A Deep Dive into ThreatNeedle cluster of Lazarus Group

Seongsu Park,
Senior security researcher
Kaspersky Global Research and Analysis Team

whoami

- Name : Seongsu Park (@unpacker)
- GReAT Senior Security Researcher
- Threat intelligence analyst, Cyber threat hunter
- Focused on Korean-speaking APT actors

Author of Securelist

- Lazarus covets COVID-19 related intelligence
- MATA: Multi-platform targeted malware framework
- Operation AppleJeus Sequel
- ScarCruft continues to evolve, introduces Bluetooth harvester
- Cryptocurrency businesses still being targeted by Lazarus
- Operation AppleJeus
- OlympicDestroyer is here to trick the industry

Lazarus group

Adversary

Lazarus(a.k.a Hidden Cobra)

Published by Novetta in 2014

Several campaigns/subgroups

Victim

Financial profit

Cyber espionage

Capability

Weaponized document

Manuscrypt/ThreatNeedle

Multi-stage components

Several malware clusters

Infrastructure

Compromised server

Commercial hosting service

GREAT

kaspersky

Malware clusters of Lazarus group

ThreatNeedle cluster

MATA(a.k.a Dacls) cluster

AppleJeus cluster

Bookcode cluster

DeathNote(a.k.a DreamJob) cluster

Manuscrypt cluster

Feb 2018

May 2018

June 2018

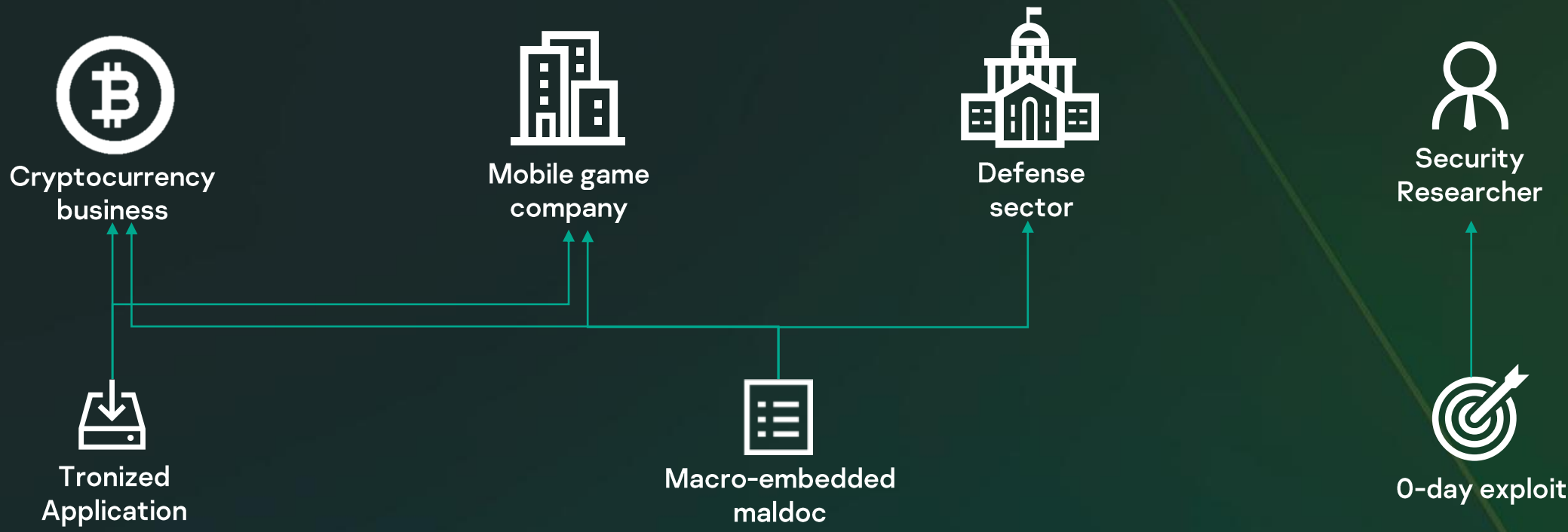
Jul 2018

Oct 2018

GREAT

kaspersky

Initial Infection



GREAT

kaspersky

ThreatNeedle Malware

Malware components

Installer

- Delivered by infection vector
- Contain payload and config
- Install payload

Downloader

- Fetch payload
- Load directly fetch payload
- Send triage information

Loader

- Various types
- Load next payload after decrypting
- Refelctive loading

Injector

- Decrypt payload
- Inject to legitimate process

Backdoor

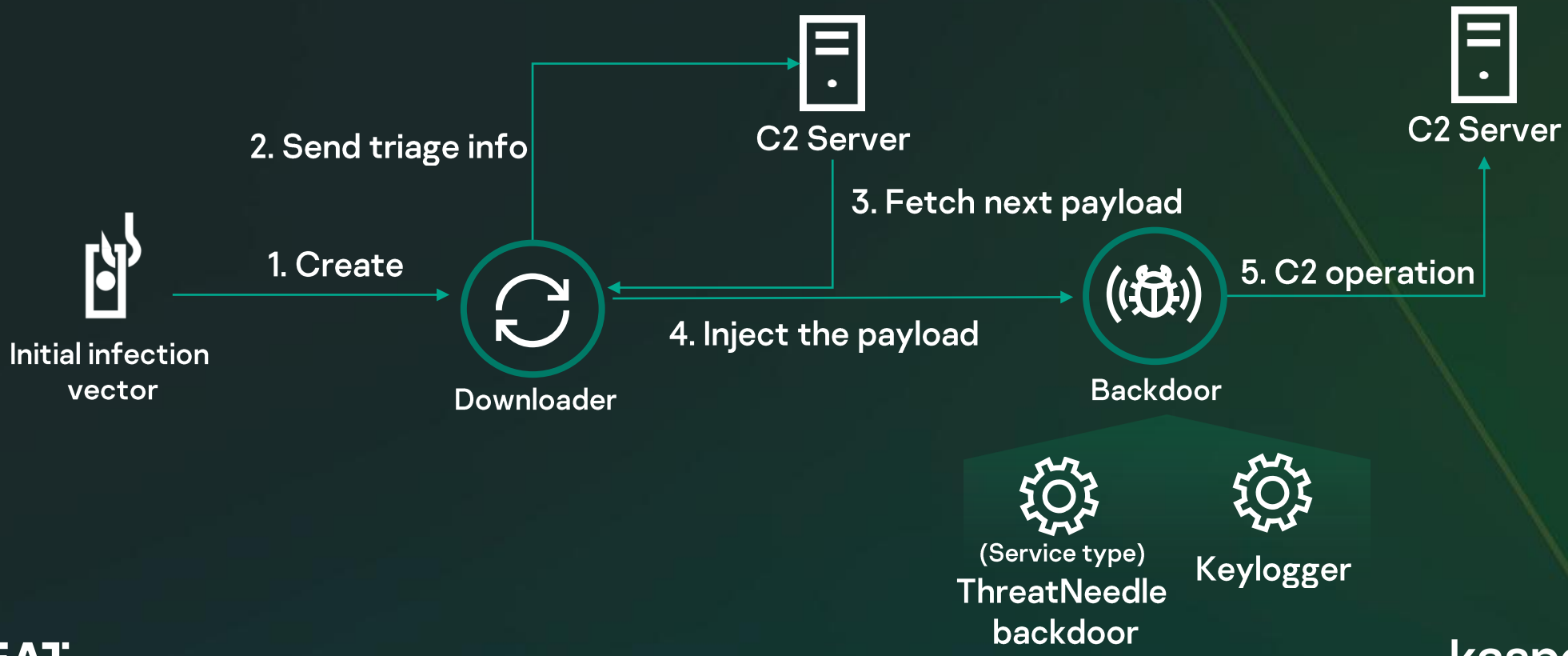
- Final payload
- Full-featured backdoor
- Handle keyboard-hands-on activities

GREAT

kaspersky

ThreatNeedle Malware

Infection Scheme



GREAT

kaspersky

Post-exploitation

- Windows commands
- Custom SMB scanner

Discovery

- Sniffing
- Responder(NBT-NS poisoning)
- Browser storeed credential

Crendential Gathering

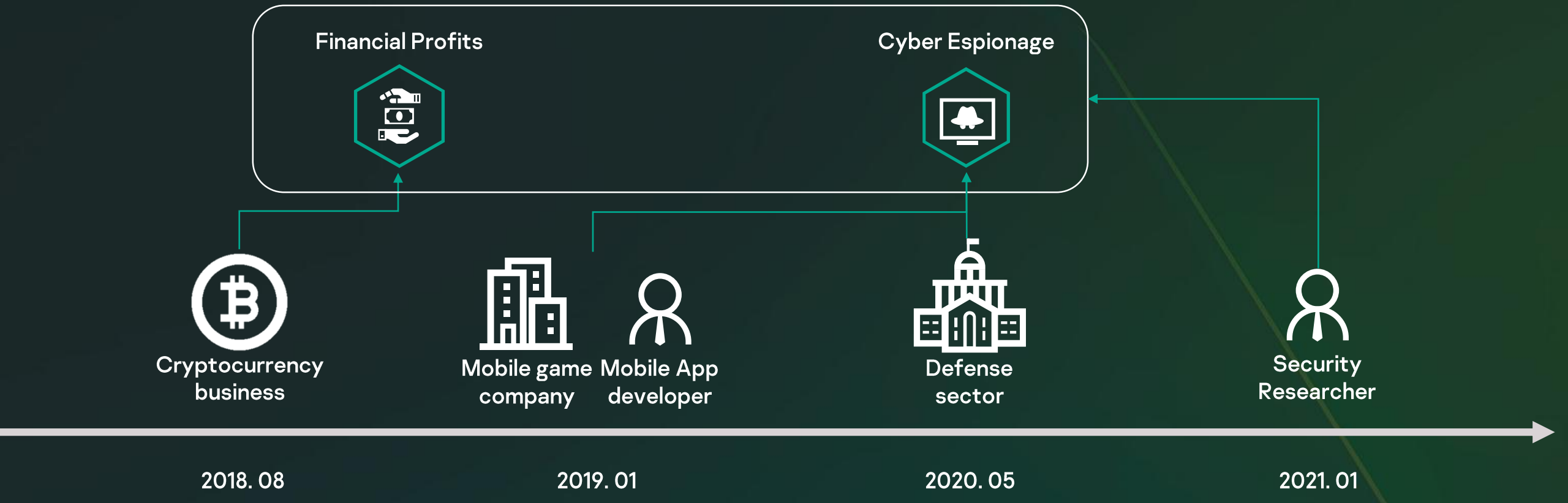
- Windows commands (WMIC)
- Copy ThreatNeedle
- Overcome air-gap network

Lateral Movement

- Tunneling tool
- Exfiltration tool disguised as VNC viewer

Exfiltration

Victimology



GREAT

kaspersky

Polling

GREAT

kaspersky

Summary

- ThreatNeedle: Multi-component based multi-stage infection
- Highly sophisticated and rapid keyboard-hands-on activity
- Strong motivation target for various industry, even you can be the victim

Question?


@unpacker


seongsu.park@kaspersky.com