



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

Seongsu Park

Senior Security Researcher

INTRODUCTION

whoami

- Name : Seongsu Park
- GReAT Senior Security Researcher
- Threat intelligence analyst, Cyber threat hunter

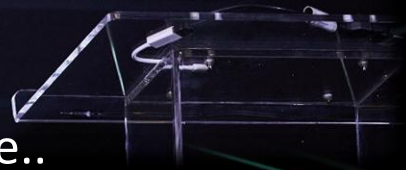
history

- Worked as Malware Researcher and Incident Responder
- Malware Researching, Incident Response, Threat Intelligence..



Kaspersky®

SECURITY
ANALYST
SUMMIT



AGENDA



C&C Infrastructure



Malwares, Tools



Victim

INTRODUCTION



2014

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

2017

Wannacry –
Ransomware spread
quickly using by exploit

2013

Dark Seoul – Attack on
South Korean
broadcaster and bank

2016

Bangladesh bank heist –
Attack on financial
sector around world

RECENT ACTIVITY OF LAZARUS

TLP: AMBER



Lazarus targets electronic currency operators

Version: 1.0 (14.June.2017)

TLP: AMBER



Manuscript - malware family distributed by Lazarus

Manuscript – Tool set of Bluenoroff

Version: 1.0 (23.November.2017)

Executive summary

In April 2017, we published a report¹ about the Bluenoroff. According to our research, Bluenoroff's main focus has been financial organizations, software developers for investment even casinos. Furthermore, we observed² Bluenoroff attack compromising the software typically used when dealing with

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 'Manuscript' used by Lazarus to target not only diplomatic targets in South Korea, but also people using virtual currency and electronic payment sites. Most recently, 'Manuscript' has become the primary backdoor used by the BlueNoroff sub-group to target financial institutions.



ABOUT MANUSCRIPT TOOLSET

- **From when?**

- Start to use Manuscript 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 MANUSCRIPT

Decoy type	Created	Theme	Sender
------------	---------	-------	--------

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 moratorium on nuclear tests," Hua Chunying said when asked about the

▪ [South Korea: Typhoon delayed drill \(Korea I...\)](#)

- The U.S., Korea and Japan are delaying the start of a joint military exercise after South Korea's warning of a "horrible disaster" and
- The defense ministry in Seoul declined to comment on the



Ministry of Foreign Affairs

16
University of Southern California

ry of
rs
November 4, 2015

Word 2016-0

Invitation to Semina
"Northeast Asia Peace and Coop
Monday 16th Nov 2015
meeting in June 2016

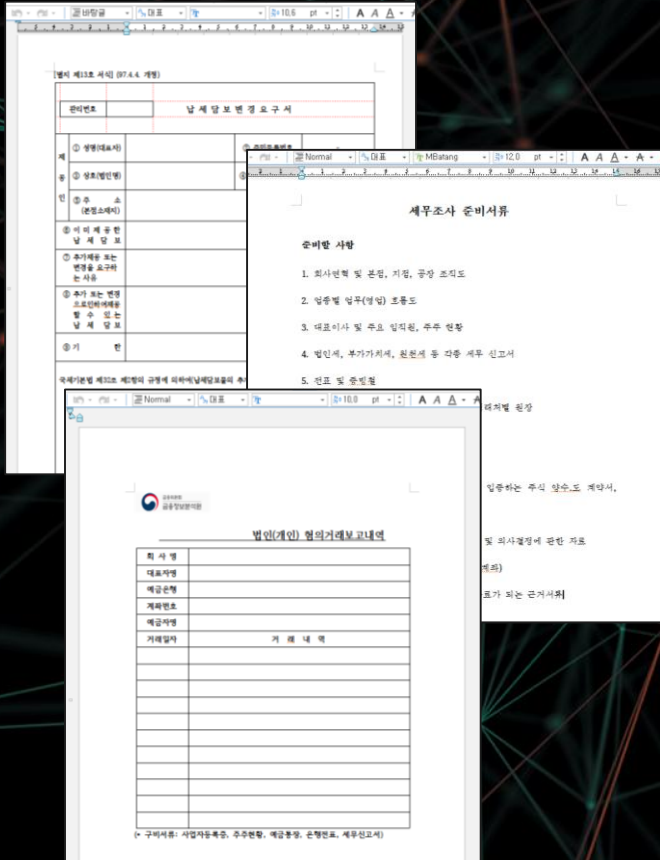
Draft agenda for HMI Team Meeting in June 2016+

Word 2013-10-10

STRATEGY DIVISION M
UPDATE – 20151221

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 MANUSCRIPT ATTACK CASE



납세담보변경요구서.hwp



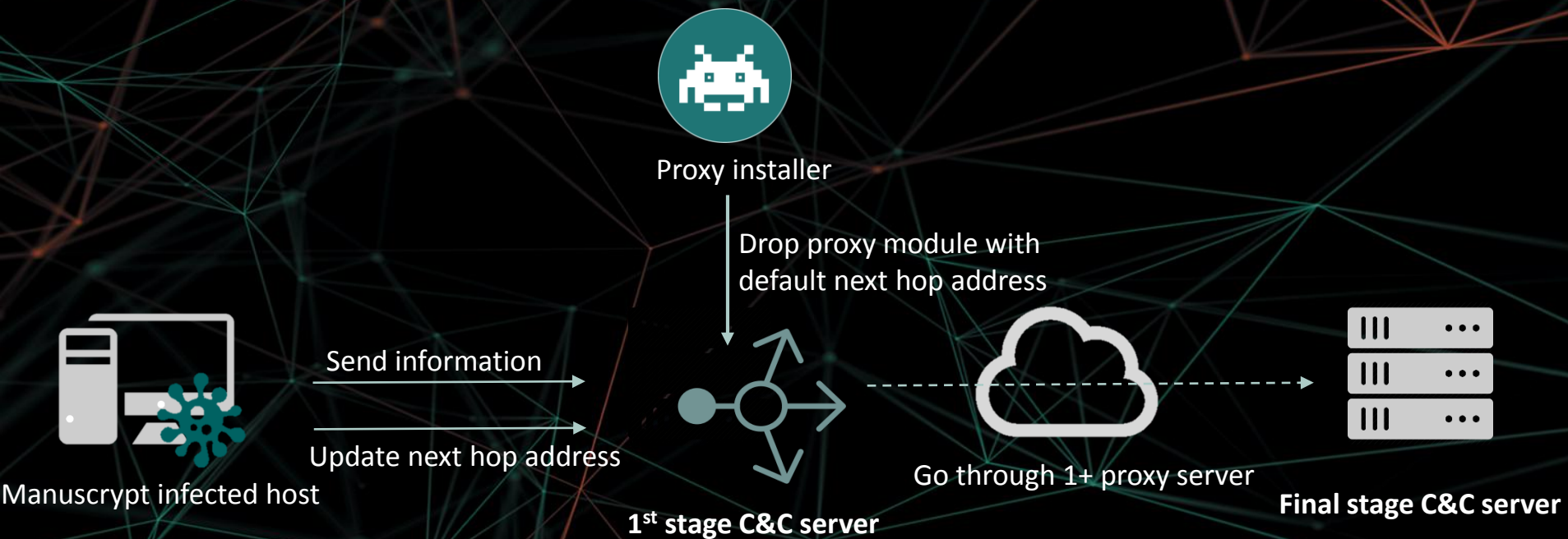
법인(개인)혐의거래보고내역.hwp



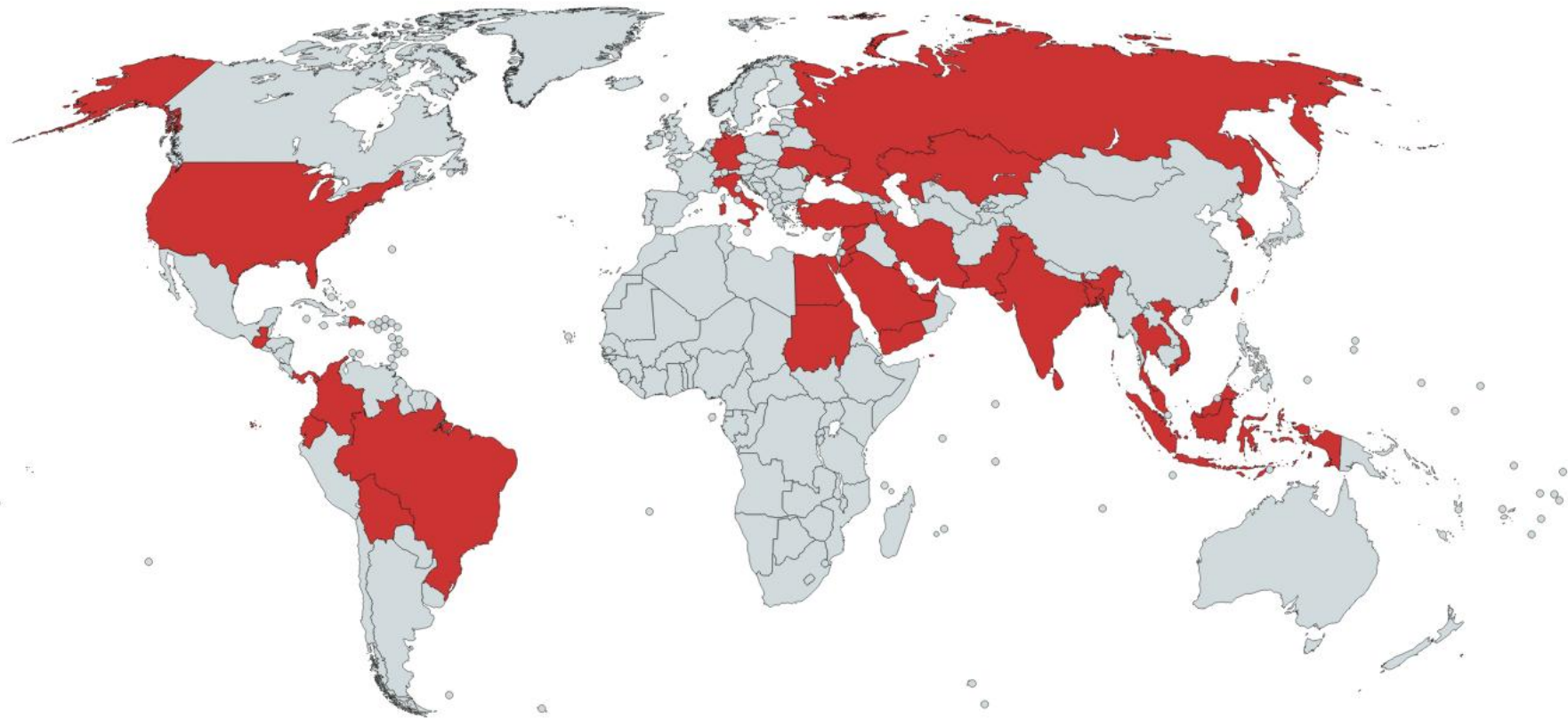
세무조사준비서류.hwp



MANUSCRIPT C2 INFRASTRUCTURE



C2 GEOLOCATION



C2 GEOLOCATION - ASIA

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



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

2017-03-31

PoC for CVE-2017-7269
added to Metasploit
module

2017-06-13

Microsoft published
patch for this
vulnerability

2017-03-26

CVE-2017-7269
published

2017-04-11

Attack tool for this
exploit was created

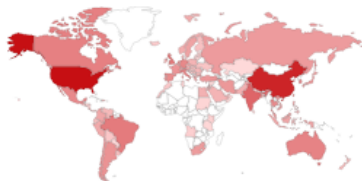
VULNERABILITY INFORMATION

- 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=HOODJHFCIHNKDPJHIABIPIK; path=/
Date: Sat, 16 Sep 2017 05:00:49 GMT
```

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

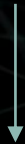
MALWARES/TOOLS FROM C&C SERVER

	Active Backdoor	Passive Backdoor	Proxy	TCP conn Harvester	IIS Backdoor	HTTP Backdoor
Indonesia	<input type="radio"/>					
India	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>
Malaysia						<input type="radio"/>
Bangladesh						<input type="radio"/>
Vietnam		<input type="radio"/>		<input type="radio"/>		<input type="radio"/>
Korea	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>			<input type="radio"/>
Thailand				<input type="radio"/>		
Taiwan				<input type="radio"/>		

MALWARES/TOOLS FROM C&C SERVER



Active backdoor



Columbia Indonesia Germany India
Dominican Republic Korea Sri Lanka

Panama



Proxy

HTTP
Backdoor

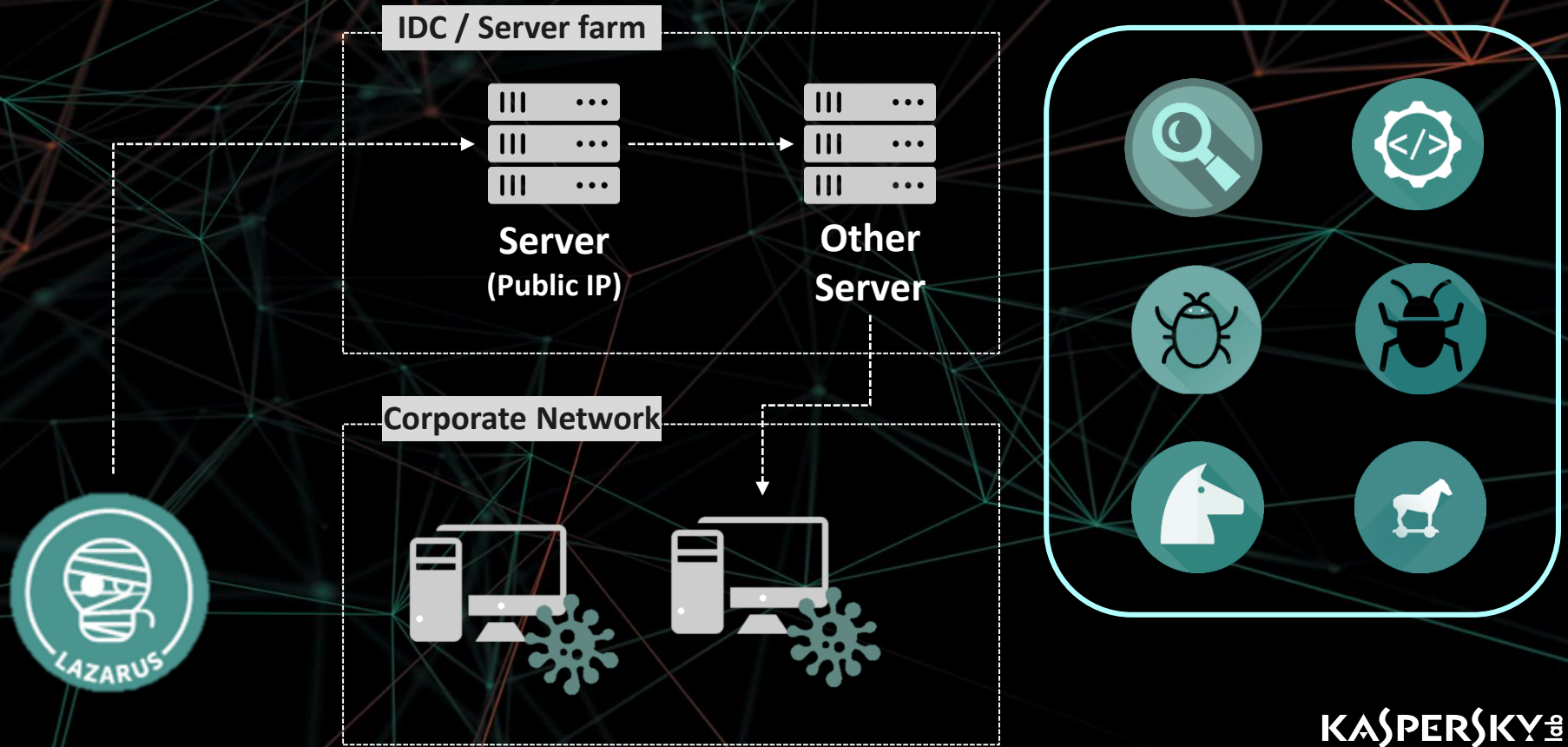
Passive
Backdoor

TCP Conn
Harvester



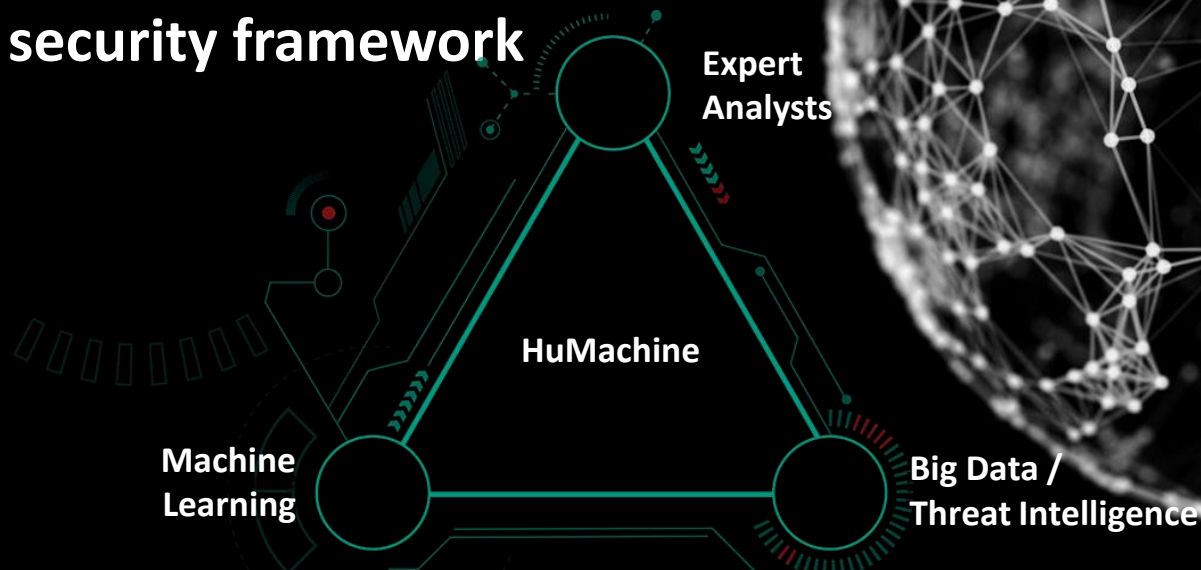
Vietnam

HOW THREAT ACTOR USED THIS TOOLS



CONCLUSION

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



A digital illustration of a globe with a network overlay. The globe is shown from a low angle, with the horizon line visible. The network consists of numerous glowing nodes in shades of cyan and orange, connected by thin lines. The background is dark, with a gradient from black to a deep blue. The text 'LET'S TALK?' is centered in a white speech bubble.

LET'S TALK?