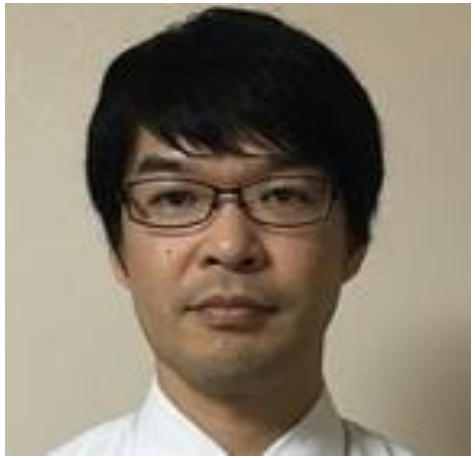
CODE BLUE 2024

Did Subdomain Abuse by BlackTech “Evolve”?

Tsuyoshi Taniguchi and Kotaro Ohsugi
Fujitsu Defense & National Security Limited
November 15, 2024

WHO Are We?



Tsuyoshi Taniguchi

FUJITSU DEFENSE & NATIONAL SECURITY
Researcher, Ph.D.

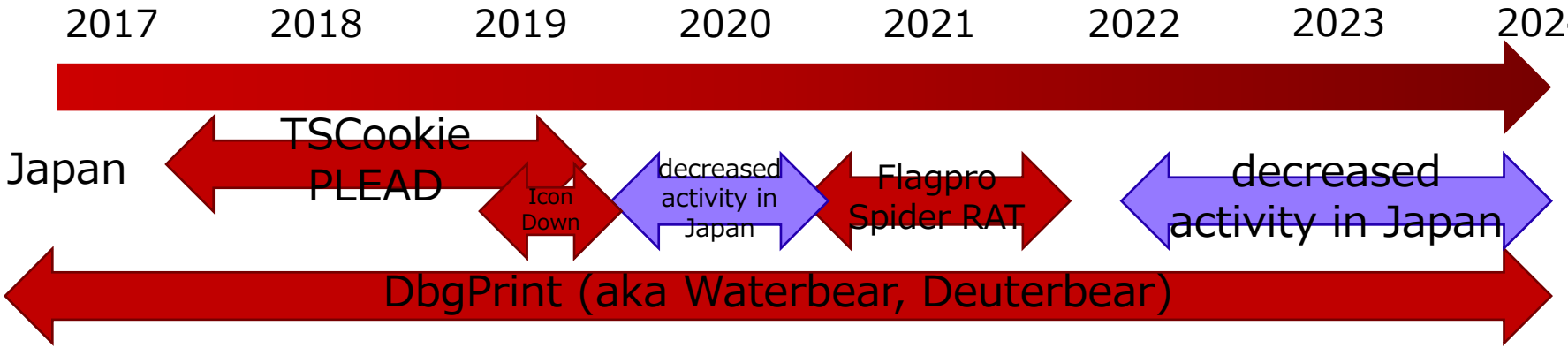
- CODE BLUE 2017 Day0 Special Track Counter Cyber Crime Track, CODE BLUE 2018, 2020, 2021, 2022
- Black Hat Asia 2021 Briefing
- ACM ASIACCS 2021: Core A
- HITCON ENT 2024

Kotaro Ohsugi

FUJITSU DEFENSE & NATIONAL SECURITY
Researcher

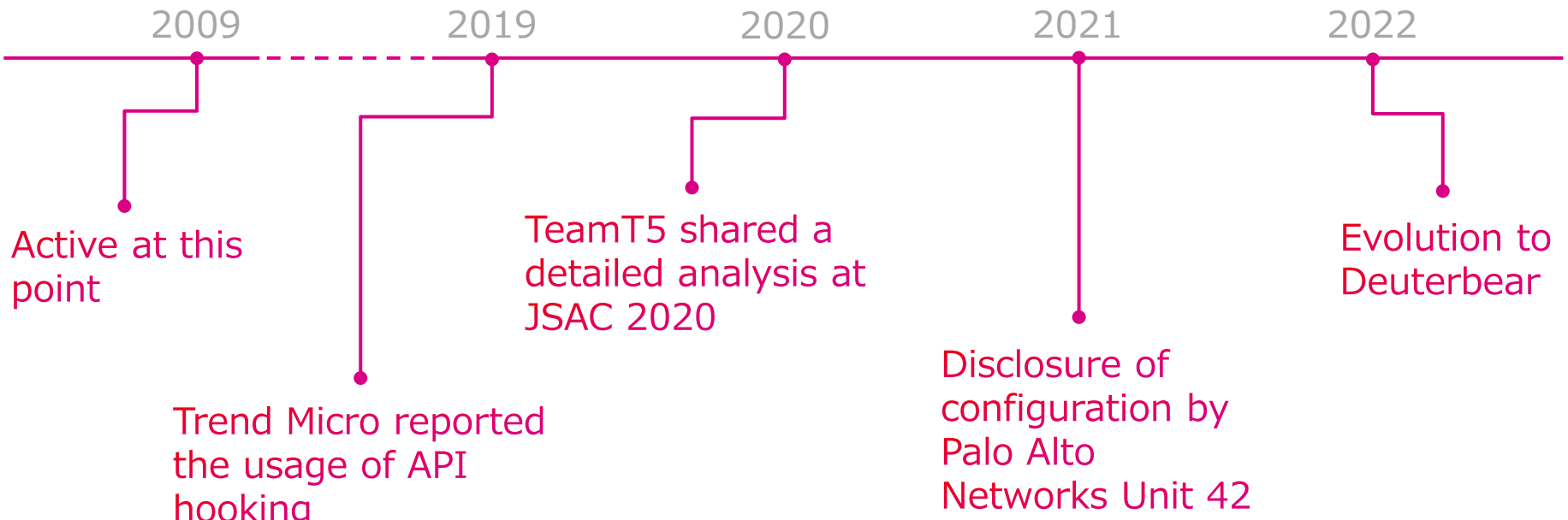
- Digital Forensics
- Reverse-engineering

Malicious Activities by BlackTech



- On Sep. 27, 2023, National Police Agency, NISC, NSA, FBI, and CISA jointly called attention to the threat by BlackTech
- Many excellent reports regarding RAT tools like DbgPrint (aka Waterbear and Deuterbear): hard-to-detect
- These reports did not analyze DNS abuse at all

Timeline of DbgPrint aka Waterbear



DbgPrint Downloader – An Obfuscation Freak

FUJITSU

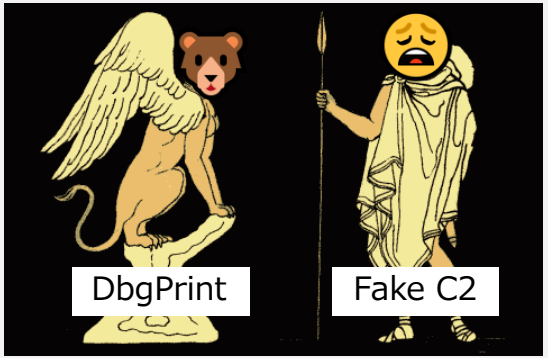
- Typical components: launcher, **downloader**, RAT

```
Decrypt(func);
func();
Encrypt(func);
```

Some functions are decrypted & encrypted on the fly

d1	9c	90	92
.	c	o	m

Bitwise not



Challenge-response using modified RC4

One More Thing

FUJITSU

- Evolution to Deuterbear
  - Transition to HTTPS, even harder to analyze
  - New anti-analysis features were implemented

Analysis can be hard due to its sophisticated implementations and continuous evolvement

Evolution? Strategic Change?

FUJITSU

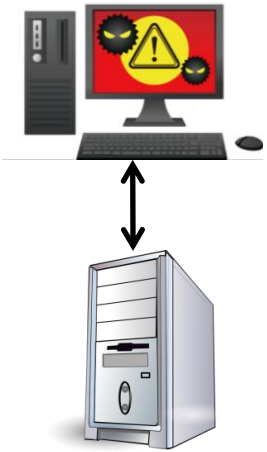
Malware implementation

Evolution ?

Strategic change ?

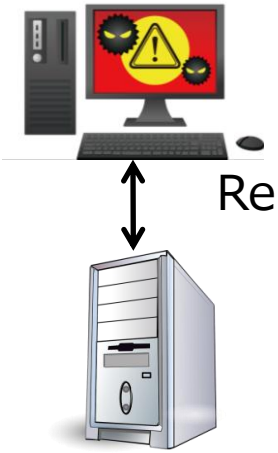
Obfuscation
Anti-sandbox

DNS operation



Evolution ?

Strategic change ?



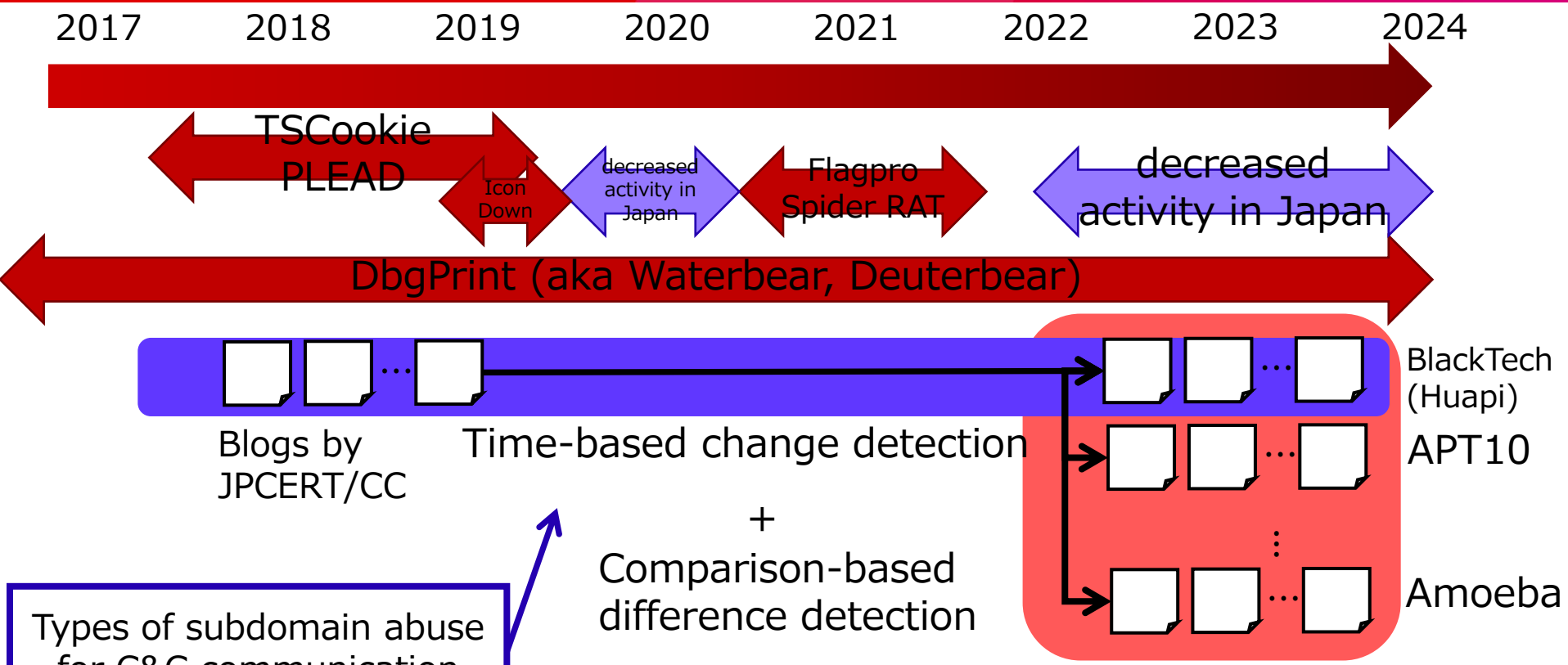
Reused parent domains

Contribution

FUJITSU

- BlackTech
  - RAT tools: **evolution** to make analysis harder
    - hard-to-analyze RAT tools
  - DNS abuse: **evolution?**
    - Security vendors did not pay attention to
    - **Did Subdomain Abuse by BlackTech “Evolve”?**
    - **-> findings and insights based on our analysis**
- Know-how sharing of digital forensics for APT attacks
  - CTI, Passive DNS, and WHOIS
  - Application of our proposed techniques in previous CODE BLUE presentations

Overview of Our Analysis

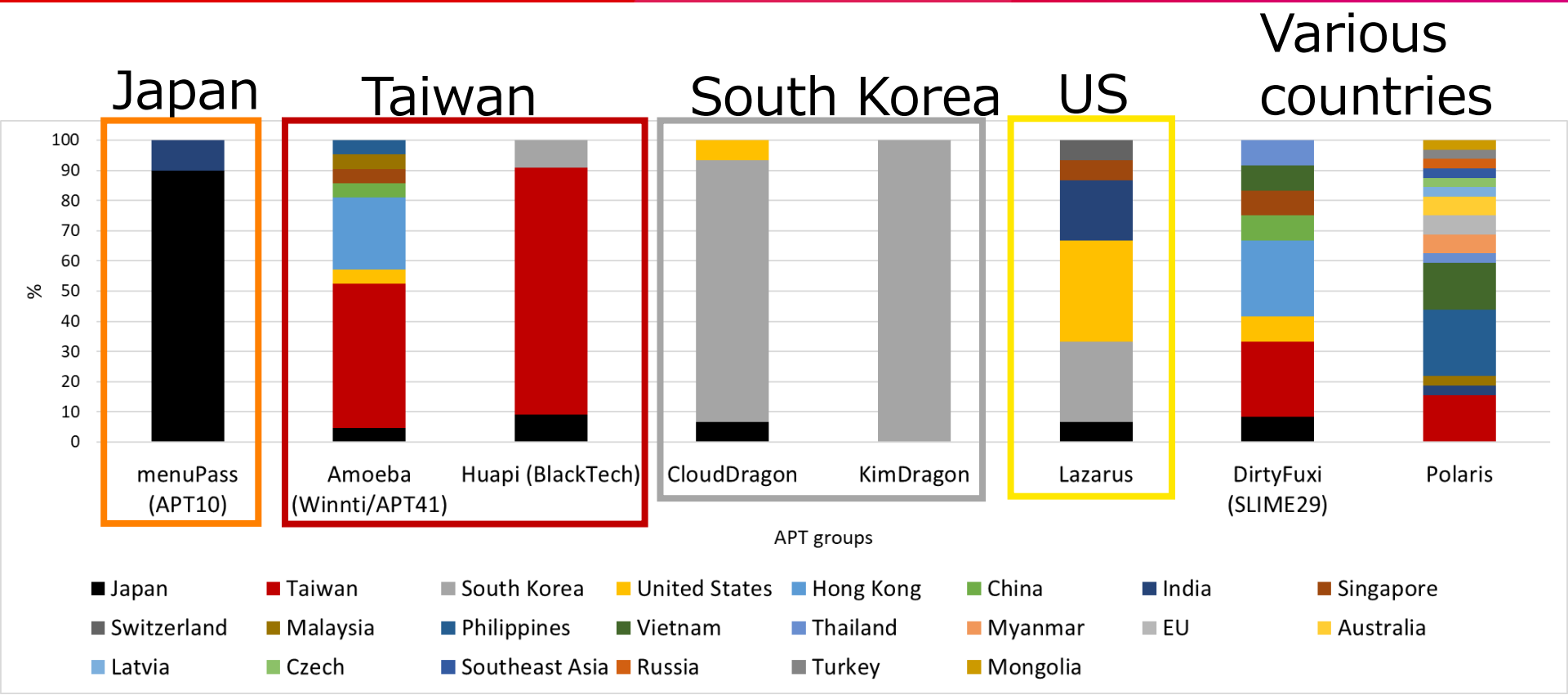


APT Groups for Comparison

FUJITSU

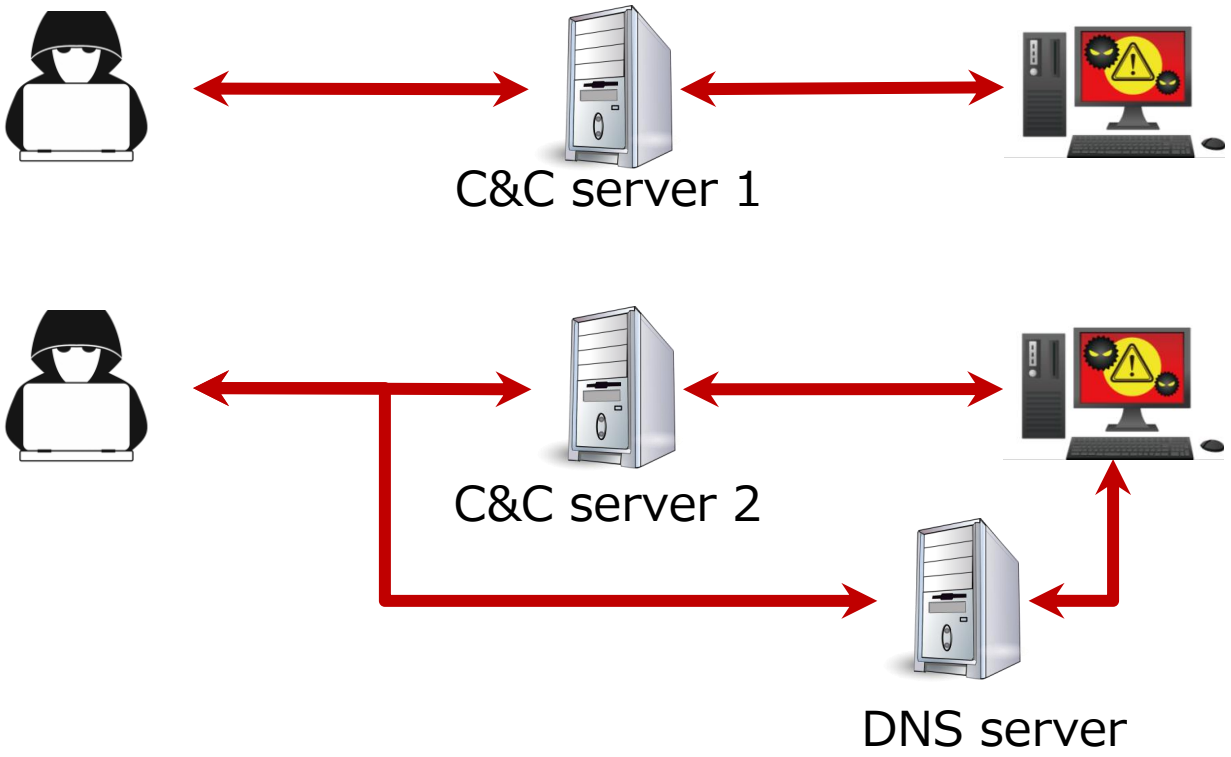
- 8 APT groups from ThreatVision by TeamT5
  - menuPass (APT10)
  - Amoeba (Winnti/APT41)
  - Huapi (BlackTech)
  - CloudDragon
  - KimDragon
  - Lazarus
  - DirtyFuxi (SLIME29)
  - Polaris
- Analysis targets: IoCs from Jan. 2022 to Mar. 2024
  - Flash reports from ThreatVision regarding the above 8 APT groups
- Acknowledgment
  - We really appreciate that TeamT5 continued to cooperate with us

Targeted Countries Based on ThreatVision

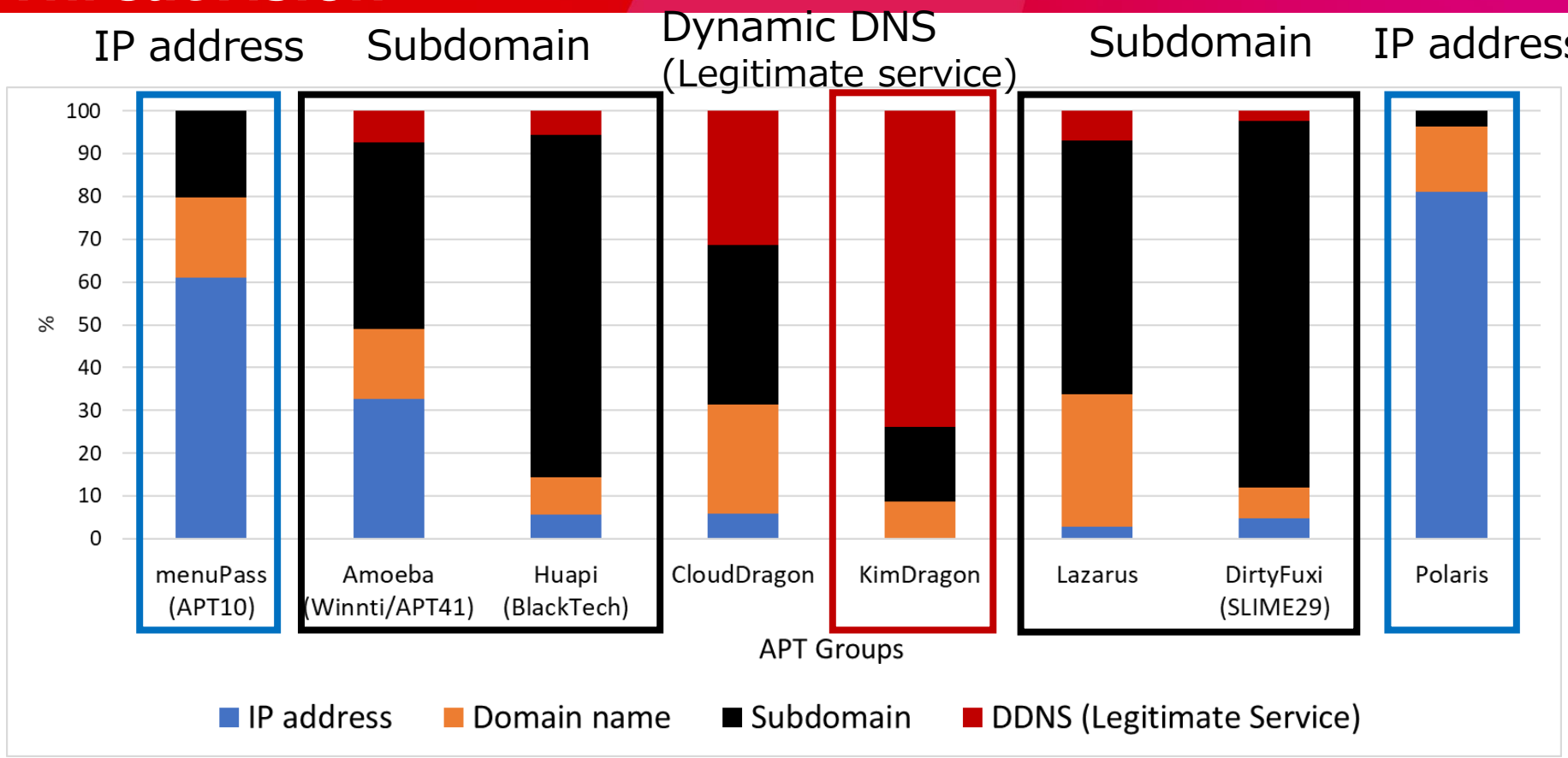


How to Communicate with C&C Servers

FUJITSU

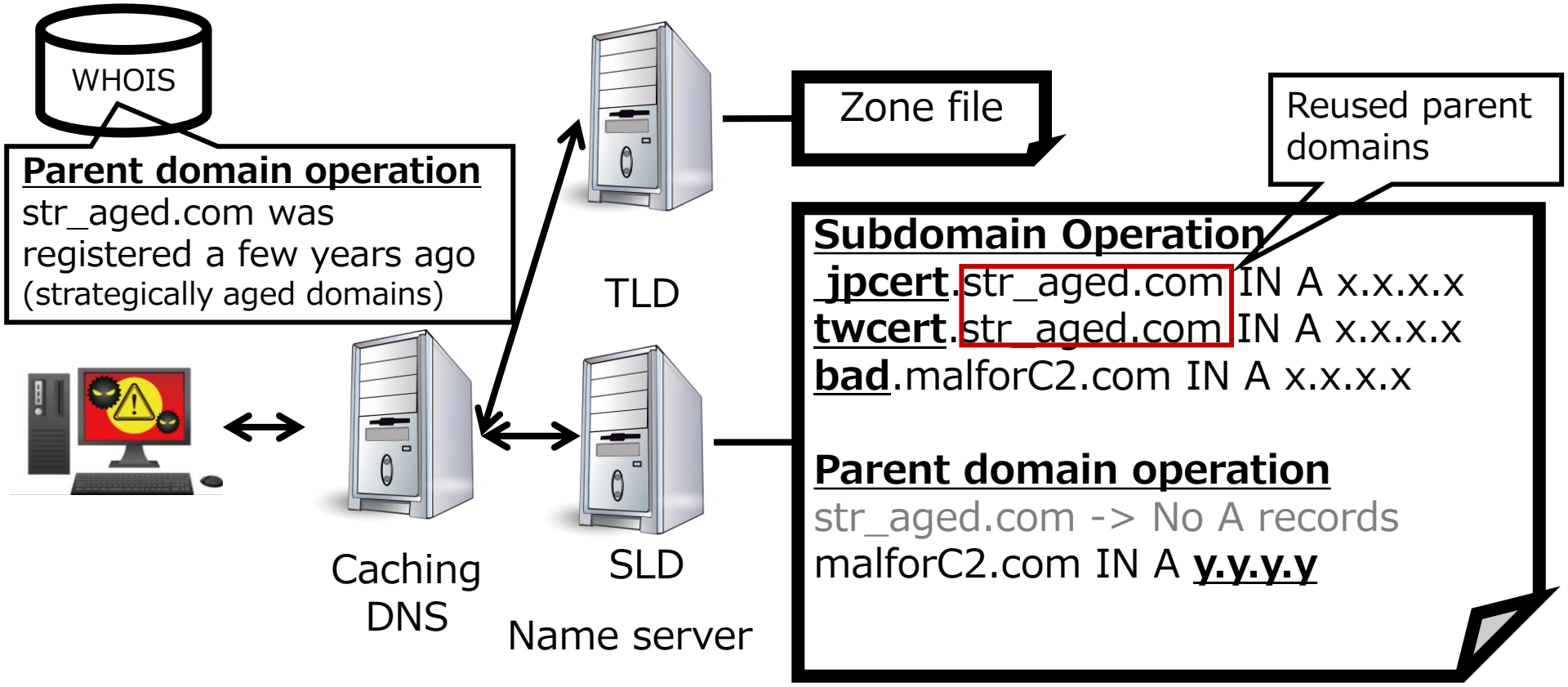


IoCs for C&C Communication Based on ThreatVision



Subdomain Operation?
Parent Domain Operation?

FUJITSU



Types of Subdomain Abuse for C&C Communication

FUJITSU

Type	Abstract
Legitimate service abuse	Dynamic DNS abuse
Subdomain operation	String abuse
	Reused parent domains
Parent domain operation	Strategically aged domains
	Fake dormant and fake response

Legitimate Service Abuse: Dynamic DNS Abuse

FUJITSU

- 23 subdomains (out of 26): Dynamic DNS abuse
- jpcert.**ignorelist.com**, twnicsi.**ignorelist.com**
- twcertcc.**jumpingcrab.com**
- okinawas.**ssl443.org**, sslmaker.**ssl443.org**
- apk36501.**flnet.org**, epayplus.**flnet.org**, newtowns.**flnet.org**
- appinfo.**fairuse.org**
- carcolors.**effers.com**, gethappy.**effers.com**, splashed.**effers.com**
- eoffice.**etowns.org**
- fatgirls.**fatdiary.org**
- iawntsilk.**dnset.com**, ktyguxs.**dnset.com**, langlang.**dnset.com**, lookatinfo.**dnset.com**, savecars.**dnset.com**
- inewdays.**csproject.org**, longdays.**csproject.org**
- lang.**suroot.com**
- office.**dns04.com**

- https://blogs.jpcert.or.jp/ja/2018/03/tscookie.html

Types of Subdomain Abuse for C&C Communication

FUJITSU

Type	Abstract
Legitimate service abuse	Dynamic DNS abuse
Subdomain operation	String abuse
	Reused parent domains
Parent domain operation	Strategically aged domains
	Fake dormant and fake response

Subdomain Operation: String Abuse

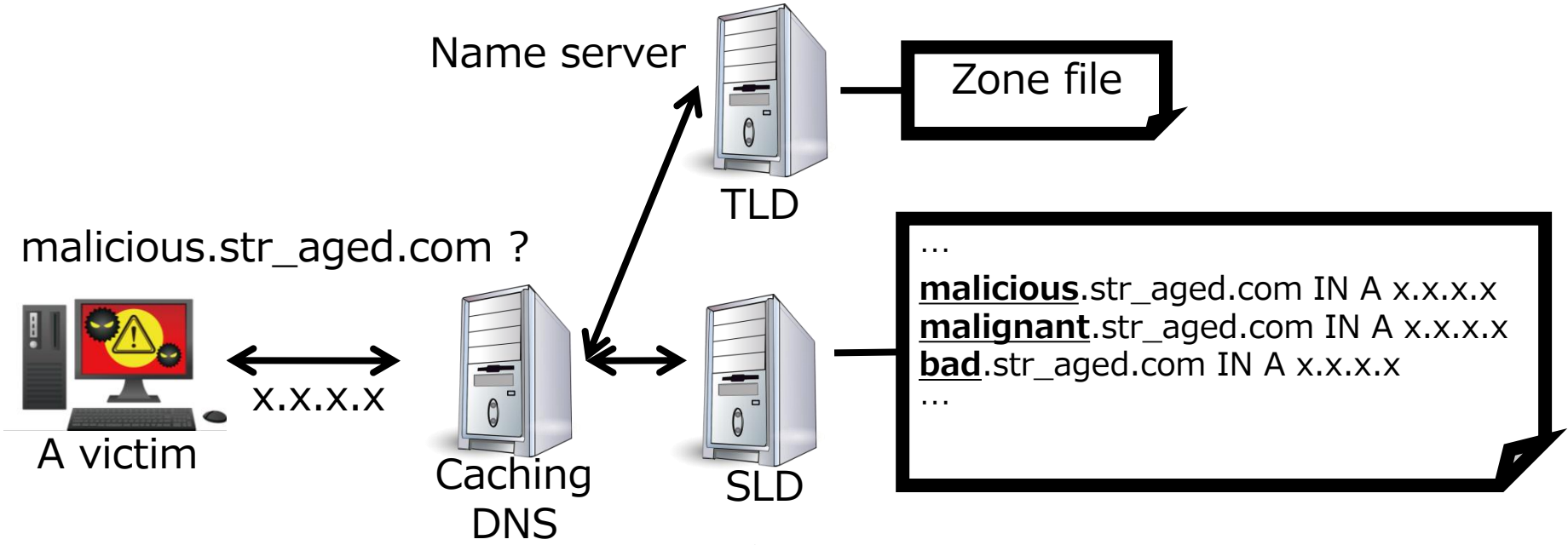
FUJITSU

- Phishing attackers often abused brand names or legitimate URLs
- APT groups rarely abuse brand names
- BlackTech abused strings like “jpcert” and “twcertcc” as subdomains for C&C communication related to TSCookie in 2018
  - **jpcert**.ignorelist.com
  - **jpcerts**.jpcertinfo.com
  - **twcertcc**.jumpingcrab.com

  - https://blogs.jpcert.or.jp/ja/2018/03/tscookie.html

Subdomain Operation: Reused Parent Domains

- Domain owners can operate subdomains as much as they like without any limitation
  - Malicious actors can omit registering domain names



How to Reuse Parent Domains for APT Attacks

FUJITSU

a1_1.parent_x.com
a1_2.parent_x.com
a1_3.parent_x.com

For single target
-> APT groups often reused for single target

For multiple targets

a2_1.parent_y.com
a2_2.parent_y.com

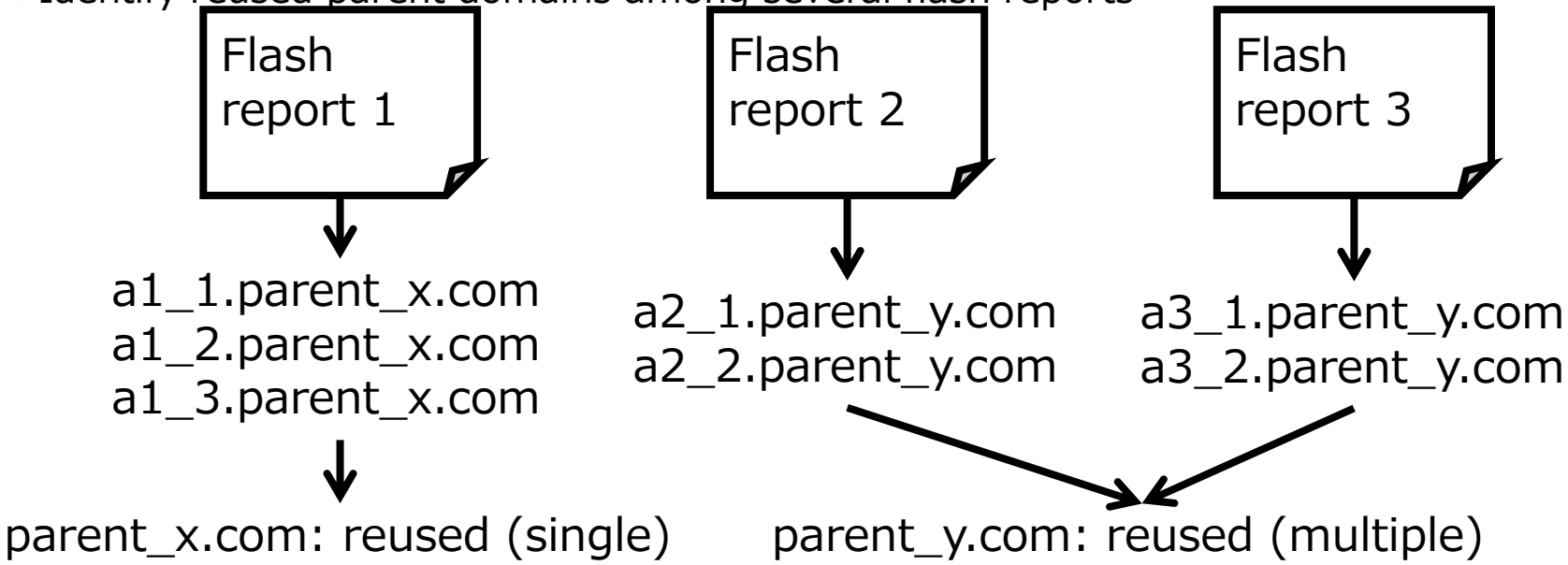
a3_1.parent_y.com
a3_2.parent_y.com

Attack 1 Attack 2 Attack 3

CODE BLUE 2021: the way of searching subdomains for a parent domain
Spring 2023: only reuse for single target -> September 2023: multiple targets

How to Evaluate Reused Parent Domains

- For single target
  - Extract reused parent domains from IoCs in flash reports
- For multiple targets
  - Identify reused parent domains among several flash reports

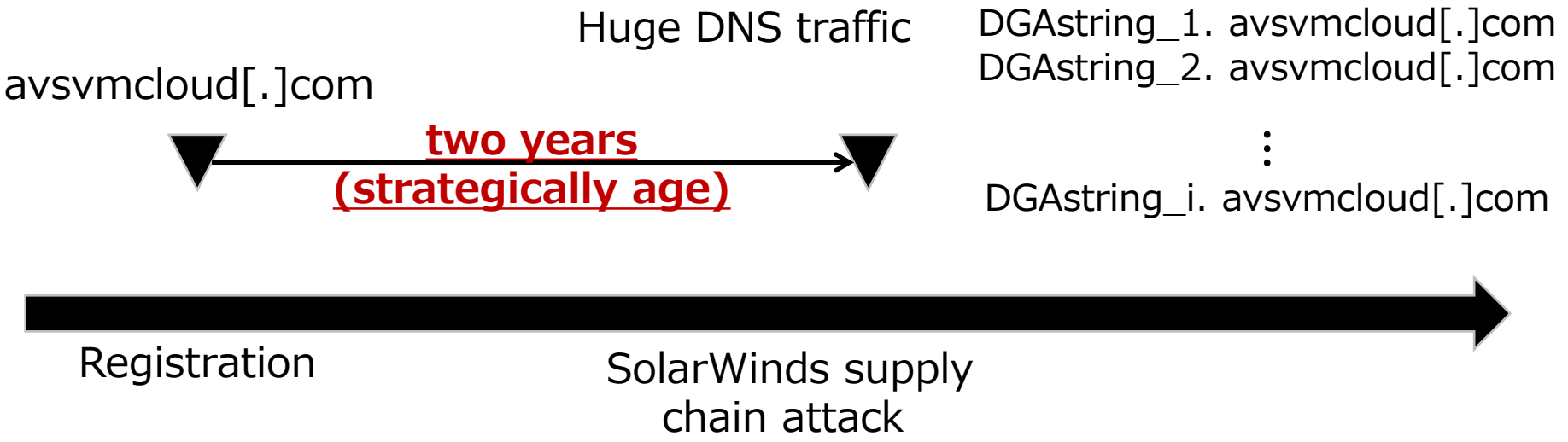


Types of Subdomain Abuse for C&C Communication

FUJITSU

Type	Abstract
Legitimate service abuse	Dynamic DNS abuse
Subdomain operation	String abuse
	Reused parent domains
Parent domain operation	Strategically aged domains
	Fake dormant and fake response

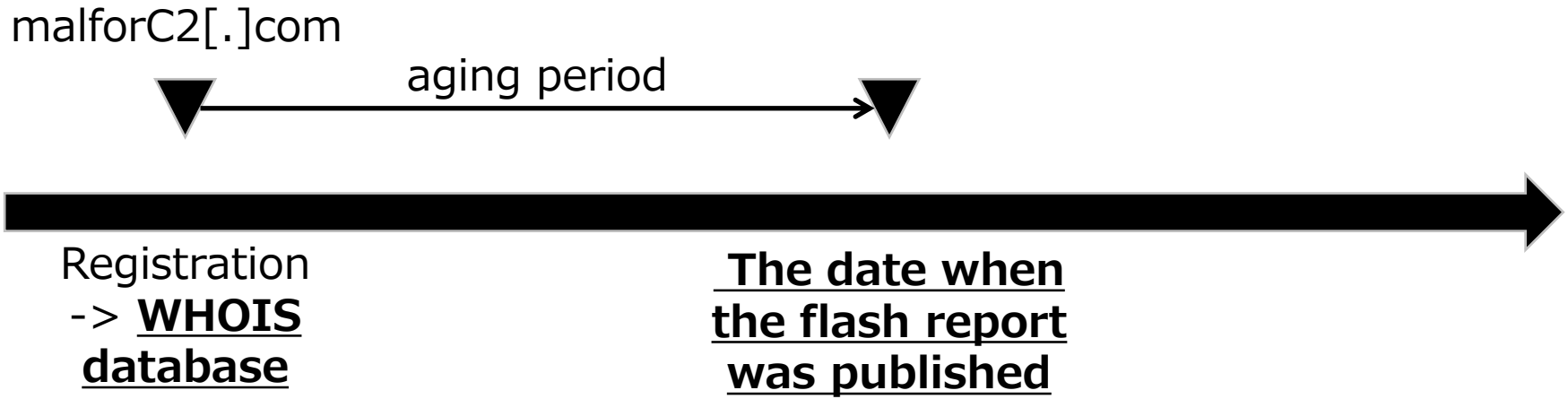
Parent Domain Operation: Strategically Aged Domains



- Strategically Aged Domain Detection: Capture APT Attacks With DNS Traffic Trends by Palo Alto Networks (Dec. 29, 2021)

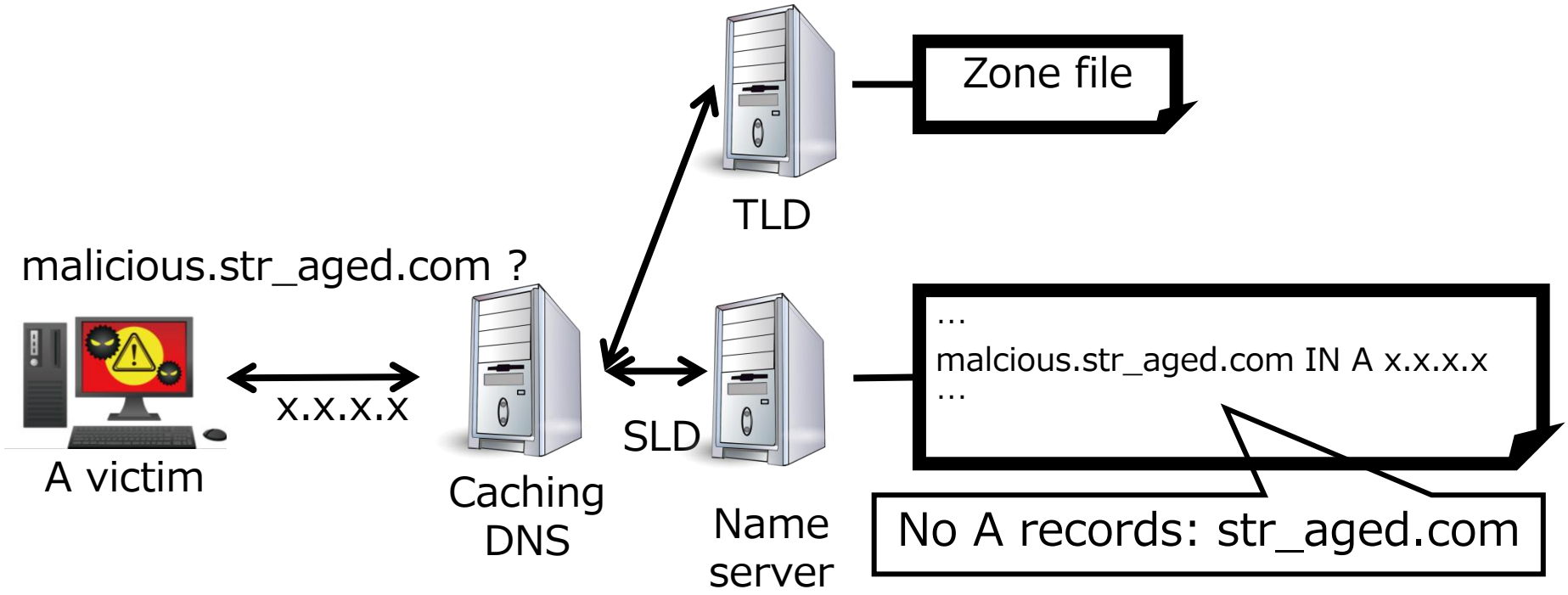
How to Evaluate Aging Period

- The difficulty:
  - When did the APT group start attacking?



Parent Domain Operation: Fake Dormant

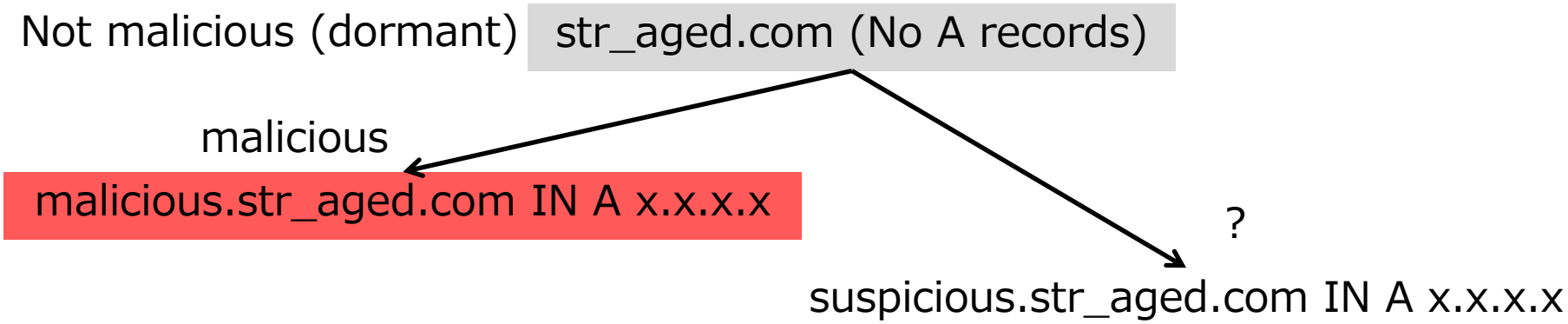
FUJITSU



Why Fake Dormant for C&C Communication?

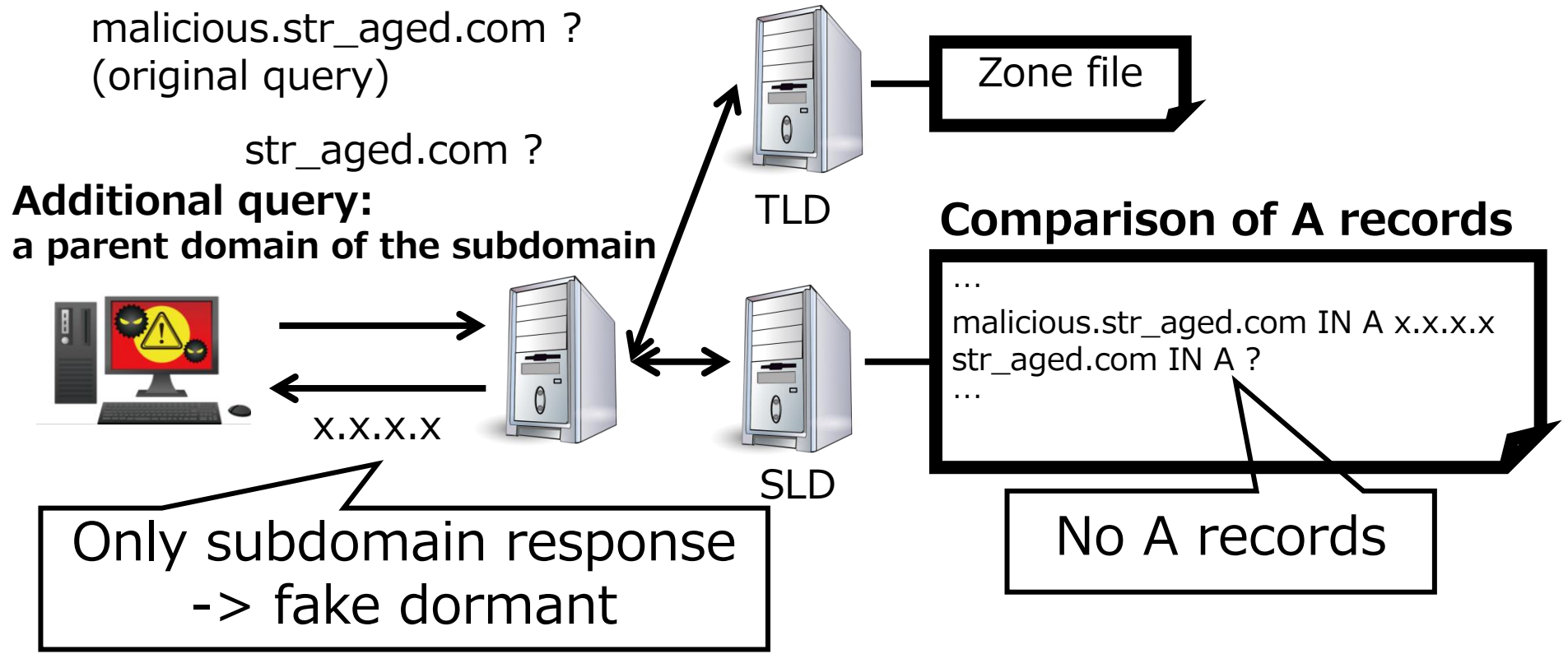
FUJITSU

- Parent domain: malicious -> its subdomains: malicious
- Subdomain: malicious -> its parent domain ?
  - DDNS abuse: parent domains are legitimate

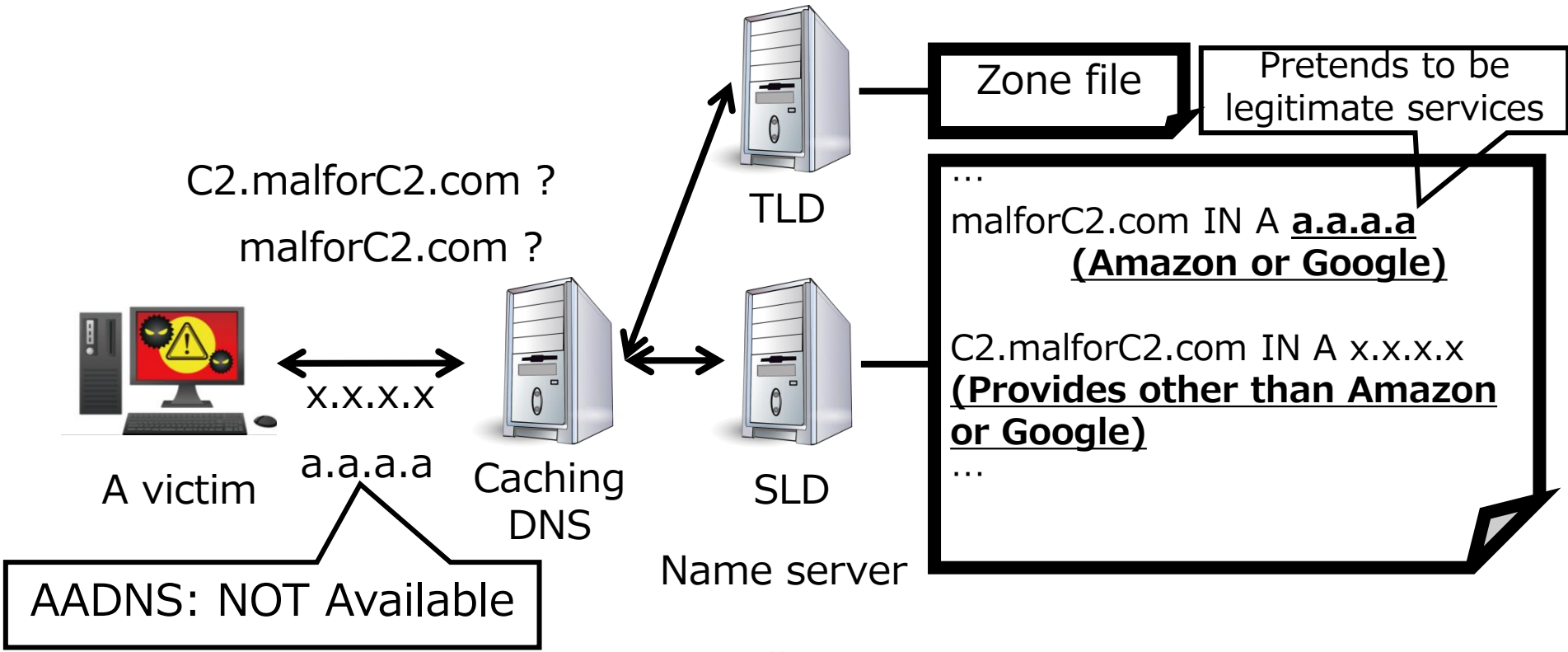


Additional Active DNS (AADNS)

FUJITSU

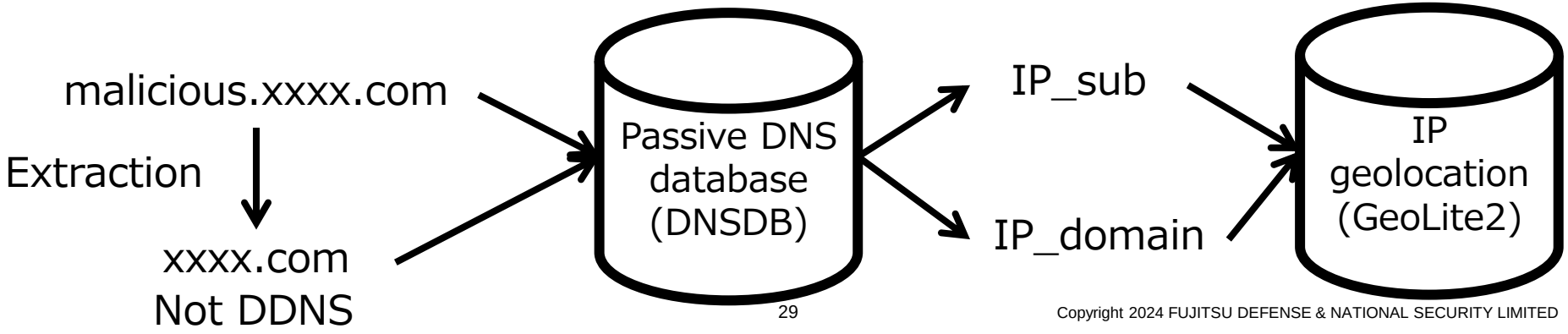


Parent Domain Operation: Fake Response

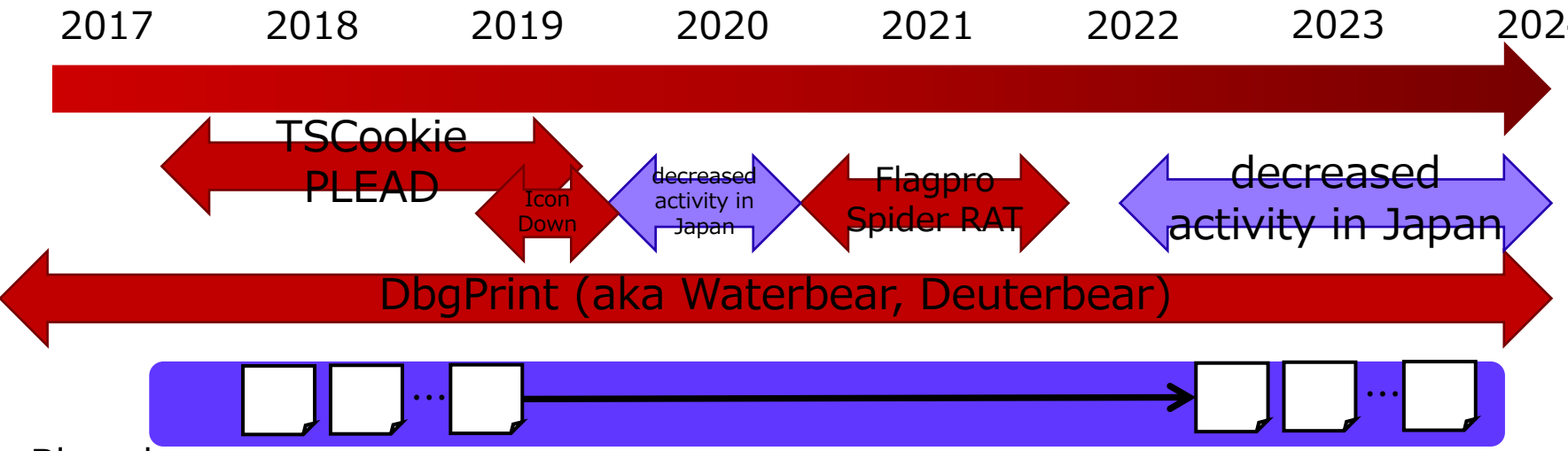


How to Evaluate Fake Dormant or Fake Response

- Passive DNS
  - **Not all name resolution histories of subdomains related to APT attacks**
  - Only if there are subdomains in Passive DNS database, we search name resolution histories of parent domains
- IP geolocation
  - It was worth investigating provides of IP addresses of parent domains



Time-Based Change Detection: TSCooke and PLEAD vs DbgPrint



Blogs by JPCERT/CC
(Analysis in Our CODE BLUE 2020)

Time-based change detection
(Ex. Our CODE BLUE 2022)

Flash reports from ThreatVision by TeamT5 Since Aug. 2023

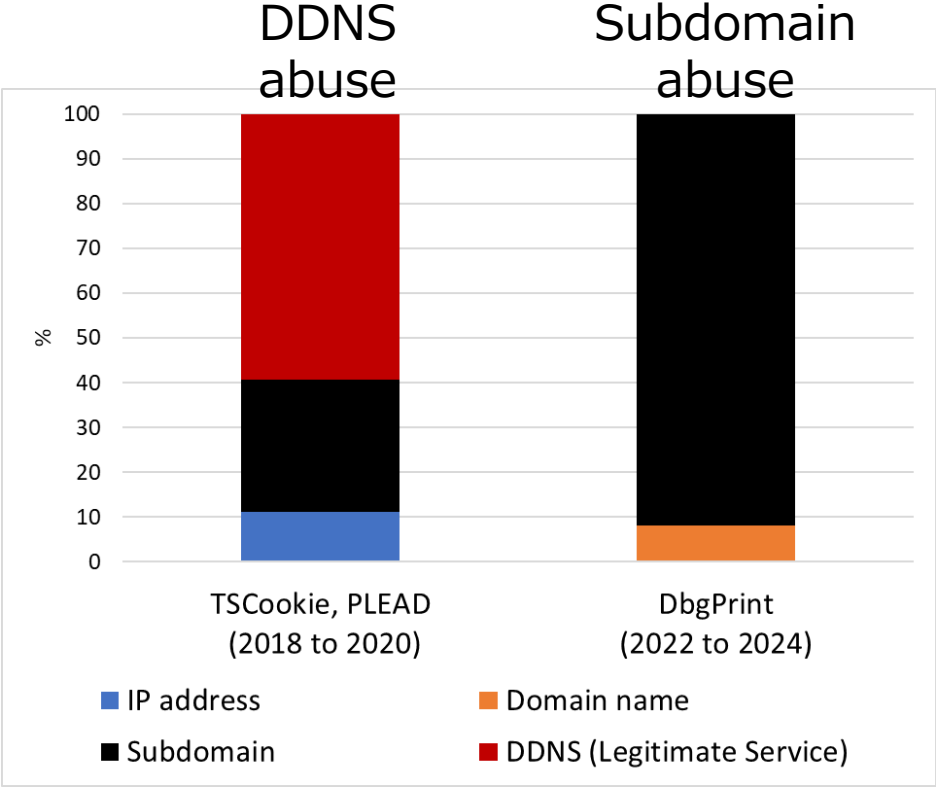
Blogs by Trend Micro on Apr. 11 and May 16

Types of subdomain abuse

- Dynamic DNS abuse or strategically aged domains
- Reused parent domains
- Fake dormant or fake response

Dynamic DNS Abuse or Domain Registration

FUJITSU

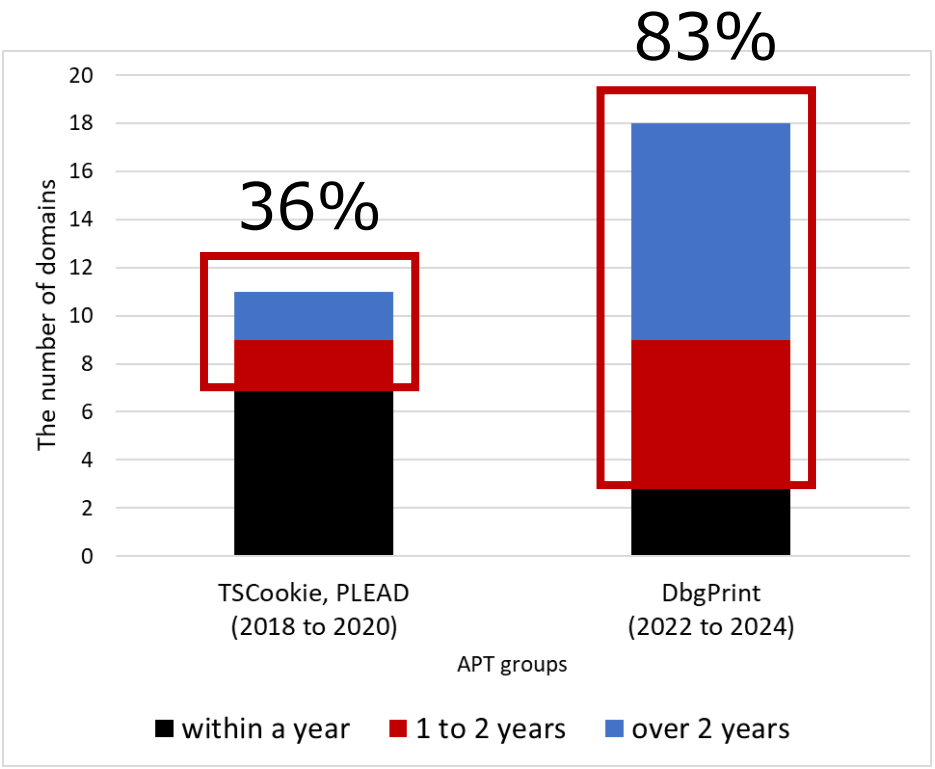


- TSCookie, PLEAD
  - around 60%: DDNS services
- DbgPrint
  - around 90%: subdomain abuse
  - BlackTech registered parent domains

DDNS abuse

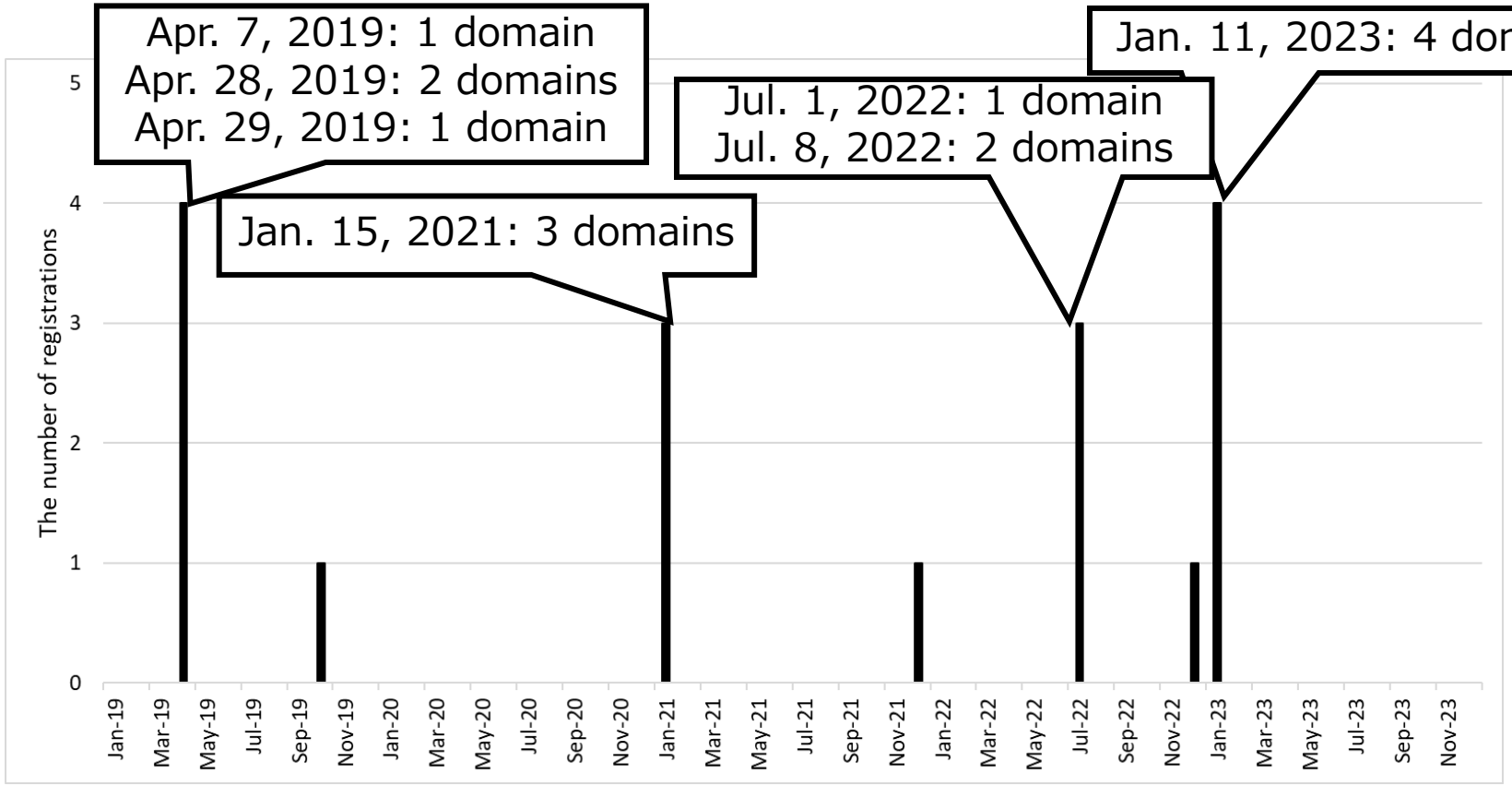
-> Subdomain abuse

Strategically Aged Domains



- TSCookie, PLEAD
  - 36%: over a year after registration
- DbgPrint
  - 83%: over a year after registration
- **Strategic registrations of several domains since 2019**

Strategic Registrations by BlackTech



TSCookie: Reused Parent Domains

FUJITSU

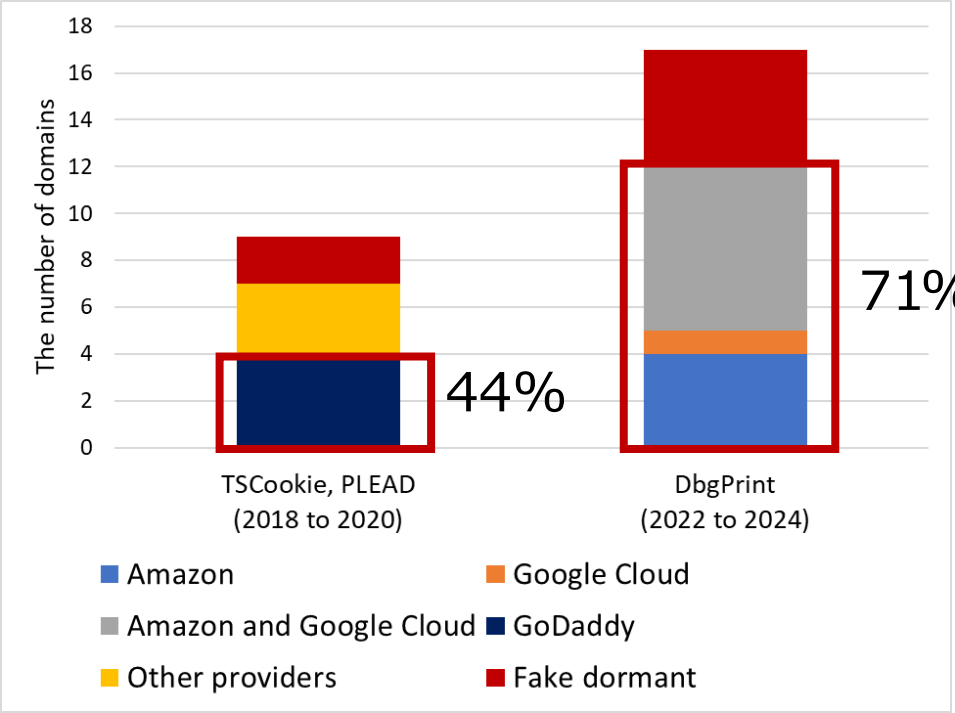
Domain	Registration	First reuse	Second reuse
bookmayae.com	2017/9/7	2018/4/25 pyc.bookmayae.com tssko.bookmayae.com	
androiddatacenter.com	2017/11/16	2018/4/25 exchange.androiddatacenter.com iphone.androiddatacenter.com	2018/10/30 fashion.androiddatacenter.com
panasocin.com	2018/1/23	2018/4/25 office.panasocin.com	2019/10/23 update.panasocin.com

DbgPrint (Deuterbear): Reused Parent Domains

FUJITSU

Domain	Registration	First reuse	Second reuse	Third reuse
lsoeman.com	Apr. 7, 2019	3 (Sep. 15, 2023)		
damienjohn.com	Apr. 28, 2019	2 (Sep. 15, 2023)		
rosetoo.com	Apr. 29, 2019	domain (Feb. 4, 2022)	1 (Sep. 15, 2023)	
taishanlaw.com	Oct. 25, 2019	1 (Sep. 15, 2023)	1 (Apr. 11, 2024)	
randaln.com	Jan. 15, 2021	2 (Jun. 17, 2022)	1 (Sep. 15, 2023)	
bakhell.com	Jan. 15, 2021	1 (Nov. 30, 2023)	1 (Apr. 11, 2024)	
availitond.com	Jul. 1, 2022	1 (Nov. 30, 2023)	3 + domain (Jan. 12, 2024)	
operatida.com	Jul. 8, 2022	1 (Aug. 24, 2023)	1 (Nov. 30, 2023)	
quadrantbd.com	Jan. 10, 2023	4 (Nov. 30, 2023)	2 (Jan. 26, 2024)	2 (Apr. 11, 2024)
rchitecture.org	Jan. 11, 2023	1 (Nov. 30, 2023)	1 (Apr. 11, 2024)	
gelatosg.com	Jan. 11, 2023	2 (Apr. 11, 2024)		

Fake Dormant or Fake Response



- TSCookie, PLEAD
  - Fake dormant: 22%
  - Fake response (GoDaddy): 44%
- DbgPrint
  - Fake dormant (Sep. 15, 2023): 29%
  - Fake response (Nov. 30, 2023, Jan. 12, 26, 2024, AWS or Google Cloud): 71%

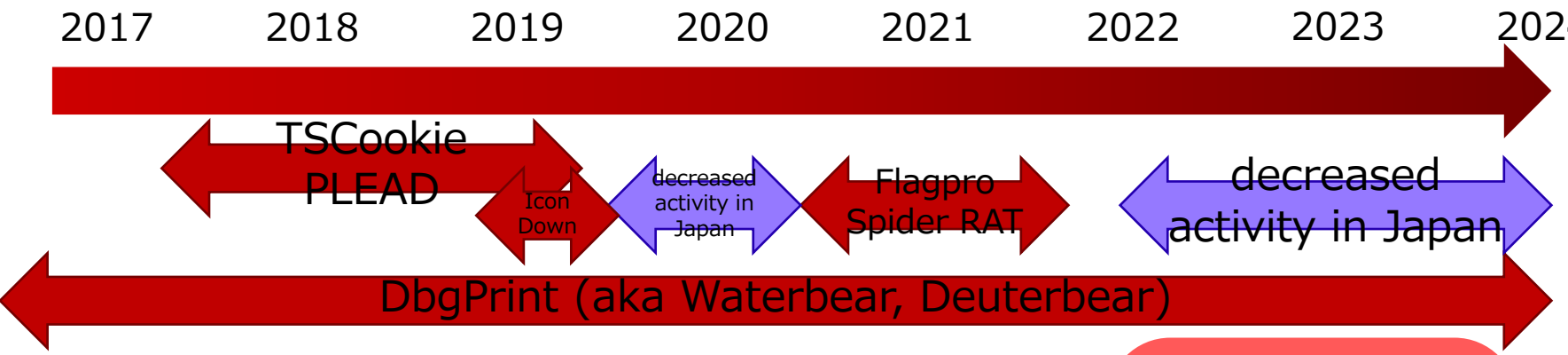
Single Target and Fake Dormant vs Multiple Targets and Fake Response

FUJITSU

Domain	Registration	Reuse Single or multiple	Fake dormant or fake response	The number of malicious in VirusTotal (on Jul. 8)
lsoeman.com	Apr. 7, 2019	Single	Fake dormant	0
damienjohn.com	Apr. 28, 2019	Single	Fake dormant	0
rosetoo.com	Apr. 29, 2019	Multiple	Fake dormant	1
taishanlaw.com	Oct. 25, 2019	Multiple	Fake response	11
randaln.com	Jan. 15, 2021	Multiple	Fake response	11
bakhell.com	Jan. 15, 2021	Multiple	Fake dormant	15
availitond.com	Jul. 1, 2022	Multiple	Fake response	14
operatida.com	Jul. 8, 2022	Multiple	Fake response	15
quadrantbd.com	Jan. 10, 2023	Multiple	Fake response	13
rchitecture.org	Jan. 11, 2023	Multiple	Fake response	14
gelatosg.com	Jan. 11, 2023	Single	Fake response	13

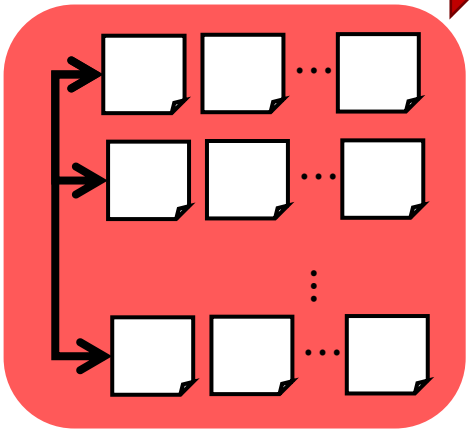
Comparison-Based Difference Detection

FUJITSU



Comparison-based difference detection
Ex. our CODE BLUE 2017 Day0 presentation

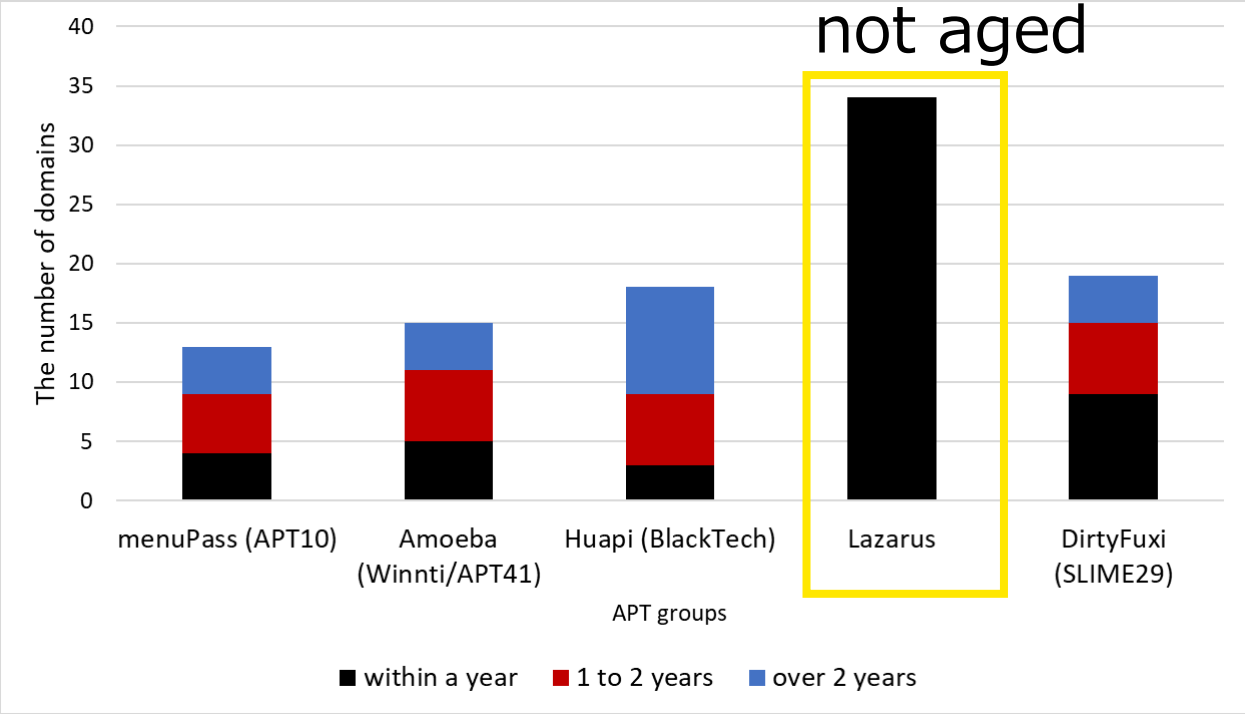
Majority (standard) or minority (original)



Flash reports from ThreatVision by TeamT5

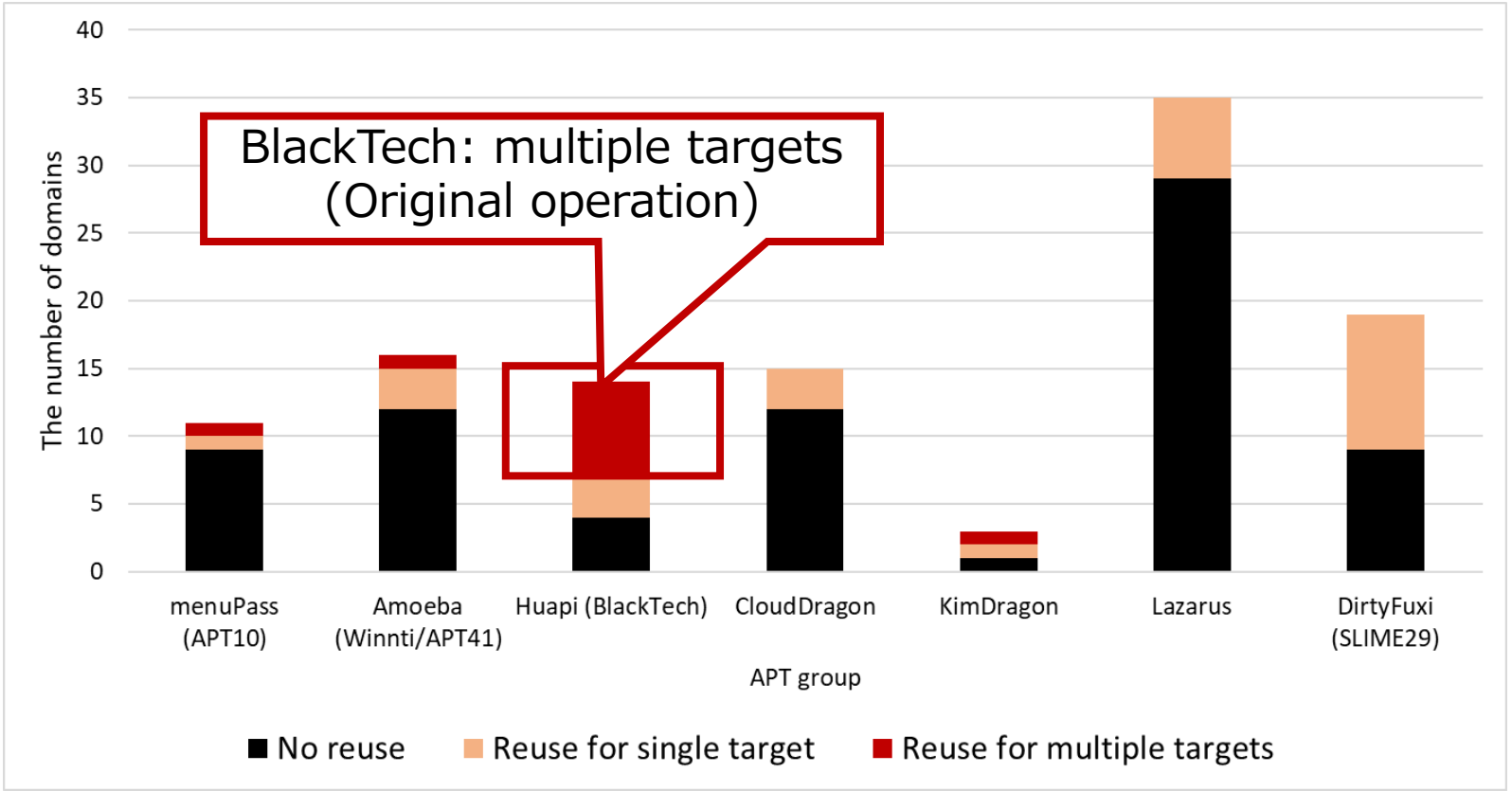
Original Operation by Lazarus

- Abused domains several months after registration
  - Out of scope: CloudDragon, KimDragon (legitimate service abuse)

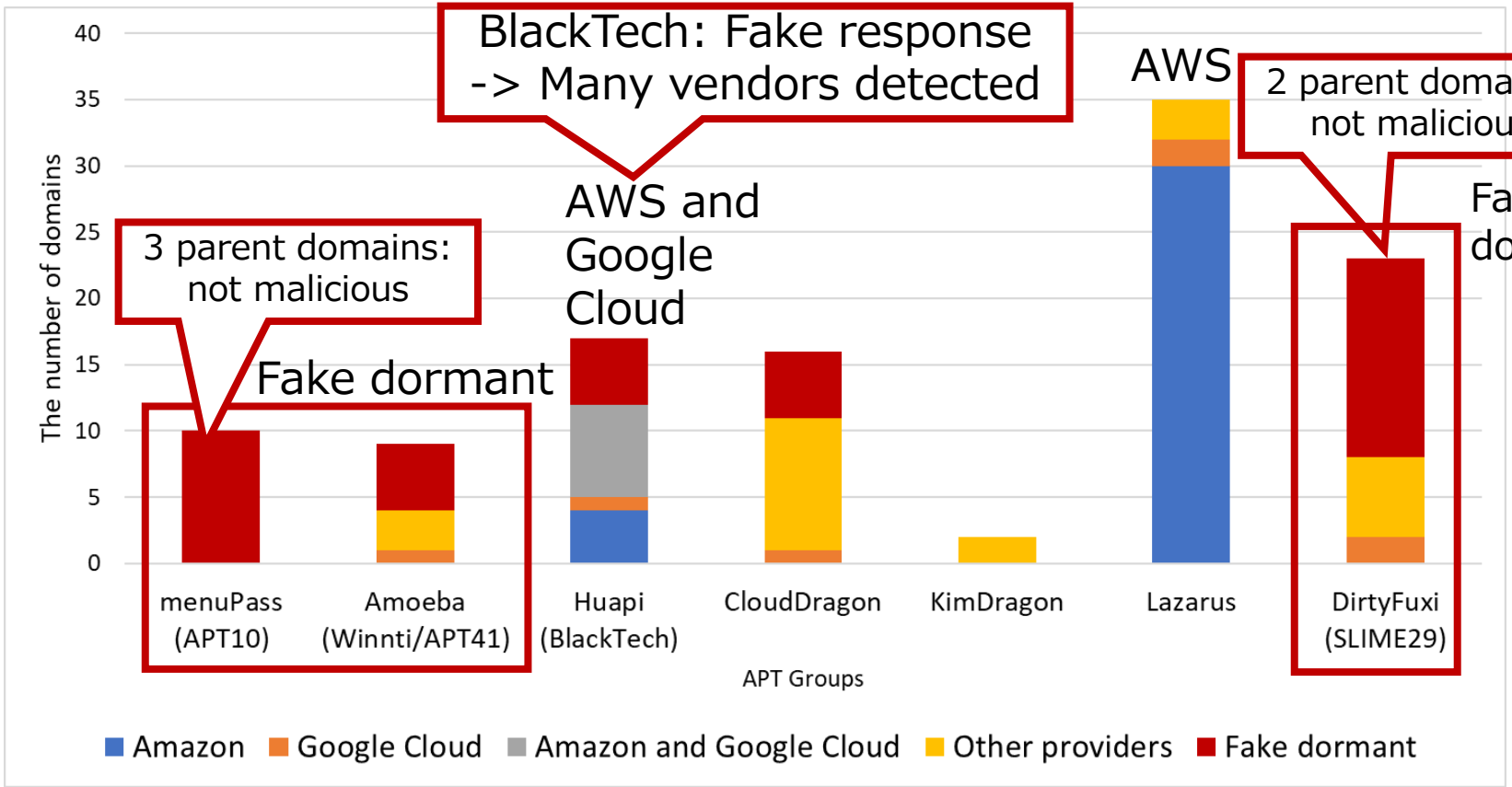


Original Operation by BlackTech
Reused Parent Domains for Multiple Targets

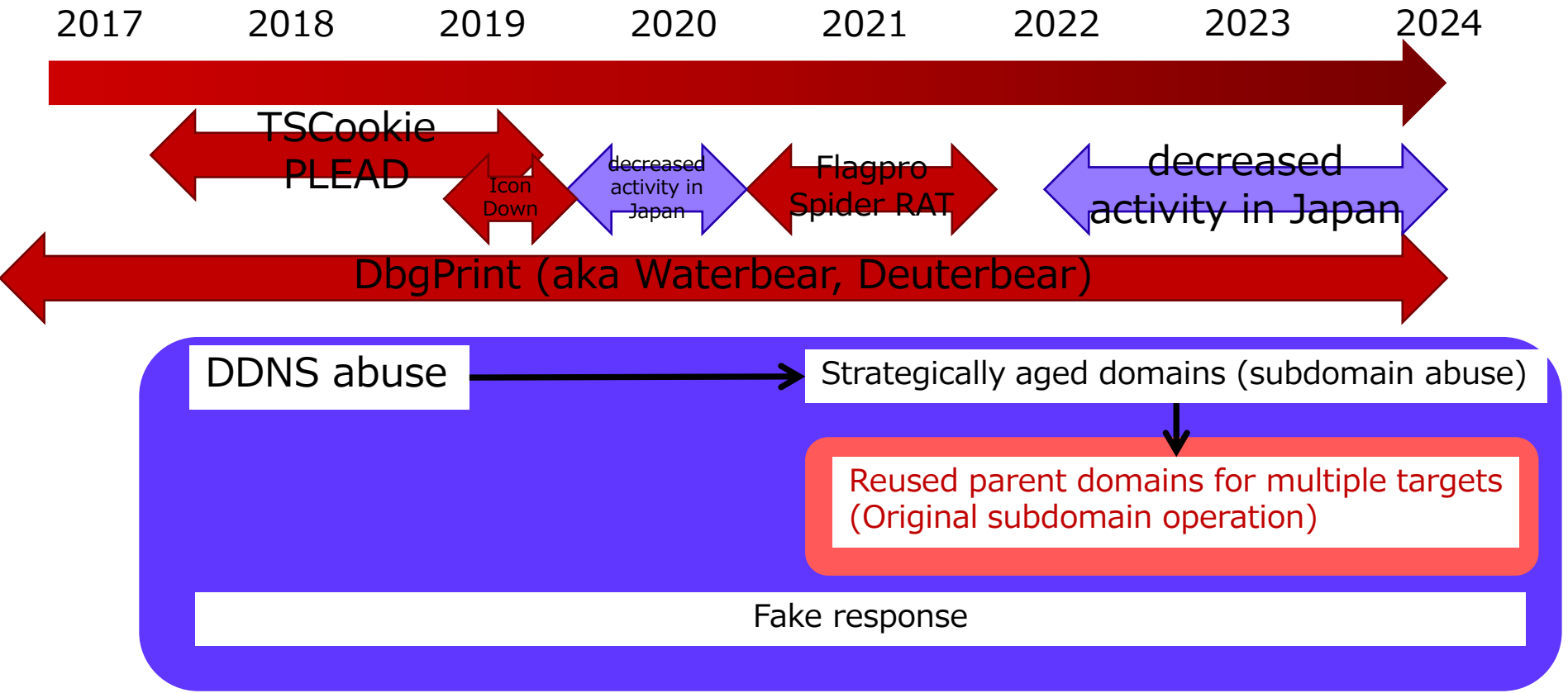
FUJITSU



Fake Dormant or Fake Response

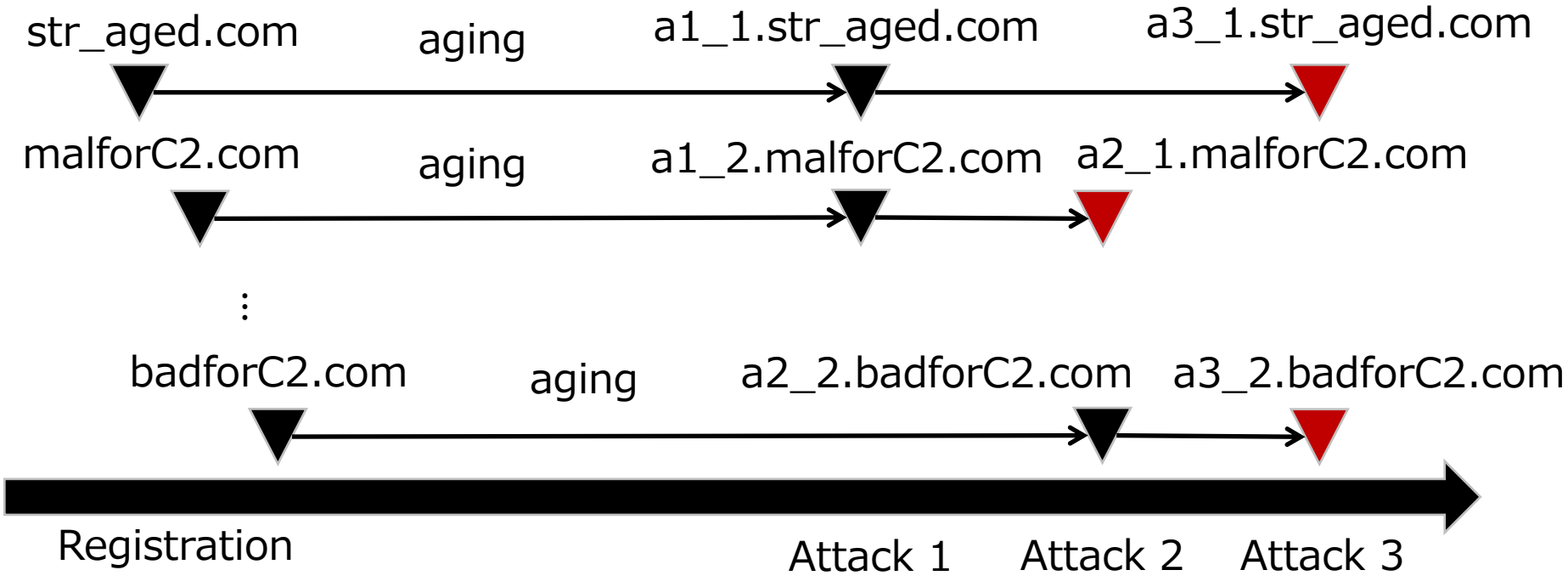


Did Subdomain Abuse by BlackTech “Evolve”?



Original Subdomain Abuse by BlackTech

FUJITSU



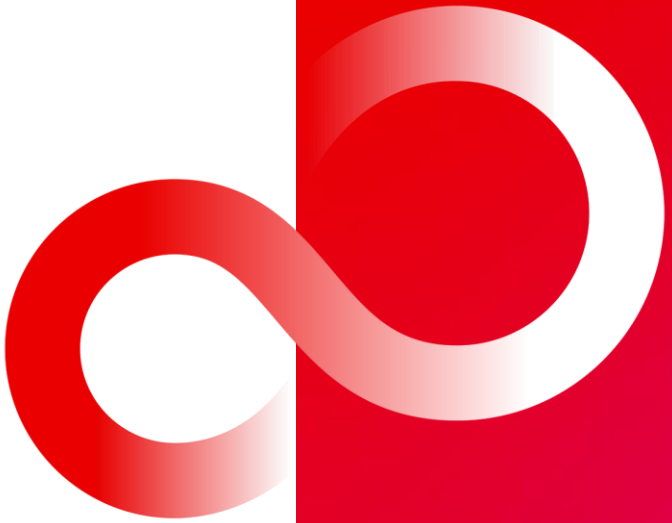
Multiple targets for reused parent domains

Summary

FUJITSU

- The starting point: Did subdomain abuse by BlackTech "evolve"?
- RAT tools: **evolution**
  - Waterbear → Deuterbear
- DNS abuse: **strategic change + original operation**
  - Not evolution for detection evasion
  - Original subdomain abuse: reused parent domains for multiple targets
  - Efficiency of constructing attack infrastructure to utilize strategically aged domains
- Defenders got a chance of detection

Thank you



Blogs by JPCERT/CC: TSCookie, PLEAD, IconDown

FUJITSU

- 2018年1月の文科省なりすましメールについてまとめてみた, piyolog
  - https://piyolog.hatenadiary.jp/entry/20180119/1516391079
- 2018/3/1 プラグインをダウンロードして実行するマルウエアTSCookie (JPCERT, 26 domains)
  - https://blogs.jpcert.or.jp/ja/2018/03/tscookie.html
- 2018/4/25 攻撃者グループ “BlackTech”による “PLEAD”を使った日本への攻撃を確認 (ラックピープル, 9 domains)
  - https://www.lac.co.jp/lacwatch/people/20180425_001625.html
- 2018/5/28 攻撃グループBlackTechが使うマルウエアPLEADダウンローダ (JPCERT, 4 domains)
  - https://blogs.jpcert.or.jp/ja/2018/05/linopid.html
- 2018/10/30 マルウエアTSCookieの設定情報を正常に読み込めないバグ (JPCERT, 4 domains)
  - https://blogs.jpcert.or.jp/ja/2018/10/tscookie-1.html
- 2019/5/28 マルウエアTSCookieの設定情報を正常に読み込めないバグ（続報）(JPCERT, 3 domains)
  - https://blogs.jpcert.or.jp/ja/2019/05/tscookie-2.html
- 2019/9/3 攻撃グループBlackTechが侵入後に使用するマルウエア
  - https://blogs.jpcert.or.jp/ja/2019/09/tscookie_loader.html
- 2019/10/23 攻撃グループBlackTechが使うダウンローダIconDown, (JPCERT, 1 domain)
  - https://blogs.jpcert.or.jp/ja/2019/10/IconDown.html
- 2020/2/26 攻撃グループBlackTech が使用するLinux用マルウエア (ELF_TSCookie) (JPCERT, 2 domains)
  - https://blogs.jpcert.or.jp/ja/2020/02/elf_tscookie.html
- 2020/11/10 攻撃グループBlackTechが使用するLinux版マルウェア（ELF_PLEAD）(JPCERT, 1 domain)
  - https://blogs.jpcert.or.jp/ja/2020/11/elf_plead.html

DbgPrint, Waterbear, Deuterbear

FUJITSU

- Evil Hidden in Shellcode: The Evolution of Malware DBGPRINT
  - https://blogs.jpcert.or.jp/ja/2020/02/japan-security-analyst-conference-2020-1.html
- Exposing the Sophisticated Cyber Espionage Tool Known as BendyBear
  - https://www.paloaltonetworks.com/blog/2021/02/u42-bendybear/
- Cyberespionage Group Earth Hundun's Continuous Refinement of Waterbear and Deuterbear
  - https://www.trendmicro.com/en_ph/research/24/d/earth-hundun-waterbear-deuterbear.html
- Tracking the Progression of Earth Hundun's Cyberespionage Campaign in 2024
  - https://www.trendmicro.com/en_us/research/24/e/earth-hundun-2.html