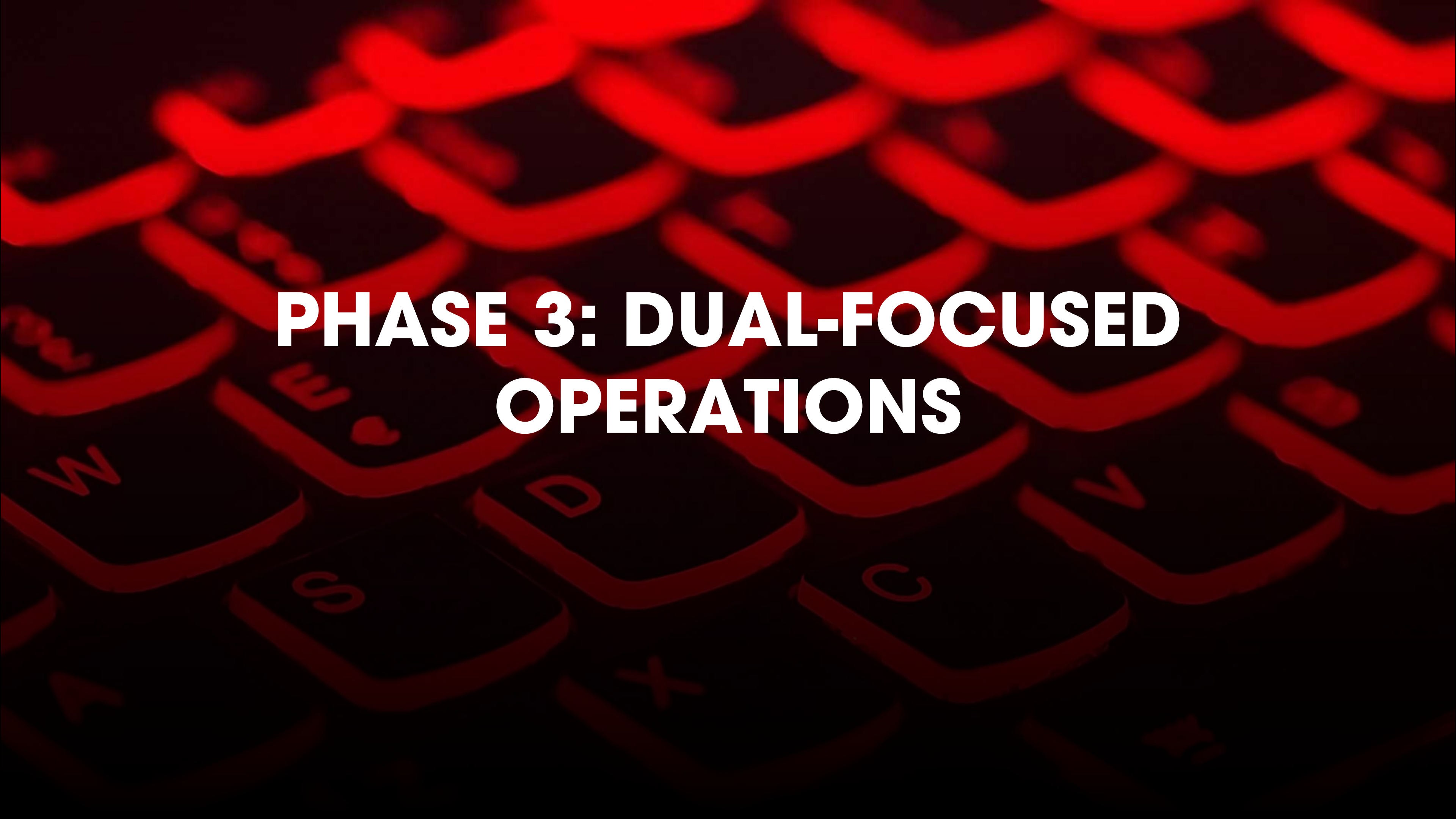
- Begins with TwoPence Framework to establish a beachhead
- Specialized AIX Operating system specific malware
- Attack allowed ATM Jackpotting in more than 30 countries
- One case 10,000 fraudulent cash withdraws in 20 countries in only 5 hours.

Ransomware (WannaCry) Operations

- While WannaCry operations were observed in May 2017 other variants date back to February 2017
  - Earlier victims had destructive malware on their network
- Infection vector with ties to the KorDLL framework
- Utilized EternalBlue so anyone with open SMB ports was a target
- 200,000 Systems infected worldwide demanding $300+ in bitcoin but only made a around 139k in revenue

Malware Demo: WannaCry

Going Nuclear



PHASE 3: DUAL-FOCUSED OPERATIONS

PHASE 3: DUAL-FOCUSED OPERATIONS

Economic Growth Targeting

Targeting in order to steal intellectual property in support of DPRK’s economic growth objectives

Expanded Criminal Operations

Targeting against non-traditional financial entities such as cryptocurrency exchanges and markets

Targeting Gov-Related Entities

Targeting against gov-nexus entities such as think tanks, NGOs, & international orgs

Military-Focused Targeting
Currency Generation Operations
Dual-Focused Operations

Economic Growth Targeting

- 2017 Targeting of North America similar to previous RoK targeting
  - Energy focused and espionage motivated but did not disrupt energy production
  - 2018 ceased targeting of US but continued EU and APAC
- 2019 Indian Powerplant targeting
  - Targeting made to look destructive but really espionage focused
    - Dtrack Malware tied back to Indian ATMs and even RoK banks because you need to keep the lights on

Expanded Criminal Operations (Crypto)

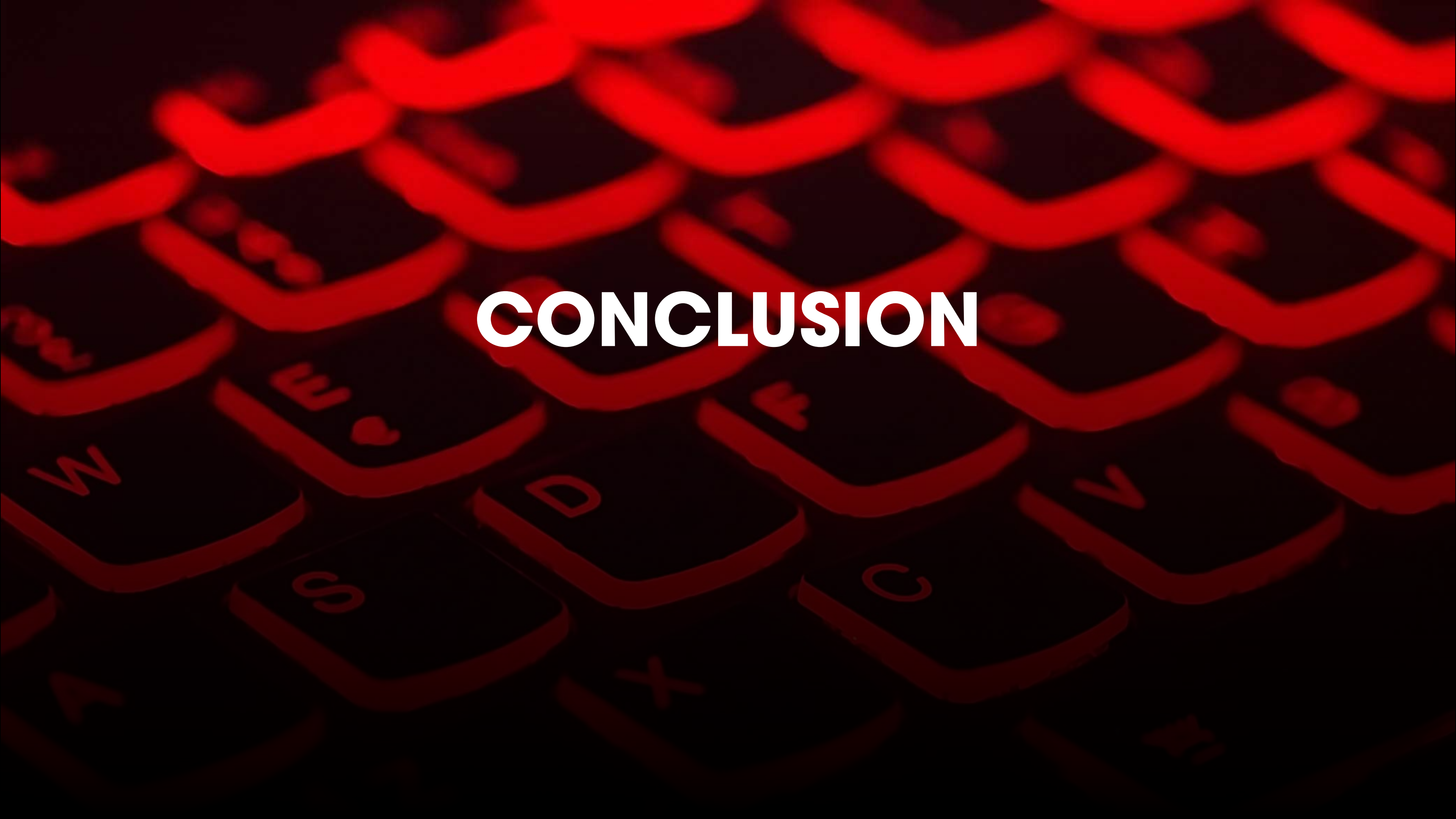
- Crypto Currency targeting via fake applications
  - Included the use of front companies to gain legitimacy

- eCrime collaboration with multiple different actors
  - Lazarus collaboration and delivery via Trickbot

- MataNet malware which works on Windows, Mac and Unix OS
  - VHD Ransomware

Malware Demo: Hermes

Lazarus Head Fake



CONCLUSION

WHAT THE FUTURE MAY HOLD FOR THE NORTH KOREAN REGIME

Advanced Ransomware Operations

DPRK may engage in more advanced ransomware ops techniques to include data extortion, ransomware-as-a-service, etc.

Taking a Page out of China's Playbook

Similar to China, DPRK will likely refine their focus on economic growth targets in support of their five-year plan objectives

Cyber Brinkmanship

In order to avoid kinetic retaliation, DPRK may transition focus away from nuclear deterrence more towards cyber deterrence

THANK YOU FOR YOUR TIME