ISCR 2020
International Symposium on Cybercrime Response

Deep Dive Into Cybercrime-like APT Attack of Lazarus Group

Seongsu Park
Kaspersky, GReAT Senior security researcher

About me

SEONGSU PARK

Global Research and Analysis Team

Senior security researcher

Tracking targeted attacks focused on APAC

Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

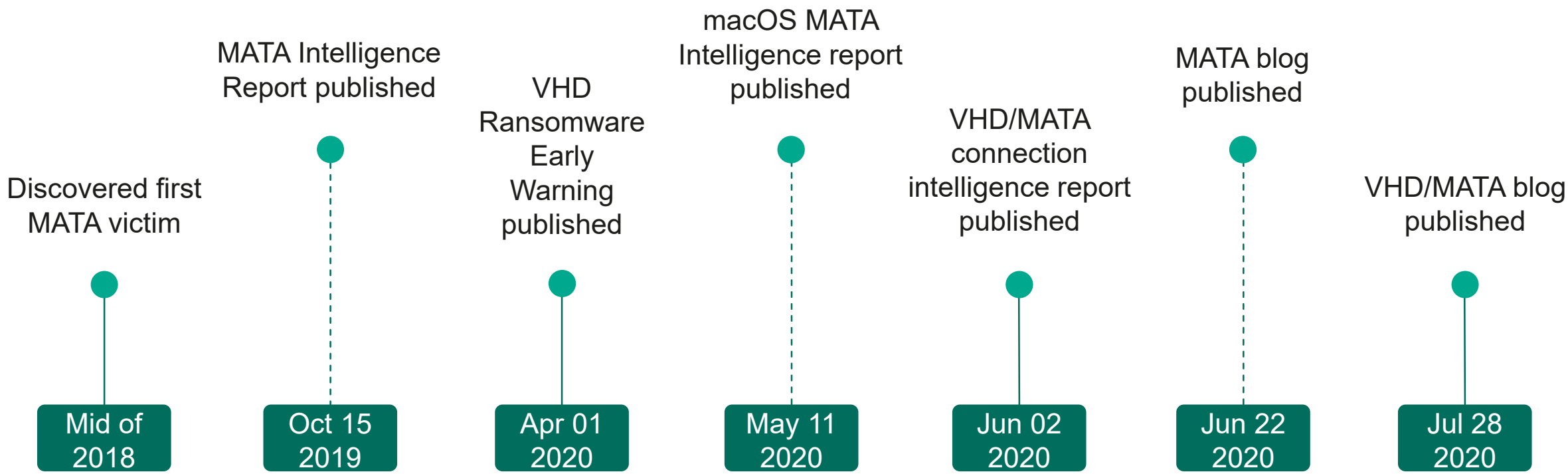
Abstract

Emergence of new multiplatform target malwre cluster: MATA

Connection between MATA and other cybercrime-like attack

Ambiguous boundary of cybercrime and targeted attack

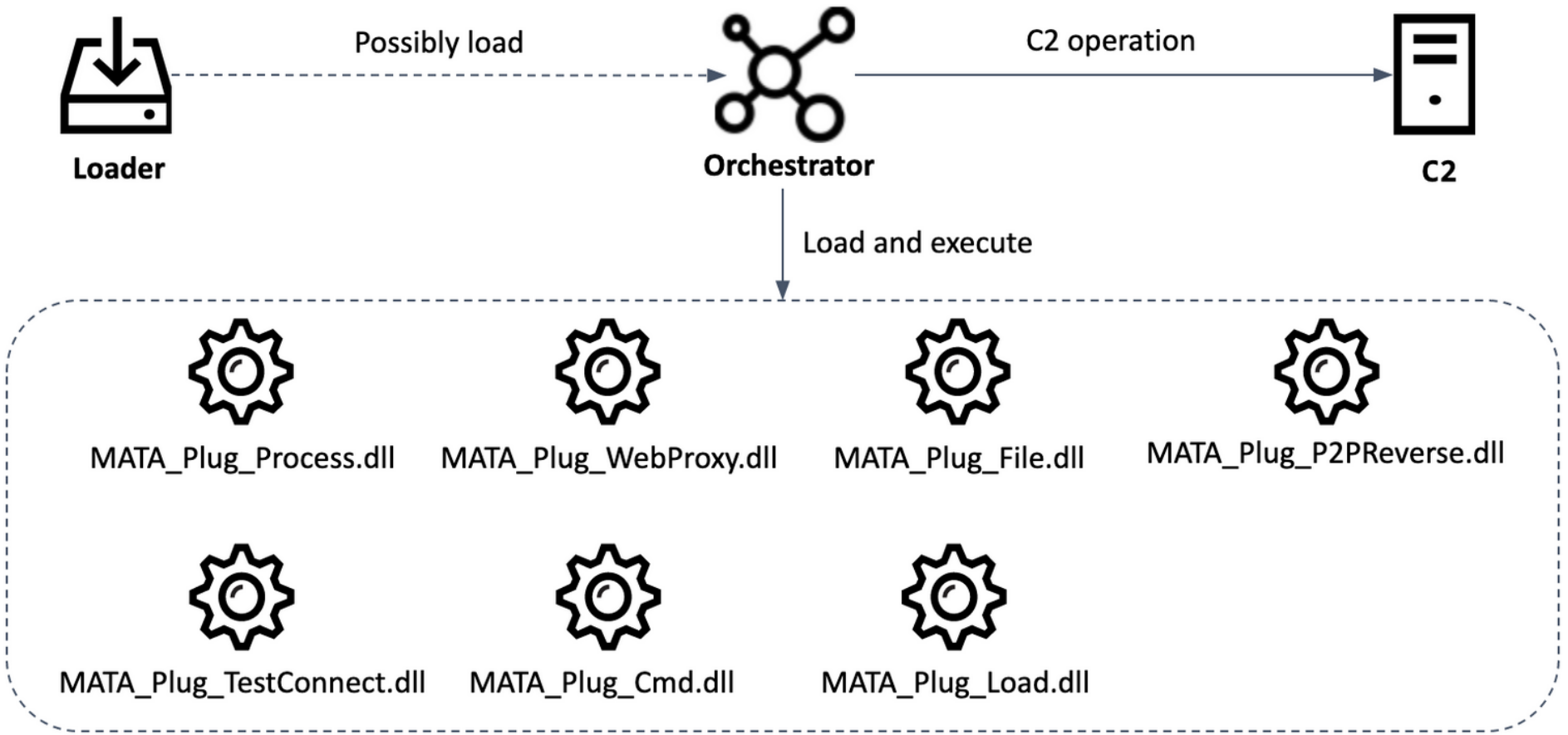
Timeline of this research



MATA Framework

kaspersky

MATA Framework



Loader

Malware to load orchestrator of MATA framework

Retrieve file path to load
Decrypt hardcoded hex-string with AES to obtain the file path.

Load DLL file
Decrypt file with AES and load as DLL.

Interesting parent process
Executed by WmiPrvSE.exe(WMI Provider Host process) process.

Orchestrator

C2 operation and loading plugins

Loading configuration

Found in “lasss.exe” process.
Load and decrypt config from registry.
e.g.) HKLM\Software\Microsoft\KxtNet

C2 operation

Use openssl library and RC4 session key.
CMataNet: client/server mode.
Send a profile of the victim.
Download and load plugins.
Update configuration.

MATA Plugins

Enrich plugins: 7 plugins in Windows version of MATA

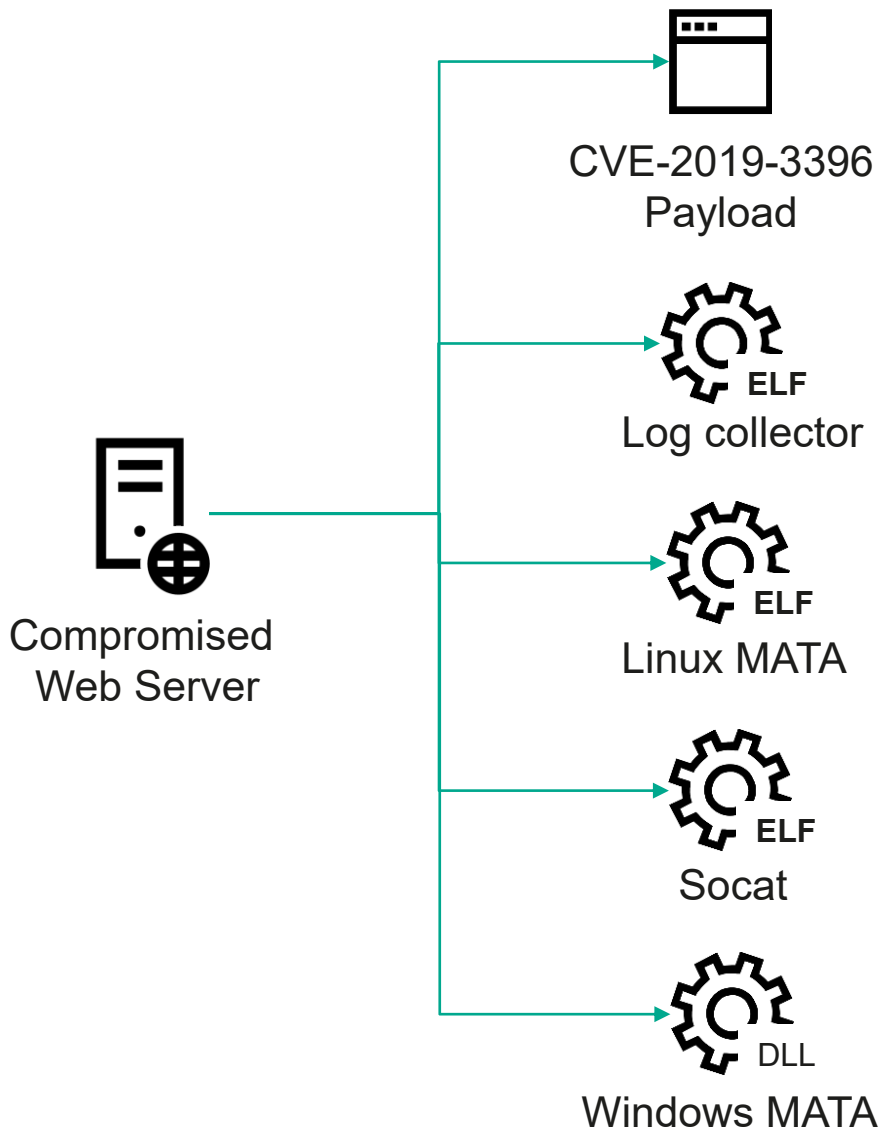
How to retrieve plugins?

Download plugins from remote server
Load AES-encrypted plugin DLL
Download plugin DLL from current MataNet

Type of Plugins

Plugin name	Description
MATA_Plug_Cmd.dll	Run “cmd.exe /c” or “powershell.exe” with the specified parameters.
MATA_Plug_Process.dll	Manipulate process
MATA_Plug_TestConnect.dll	Check TCP connection with given IP:port or IP range. Ping given host or IP range.
MATA_Plug_WebProxy.dll	Configure a HTTP proxy server.
MATA_Plug_File.dll	Manipulate files
MATA_Plug_Load.dll	Inject payload into the given process
MATA_Plug_P2PReverse.dll	Connect between MataNet server on one side and an arbitrary TCP server on the other, then forward traffic between them.

Malware Set of MATA: Linux version



Script for exploiting Atlassian Confluence server

Linux tool for listing folder

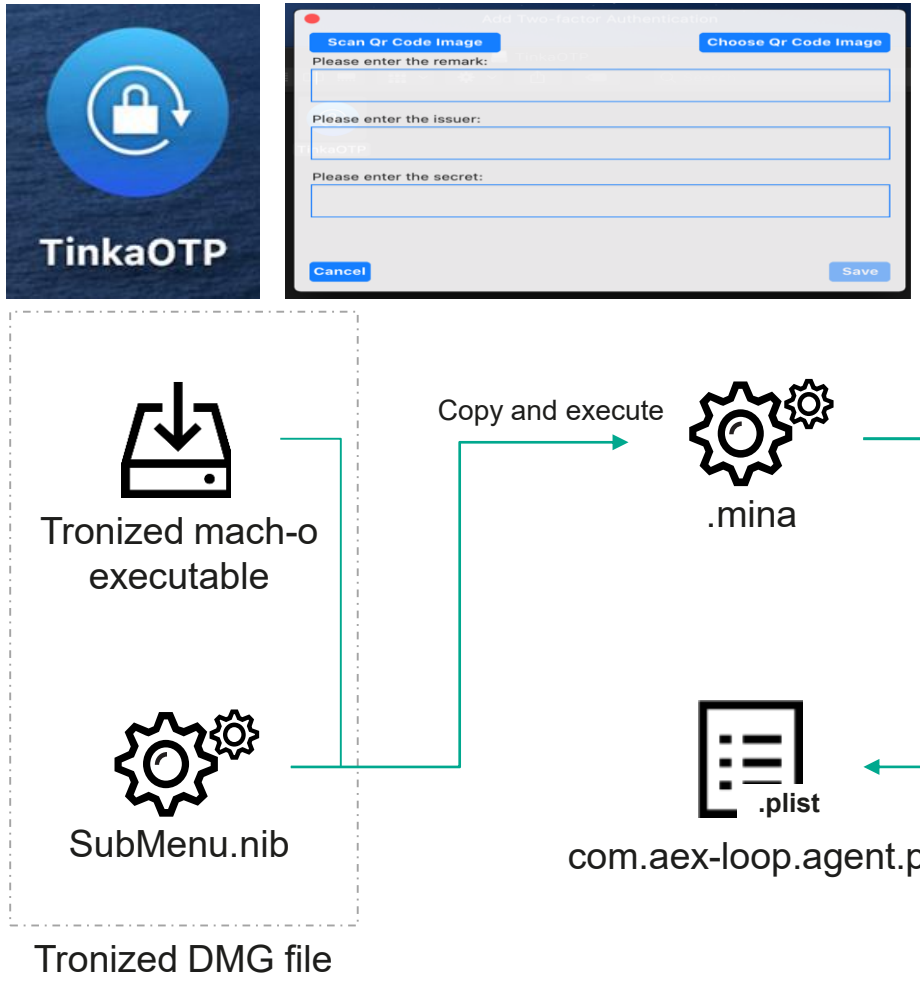
Linux version MATA

- Orchestrator + plugins
- Target diskless network devices.
- Run “scan” command against TCP 8291, 8292 ports

Legitimate linux utility for relay

Windows version MATA Orchestrator

Malware Set of MATA: macOS version



Tronized open-source application for managing 2FA.

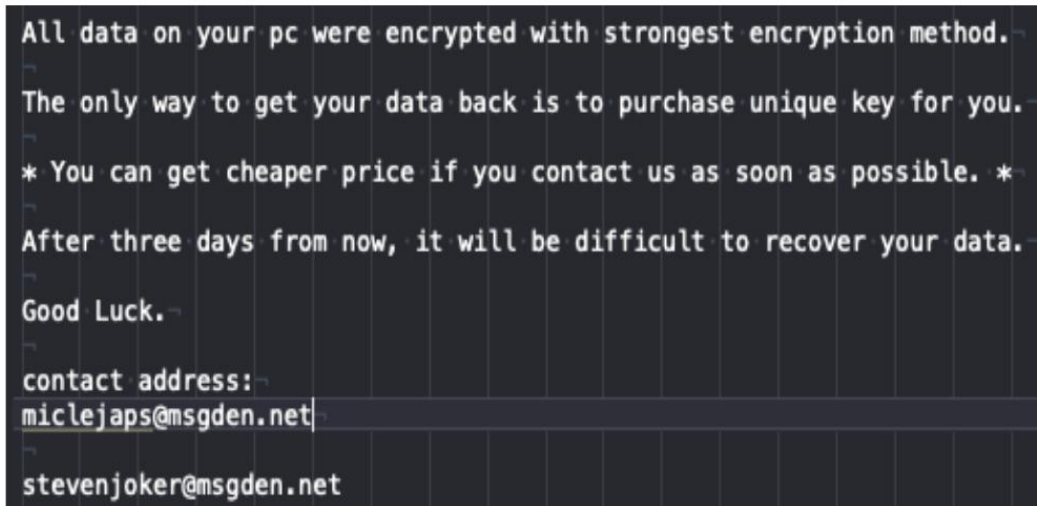
Functionality of plugins is almost identical with Linux MATA.

Certification file names and configuration structure are similar with old Lazarus's tool.

Prime Intention of MATA

kaspersky

Unknown Ransomware Family



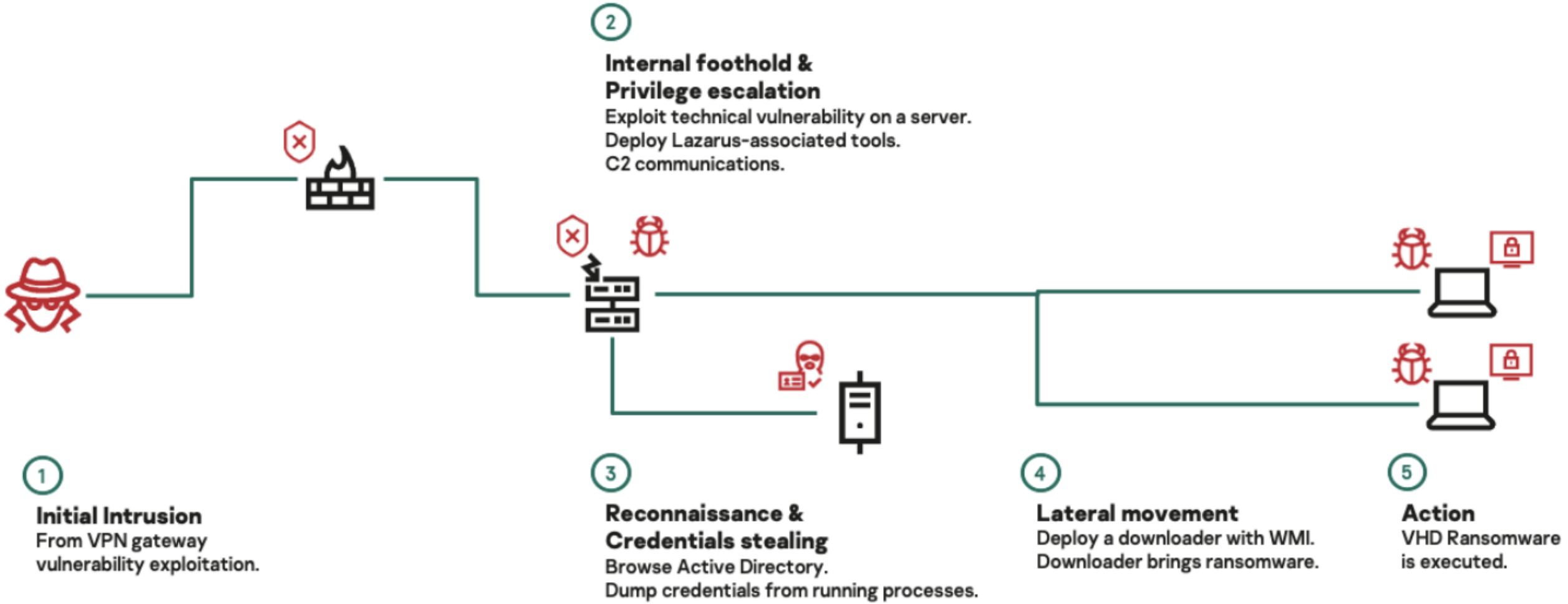
Self spreading ransomware

Combination of worm-like tool + ransomware.
Using net share, remote copy, execute with WMIC.

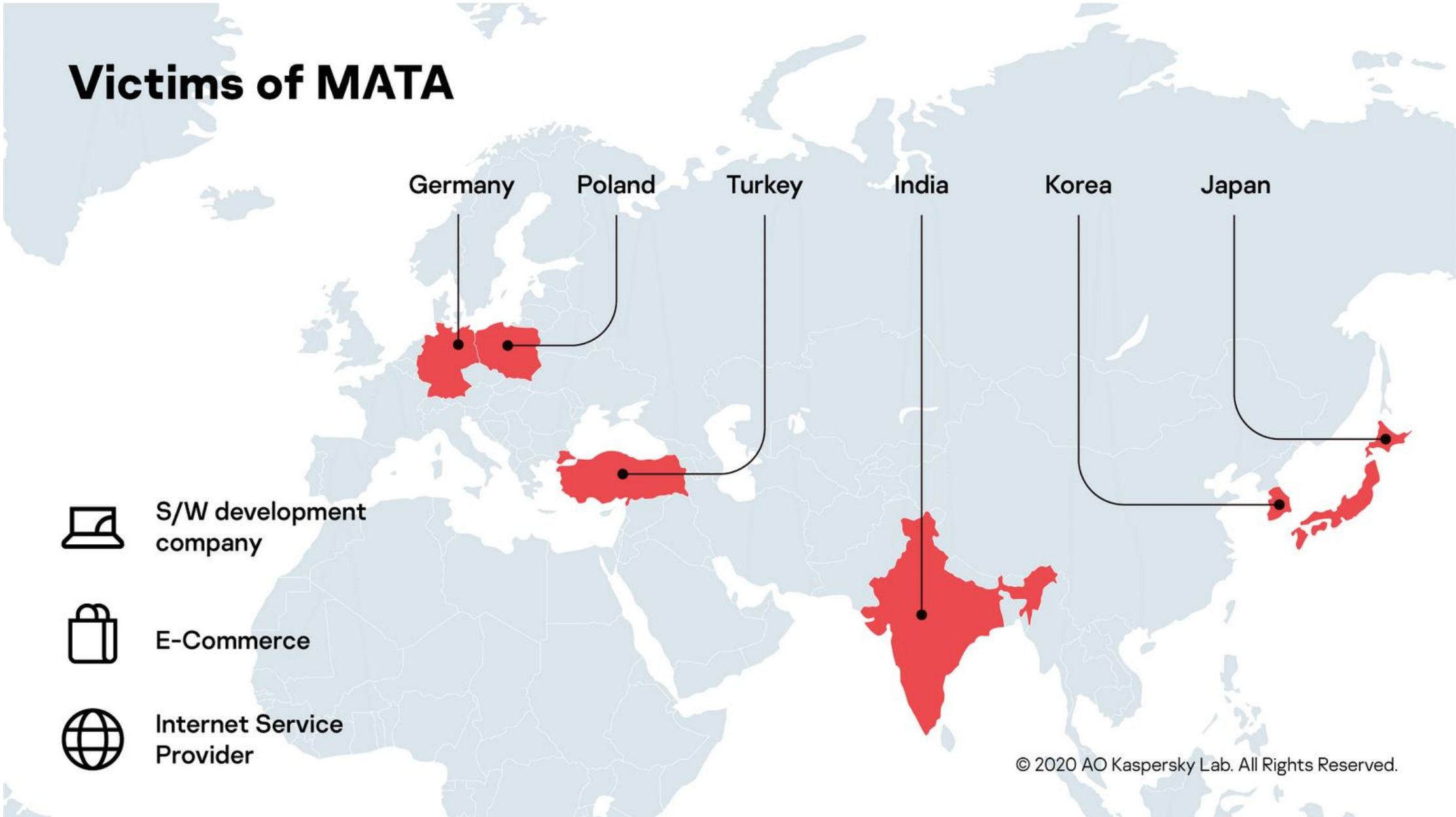
Ransomware functionality

Combination of AES-256 in ECB mode and RSA-2048.
Use Mersenne Twister as a source of randomness.

VHD Ransomware



Victims


Victims of MATA
Germany
Poland
Turkey
India
Korea
Japan
S/W development company
E-Commerce
Internet Service Provider
© 2020 AO Kaspersky Lab. All Rights Reserved.

Ambiguous Boundary

kaspersky

Common Cybercrime Attack

Spray-and-Pray, Fire-and-Forget

Common Targeted Attack

Well-prepared sophisticated attack

Targeted ransomware vs Cybercrime-like APT attack

Deployment
- Phishing
- Vulnerability exploitation

Installation
- Implant
- Evasion

Command-and-Control
- Execute command
- Move laterally

Destruction
- Encryption
- Locking

Extortion
- Publish data
- Blackmail

Deployment
- Phishing
- Vulnerability exploitation

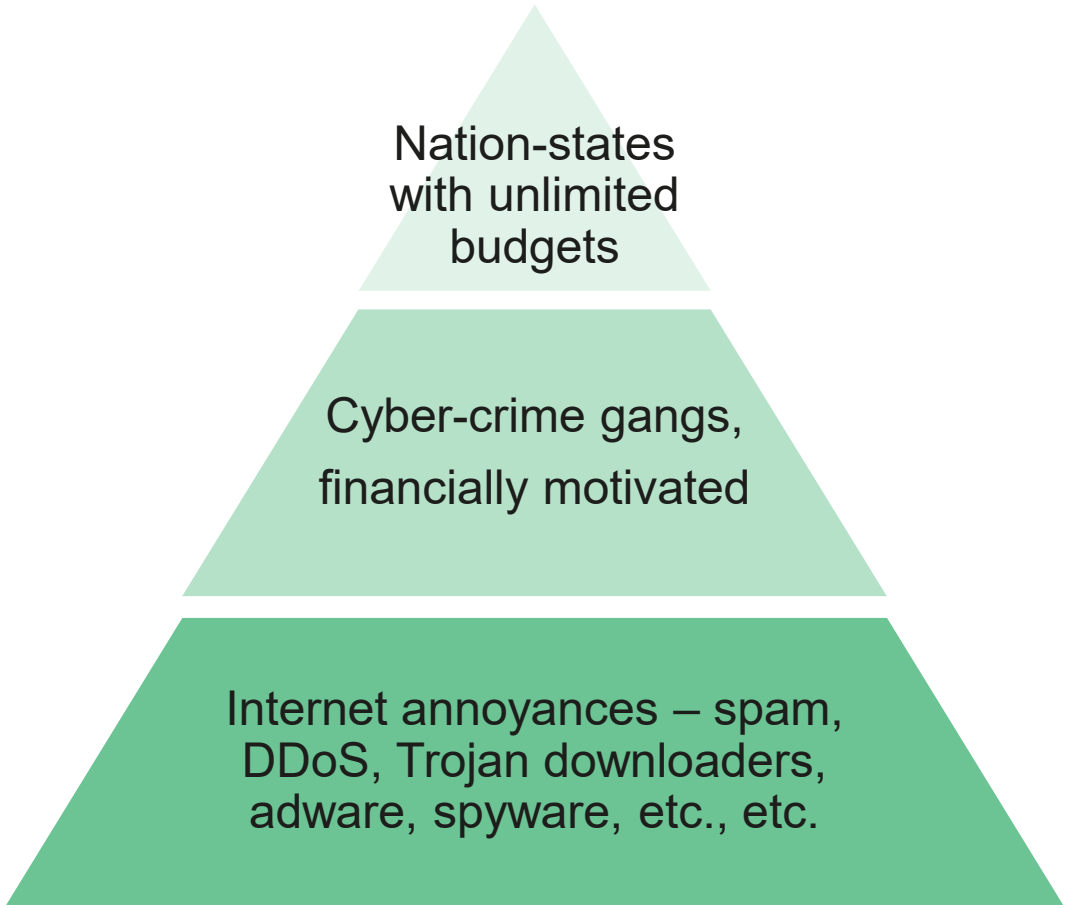
Installation
- Implant
- Evasion

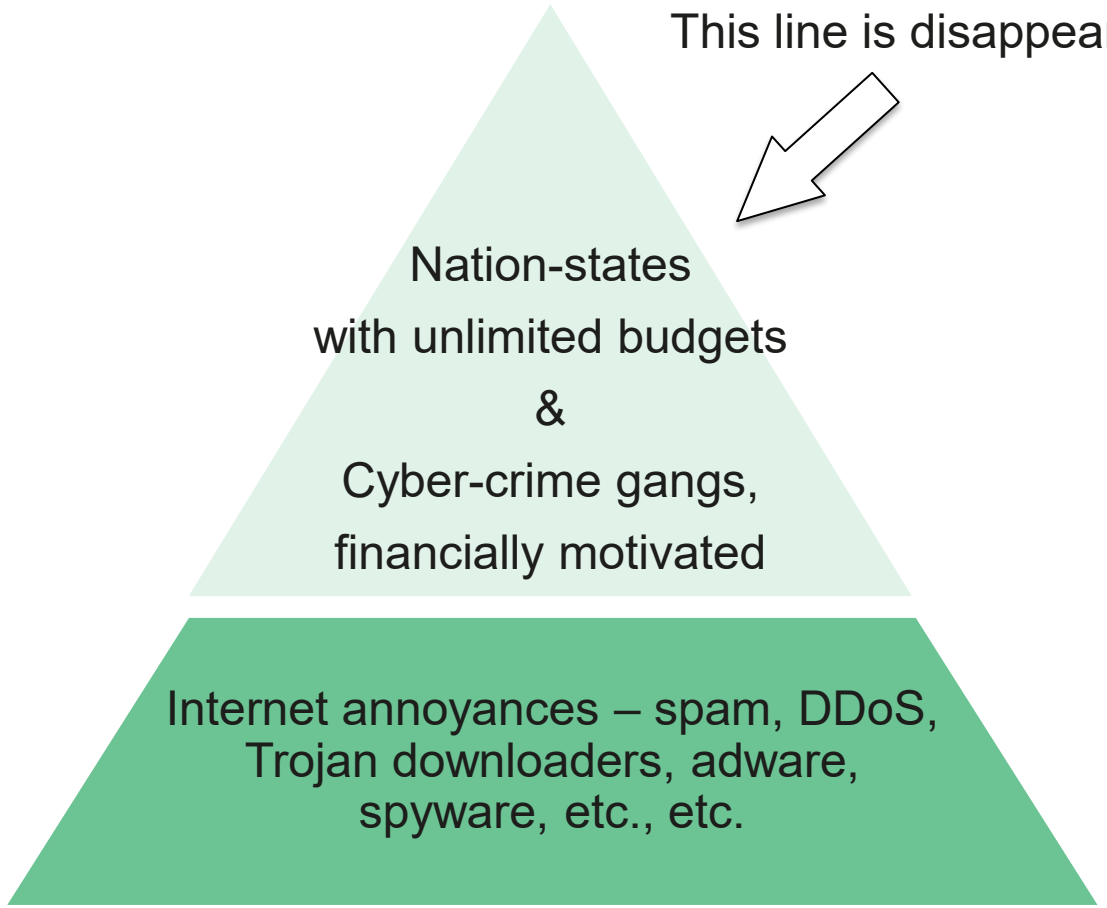
Command-and-Control
- Execute command
- Move laterally

Exfiltration
- Stolen data
- Locking

Leave silent
- Go next phase

Targeted ransomware vs Cybercrime-like APT attack





Conclusion

Risk of Network Device

Internet exposed network device is juicy entry point for threat actor. How can we monitor?

Multi-platform

Several campaings of Lazarus adopted macOS/linux attack. How can we respond?

APT-like cybercriminal

MATA is advanced well-made malware framework, but only for cybercrime-like attack?

THANK YOU

@unpacker

seongsu.park@kaspersky.com

kaspersky