A Decade-long Landscape of Advanced Persistent Threats: Longitudinal Analysis and Global Trends

Shakhzod Yuldoshkhujaev
Sungkyunkwan University
shakzod02@g.skku.edu

Mijin Jeon
Sungkyunkwan University
jinijxxn@g.skku.edu

Doowon Kim
University of Tennessee
doowon@utk.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

Hyungjoon Koo
Sungkyunkwan University
kevin.koo@skku.edu

Introduction

Advanced Persistent Threats Overview

✓ **Advanced Persistent Threats (APTs)**

- Sustained, targeted, and highly sophisticated attacks
- Motives: political, economic, and military

	Traditional Attacks	APT Attacks
Attacker	Individuals	Highly organized group
Target	Unspecified, mostly individual	Specific entities, organizations
Purpose	Financial benefits, demonstrating abilities	Competitive advantages, strategic benefits
Approach	Short-term, “smash & grab”	Long-term, stealthy

A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities.
IEEE Communications Surveys & Tutorials, 2019

Existing APT Documentation

✓ **Plethora of publicly available APT dossiers**

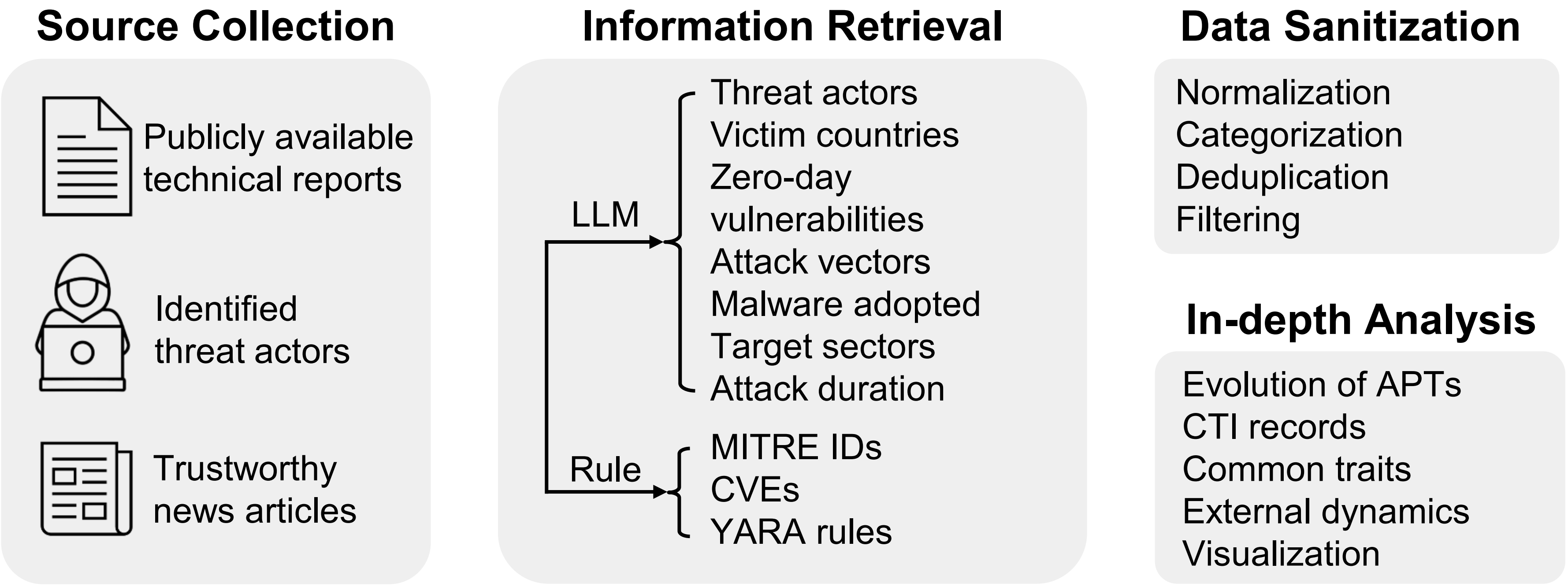
- BUT! Limited research on longitudinal APT analysis
- Previous works → *microscopic focus*

This Work

- ✓ **Decade-long analysis** of APT incidents (2014 - 2023) → *macroscopic focus*
- ✓ Analyze existing dossiers to understand
  - Evolution of APT campaigns
  - Trends in Cyber Threat Intelligence (CTI) records
  - Common traits of APTs
  - Influence of external factors
- ✓ **Method:** Hybrid (rule-based extraction + LLM)

Methodology

Methodology Overview



Source Collection

- Publicly available technical reports
- Identified threat actors
- Trustworthy news articles

Information Retrieval

LLM

- Threat actors
- Victim countries
- Zero-day vulnerabilities
- Attack vectors
- Malware adopted
- Target sectors
- Attack duration

Rule

- MITRE IDs
- CVEs
- YARA rules

Data Sanitization

- Normalization
- Categorization
- Deduplication
- Filtering

In-depth Analysis

- Evolution of APTs
- CTI records
- Common traits
- External dynamics
- Visualization

Source Collection

✓ **Technical reports (TRs)**

- Combined from three sources
- 2,563 reports on APT campaigns (2014 - 2023)

Source Collection

✓ **Technical reports (TRs)**

- Combined from three sources
- 2,563 reports on APT campaigns (2014 - 2023)

✓ **Threat actors (TAs)**

- No APT group information in TRs
- Combined from three sources
- 1,684 APT groups with metadata

Source Collection

✓ **Technical reports (TRs)**

- Combined from three sources
- 2,563 reports on APT campaigns (2014 - 2023)

✓ **Threat actors (TAs)**

- No APT group information in TRs
- Combined from three sources
- 1,684 APT groups with metadata

✓ **News articles**

- News articles and media reports
- 177 articles on APT campaigns

Information Retrieval

✓ **LLM-based approach**

- Evaluated three LLMs against ground truth
- Ground truth: manually inspected answers (around 10% of TRs collection)
- Selected GPT-4-Turbo for best performance (F1 score: 0.90)

Information Retrieval

✓ **LLM-based approach**

- Evaluated three LLMs against ground truth
- Ground truth: manually inspected answers (around 10% of TRs collection)
- Selected GPT-4-Turbo for best performance (F1 score: 0.90)

✓ **Rule-based approach**

- Chose IoCParser
- Outperformed GPT-4-Turbo in extracting IoCs

Information Retrieval

✓ **LLM-based approach**

- Evaluated three LLMs against ground truth
- Ground truth: manually inspected answers (around 10% of TRs collection)
- Selected GPT-4-Turbo for best performance (F1 score: 0.90)

✓ **Rule-based approach**

- Chose IoCParser
- Outperformed GPT-4-Turbo in extracting IoCs

✓ **Manual inspection**

- Verified the attack duration from LLM outputs
- Helps estimate the lifecycle of APTs

Information Retrieval

✓ **LLM-based approach**

- Evaluated three LLMs against ground truth
- Ground truth: manually inspected answers
- Selected GPT-4-Turbo for best performance

✓ **Rule-based approach**

- Chose IoCParser
- Outperformed GPT-4-Turbo in extracting IoCs

✓ **Manual inspection**

- Verified the attack duration from LLM outputs
- Helps estimate the lifecycle of APTs

Search Item	Retrieval Approach	# of TRs	Ratio
CVE	Rule	416	27.6%
MITRE ID	Rule	175	11.6%
YARA	Rule	131	8.7%
Threat actor	LLM	1,089	72.2%
Victim country	LLM	886	58.7%
Zero-day	LLM	839	55.6%
Attack vector	LLM	1,186	78.6%
Malware	LLM	1,287	85.3%
Target sector	LLM	1,228	81.4%
Attack duration	LLM	235	15.6%

Refining Responses

✓ **Normalization:** Victim country names → two-letter country code

✓ **Categorization:** Attack vectors and target sectors → 12 groups each

✓ **Deduplication:** Removed duplicates

- TR collection: 2,563 → 1,509
- TA collection: 1,684 → 884

✓ **Filtering:** Excluded TAs with insufficient metadata (884 → 603)

Decadal Landscape of APT Campaigns

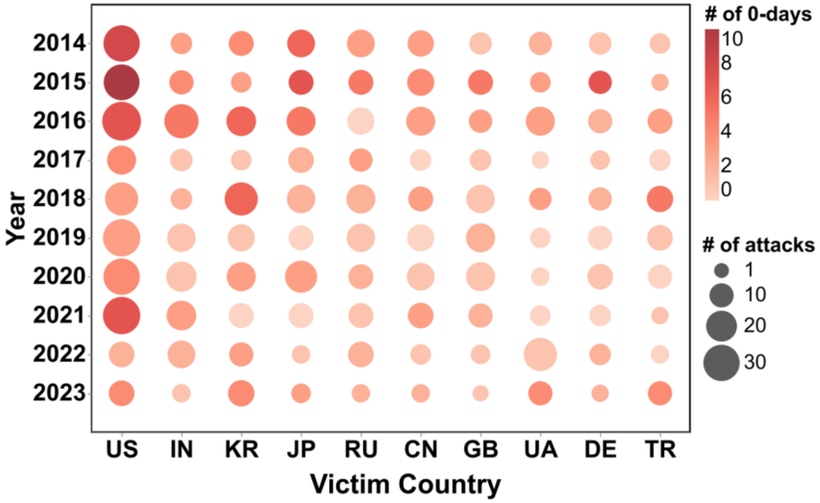
Research Questions

- ✓ **RQ1: Evolution of APTs over a decade**
- ✓ **RQ2: Cyber Threat Intelligence records for APTs**
- ✓ **RQ3: Common traits of APTs**
- ✓ **RQ4: External dynamics affecting APTs**

RQ1: Evolution of APTs Over a Decade

✓ **Victim countries:**

- 154 out of 195 countries were victimized
- Top 10: 43% of all incidents



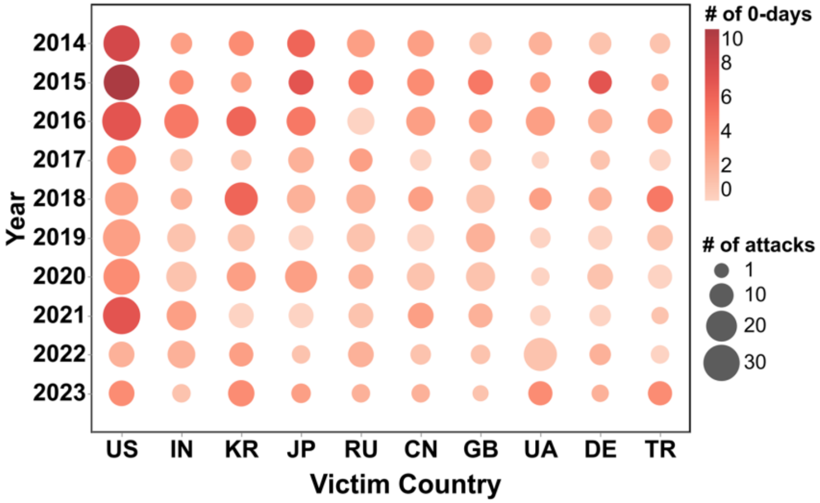
RQ1: Evolution of APTs Over a Decade

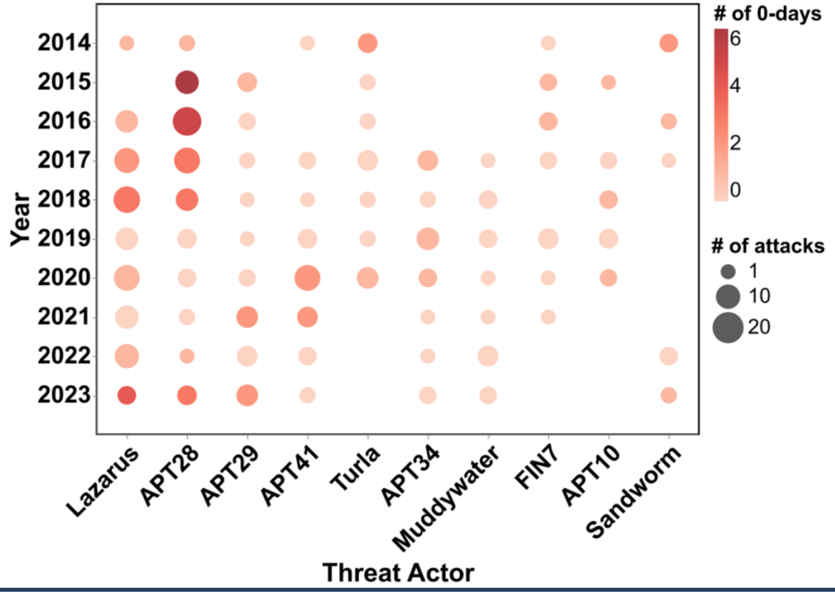
✓ **Victim countries:**

- 154 out of 195 countries were victimized
- Top 10: 43% of all incidents

✓ **Threat actors:**

- 446 groups were identified
- Top 10: 21.6% of all incidents





SecAI Lab

SUNG KYUN KWAN UNIVERSITY(SKKU)

RQ1: Evolution of APTs Over a Decade

✓ **Victim countries:**

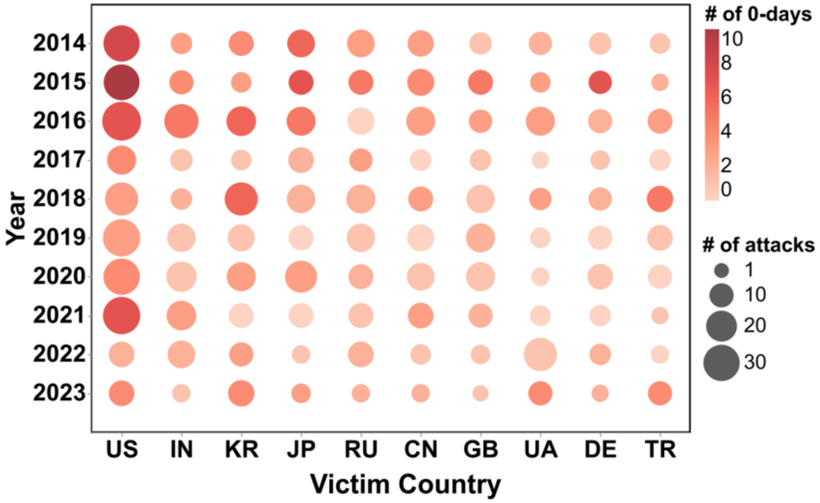
- 154 out of 195 countries were victimized
- Top 10: 43% of all incidents

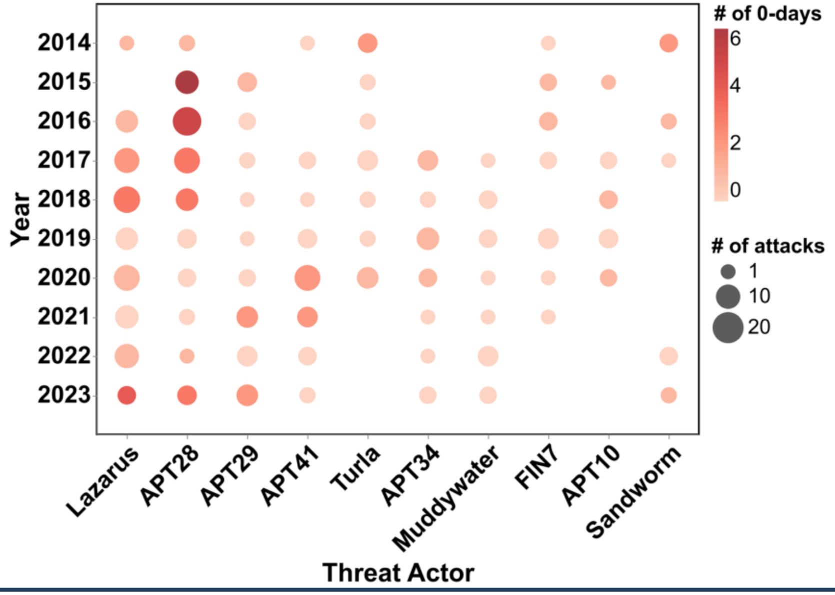
✓ **Threat actors:**

- 446 groups were identified
- Top 10: 21.6% of all incidents

✓ **Zero-day usage:**

- General downward trend from 2016 (lighter red)
- Usage of one-day vulnerabilities increased





SecAI Lab SUNG KYUN KWAN UNIVERSITY(SKKU)

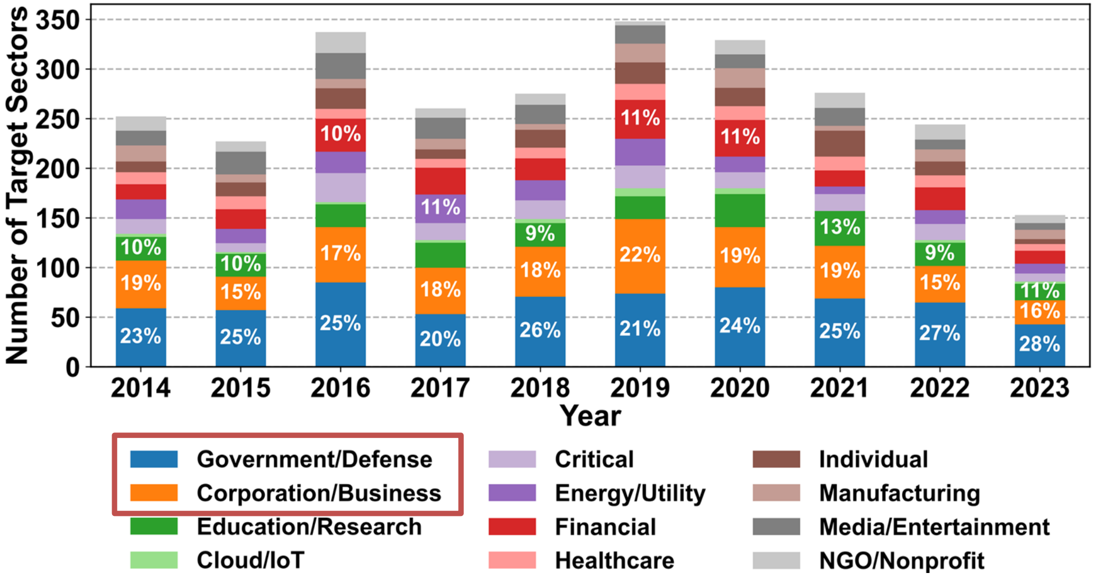
RQ1: Evolution of APTs Over a Decade

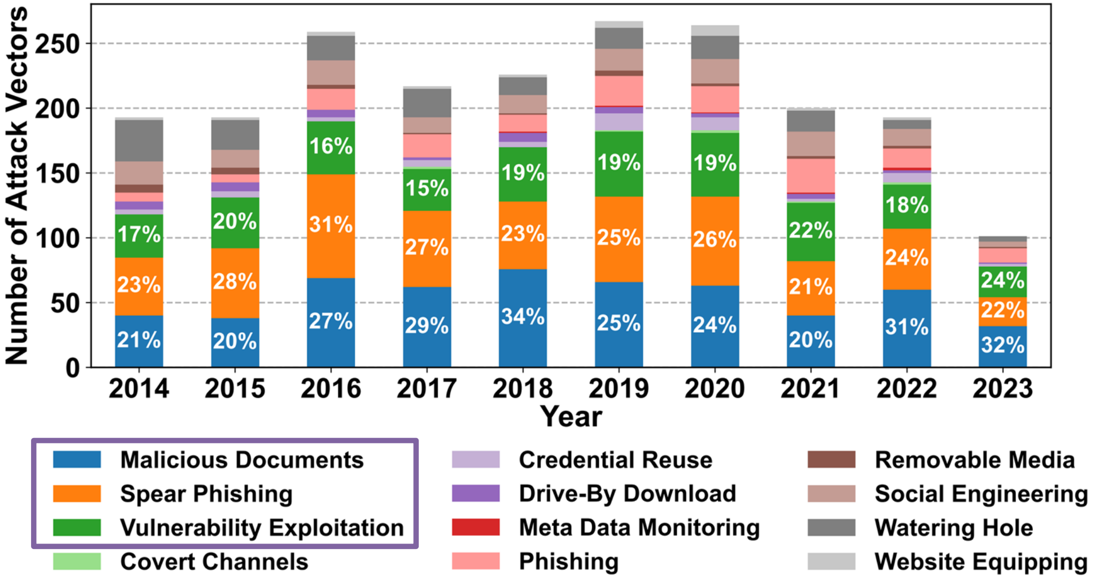
✓ **Target Sectors**

- Consistent targets: □

✓ **Initial Attack Vectors**

- Consistent vectors: □

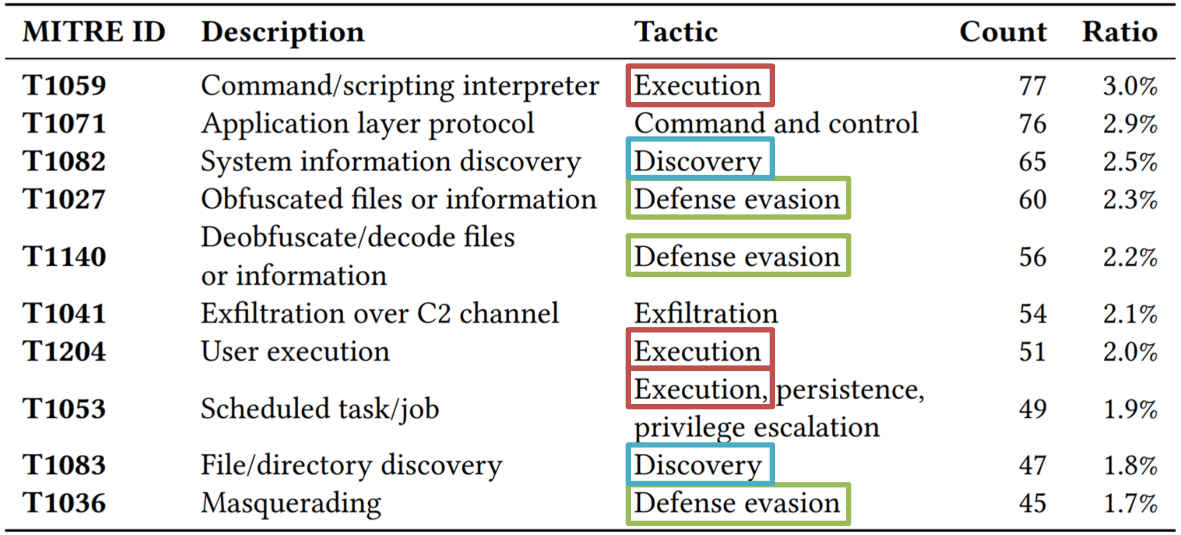




RQ2: CTI Records in APT Campaigns

✓ **MITRE IDs:** Total 2,582 extracted *(263 unique)*

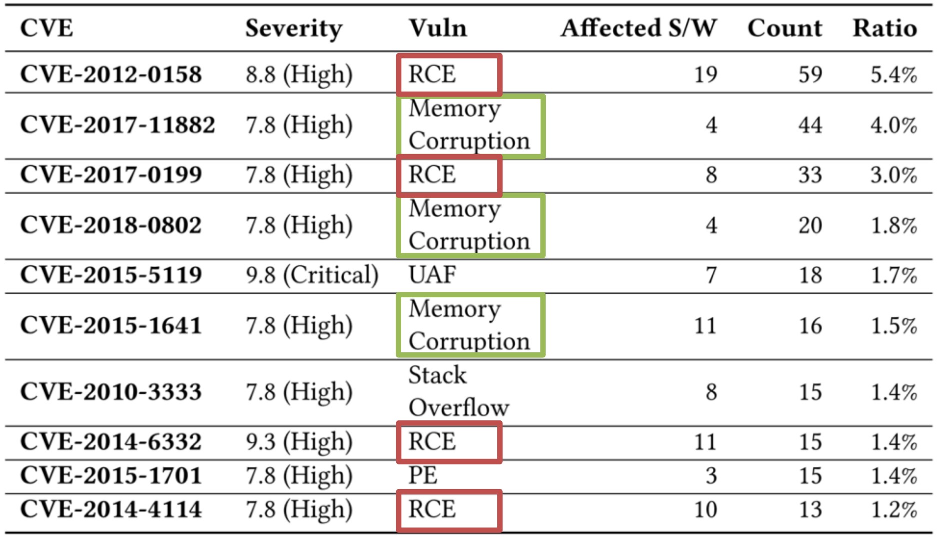
- Top tactics: execution, defense evasion, discovery



MITRE ID	Description	Tactic	Count	Ratio
T1059	Command/scripting interpreter	Execution	77	3.0%
T1071	Application layer protocol	Command and control	76	2.9%
T1082	System information discovery	Discovery	65	2.5%
T1027	Obfuscated files or information	Defense evasion	60	2.3%
T1140	Deobfuscate/decode files or information	Defense evasion	56	2.2%
T1041	Exfiltration over C2 channel	Exfiltration	54	2.1%
T1204	User execution	Execution	51	2.0%
T1053	Scheduled task/job	Execution, persistence, privilege escalation	49	1.9%
T1083	File/directory discovery	Discovery	47	1.8%
T1036	Masquerading	Defense evasion	45	1.7%

RQ2: CTI Records in APT Campaigns

- ✓ **CVEs:** Total 1,088 extracted *(431 unique)*
  - Top vulnerabilities: RCE, memory corruption
- ✓ **YARA Rules:** Total 419 extracted *(all unique)*
  - Limited coverage due to sensitivity of APTs

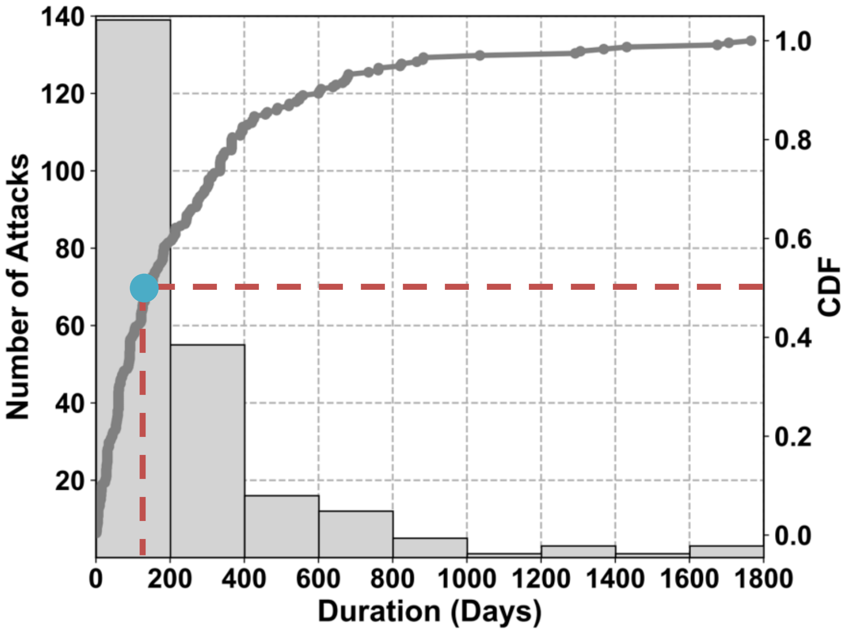


CVE	Severity	Vuln	Affected S/W	Count	Ratio
CVE-2012-0158	8.8 (High)	RCE	19	59	5.4%
CVE-2017-11882	7.8 (High)	Memory Corruption	4	44	4.0%
CVE-2017-0199	7.8 (High)	RCE	8	33	3.0%
CVE-2018-0802	7.8 (High)	Memory Corruption	4	20	1.8%
CVE-2015-5119	9.8 (Critical)	UAF	7	18	1.7%
CVE-2015-1641	7.8 (High)	Memory Corruption	11	16	1.5%
CVE-2010-3333	7.8 (High)	Stack Overflow	8	15	1.4%
CVE-2014-6332	9.3 (High)	RCE	11	15	1.4%
CVE-2015-1701	7.8 (High)	PE	3	15	1.4%
CVE-2014-4114	7.8 (High)	RCE	10	13	1.2%

RQ3: Common Traits of APTs

✓ **APT duration**

- Median: 137 days ●
- Longest APT: 1,766 days → Project Sauron
- Shortest APT: one day → TV5Monde attack



SecAI Lab SUNGKYUNKWAN UNIVERSITY(SKKU)

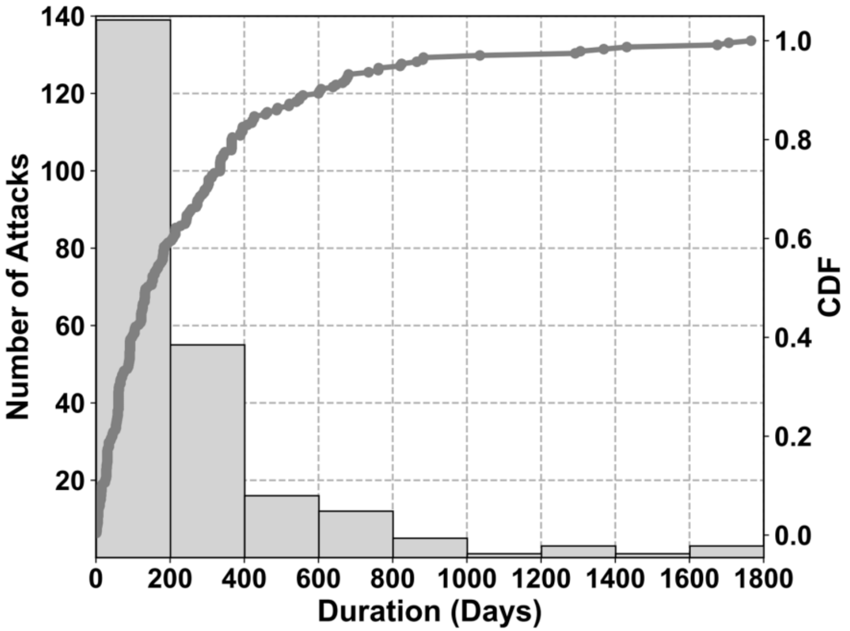
RQ3: Common Traits of APTs

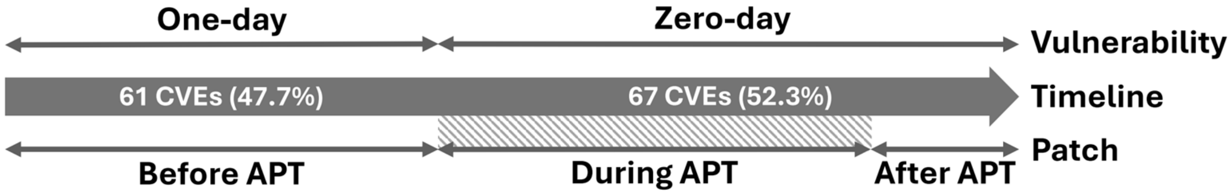
✓ **APT duration**

- Median: 137 days
- Longest APT: 1,766 days → Project Sauron
- Shortest APT: one day → TV5Monde attack

✓ **Vulnerabilities and Patches**

- CVE - attack duration analysis
- ~50% exploited as zero-day
- Avg patching time: ~200 days





One-day

Zero-day

Vulnerability

61 CVEs (47.7%)

67 CVEs (52.3%)

Timeline

Patch

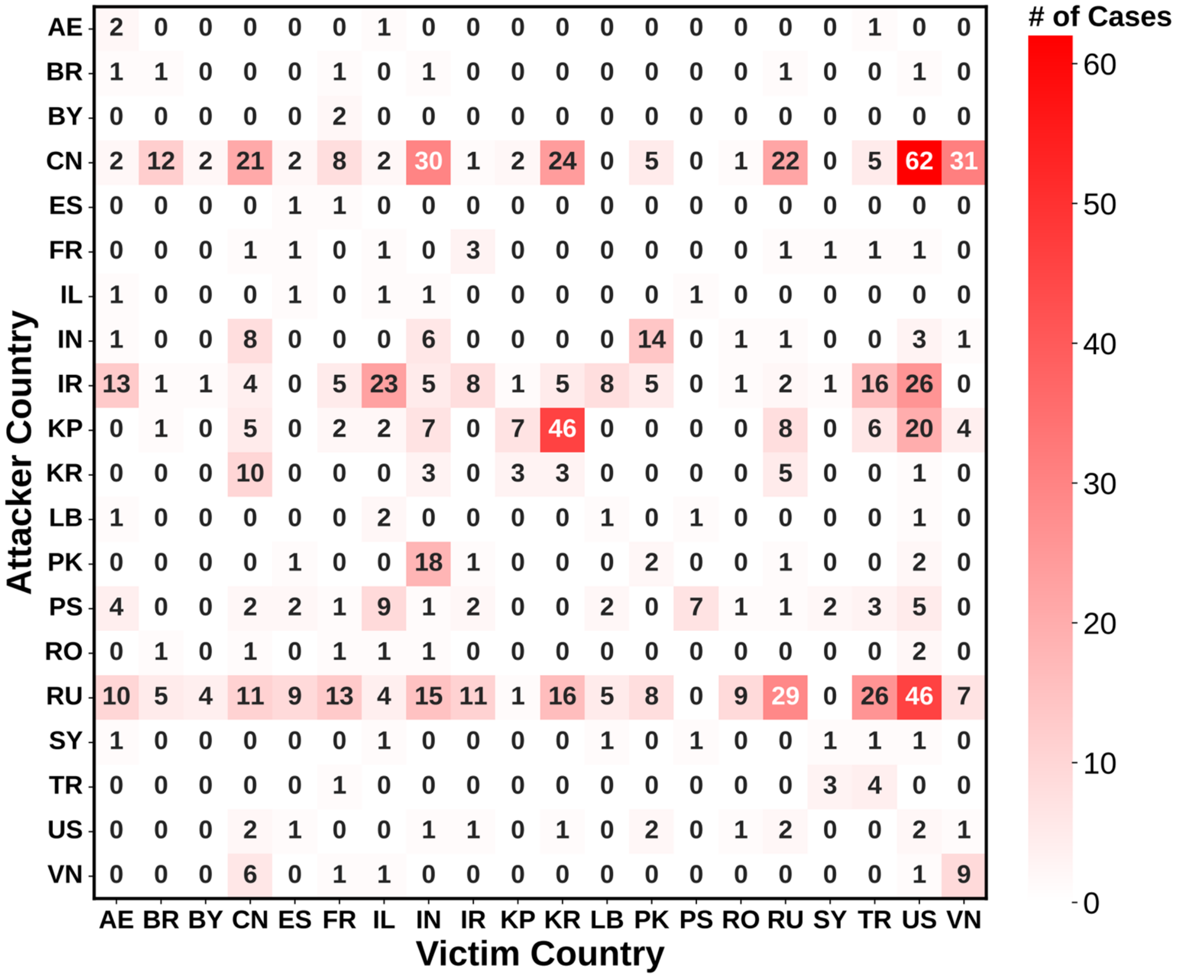
Before APT

During APT

After APT

RQ3: Common Traits of APTs

✓ **Two-sided Nature as Both Attacker and Victim**

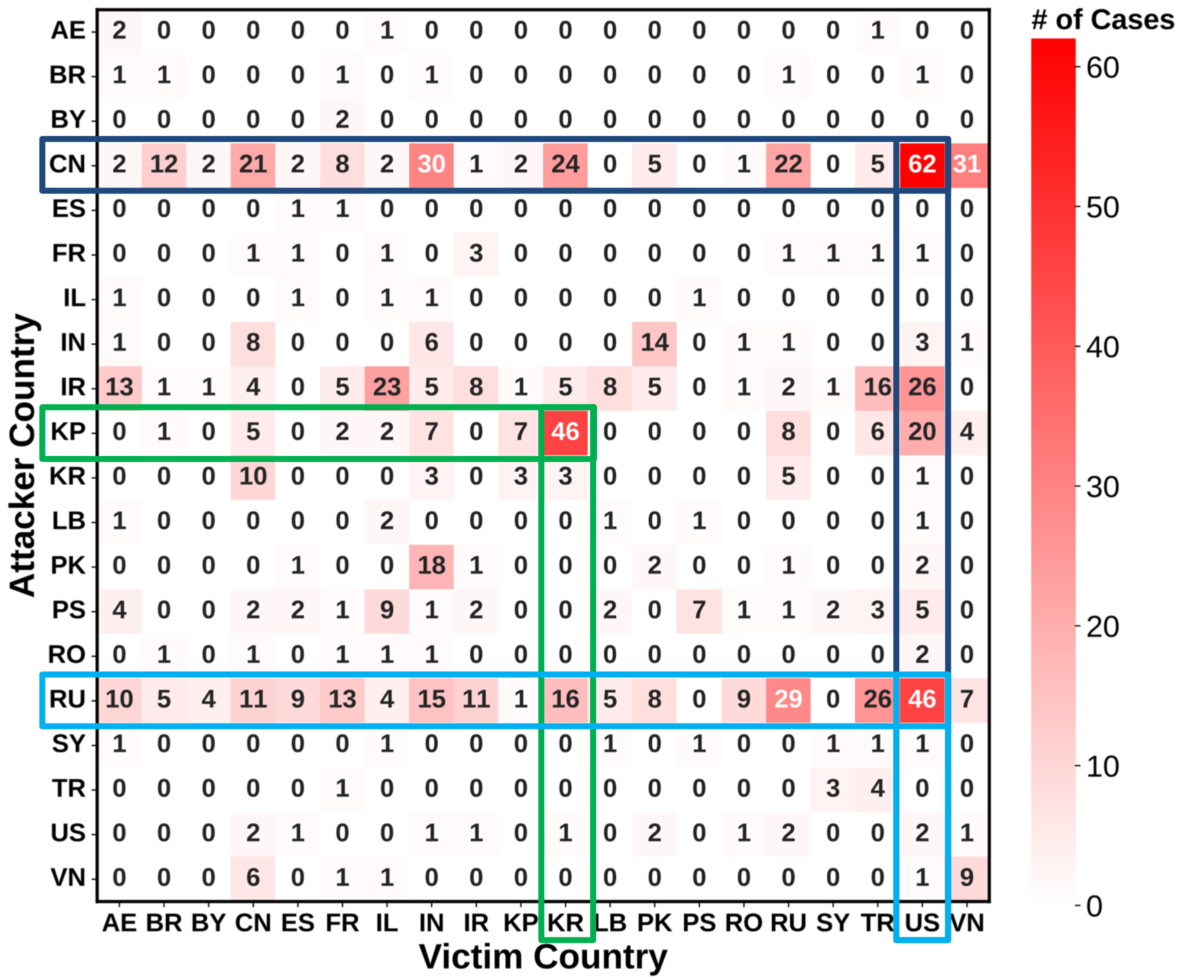


Attacker Country \ Victim Country	AE	BR	BY	CN	ES	FR	IL	IN	IR	KP	KR	LB	PK	PS	RO	RU	SY	TR	US	VN
AE	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
BR	1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
BY	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CN	2	12	2	21	2	8	2	30	1	2	24	0	5	0	1	22	0	5	62	31
ES	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR	0	0	0	1	1	0	1	0	3	0	0	0	0	0	0	1	1	1	1	0
IL	1	0	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
IN	1	0	0	8	0	0	0	6	0	0	0	0	14	0	1	1	0	0	3	1
IR	13	1	1	4	0	5	23	5	8	1	5	8	5	0	1	2	1	16	26	0
KP	0	1	0	5	0	2	2	7	0	7	46	0	0	0	0	8	0	6	20	4
KR	0	0	0	10	0	0	0	3	0	3	3	0	0	0	0	5	0	0	1	0
LB	1	0	0	0	0	0	2	0	0	0	0	1	0	1	0	0	0	0	1	0
PK	0	0	0	0	1	0	0	18	1	0	0	0	2	0	0	1	0	0	2	0
PS	4	0	0	2	2	1	9	1	2	0	0	2	0	7	1	1	2	3	5	0
RO	0	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	2	0
RU	10	5	4	11	9	13	4	15	11	1	16	5	8	0	9	29	0	26	46	7
SY	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	1	1	0
TR	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	4	0	0
US	0	0	0	2	1	0	0	1	1	0	1	0	2	0	1	2	0	0	2	1
VN	0	0	0	6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	9

RQ3: Common Traits of APTs

✓ **Two-sided Nature as Both Attacker and Victim**

- Top attack pairs:
  - CN-US, KP-KR, RU-US

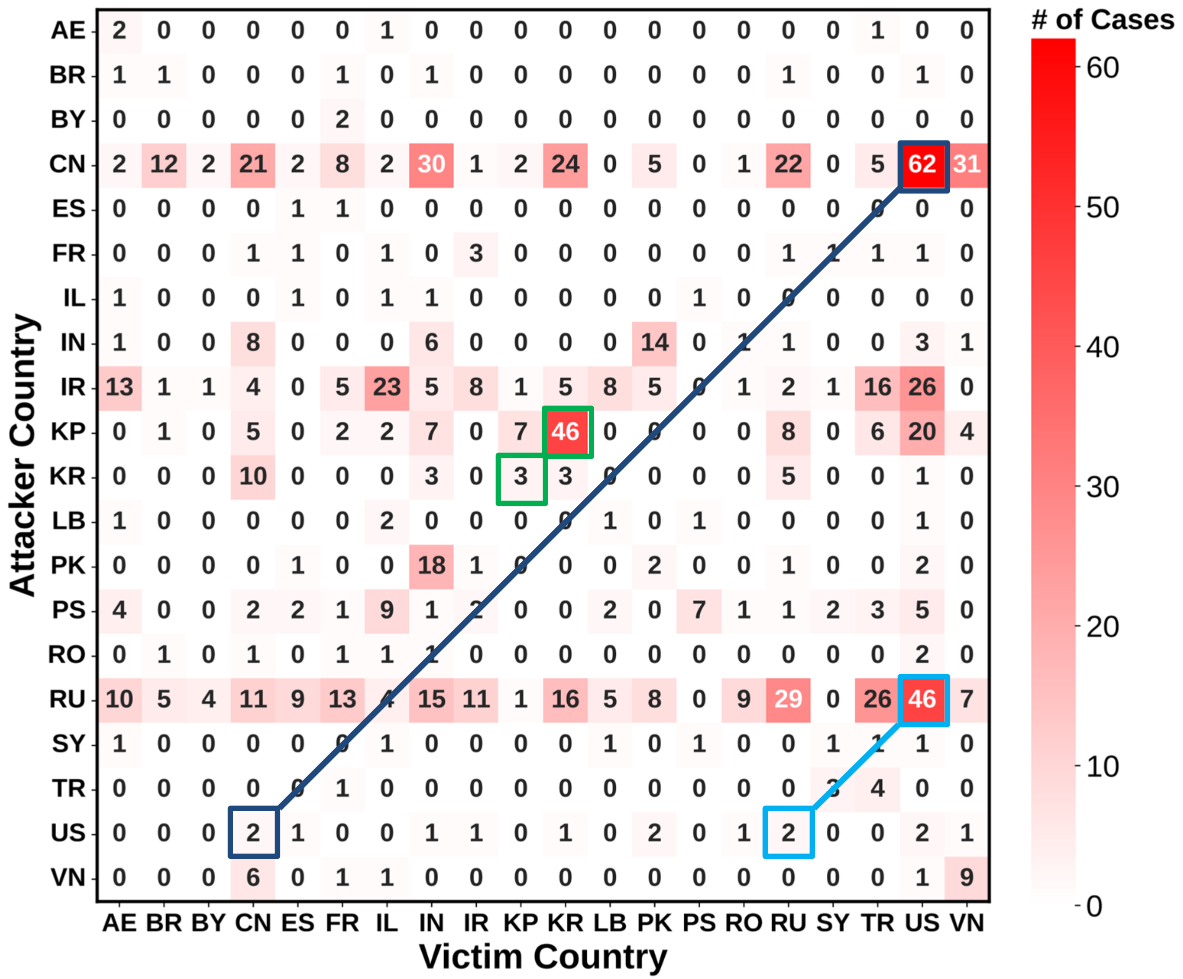


	AE	BR	BY	CN	ES	FR	IL	IN	IR	KP	KR	LB	PK	PS	RO	RU	SY	TR	US	VN
AE	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
BR	1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
BY	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CN	2	12	2	21	2	8	2	30	1	2	24	0	5	0	1	22	0	5	62	31
ES	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR	0	0	0	1	1	0	1	0	3	0	0	0	0	0	0	1	1	1	1	0
IL	1	0	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
IN	1	0	0	8	0	0	0	6	0	0	0	0	14	0	1	1	0	0	3	1
IR	13	1	1	4	0	5	23	5	8	1	5	8	5	0	1	2	1	16	26	0
KP	0	1	0	5	0	2	2	7	0	7	46	0	0	0	0	8	0	6	20	4
KR	0	0	0	10	0	0	0	3	0	3	3	0	0	0	0	5	0	0	1	0
LB	1	0	0	0	0	0	2	0	0	0	0	1	0	1	0	0	0	0	1	0
PK	0	0	0	0	1	0	0	18	1	0	0	0	2	0	0	1	0	0	2	0
PS	4	0	0	2	2	1	9	1	2	0	0	2	0	7	1	1	2	3	5	0
RO	0	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	2	0
RU	10	5	4	11	9	13	4	15	11	1	16	5	8	0	9	29	0	26	46	7
SY	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	1	1	0
TR	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	4	0	0
US	0	0	0	2	1	0	0	1	1	0	1	0	2	0	1	2	0	0	2	1
VN	0	0	0	6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	9

RQ3: Common Traits of APTs

✓ **Two-sided Nature as Both Attacker and Victim**

- Top attack pairs:
  - CN-US, KP-KR, RU-US
- Asymmetry ratios:
  - CN-US: 31 to 1
  - KP-KR, RU-US: 15 to 1

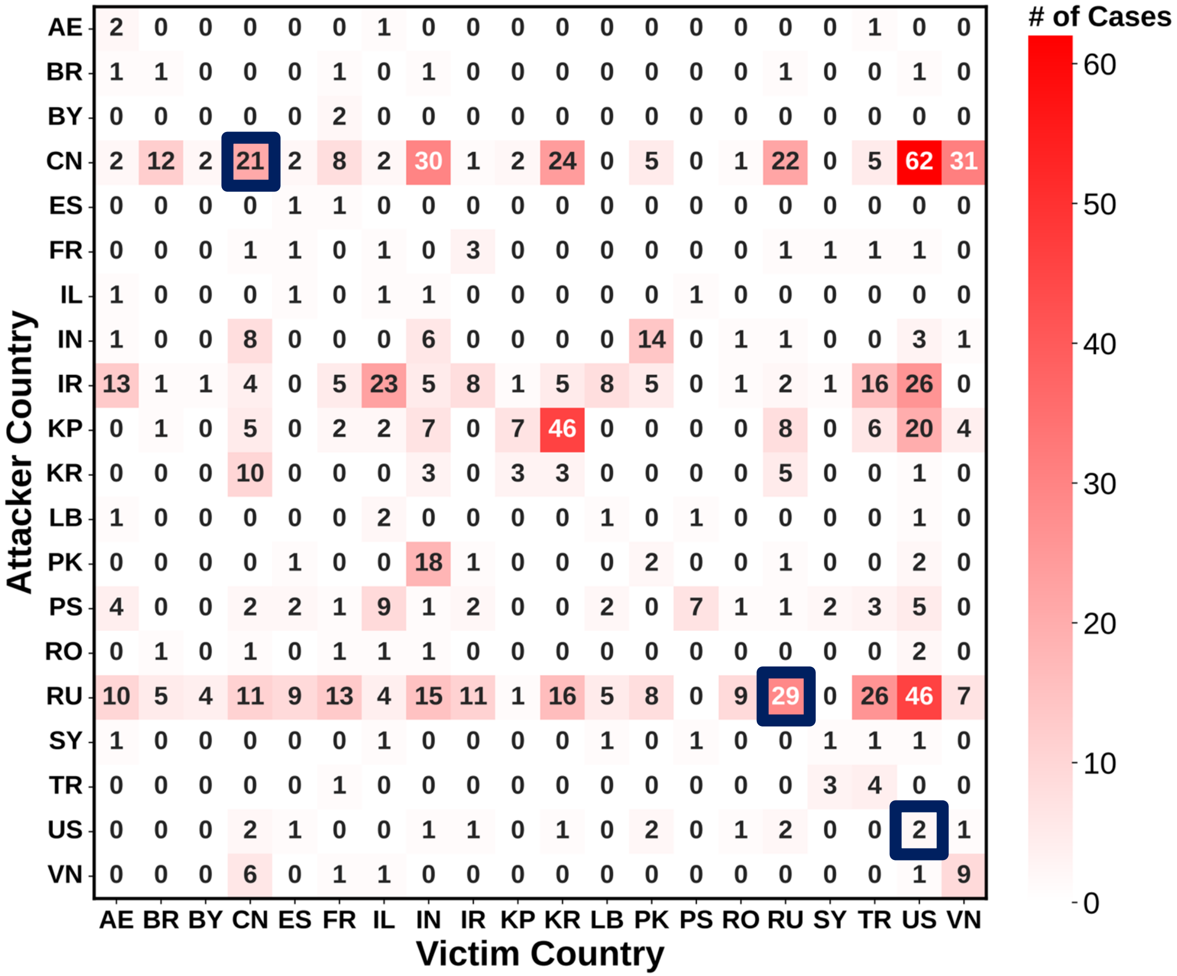


Attacker Country \ Victim Country	AE	BR	BY	CN	ES	FR	IL	IN	IR	KP	KR	LB	PK	PS	RO	RU	SY	TR	US	VN
AE	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
BR	1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
BY	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CN	2	12	2	21	2	8	2	30	1	2	24	0	5	0	1	22	0	5	62	31
ES	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR	0	0	0	1	1	0	1	0	3	0	0	0	0	0	0	1	1	1	1	0
IL	1	0	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
IN	1	0	0	8	0	0	0	6	0	0	0	0	14	0	1	1	0	0	3	1
IR	13	1	1	4	0	5	23	5	8	1	5	8	5	0	1	2	1	16	26	0
KP	0	1	0	5	0	2	2	7	0	7	46	0	0	0	0	8	0	6	20	4
KR	0	0	0	10	0	0	0	3	0	3	3	0	0	0	0	5	0	0	1	0
LB	1	0	0	0	0	0	2	0	0	0	0	1	0	1	0	0	0	0	1	0
PK	0	0	0	0	1	0	0	18	1	0	0	0	2	0	0	1	0	0	2	0
PS	4	0	0	2	2	1	9	1	2	0	0	2	0	7	1	1	2	3	5	0
RO	0	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	2	0
RU	10	5	4	11	9	13	4	15	11	1	16	5	8	0	9	29	0	26	46	7
SY	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	1	1	0
TR	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	4	0	0
US	0	0	0	2	1	0	0	1	1	0	1	0	2	0	1	2	0	0	2	1
VN	0	0	0	6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	9

RQ3: Common Traits of APTs

✓ **Self-directed APT Attacks**

- Origin and target countries are same
  - RU-RU, CN-CN, US-US
- Reasons:
  - Domestic targeting of individuals
  - Foreign organizations within a country
  - Geopolitical/territorial disputes



	AE	BR	BY	CN	ES	FR	IL	IN	IR	KP	KR	LB	PK	PS	RO	RU	SY	TR	US	VN
AE	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
BR	1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
BY	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CN	2	12	2	21	2	8	2	30	1	2	24	0	5	0	1	22	0	5	62	31
ES	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FR	0	0	0	1	1	0	1	0	3	0	0	0	0	0	0	1	1	1	1	0
IL	1	0	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0
IN	1	0	0	8	0	0	0	6	0	0	0	0	14	0	1	1	0	0	3	1
IR	13	1	1	4	0	5	23	5	8	1	5	8	5	0	1	2	1	16	26	0
KP	0	1	0	5	0	2	2	7	0	7	46	0	0	0	0	8	0	6	20	4
KR	0	0	0	10	0	0	0	3	0	3	3	0	0	0	0	5	0	0	1	0
LB	1	0	0	0	0	0	2	0	0	0	0	1	0	1	0	0	0	0	1	0
PK	0	0	0	0	1	0	0	18	1	0	0	0	2	0	0	1	0	0	2	0
PS	4	0	0	2	2	1	9	1	2	0	0	2	0	7	1	1	2	3	5	0
RO	0	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	2	0
RU	10	5	4	11	9	13	4	15	11	1	16	5	8	0	9	29	0	26	46	7
SY	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	1	1	0
TR	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	4	0	0
US	0	0	0	2	1	0	0	1	1	0	1	0	2	0	1	2	0	0	2	1
VN	0	0	0	6	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	9

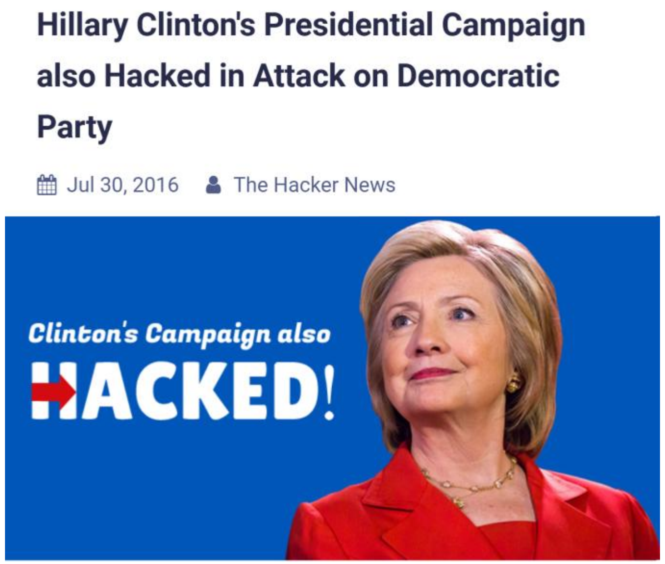
RQ4: External Dynamics of APT Campaigns

✓ **Political Events**

- 2016 US presidential election: APT28’s attack campaign

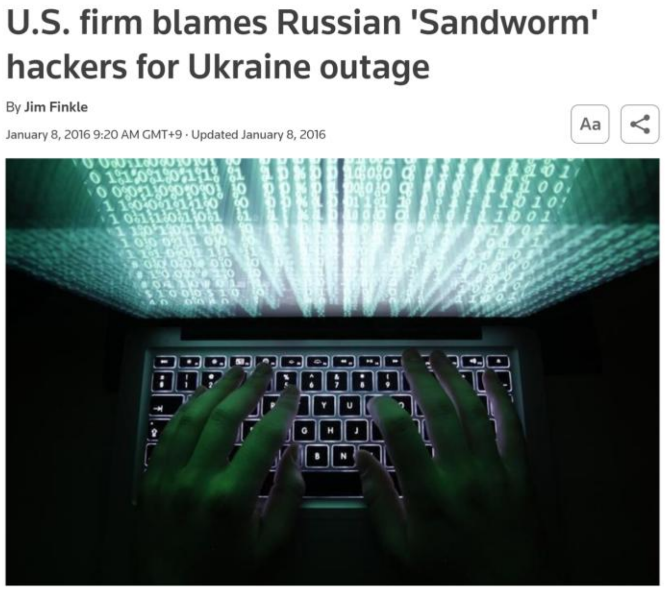
✓ **International Conflicts**

- Russo-Ukrainian war: Sandworm’s attack on energy sector



Hillary Clinton's Presidential Campaign also Hacked in Attack on Democratic Party

Jul 30, 2016 The Hacker News



U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage

By Jim Finkle

January 8, 2016 9:20 AM GMT+9 · Updated January 8, 2016

RQ4: External Dynamics of APT Campaigns

✓ **Global Pandemics**

- COVID-19 pandemic: Lazarus's attempt to steal intelligence

✓ **Economic Gains**

- Rise of cryptocurrencies: Lazarus's crypto heist

Lazarus covets COVID-19-related intelligence

APT REPORTS 23 DEC 2020 ⌛ 11 minute read

North Korean hackers target gamers in $615m crypto heist - US

15 April 2022

Share Save

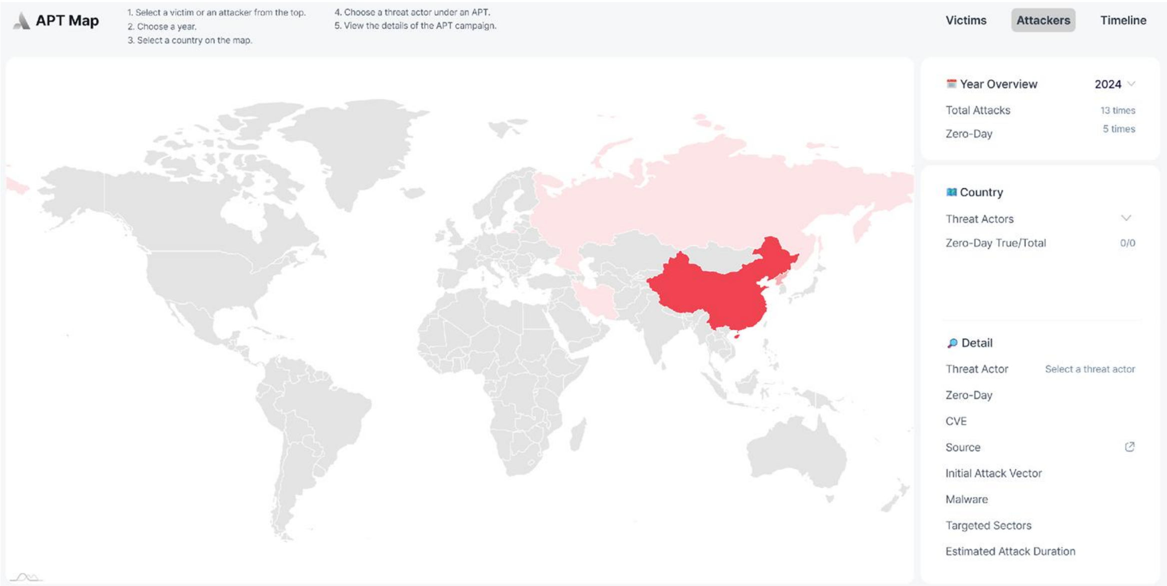
Visual Representations

✓ APT Map

- Interactive map of worldwide APT campaigns

✓ Sankey Diagram

- Relationship between top 10 threat actors and top 30 victim countries



1. Select a victim or an attacker from the top.
2. Choose a year.
3. Select a country on the map.
4. Choose a threat actor under an APT.
5. View the details of the APT campaign.

Year Overview 2024

Total Attacks 13 times

Zero-Day 5 times

Country

Threat Actors

Zero-Day True/Total 0/0

Detail

Threat Actor: Select a threat actor

Zero-Day

CVE

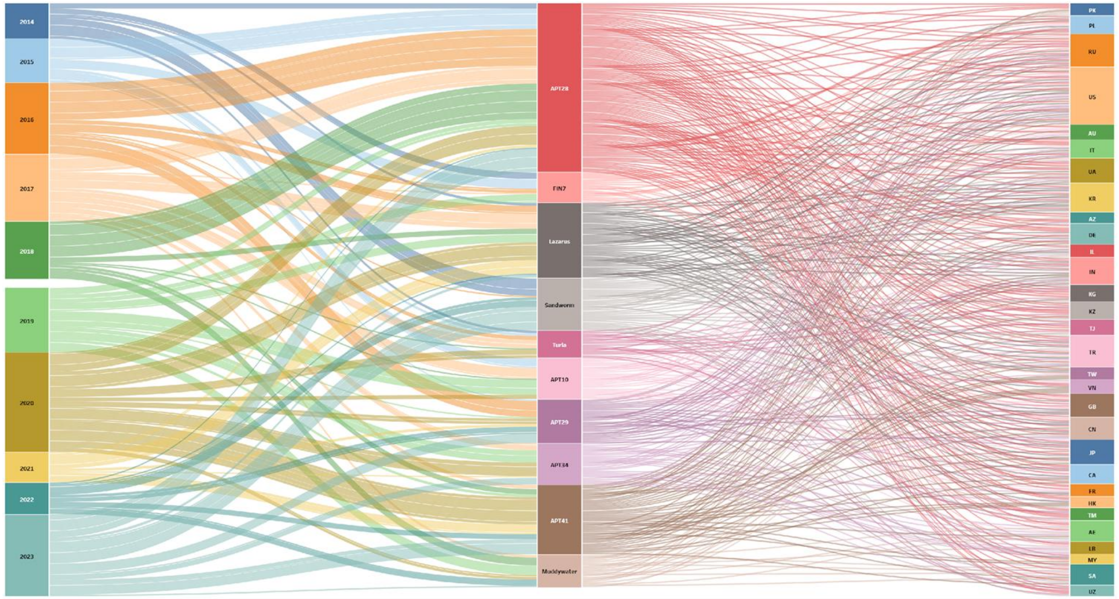
Source

Initial Attack Vector

Malware

Targeted Sectors

Estimated Attack Duration



Limitations

- ✓ **Representativeness of APT Campaigns**
  - Not all APT cases can be captured
- ✓ **Limited Responses from an LLM**
  - LLM retrieval limited by model capability
- ✓ **Attack Duration**
  - Challenging to determine precise attack duration
- ✓ **CVE and Patch Timing**
  - Patch not always aligned with CVE release

Conclusion

✓ **Decade-long APT study (2014-2023):**

- 1,509 reports analyzed with a hybrid (LLM + rule-based) approach

✓ **Research questions:**

- Evolution of APTs, CTI records, common traits, and external factors

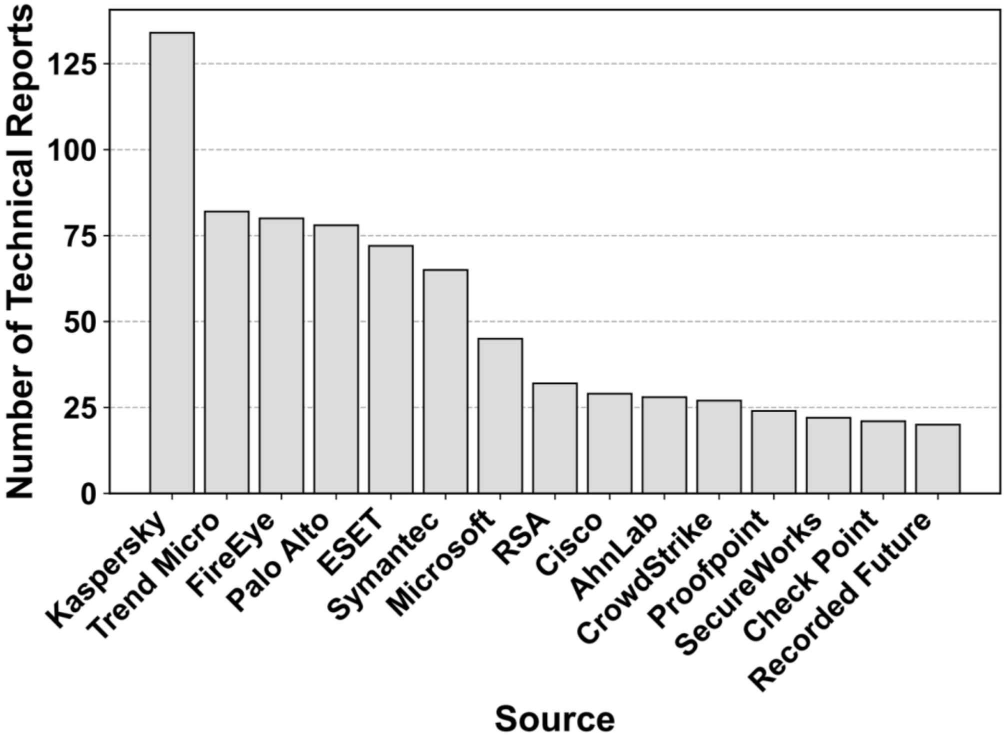
APT Map

Sankey Diagram

Thank you

Appendix

Collection	Source of TA’s Information	# of TAs
TA#1	MISP Project	562
TA#2	Palo Alto, IBM X-Force, Malpedia, Kaspersky, Crowdstrike, Mandiant, Secureworks, Dragos, Venafi, CERT-UA, Microsoft	692
TA#3	MITRE ATT&CK, ETDA, VX-underground	430
Total	–	603 (1,684)



Total: 1,412 (93.6%) TRs