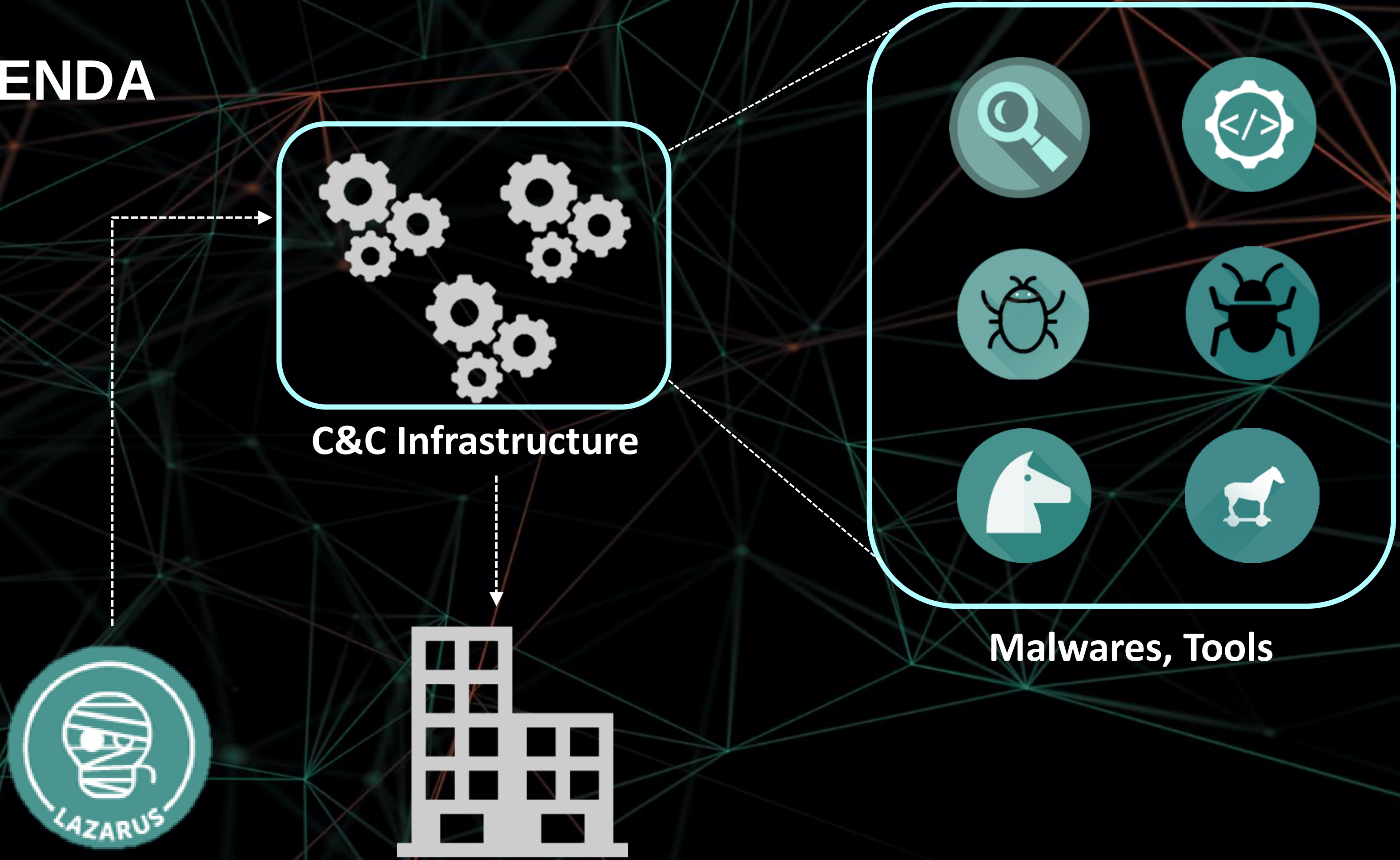
# Never Let Your Infrastructure Go Malicious: Digging Into C&C Infrastructure of Lazarus

*Seongsu Park*

*Senior Security Researcher*

# AGENDA



C&C Infrastructure

Malwares, Tools

Victim

# INTRODUCTION

## 2013

Dark Seoul – Attack on South Korean broadcaster and bank

## 2014

Sony Pictures hacking – Attacker leaked a release of confidential data from SPE and wipe hosts

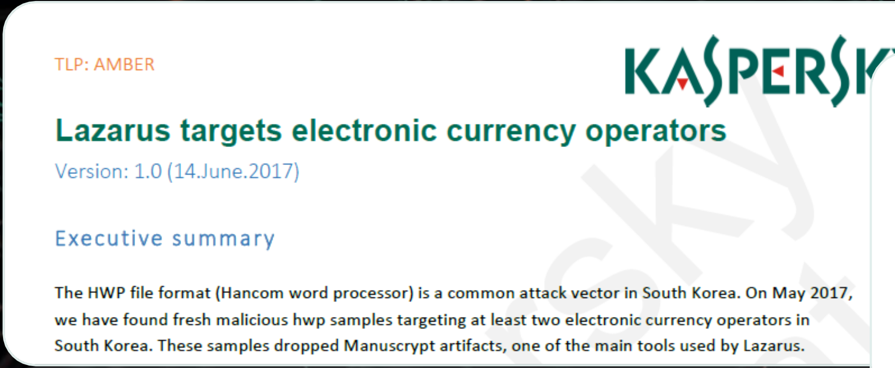
## 2016

Bangladesh bank heist – Attack on financial sector around world

## 2017

Wannacry – Ransomware spread quickly using by exploit

# RECENT ACTIVITY OF LAZARUS



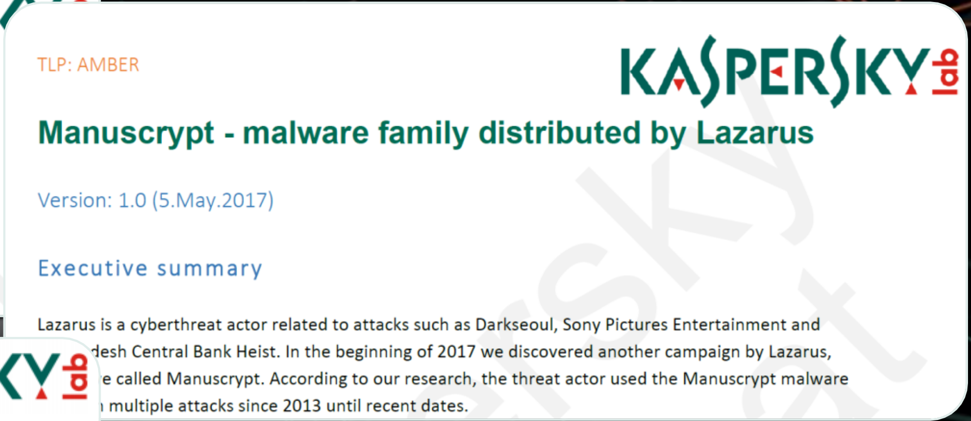
TLP: AMBER

## Lazarus targets electronic currency operators

Version: 1.0 (14.June.2017)

### Executive summary

The HWP file format (Hancom word processor) is a common attack vector in South Korea. On May 2017, we have found fresh malicious hwp samples targeting at least two electronic currency operators in South Korea. These samples dropped Manuscrypt artifacts, one of the main tools used by Lazarus.



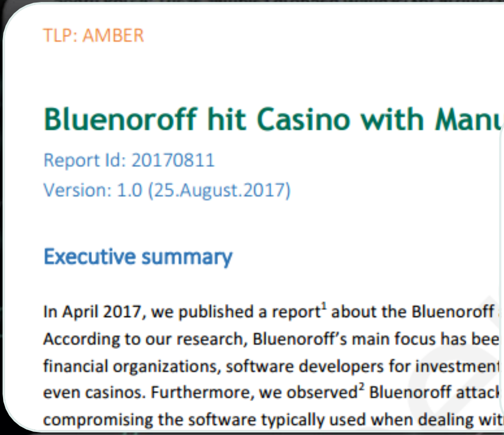
TLP: AMBER

## Manuscrypt - malware family distributed by Lazarus

Version: 1.0 (5.May.2017)

### Executive summary

Lazarus is a cyberthreat actor related to attacks such as Darkseoul, Sony Pictures Entertainment and desh Central Bank Heist. In the beginning of 2017 we discovered another campaign by Lazarus, e called Manuscrypt. According to our research, the threat actor used the Manuscrypt malware multiple attacks since 2013 until recent dates.



TLP: AMBER

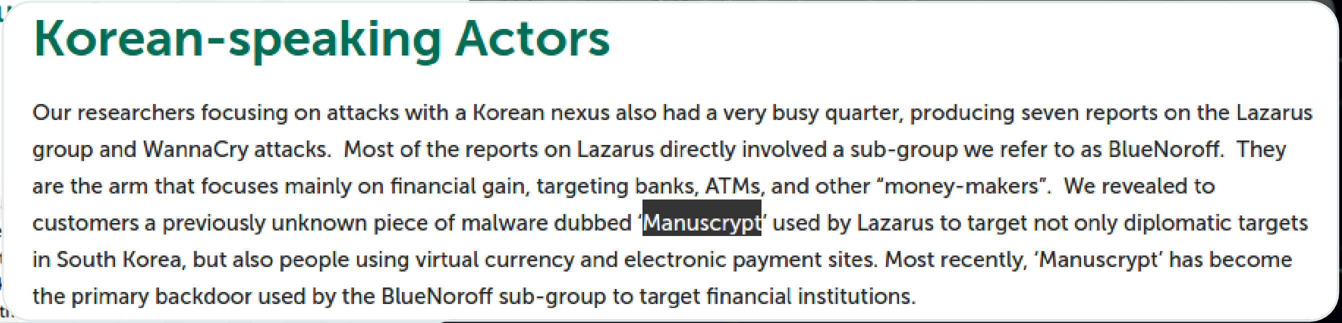
## Bluenoroff hit Casino with Manu

Report Id: 20170811

Version: 1.0 (25.August.2017)

### Executive summary

In April 2017, we published a report[1] about the Bluenoroff According to our research, Bluenoroff's main focus has bee financial organizations, software developers for investment even casinos. Furthermore, we observed[2] Bluenoroff attack compromising the software typically used when dealing with



## Korean-speaking Actors

Our researchers focusing on attacks with a Korean nexus also had a very busy quarter, producing seven reports on the Lazarus group and WannaCry attacks. Most of the reports on Lazarus directly involved a sub-group we refer to as BlueNoroff. They are the arm that focuses mainly on financial gain, targeting banks, ATMs, and other "money-makers". We revealed to customers a previously unknown piece of malware dubbed 'Manuscrypt' used by Lazarus to target not only diplomatic targets in South Korea, but also people using virtual currency and electronic payment sites. Most recently, 'Manuscrypt' has become the primary backdoor used by the BlueNoroff sub-group to target financial institutions.

# ABOUT MANUSCRYPT TOOLSET

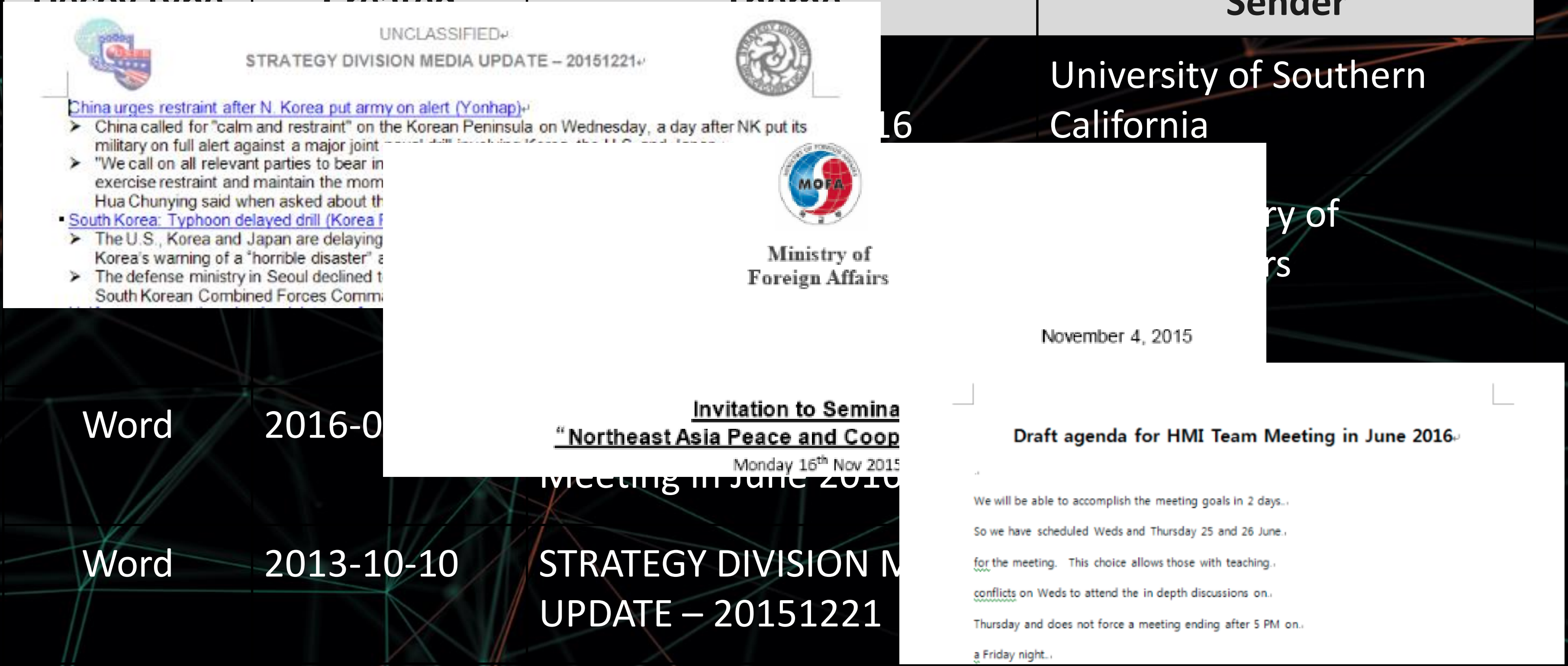
- **From when?**
  - Start to use Manuscrypt from around 2013
  - Use it actively until recent
- **Connection?**
  - Many overlap with known Lazarus code style and C&C infrastructure
- **Attack where?**
  - Usually attack national intelligence before
  - Usually use when they attack Korean financial sector

# ABOUT MANUSCRYPT

| Decoy type | Created | Theme | Sender |
|---|---|---|---|
| Word | 2016-05-13 | Reunion Weekend November 4 – 5, 2016 | University of Southern California |
| PDF | 2015-11-04 | Invitation to Seminar on "Northeast Asia Peace and Cooperation Initiative" | Korea Ministry of Foreign Affairs |
| Word | 2016-05-04 | Draft agenda for HMI Team Meeting in June 2016 | Stanford University |
| Word | 2013-10-10 | STRATEGY DIVISION MEDIA UPDATE – 20151221 | Strategy Division of United States Forces Korea |

# ABOUT MANUSCRYPT

| Decoy type | Created | Theme | Sender |
|---|---|---|---|
| | | 16 | University of Southern California |
| | | | ry of<br>rs |
| Word | 2016-0 | Meeting in June 2016 | |
| Word | 2013-10-10 | STRATEGY DIVISION M<br>UPDATE – 20151221 | |



UNCLASSIFIED

STRATEGY DIVISION MEDIA UPDATE – 20151221

China urges restraint after N. Korea put army on alert (Yonhap)

- ➢ China called for "calm and restraint" on the Korean Peninsula on Wednesday, a day after NK put its military on full alert against a major joint
- ➢ "We call on all relevant parties to bear in exercise restraint and maintain the mom Hua Chunying said when asked about th
- ▪ South Korea: Typhoon delayed drill (Korea
- ➢ The U.S., Korea and Japan are delaying Korea's warning of a "horrible disaster" a
- ➢ The defense ministry in Seoul declined t South Korean Combined Forces Comm

Ministry of Foreign Affairs

November 4, 2015

**Invitation to Semina**
**"Northeast Asia Peace and Coop**
Monday 16th Nov 2015

**Draft agenda for HMI Team Meeting in June 2016**

We will be able to accomplish the meeting goals in 2 days.

So we have scheduled Weds and Thursday 25 and 26 June.

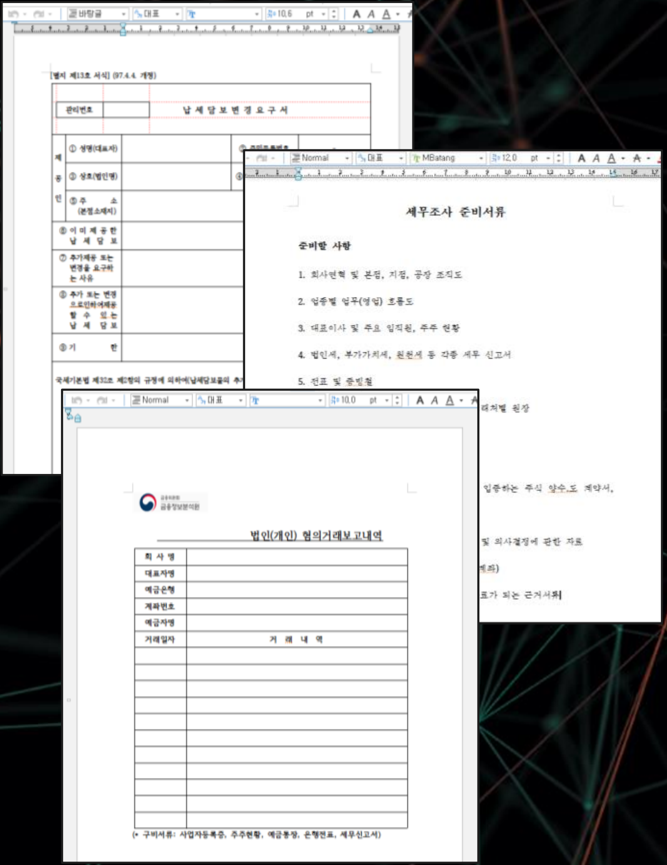
for the meeting. This choice allows those with teaching.

conflicts on Weds to attend the in depth discussions on.

Thursday and does not force a meeting ending after 5 PM on.

a Friday night.

# RECENT MANUSCRYPT ATTACK CASE



[별지 제13호 서식] (97.4.4. 개정)

| | | |
|---|---|---|
| 관리번호 | | 납 세 담 보 변 경 요 구 서 |
| 제공인 | ① 성명(대표자) | ② 주민등록번호 |
| | ③ 상호(법인명) | ④ |
| | ⑤ 주 소 (본점소재지) | |
| ⑥ 이미 제공한 납세담보 | | |
| ⑦ 추가제공 또는 변경을 요구하는 사유 | | |
| ⑧ 추가 또는 변경으로인하여제공할 수 있는 납세담보 | | |
| ⑨ 기 한 | | |

국세기본법 제32조 제2항의 규정에 의하여(납세담보물의 추

세무조사 준비서류

준비할 사항

1. 회사연혁 및 본점, 지점, 공장 조직도

2. 업종별 업무(영업) 흐름도

3. 대표이사 및 주요 임직원, 주주 현황

4. 법인세, 부가가치세, 원천세 등 각종 세무 신고서

5. 전표 및 증빙철

래처별 원장

입증하는 주식 양수도 계약서,

및 의사결정에 관한 자료

계좌)

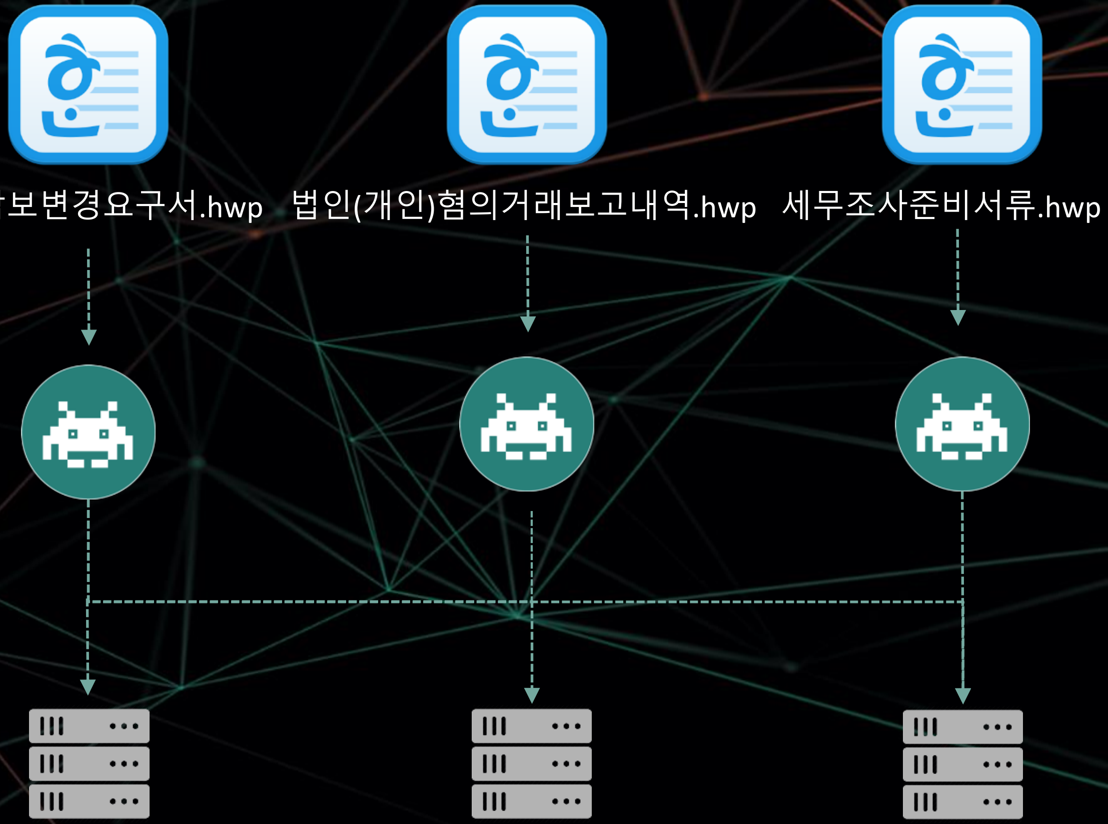
료가 되는 근거서류

금융위원회
금융정보분석원

법인(개인) 혐의거래보고내역

| | |
|---|---|
| 회 사 명 | |
| 대표자명 | |
| 예금은행 | |
| 계좌번호 | |
| 예금자명 | |
| 거래일자 | 거 래 내 역 |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

(• 구비서류: 사업자등록증, 주주현황, 예금통장, 은행전표, 세무신고서)

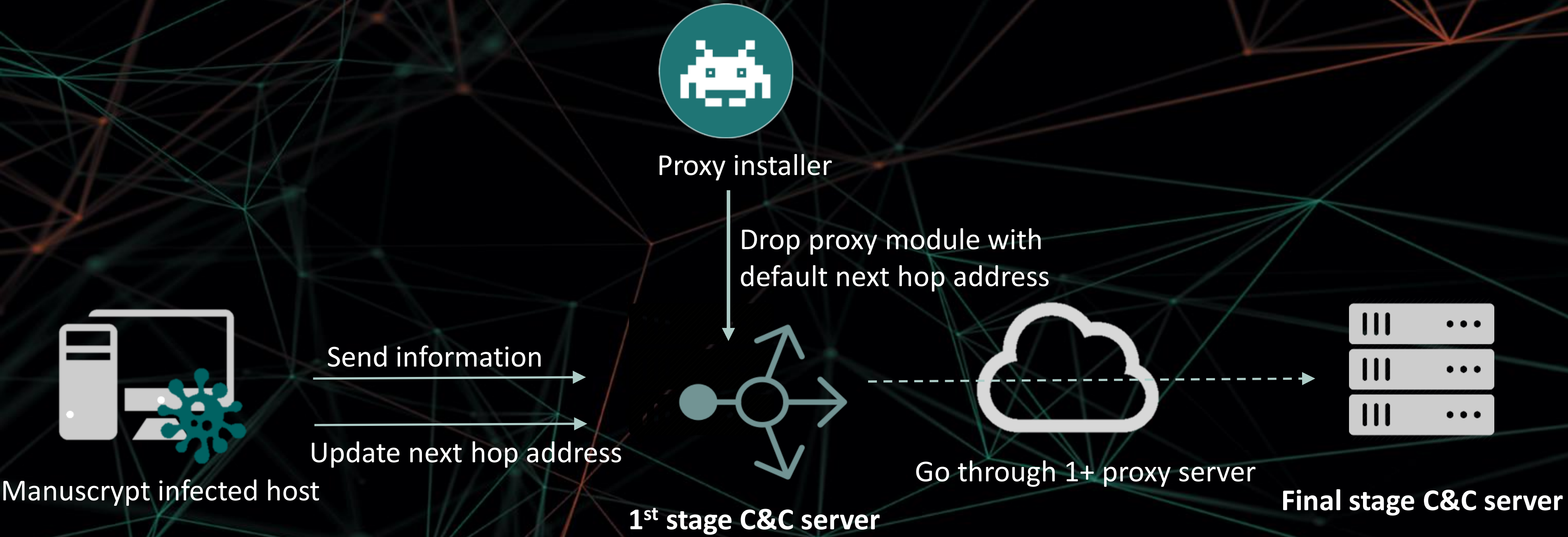


납세담보변경요구서.hwp

법인(개인)협의거래보고내역.hwp

세무조사준비서류.hwp

# MANUSCRYPT C2 INFRASTRUCTURE



Proxy installer

Drop proxy module with default next hop address

Send information

Update next hop address

Manuscrypt infected host

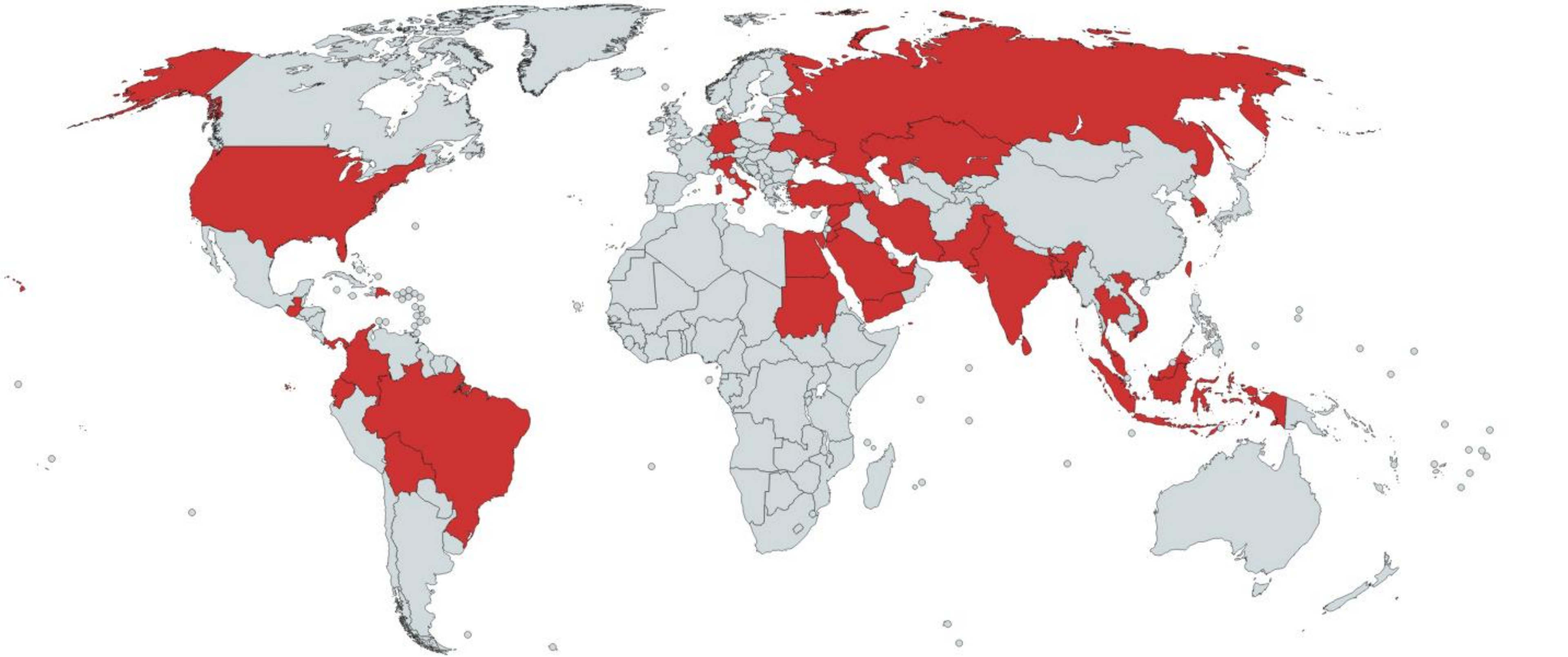
1st stage C&C server

Go through 1+ proxy server

**Final stage C&C server**

KASPERSKY lab

# C2 GEOLOCATION



# C2 GEOLOCATION - ASIA

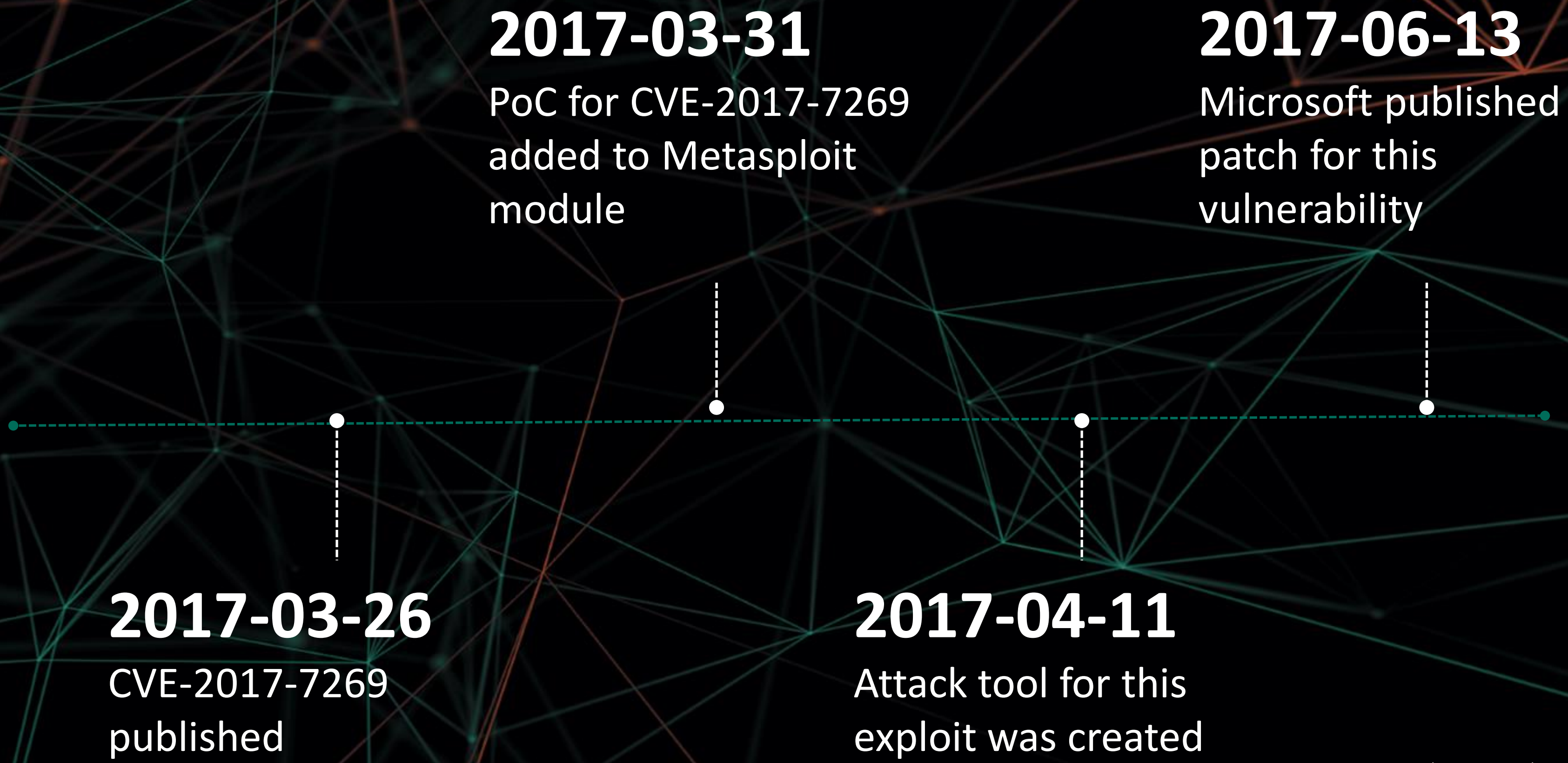
- Indonesia
- India
- Bangladesh
- Malaysia
- Vietnam
- Korea
- Taiwan
- Thailand

KASPERSKY lab

# VULNERABILITY INFORMATION

| IP | Web server ver | OS fingerprinting |
|---|---|---|
| 2xx.xx.xx.xxx | N/A | Windows Server 2003 R2 |
| 5x.xx.xx.xxx | IIS 6.0 | Aggressive OS guesses: Microsoft Windows Server 2003 (91%), Microsoft Windows Server 2003 SP2 (91%) |
| 2xx.xx.xx.xxx | IIS 6.0 | N/A |
| 1xx.xx.xx.xxx | IIS 6.0 | Aggressive OS guesses: Microsoft Windows 2003 R2 (93%), Microsoft Windows Server 2003 (93%), Microsoft Windows Server 2003 SP2 (93%) |
| 2xx.xx.xx.xxx | IIS 6.0 | Aggressive OS guesses: Microsoft Windows XP SP3 or Windows Server 2003 SP2 (97%), Microsoft Windows Server 2003 SP2 (94%), |
| 1xx.xx.xx.xxx | IIS 6.0 | Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (99%), Microsoft Windows XP SP3 or Windows Server 2003 SP2 (97%), Microsoft Windows Server 2003 SP2 (94%), |
| 2xx.xx.xx.xxx | IIS 6.0 | N/A |
| 2xx.xx.xx.xxx | IIS 6.0 | Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (89%) |
| 5x.xx.xx.xxx | N/A | Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows Server 2003 SP1 - SP2 (92%) |

# VULNERABILITY INFORMATION



**2017-03-26**

CVE-2017-7269
published

**2017-03-31**

PoC for CVE-2017-7269
added to Metasploit
module

**2017-04-11**

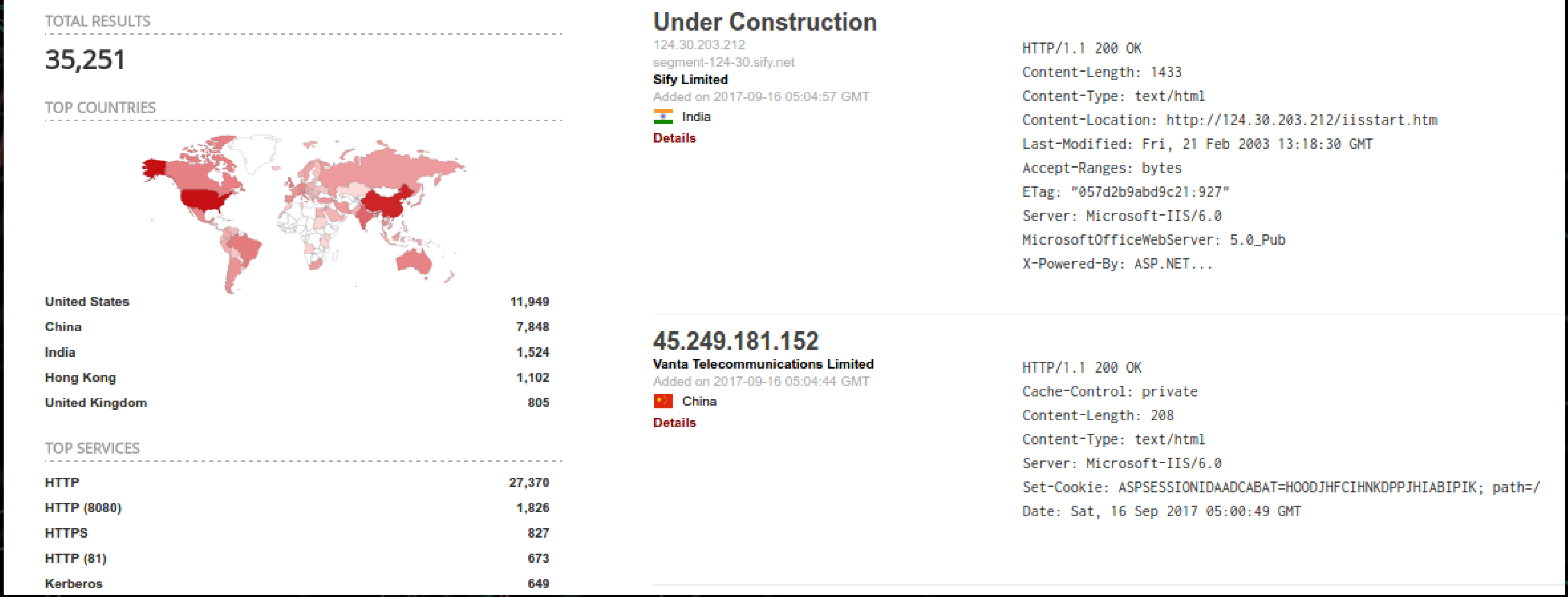
Attack tool for this
exploit was created

**2017-06-13**

Microsoft published
patch for this
vulnerability

# VULNERABILITY INFORMATION

- **Vulnerable host with CVE-2017-7269**



TOTAL RESULTS

35,251

TOP COUNTRIES

| | |
|---|---|
| United States | 11,949 |
| China | 7,848 |
| India | 1,524 |
| Hong Kong | 1,102 |
| United Kingdom | 805 |

TOP SERVICES

| | |
|---|---|
| HTTP | 27,370 |
| HTTP (8080) | 1,826 |
| HTTPS | 827 |
| HTTP (81) | 673 |
| Kerberos | 649 |

**Under Construction**

124.30.203.212
segment-124-30.sify.net
**Sify Limited**
Added on 2017-09-16 05:04:57 GMT
India
Details

```
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://124.30.203.212/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 13:18:30 GMT
Accept-Ranges: bytes
ETag: "057d2b9abd9c21:927"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET...
```

**45.249.181.152**

**Vanta Telecommunications Limited**
Added on 2017-09-16 05:04:44 GMT
China
Details

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 208
Content-Type: text/html
Server: Microsoft-IIS/6.0
Set-Cookie: ASPSESSIONIDAADCABAT=HOODJHFCIHNKDPPJHIABIPIK; path=/
Date: Sat, 16 Sep 2017 05:00:49 GMT
```

Source : Shodan

# MALWARES/TOOLS FROM C&C SERVER

**Backdoor Variants**

Threat actor use many kind of backdoors - Active backdoor, Passive backdoor, HTTP backdoor, IIS backdoor

**Proxy Malware**

Main component of multi stage of proxy structure, forward incoming traffic to other host

**Information Harvester**

TCP connection harvester to steal inbound/outbound network connections

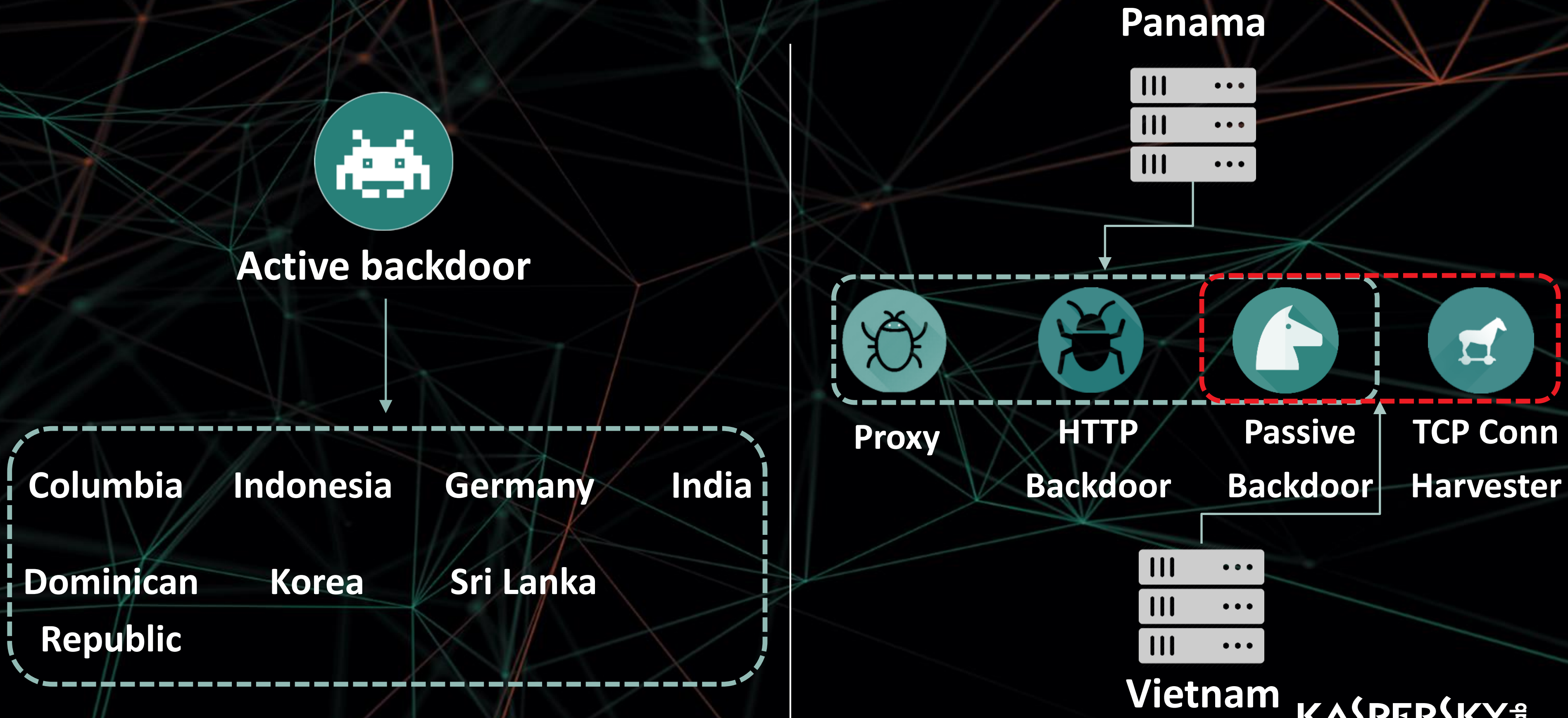
**Other Tools**

Loader to decrypt and execute encrypted payload, File wiper to wipe out specific file securely

# MALWARES/TOOLS FROM C&C SERVER

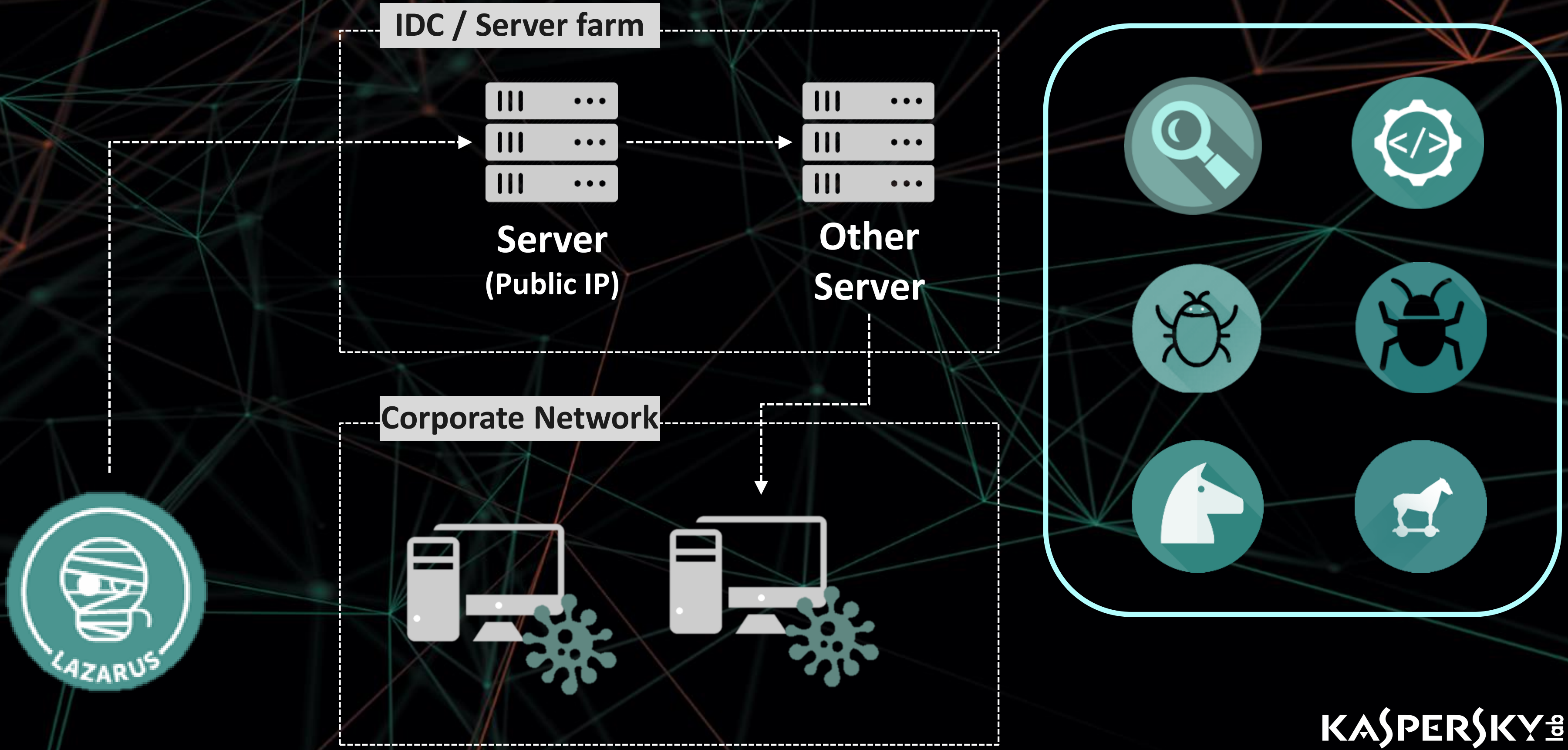
| | Active Backdoor | Passive Backdoor | Proxy | TCP conn Harvester | IIS Backdoor | HTTP Backdoor |
|---|---|---|---|---|---|---|
| Indonesia | ○ | | | | | |
| India | ○ | ○ | ○ | | ○ | ○ |
| Malaysia | | | | | | ○ |
| Bangladesh | | | | | | ○ |
| Vietnam | | ○ | | ○ | | ○ |
| Korea | ○ | ○ | ○ | | | ○ |
| Thailand | | | | ○ | | |
| Taiwan | | | | ○ | | |

# MALWARES/TOOLS FROM C&C SERVER



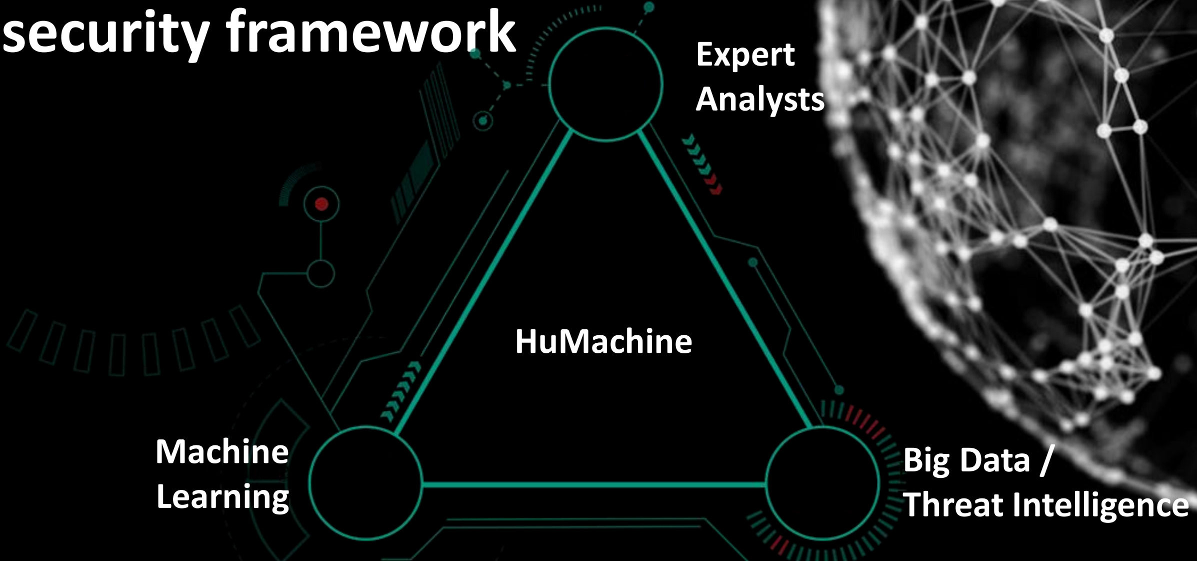
KASPERSKY lab

# HOW THREAT ACTOR USED THIS TOOLS



# CONCLUSION

- Identify your IT infrastructure accurately
- Check vulnerable host
- Protect your valuable hosts with adaptive security framework



Expert Analysts

HuMachine

Machine Learning

Big Data / Threat Intelligence

# LET'S TALK?