Executing RATs in a Long-Term Observable Customized Online Sandbox

National Institute of Information and Communications Technology
Cyber Security Laboratory
Shohei Hiruta, Yuki Umemura, Masaki Kubo, Nobuyuki Kanaya,
And Takahiro Kasama

CYNEX
CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

Agenda

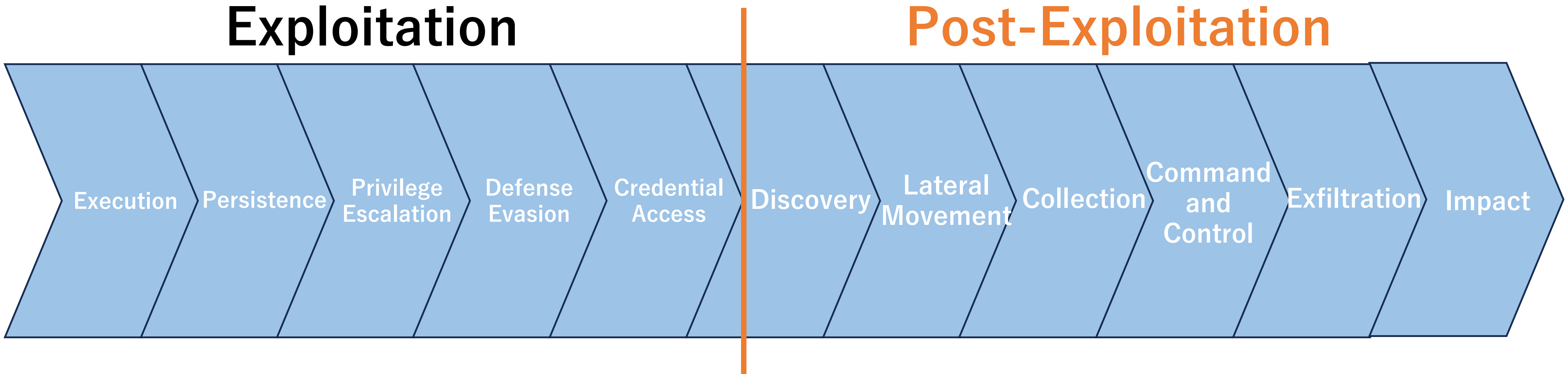
- Background: Collection of Post-Exploitation Artifacts
- STARDUST
  - Analysis Platform for Long-term Observation of Post-Exploitation
  - Collectible Artifacts
- Long-term Observation Results of RATs
  - Dataset
  - Observation Results
    - Post-Exploitation and Its Artifacts for Each RAT
    - Summary of C2 Communications
    - Details of Post-Exploitation
  - Logs Effective for Understanding Post-Exploitation
- Conclusion

Background

Background: Collection of Post-Exploitation Artifacts

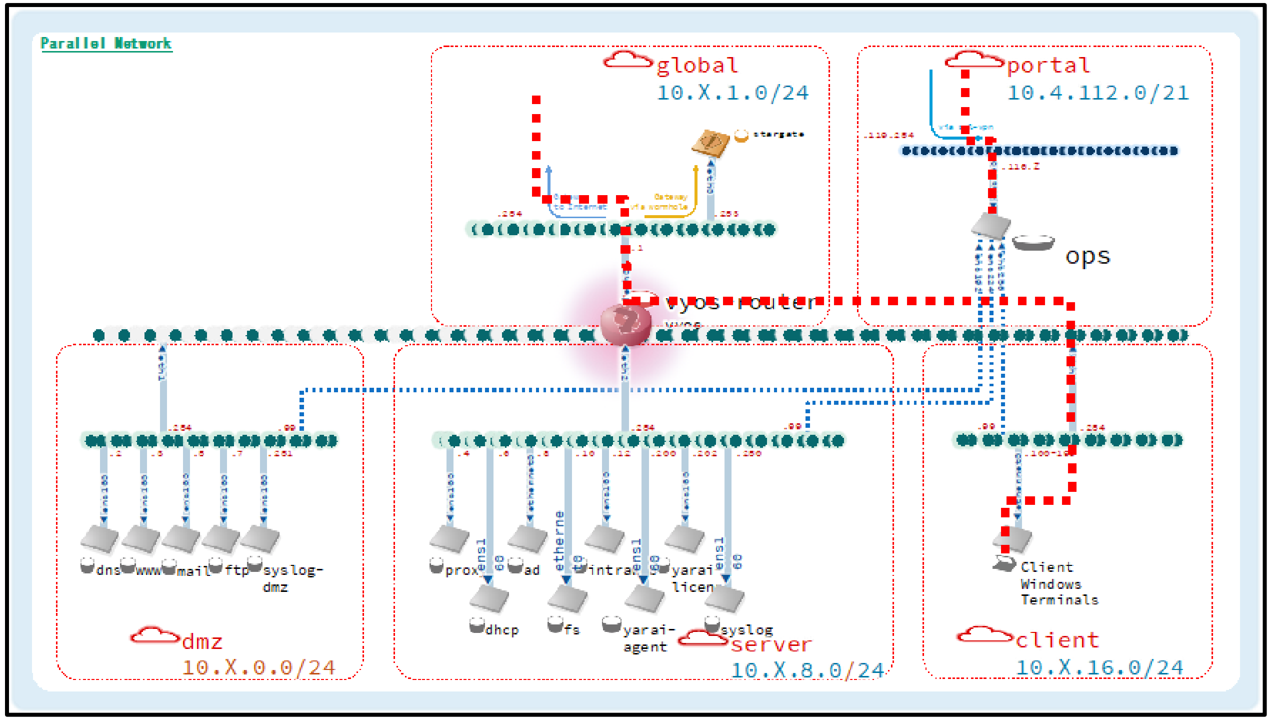
- Information obtained by running a RAT in a sandbox is limited to Exploitation

- In incident response and threat hunting, threat intelligence on the Post-Exploitation is also important
  - Downloading of additional malware
  - Lateral movement within the network



Approach

- Development and operation of a Platform (**STARDUST**) for observing Post-Exploitation
  - **Pre-built simulated ICT environment**
    - Active Directory environment consisting of multiple hosts
  - **No execution time limits**
  - **On-demand** log collection available



Take Away

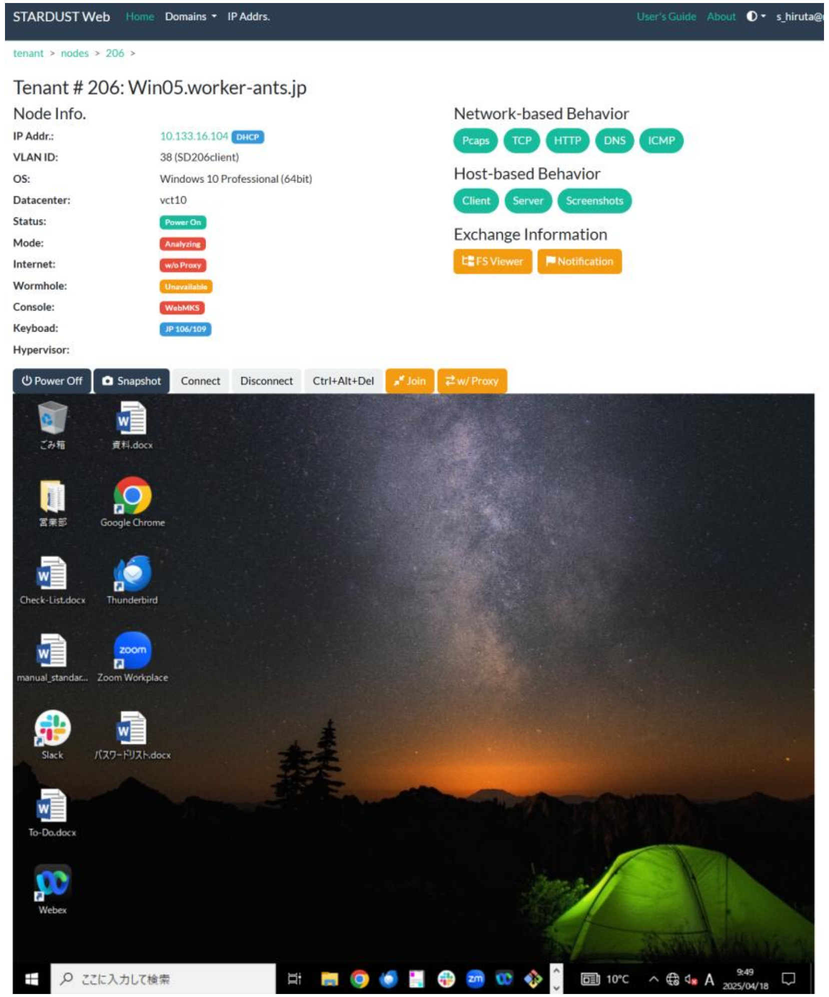
- Introducing results obtained from long-term observation of a RAT using STARDUST
  - Post-Exploitation Tactics and Techniques
  - Artifacts
  - Total duration of C2 communication
  - Time until the first observation of Post-Exploitation

➡ **Sharing logs that were effective** in understanding Post-Exploitation

STARDUST

STARDUST

- A platform for long-term observation of Post-Exploitation activities
  - Constructing an ICT environment to deceive attackers
  - Implementing support functions for long-term observation



Tenant # 206: Win05.worker-ants.jp

Node Info.

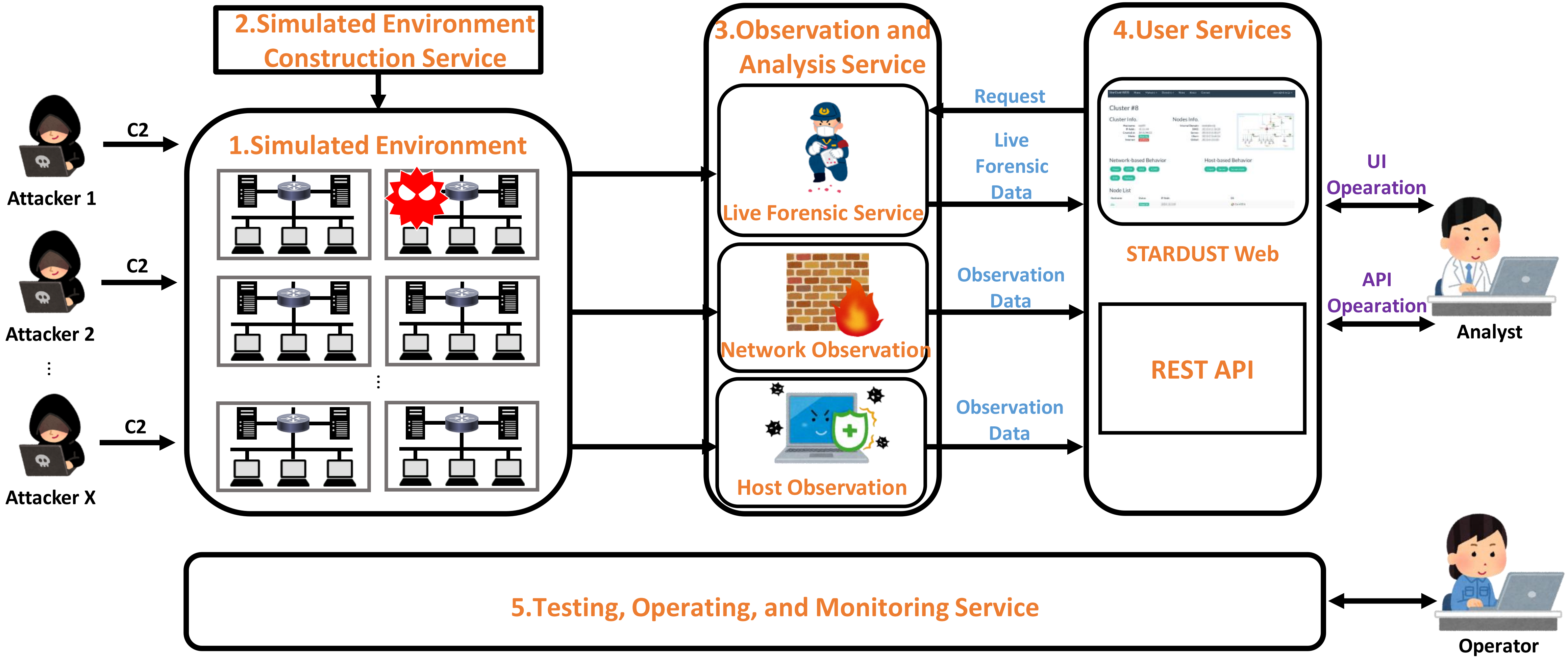
IP Addr.: 10.133.16.104 DHCP
VLAN ID: 38 (SD206client)
OS: Windows 10 Professional (64bit)
Datacenter: vct10
Status: Power On
Mode: Analyzing
Internet: w/o Proxy
Wormhole: Unavailable
Console: WebMKS
Keyboad: JP 106/109
Hypervisor:

Network-based Behavior

Host-based Behavior

Exchange Information

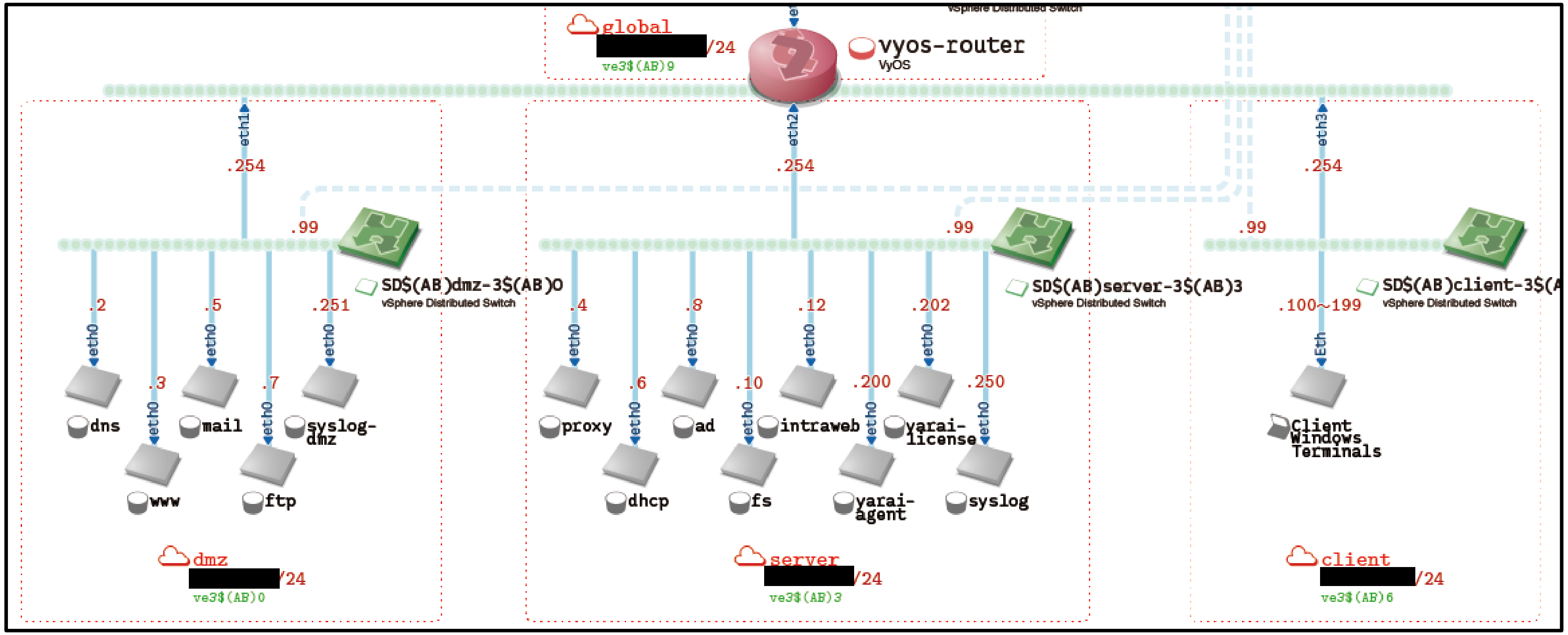
Overall view of STARDUST

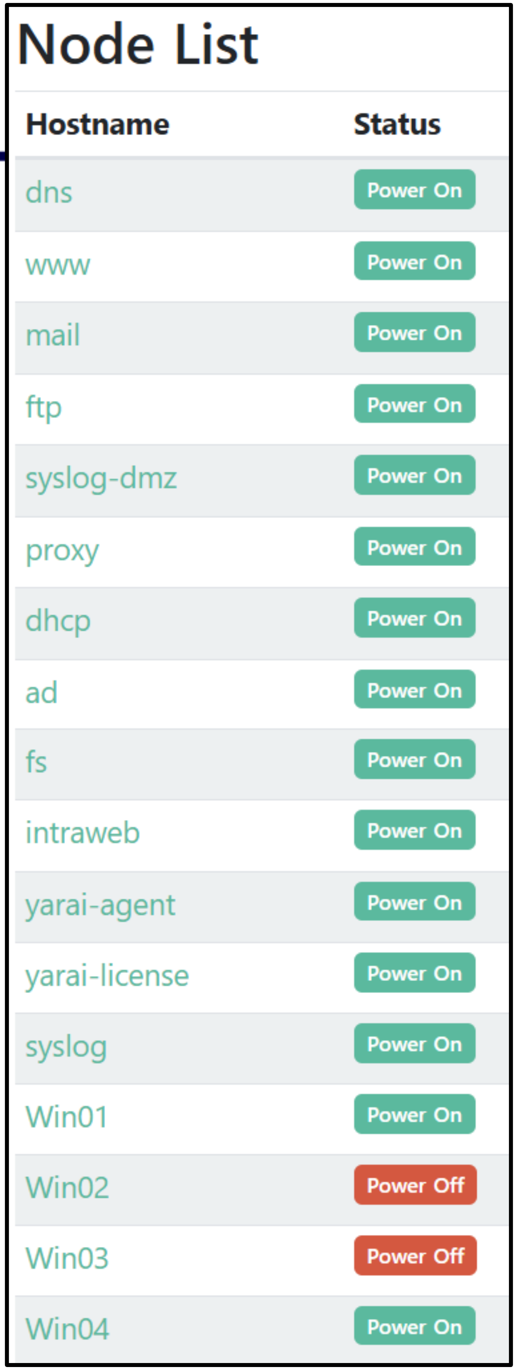


Simulated Environment

- Composed of multiple segments by default

➡ To observe lateral movement





Node List

Hostname	Status
dns	Power On
www	Power On
mail	Power On
ftp	Power On
syslog-dmz	Power On
proxy	Power On
dhcp	Power On
ad	Power On
fs	Power On
intraweb	Power On
yarai-agent	Power On
yarai-license	Power On
syslog	Power On
Win01	Power On
Win02	Power Off
Win03	Power Off
Win04	Power On

Artifacts Collectible with STARDUST

- Available on demand

Live Forensic Service	Host Observation
Windows Event Logs	Process information
Master File Table (MFT)	Screen shot
USN Journal	
Prefetch	
Registry	**Network Observation**
System Resource Usage Monitor (SRUM)	Pcap
Windows Management Instrumentation (WMI)	
Web Browsing History	
Process dump	

Feature List of STARDUST

Category	Functions
Live Forensic Service	File Upload and Download, Memory Dump, Registry Dump, URL-Specified Download, Process Information Retrieval, ArbitraryProgram Execution, TCP Tunneling, File System Sharing within the VM, Directory History Reconstruction within the VM
Event Monitoring & Notification	Network Communication Monitoring, Directory/File Creation, Modification, and Deletion Monitoring, Process Start and Termination Monitoring, Web Notifications and Slack Notifications
UI & Data Acquisition	Bulk Download, Artifact Collection from Virtual Disks, Video Generation from VM Console Screenshots, On-Screen Keyboard
Automation	Recording and Playback of VM Console Operations, Automatic Generation of Browser Browsing History, Automated Analysis of Malicious URLs, Automated Execution of Malware

Long-term Observation of RATs

Dataset

- RATs: 7 families, 41 samples
- Collection period: **May-October 2024 (6 months)**
- Source: **VirusTotal**
  - Collected using LiveHunt rules targeting samples uploaded from Japan
  - Only recently uploaded RATs were selected

➡ To increase the likelihood of connecting to C2 servers

Dataset

Family name	Samples	Tactic	Technique	
AsyncRAT	9	Command and Control	T1105	Ingress Tool Transfer
		Collection	T1056.001	Input Capture: Keylogging
			T1113	Screen Capture
			T1125	Video Capture
DCRat	2	Credential Access	T1555.003	Credentials from Password Stores: Credentails from Web Browsers
		Command and Control	T1105	Ingress Tool Transfer
		Collection	T1115	Clipboard Data
			T1056.001	Input Capture: Keylogging
			T1113	Screen Capture

Dataset

Family name	Samples	Tactic	Technique	
Gh0stRAT	4	Command and Control	T1105	Ingress Tool Transfer
		Collection	T1056.001	Input Capture: Keylogging
			T1113	Screen Capture
njRAT	1	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
		Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
		Command and Control	T1105	Ingress Tool Transfer
		Collection	T1005	Data from Local System
			T1056.001	Input Capture: Keylogging
			T1113	Screen Capture
			T1125	Video Capture
		Exfiltration	T1041	Exfiltration Over C2 Channel

Dataset

Family name	Samples	Tactic	Technique	
QuasarRAT	4	Execution	T1059.003	Command and Scripting: Interpreter Windows Command Shell
		Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
			T1552.001	Unsecured Credentials: Credentials in Files
		Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
		Command and Control	T1105	Ingress Tool Transfer
		Collection	T1005	Data from Local System
			T1056.001	Input Capture: Keylogging
RemcosRAT	19	Command and Control	T1105	Ingress Tool Transfer
		Collection	T1123	Audio Capture
			T1115	Clipboard Data
			T1056.001	Input Capture: Keylogging
			T1113	Screen Capture
			T1125	Video Capture
StrRat	2	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
		Command and Control	T1105	Ingress Tool Transfer
		Collection	T1056.001	Input Capture: Keylogging

Observation Conditions

- OS: **Windows 10**
- Windows Defender: **OFF**
- Execution Privileges: **Administrators** (Right-click → Run as administrator)
- Observation Time: **Japanese office hours**
- Observation Duration: **Until the RAT stops connecting to its C2 server**

Observation Results

- RATs that connected to C2 servers: 14 samples
- RATs that post-exploitation was observed: 10 samples
- Techniques used during post-exploitation: 14 techniques
- Total C2 connection duration:
  - Max: 293 hours 45 minutes (35 days)
  - Min: 3 hours 15 minutes (1 day)
- Time until first observed post-exploitation activity:
  - Max: 25 hours 23 minutes (2 days)
  - Min: 1 minute

Observation Results

■ Reported
🟥 Unreported

Family name	Samples	Samples that connected to C2	Samples in which post-exploitaton was observed	Observed Tactics	Observed Techniques		Artifacts
AsyncRAT	9	2	1	Command and Control	T1105	Ingress Tool Transfer	Process information Pcap
				Collection	T1056.001	Input Capture: Keylogging	
					T1113	Screen Capture	
					T1125	Video Capture	
DCRat	2	2	2	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	MFT Prefetch Process information Pcap
				Discovery	T1082	System Information Discovery	
					T1518	Software Discovery	
				Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1115	Clipboard Data	
					T1056.001	Input Capture: Keylogging	
					T1113	Screen Capture	
					T1005	Data from Local System	
					T1560	Archive Collected Data	
				Exfiltration	T1041	Exfiltration Over C2 Channel	

Observation Results

⬛ Reported
🟥 Unreported

Family name	Samples	Samples that connected to C2	Samples in which post-exploitaton was observed	Observed Tactics	Observed Techniques		Artifacts
Gh0stRAT	4	**0**	**0**	Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1056.001	Input Capture: Keylogging	
					T1113	Screen Capture	
njRAT	1	**0**	**0**	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	
				Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	
				Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1005	Data from Local System	
					T1056.001	Input Capture: Keylogging	
					T1113	Screen Capture	
					T1125	Video Capture	
				Exfiltration	T1041	Exfiltration Over C2 Channel	

Observation Results

■ Reported
🟥 Unreported

Family name	Samples	Samples that connected to C2	Samples in which post-exploitaton was observed	Observed Tactics	Observed Technique		Artifacts
QuasarRAT	4	1	1	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Windows Event Log MFT Prefetch Process information Pcap
					T1552.001	Unsecured Credentials: Credentials in Files	
				Discovery	T1033	System Owner/User Discovery	
					T1046	Network Service Discovery	
				Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	
				Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1005	Data from Local System	
					T1056.001	Input Capture: Keylogging	
				Exfiltration	T1041	Exfiltration Over C2 Channel	
RemcosRAT	19	8	5	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	MFT Prefetch Process dump Process information Pcap
				Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1123	Audio Capture	
					T1115	Clipboard Data	
					T1056.001	Input Capture: Keylogging	
					T1113	Screen Capture	
					T1125	Video Capture	
				Exfiltration	T1041	Exfiltration Over C2 Channel	
StrRat	2	1	1	Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Pcap
				Command and Control	T1105	Ingress Tool Transfer	
				Collection	T1056.001	Input Capture: Keylogging	
				Exfiltration	T1041	Exfiltration Over C2 Channel	

Observation Results

- Malware additionally downloaded

Family name	Samples	Observed Tactics	Observed Techniques		Artifacts
AgentTesla	3	Credential Access Exfiltration	T1555.003 T1048	Credentials from Password Stores: Credentials from Web Browsers Exfiltration Over Alternative Protocol	MFT Process information Pcap
Redline Stealer	1	Discovery Collection Exfiltration	T1217 T1113 T1041	Browser Information Discovery Screen Capture Exfiltration Over C2 Channel	Process information Pcap
AsyncRAT	2	Command and Control Exfiltration	T1105 T1041	Ingress Tool Transfer Exfiltration Over C2 Channel	MFT Prefetch Process information Pcap
Gh0stRAT	1	Discovery Exfiltration	T1010 T1041	Application Window Discovery Exfiltration Over C2 Channel	Process information Pcap

Summary of C2 Communications

Family name	C2	Destination Port	TLS
AsyncRAT #1	scar77747[.]duckdns[.]org	6606, 7707, 8808	TRUE
AsyncRAT #2	twart[.]myfirewall[.]org	14143	TRUE
DCRat #1	ca46476[.]tw1[.]ru	80	FALSE
DCRat #2	27[.]124[.]45[.]70	8848	TRUE
QuasarRAT	104[.]194[.]152[.]90	9762	TRUE
RemcosRAT #1	b64c611[.]ddnss[.]eu	3154	FALSE
RemcosRAT #2	eadzagba1[.]duckdns[.]org	4877	TRUE
RemcosRAT #3	magaji[.]duckdns[.]org	2404	FALSE
RemcosRAT #4	23[.]95[.]235[.]18	2557	TRUE
RemcosRAT #5	gabrielgarcia2014kua[.]duckdns[.]org	2404	FALSE
RemcosRAT #6	ramcxx[.]duckdns[.]org	50312	TRUE
RemcosRAT #7	cavps7[.]duckdns[.]org	1991	TRUE
RemcosRAT #8	teebro1800[.]dynamic-dns[.]net	2195	TRUE
StrRat	141[.]98[.]10[.]79	1500	FALSE

Summary of C2 Communications

Family name	Total Observation Days	Total C2 Connection Time	Time until First Observed Post-Exploitation	Total Post-Exploitation Activities
AsyncRAT #1	3	22h15m	-	-
AsyncRAT #2	7	53h40m	1h21m	3
DCRat #1	9	76h00m	1m	2
DCRat #2	35	293h45m	25h23m	5
QuasarRAT	3	23h44m	7h42m	6
RemcosRAT #1	11	94h20m	-	-
RemcosRAT #2	14	76h26m	1h6m	3
RemcosRAT #3	19	165h00m	12h28m	19
RemcosRAT #4	7	55h00m	4h6m	8
RemcosRAT #5	1	6h35m	-	-
RemcosRAT #6	4	32h30m	1h1m	6
RemcosRAT #7	1	3h15m	-	-
RemcosRAT #8	5	37h38m	3h6m	2
StrRat	1	4h37m	4h36m	1

Details of Observed Post-Exploitation Activities

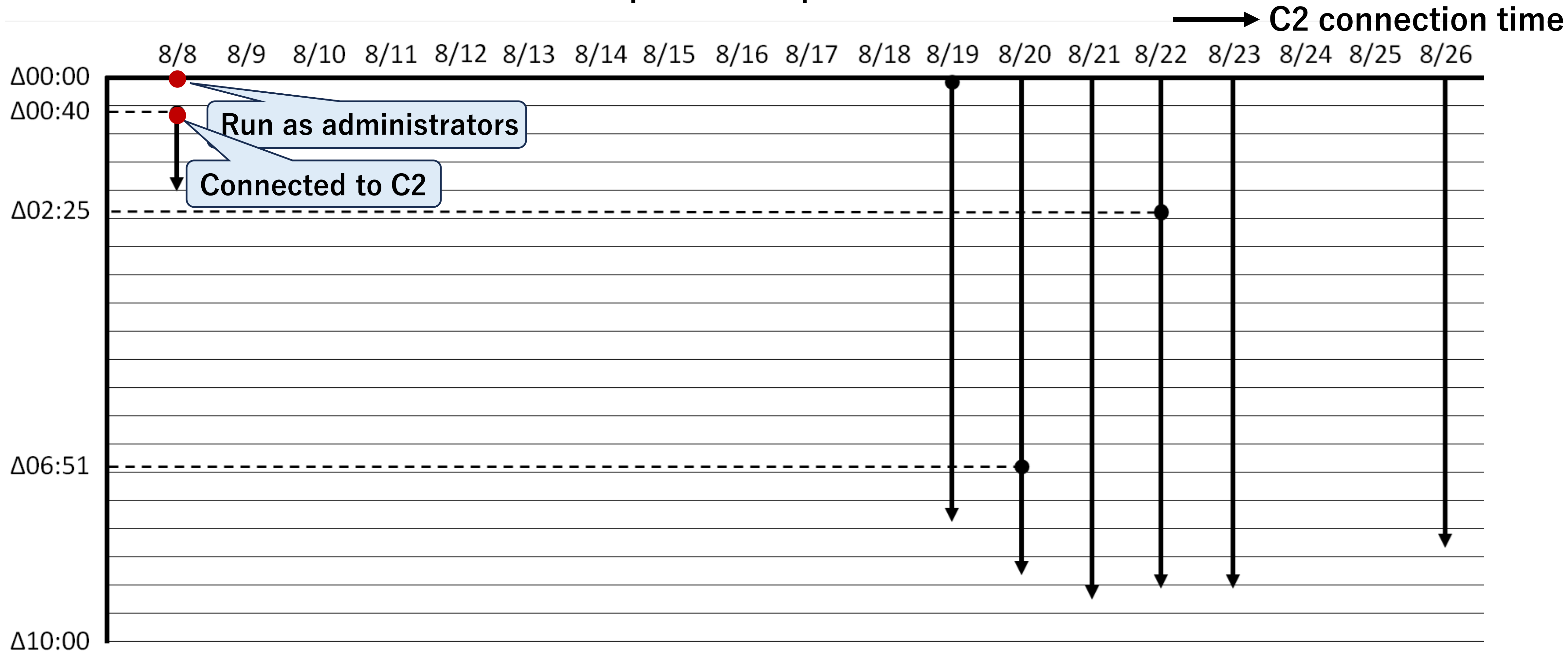
- Case 1: Execution of AgentTesla[1] via AsyncRAT
- Case 2: Execution of AsyncRAT and Gh0stRAT via DCRat
- Case 3: Execution of NirSoft WebBrowserPassView[2] via RemcosRAT to steal credentials from the infected device
- Case 4: Login to a Google account using stolen credentials via RemcosRAT

[1] AgentTesla: a type of InfoStealer

[2] NirSoft WebBrowserPassView: free software for recovering browser passwords

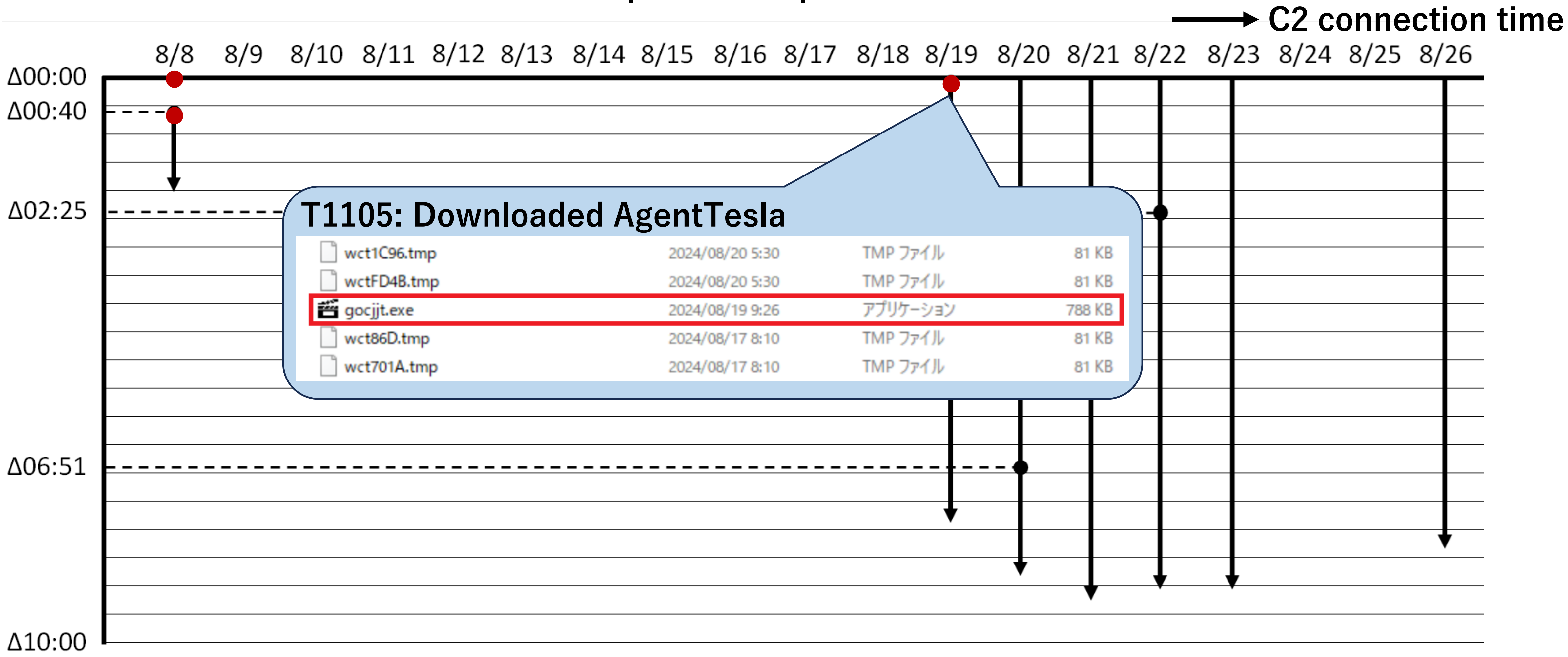
Case 1

- Total C2 connection time: 53 hours 40 minutes (7 days)
- Time until first observed post-exploitation: 1 hour 21 minutes



Case 1

- Total C2 connection time: 53 hours 40 minutes (7 days)
- Time until first observed post-exploitation: 1 hour 21 minutes

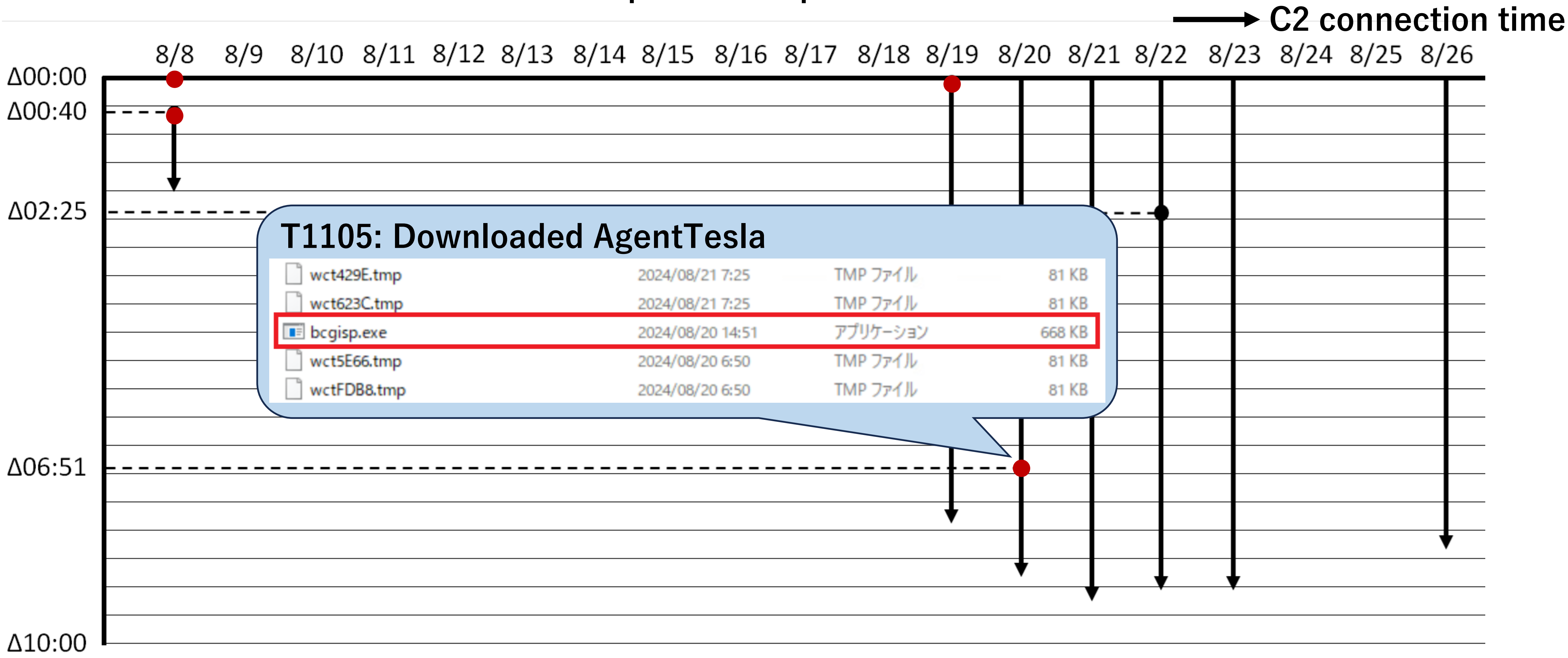


T1105: Downloaded AgentTesla

wct1C96.tmp	2024/08/20 5:30	TMP ファイル	81 KB
wctFD4B.tmp	2024/08/20 5:30	TMP ファイル	81 KB
gocjjt.exe	2024/08/19 9:26	アプリケーション	788 KB
wct86D.tmp	2024/08/17 8:10	TMP ファイル	81 KB
wct701A.tmp	2024/08/17 8:10	TMP ファイル	81 KB

Case 1

- Total C2 connection time: 53 hours 40 minutes (7 days)
- Time until first observed post-exploitation: 1 hour 21 minutes

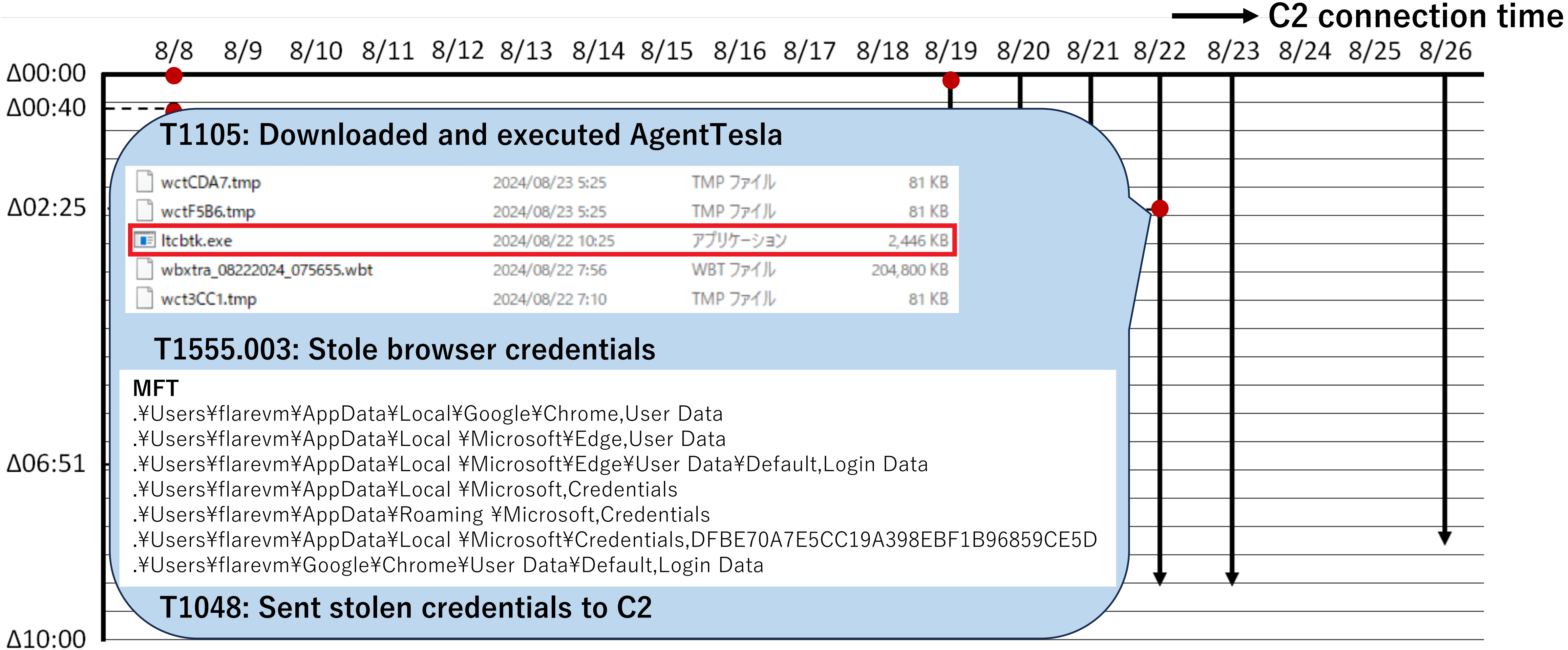


T1105: Downloaded AgentTesla

wct429E.tmp	2024/08/21 7:25	TMP ファイル	81 KB
wct623C.tmp	2024/08/21 7:25	TMP ファイル	81 KB
bcgisp.exe	2024/08/20 14:51	アプリケーション	668 KB
wct5E66.tmp	2024/08/20 6:50	TMP ファイル	81 KB
wctFDB8.tmp	2024/08/20 6:50	TMP ファイル	81 KB

Case 1

- Total C2 connection time: 53 hours 40 minutes (7 days)
- Time until first observed post-exploitation: 1 hour 21 minutes



T1105: Downloaded and executed AgentTesla

wctCDA7.tmp	2024/08/23 5:25	TMP ファイル	81 KB
wctF5B6.tmp	2024/08/23 5:25	TMP ファイル	81 KB
ltcbtk.exe	2024/08/22 10:25	アプリケーション	2,446 KB
wbxtra_08222024_075655.wbt	2024/08/22 7:56	WBT ファイル	204,800 KB
wct3CC1.tmp	2024/08/22 7:10	TMP ファイル	81 KB

T1555.003: Stole browser credentials

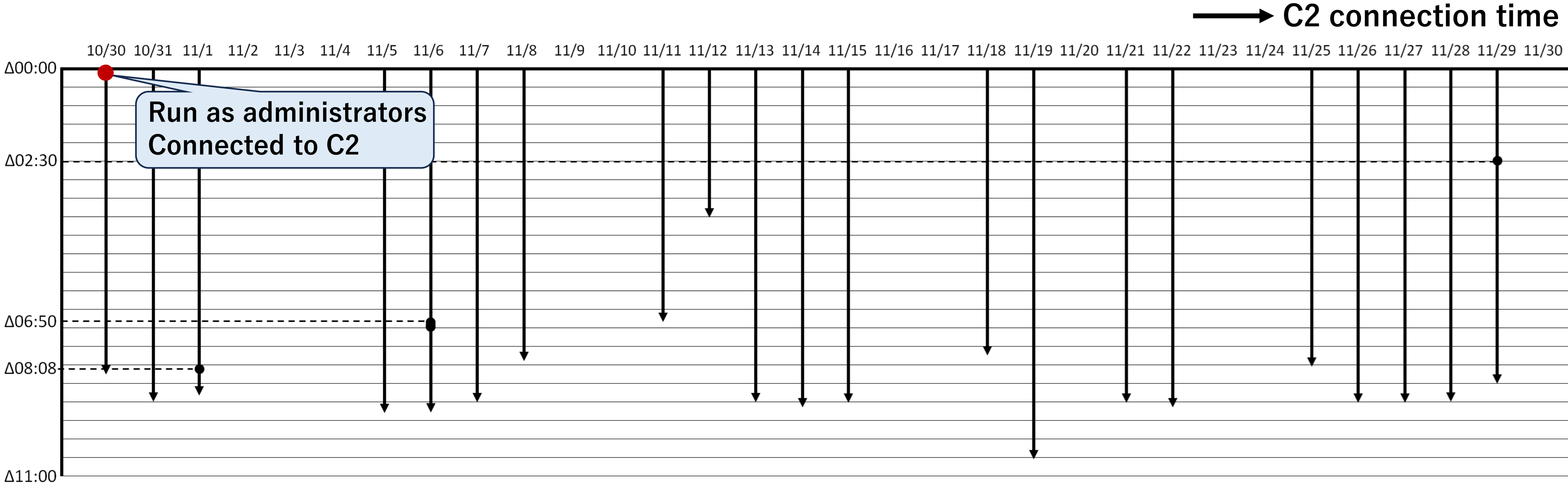
MFT

```
.¥Users¥flarevm¥AppData¥Local¥Google¥Chrome,User Data
.¥Users¥flarevm¥AppData¥Local ¥Microsoft¥Edge,User Data
.¥Users¥flarevm¥AppData¥Local ¥Microsoft¥Edge¥User Data¥Default,Login Data
.¥Users¥flarevm¥AppData¥Local ¥Microsoft,Credentials
.¥Users¥flarevm¥AppData¥Roaming ¥Microsoft,Credentials
.¥Users¥flarevm¥AppData¥Local ¥Microsoft¥Credentials,DFBE70A7E5CC19A398EBF1B96859CE5D
.¥Users¥flarevm¥Google¥Chrome¥User Data¥Default,Login Data
```

T1048: Sent stolen credentials to C2

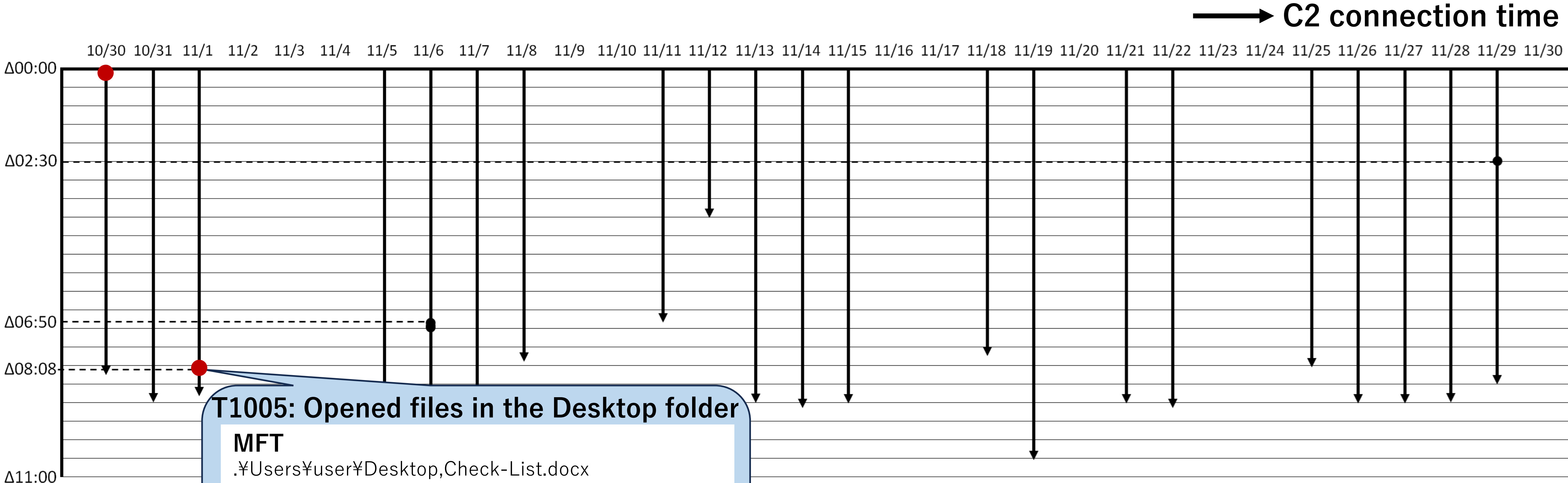
Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes



Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes

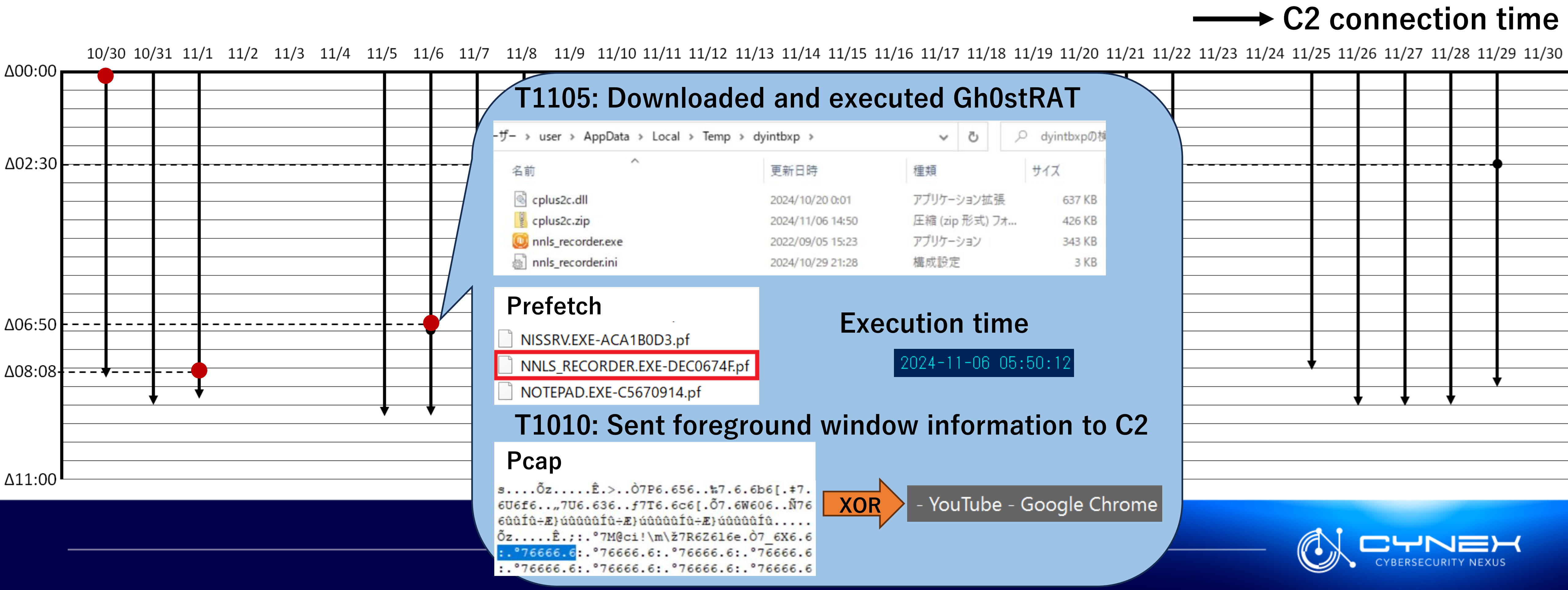


T1005: Opened files in the Desktop folder

MFT
.¥Users¥user¥Desktop,Check-List.docx
.¥Users¥user¥Desktop,manual_standard.docx
.¥Users¥user¥Desktop,To-Do.docx
.¥Users¥user¥Desktop,パスワードリスト.docx (PW)
.¥Users¥user¥Desktop,資料.docx

Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes



T1105: Downloaded and executed Gh0stRAT

-ザ- › user › AppData › Local › Temp › dyintbxp ›

名前	更新日時	種類	サイズ
cplus2c.dll	2024/10/20 0:01	アプリケーション拡張	637 KB
cplus2c.zip	2024/11/06 14:50	圧縮 (zip 形式) フォ...	426 KB
nnls_recorder.exe	2022/09/05 15:23	アプリケーション	343 KB
nnls_recorder.ini	2024/10/29 21:28	構成設定	3 KB

Prefetch

NISSRV.EXE-ACA1B0D3.pf
NNLS_RECORDER.EXE-DEC0674F.pf
NOTEPAD.EXE-C5670914.pf

Execution time

2024-11-06 05:50:12

T1010: Sent foreground window information to C2

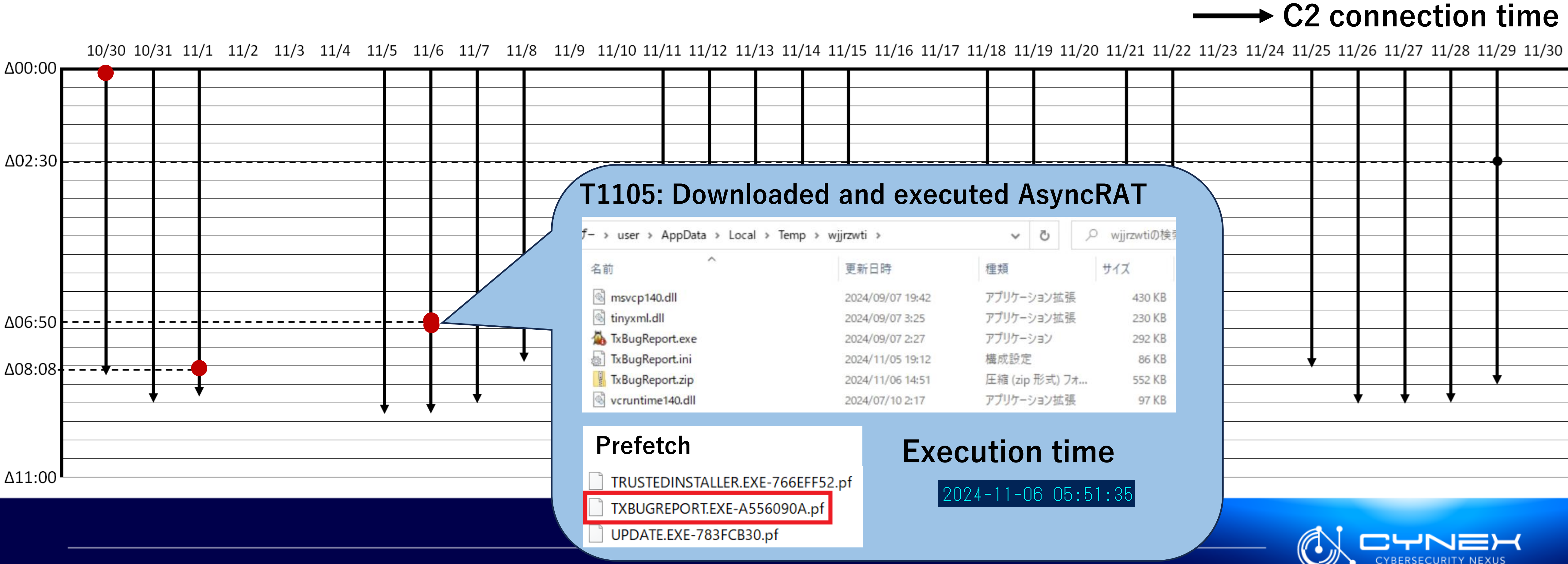
Pcap

```
s....Õz.....Ê.>..Ò7P6.656..‰7.6.6b6[.‡7.
6U6f6..„7U6.636..ƒ7T6.6c6[.Õ7.6W606..Ñ76
6ûûÍû÷Æ}úûûûûÍû÷Æ}úûûûûÍû÷Æ}úûûûûÍû.....
Õz.....Ê.;:.°7M@ci!\m\ž7R6Z616e.Ò7_6X6.6
:.°76666.6:.°76666.6:.°76666.6:.°76666.6
:.°76666.6:.°76666.6:.°76666.6:.°76666.6
```

XOR → - YouTube - Google Chrome

Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes



T1105: Downloaded and executed AsyncRAT

ﾃﾞｰ › user › AppData › Local › Temp › wjjrzwti ›

名前	更新日時	種類	サイズ
msvcp140.dll	2024/09/07 19:42	アプリケーション拡張	430 KB
tinyxml.dll	2024/09/07 3:25	アプリケーション拡張	230 KB
TxBugReport.exe	2024/09/07 2:27	アプリケーション	292 KB
TxBugReport.ini	2024/11/05 19:12	構成設定	86 KB
TxBugReport.zip	2024/11/06 14:51	圧縮 (zip 形式) フォ...	552 KB
vcruntime140.dll	2024/07/10 2:17	アプリケーション拡張	97 KB

Prefetch

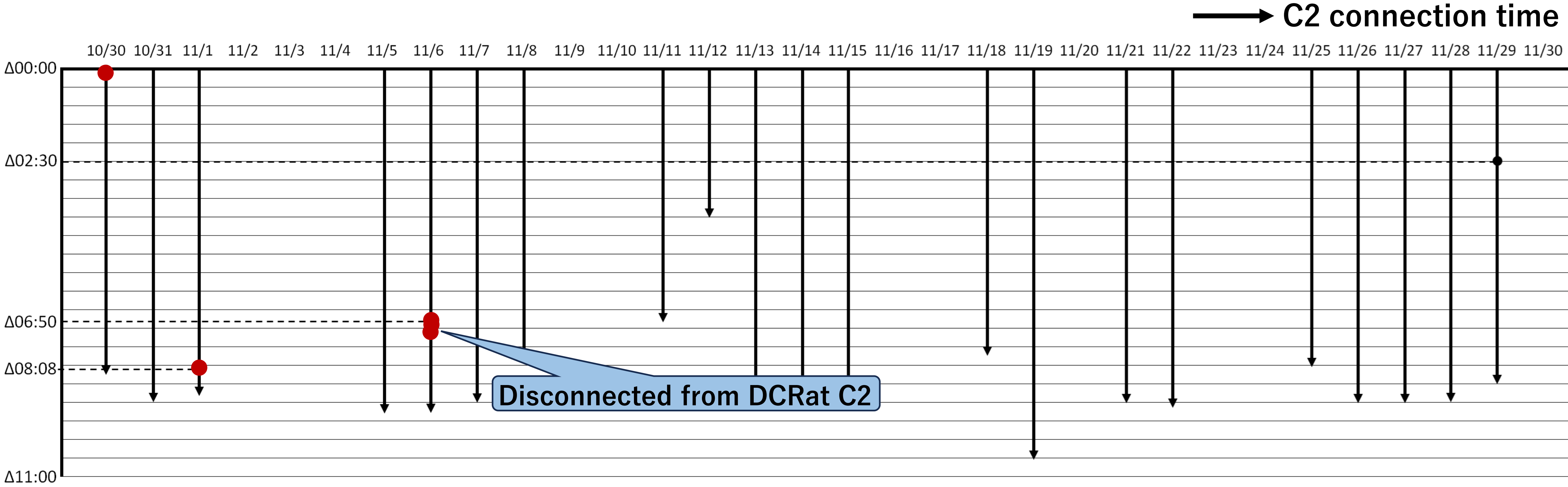
TRUSTEDINSTALLER.EXE-766EFF52.pf
TXBUGREPORT.EXE-A556090A.pf
UPDATE.EXE-783FCB30.pf

Execution time

2024-11-06 05:51:35

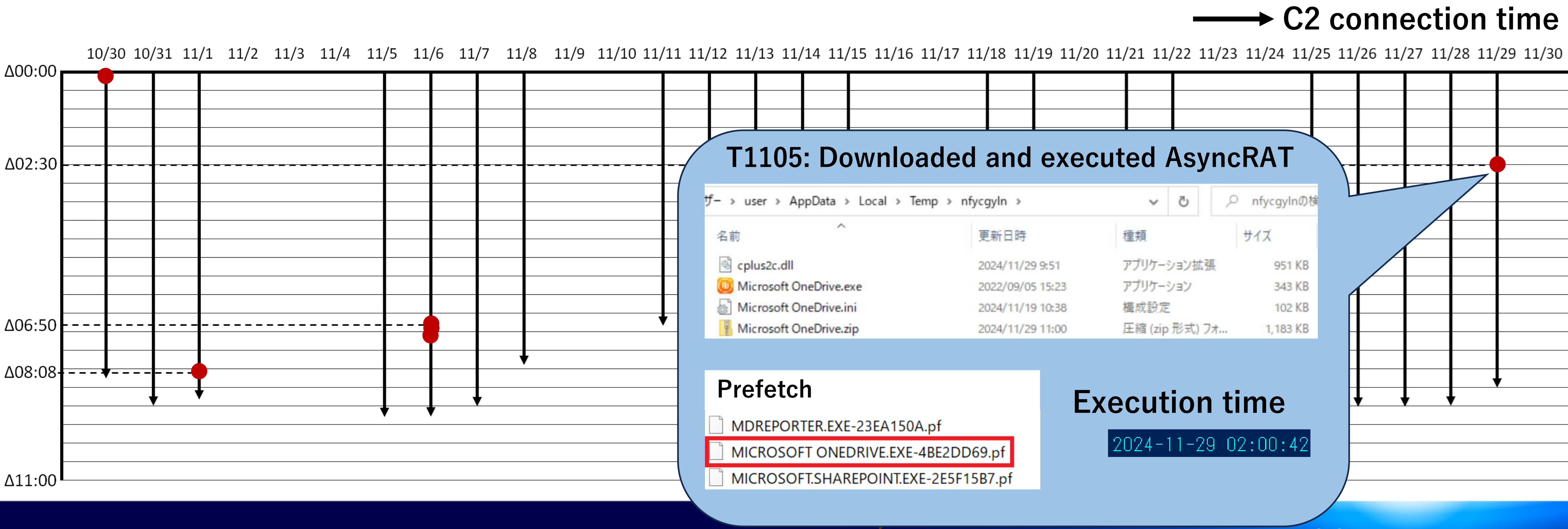
Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes



Case 2

- Total C2 connection time: 293 hours 45 minutes (35 days)
- Time until first observed post-exploitation: 25 hours 23 minutes



T1105: Downloaded and executed AsyncRAT

ザー › user › AppData › Local › Temp › nfycgyln ›

nfycgylnの検

名前	更新日時	種類	サイズ
cplus2c.dll	2024/11/29 9:51	アプリケーション拡張	951 KB
Microsoft OneDrive.exe	2022/09/05 15:23	アプリケーション	343 KB
Microsoft OneDrive.ini	2024/11/19 10:38	構成設定	102 KB
Microsoft OneDrive.zip	2024/11/29 11:00	圧縮 (zip 形式) フォ...	1,183 KB

Prefetch

MDREPORTER.EXE-23EA150A.pf

MICROSOFT ONEDRIVE.EXE-4BE2DD69.pf

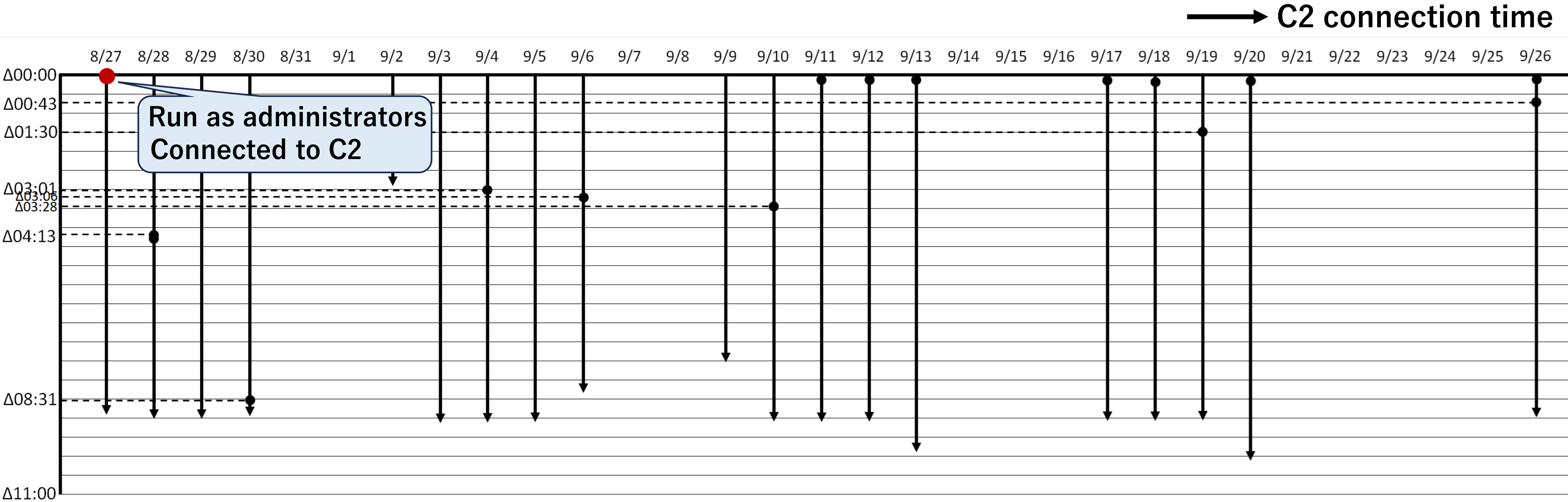
MICROSOFT.SHAREPOINT.EXE-2E5F15B7.pf

Execution time

2024-11-29 02:00:42

Case 3

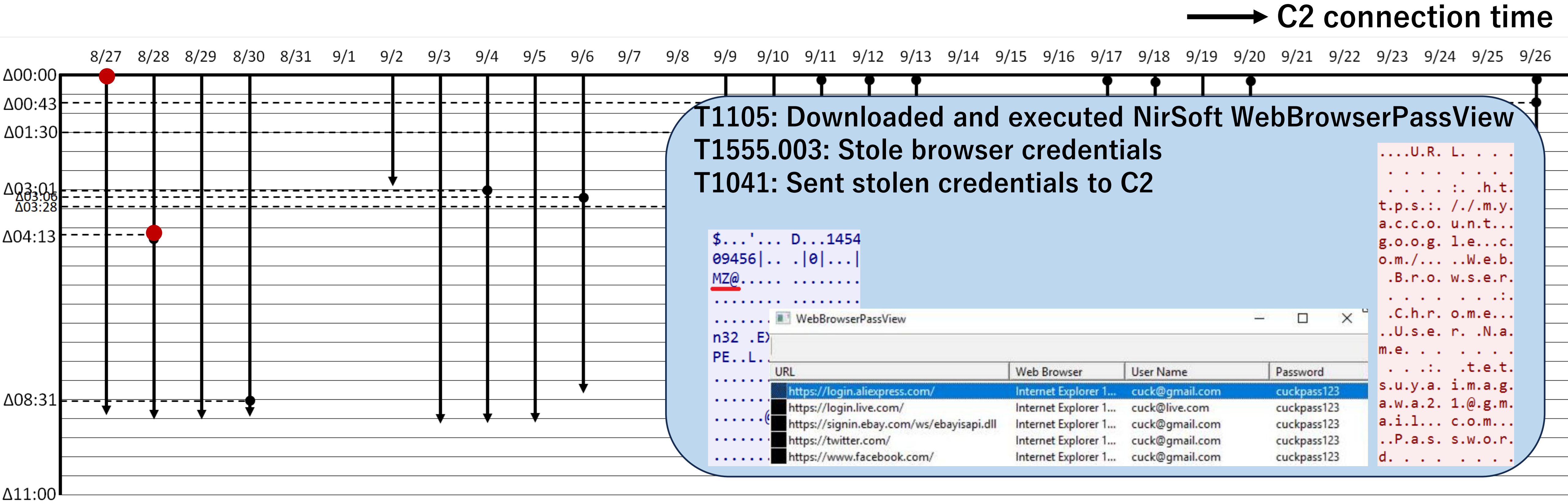
- Total C2 connection time: 165 hours (19 days)
- Time until first observed post-exploitation: 12 hours 28 minutes



Run as administrators
Connected to C2

Case 3

- Total C2 connection time: 165 hours (19 days)
- Time until first observed post-exploitation: 12 hours 28 minutes



T1105: Downloaded and executed NirSoft WebBrowserPassView

T1555.003: Stole browser credentials

T1041: Sent stolen credentials to C2

```
$...'... D...1454
09456|.. .|0|...|
MZ@..... ........
........ ........
.......
n32 .EX
PE..L..
.......
.......
.......(
.......
.......
```

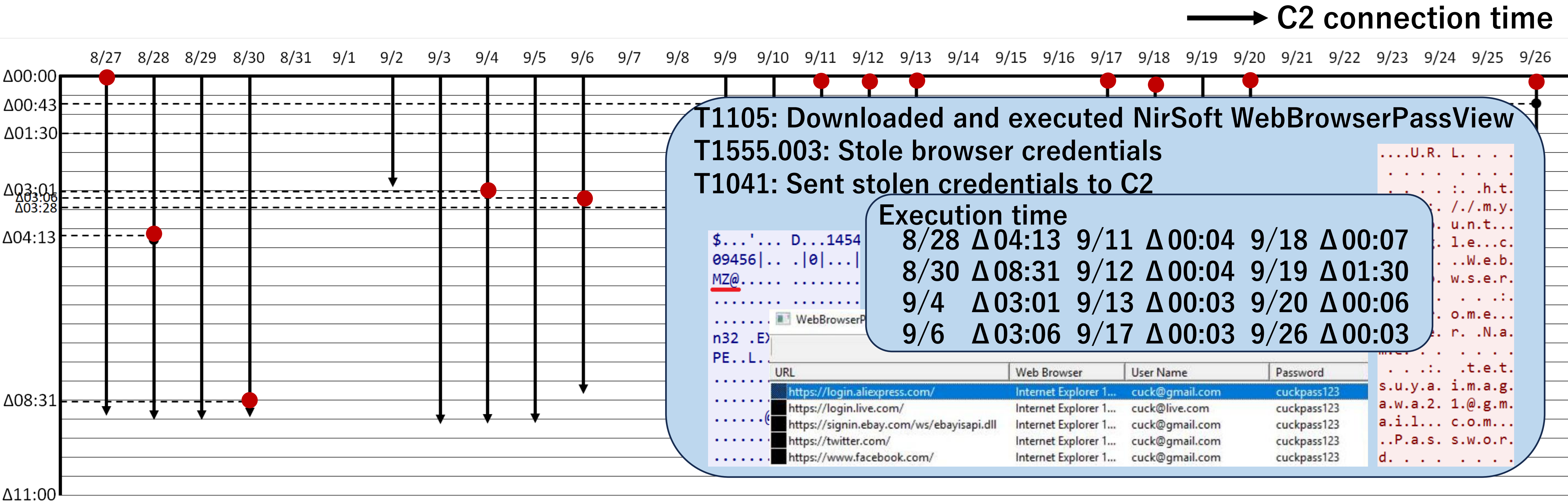
WebBrowserPassView

URL	Web Browser	User Name	Password
https://login.aliexpress.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://login.live.com/	Internet Explorer 1...	cuck@live.com	cuckpass123
https://signin.ebay.com/ws/ebayisapi.dll	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://twitter.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://www.facebook.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123

```
....U.R. L. . . .
 . . . .  . . . .
 . . . . :. .h.t.
t.p.s.:. /./.m.y.
a.c.c.o. u.n.t...
g.o.o.g. l.e...c.
o.m./... ..W.e.b.
 .B.r.o. w.s.e.r.
 . . . .  . . .:.
 .C.h.r. o.m.e...
..U.s.e. r. .N.a.
m.e. . .  . . . .
 . . .:.  .t.e.t.
s.u.y.a. i.m.a.g.
a.w.a.2. 1.@.g.m.
a.i.l... c.o.m...
..P.a.s. s.w.o.r.
d. . . .  . . . .
```

Case 3

- Total C2 connection time: 165 hours (19 days)
- Time until first observed post-exploitation: 12 hours 28 minutes



T1105: Downloaded and executed NirSoft WebBrowserPassView
T1555.003: Stole browser credentials
T1041: Sent stolen credentials to C2

Execution time

8/28	Δ04:13	9/11	Δ00:04	9/18	Δ00:07
8/30	Δ08:31	9/12	Δ00:04	9/19	Δ01:30
9/4	Δ03:01	9/13	Δ00:03	9/20	Δ00:06
9/6	Δ03:06	9/17	Δ00:03	9/26	Δ00:03

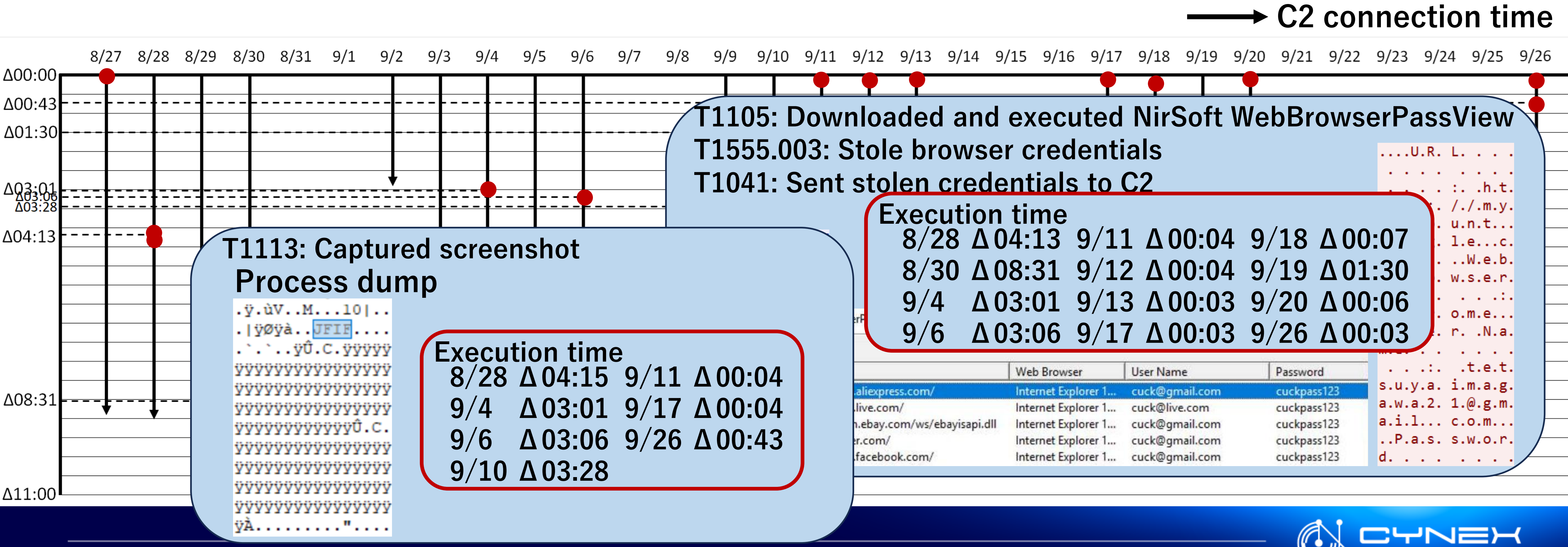
```
$...'... D...1454
09456|.. .|0|...|
MZ@..... ........
........ ........
.......
n32 .EX
PE..L..
.......
.......
.......@
.......
.......
```

URL	Web Browser	User Name	Password
https://login.aliexpress.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://login.live.com/	Internet Explorer 1...	cuck@live.com	cuckpass123
https://signin.ebay.com/ws/ebayisapi.dll	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://twitter.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
https://www.facebook.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123

```
....U.R. L. . . .
 . . . .  . . . .
 . . . . :. .h.t.
 . . . . /./.m.y.
 . . . . u.n.t...
 . . . . l.e...c.
 . . . . ..W.e.b.
 . . . . w.s.e.r.
 . . . .  . . .:.
 . . . . o.m.e...
 . . . . r. .N.a.
 . . . .  . . . .
 . . .:.  .t.e.t.
s.u.y.a. i.m.a.g.
a.w.a.2. 1.@.g.m.
a.i.l... c.o.m...
..P.a.s. s.w.o.r.
d. . . .  . . . .
```

Case 3

- Total C2 connection time: 165 hours (19 days)
- Time until first observed post-exploitation: 12 hours 28 minutes



T1113: Captured screenshot

Process dump

```
.ÿ.ùV..M...10|..
.|ÿØÿà..JFIF....
.`.`..ÿÛ.C.ÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÛ.C.
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÀ.........".....
```

Execution time

8/28	Δ04:15	9/11	Δ00:04
9/4	Δ03:01	9/17	Δ00:04
9/6	Δ03:06	9/26	Δ00:43
9/10	Δ03:28		

T1105: Downloaded and executed NirSoft WebBrowserPassView

T1555.003: Stole browser credentials

T1041: Sent stolen credentials to C2

Execution time

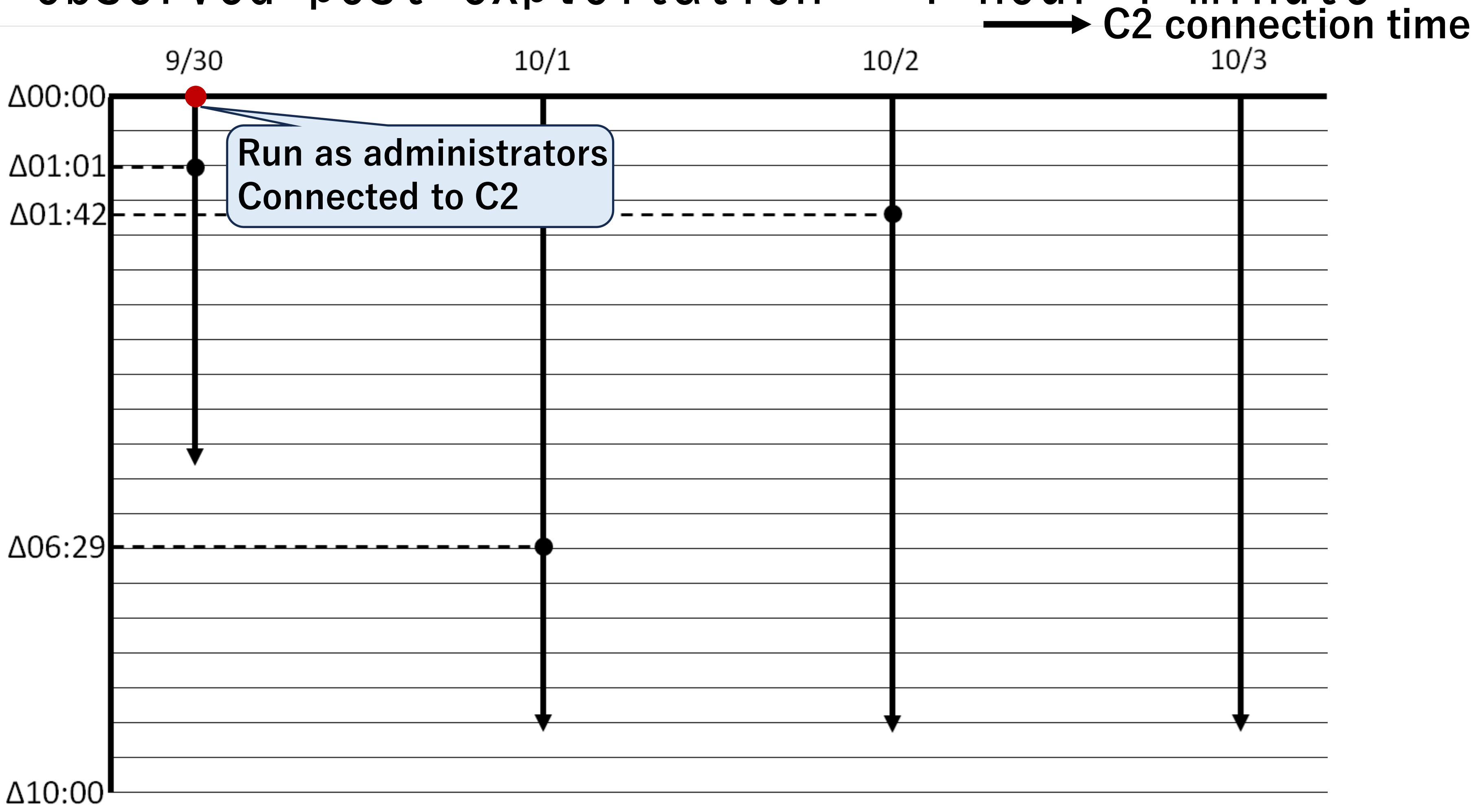
8/28	Δ04:13	9/11	Δ00:04	9/18	Δ00:07
8/30	Δ08:31	9/12	Δ00:04	9/19	Δ01:30
9/4	Δ03:01	9/13	Δ00:03	9/20	Δ00:06
9/6	Δ03:06	9/17	Δ00:03	9/26	Δ00:03

	Web Browser	User Name	Password
.aliexpress.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
.live.com/	Internet Explorer 1...	cuck@live.com	cuckpass123
n.ebay.com/ws/ebayisapi.dll	Internet Explorer 1...	cuck@gmail.com	cuckpass123
r.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123
.facebook.com/	Internet Explorer 1...	cuck@gmail.com	cuckpass123

```
....U.R. L. . . .
 . . . .  . . . .
. . . . . :. .h.t.
        /./.m.y.
        u.n.t...
        l.e...c.
        ..W.e.b.
        w.s.e.r.
         . . .:.
        o.m.e...
        r. .N.a.
 . . . .  . . . .
 . . .:.  .t.e.t.
s.u.y.a. i.m.a.g.
a.w.a.2. 1.@.g.m.
a.i.l... c.o.m...
..P.a.s. s.w.o.r.
d. . . .  . . . .
```

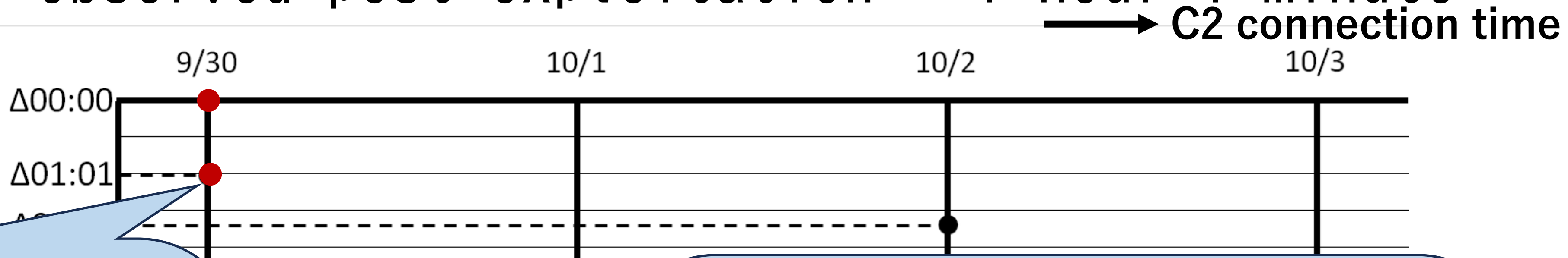
Case 4

- Total C2 connection time: 32 hours 30 minutes (4 days)
- Time until first observed post-exploitation : 1 hour 1 minute



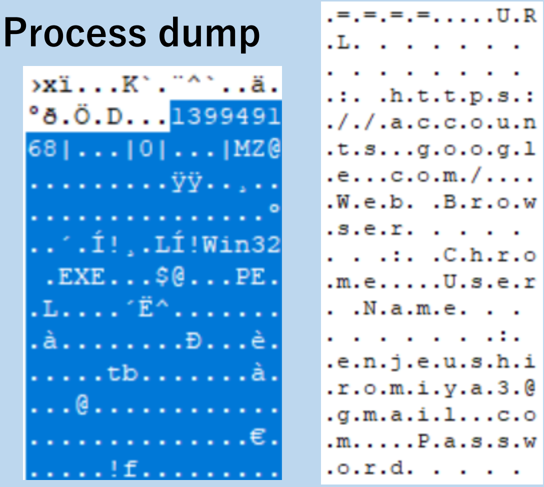
Case 4

- Total C2 connection time: 32 hours 30 minutes (4 days)
- Time until first observed post-exploitation : 1 hour 1 minute



T1105: Downloaded and executed NirSoft WebBrowserPassView
T1555.003: Stole browser credentials
T1041: Sent stolen credentials to C2

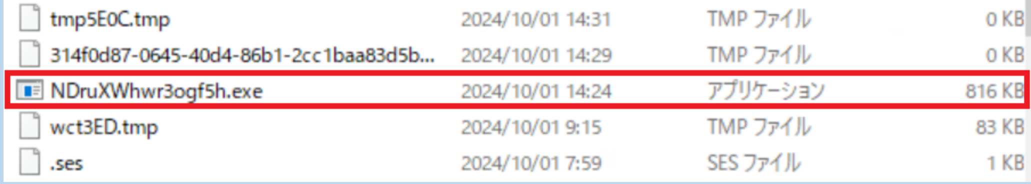
Process dump



```
›xï...K`.¨^`..ä.
°ð.Ö.D...1399491
68|...|0|...|MZ@
..........ÿÿ..¸..
.................°
..´.Í!¸.LÍ!Win32
 .EXE...$@...PE.
.L....´Ë^.......
.à........Ð...è.
.....tb.......à.
...@............
...............€.
.....!f.........
```

```
.=.=.=.=.....U.R
.L. . . . . . .
. . . . . . . .
.:. .h.t.t.p.s.:
././.a.c.c.o.u.n
.t.s...g.o.o.g.l
.e...c.o.m./....
.W.e.b. .B.r.o.w
.s.e.r. . . . .
. . .:. .C.h.r.o
.m.e.....U.s.e.r
. .N.a.m.e. . .
. . . . . . .:.
.e.n.j.e.u.s.h.i
.r.o.m.i.y.a.3.@
.g.m.a.i.l...c.o
.m.....P.a.s.s.w
.o.r.d. . . . .
```

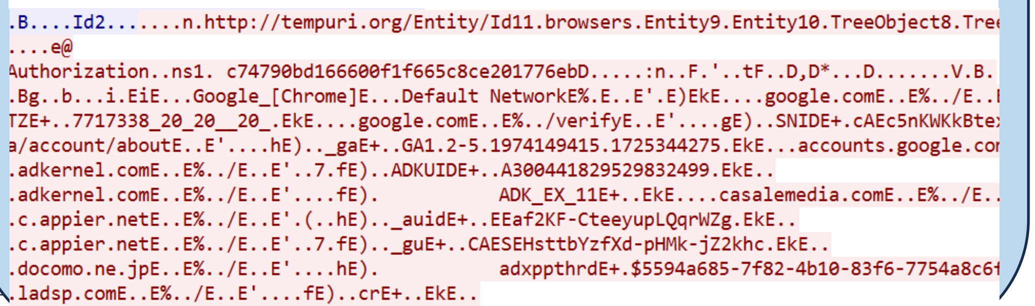
T1105: Downloaded and executed Redline Stealer



tmp5E0C.tmp	2024/10/01 14:31	TMP ファイル	0 KB
314f0d87-0645-40d4-86b1-2cc1baa83d5b...	2024/10/01 14:29	TMP ファイル	0 KB
NDruXWhwr3ogf5h.exe	2024/10/01 14:24	アプリケーション	816 KB
wct3ED.tmp	2024/10/01 9:15	TMP ファイル	83 KB
.ses	2024/10/01 7:59	SES ファイル	1 KB

T1217: Send web browser history to C2

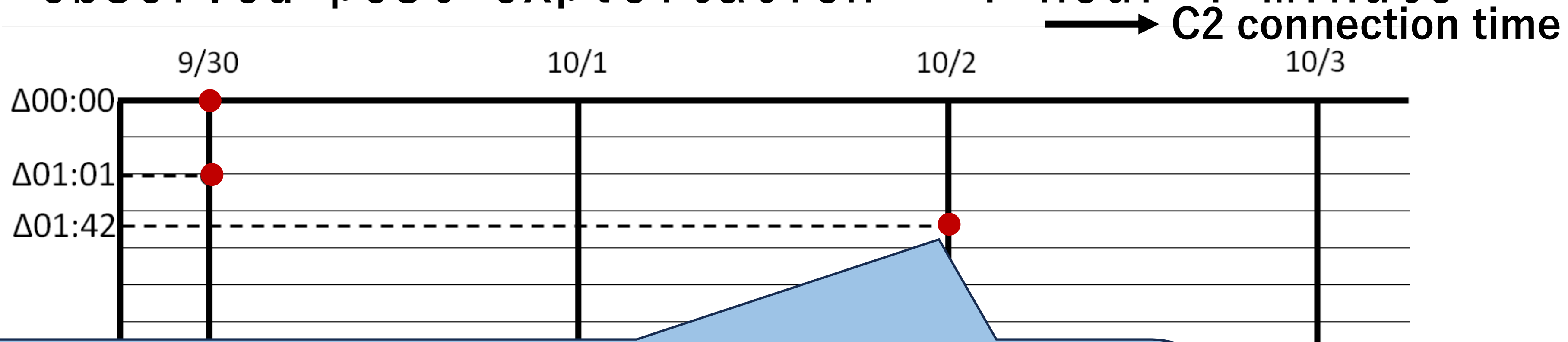
Pcap



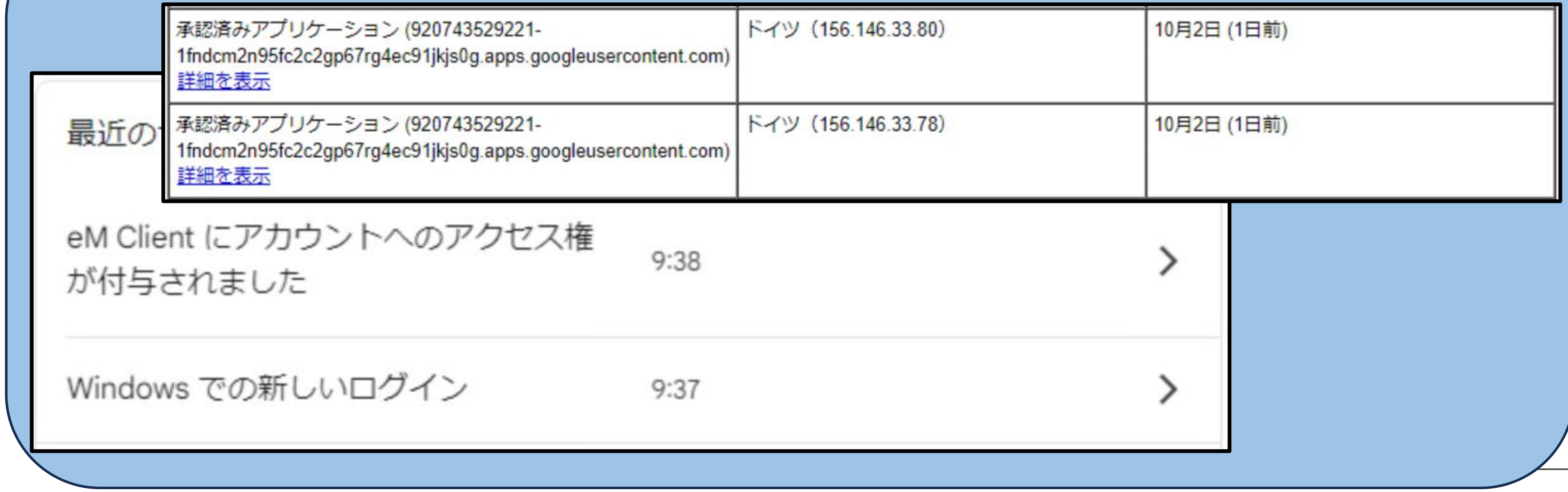
```
.B....Id2.......n.http://tempuri.org/Entity/Id11.browsers.Entity9.Entity10.TreeObject8.Tree
....e@
Authorization..ns1. c74790bd166600f1f665c8ce201776ebD.....:n..F.'..tF..D,D*...D.......V.B.
.Bg..b...i.EiE...Google_[Chrome]E...Default NetworkE%.E..E'.E)EkE....google.comE..E%../E..
TZE+..7717338_20_20__20_.EkE....google.comE..E%../verifyE..E'....gE)..SNIDE+.cAEc5nKWKkBtex
a/account/aboutE..E'....hE).._gaE+..GA1.2-5.1974149415.1725344275.EkE...accounts.google.co
.adkernel.comE..E%../E..E'..7.fE)..ADKUIDE+..A300441829529832499.EkE..
.adkernel.comE..E%../E..E'....fE).            ADK_EX_11E+..EkE....casalemedia.comE..E%../E..
.c.appier.netE..E%../E..E'.(..hE).._auidE+..EEaf2KF-CteeyupLQqrWZg.EkE..
.c.appier.netE..E%../E..E'..7.fE).._guE+..CAESEHsttbYzfXd-pHMk-jZ2khc.EkE..
.docomo.ne.jpE..E%../E..E'....hE).            adxppthrdE+.$5594a685-7f82-4b10-83f6-7754a8c6f
.ladsp.comE..E%../E..E'....fE)..crE+..EkE..
```

Case 4

- Total C2 connection time: 32 hours 30 minutes (4 days)
- Time until first observed post-exploitation : 1 hour 1 minute



Logged into Google account using stolen credentials and linked eM Client



承認済みアプリケーション (920743529221-1fndcm2n95fc2c2gp67rg4ec91jkjs0g.apps.googleusercontent.com) 詳細を表示	ドイツ（156.146.33.80）	10月2日 (1日前)
承認済みアプリケーション (920743529221-1fndcm2n95fc2c2gp67rg4ec91jkjs0g.apps.googleusercontent.com) 詳細を表示	ドイツ（156.146.33.78）	10月2日 (1日前)

最近の

eM Client にアカウントへのアクセス権が付与されました 9:38

Windows での新しいログイン 9:37

Summary of Artifacts by Technique

Tactics	Tequniques		Artifacts	Description
Credential Access	T1552.001	Credentials in Files	MFT	Check access timestamp of files containing credentials .¥Users¥user¥Documents,pass.txt
	T1555.003	Credentials from Web Browsers	MFT	Check access to the directory where browser credentials are stored .¥Users¥flarevm¥AppData¥Local¥Google¥Chrome¥User Data .¥Users¥flarevm¥AppData¥Local¥Microsoft¥Edge¥User Data .¥Users¥flarevm¥AppData¥Local¥Microsoft¥Credentials .¥Users¥flarevm¥AppData¥Local¥Microsoft¥Credentials
			Process dump	Identify stolen browser credentials from RAT process dump
			Pcap	If C2 communication is unencrypted, identify stolen browser credentials from Pcap
Discovery	T1010	Application Window Discovery	Pcap	If C2 communication is unencrypted, check the window information from Pcap
	T1033	System Owner/User Discovery	MFT	Check access to the executable files of standard Windows commands .¥Windows¥System32,net.exe .¥Windows¥System32,net1.exe
			Prefetch	Check the execution history of standard Windws commands net.exe net1.exe
			Windows Event Log	Refer to Security log Event ID: 4798 and check the CallerProcessName field
	T1046	Network Service Discovery	MFT	Check access to the executable files of standard Windows commands .¥Windows¥System32,ipconfig.exe .¥Windows¥System32,netstat.exe
			Prefetch	Check the execution history of standard Windws commands ipconfig.exe netstat.exe
	T1082	System Information Discovery	Pcap	If C2 communication is unencrypted, check the system information of the infected machine from Pcap
	T1217	Browser Information Discovery	Pcap	If C2 communication is unencrypted, identify stolen Web browser histories from Pcap
	T1518	Software Discovery	Pcap	If C2 communication is unencrypted, check the software list of the infected machine from Pcap

Summary of Artifacts by Technique

Tactics	Tequniques		Artifacts	Description
Collection	T1005	Data from Local System	MFT	Check the access timestamp of the document files
	T1056.001	Keylogging	MFT	Check the generation of keylogging file RemcosRAT: .¥User¥user¥AppData¥Roaming¥remcos,logs.dat
	T1113	Screen Capture	Process dump	Check the screenshots from the RAT process dump Magic number JFIF（0x4a 0x46 0x49 0x46） .PNG（0x89 0x50 0x4e 0x47）
			Pcap	If C2 communication is unencrypted, check the screenshots from the Pcap Magic number JFIF（0x4a 0x46 0x49 0x46） .PNG（0x89 0x50 0x4e 0x47）
	T1560	Archvie Collected Data	Pcap	If C2 communication is unencrypted, check the compressed file from the Pcap Magic number: PK（0x50 0x4b）
Command and Control	T1105	Ingress Tool Transfer	MFT	Check the generation of additionally downloaded malware .¥Users¥user¥AppData¥Local¥dyintbxp¥nnls_recorder.exe .¥Users¥user¥AppData¥Local¥wjjrzwti¥TxBugReport.exe .¥Users¥user¥AppData¥Local¥nfycgyln¥Microsoft OneDrive.exe
			Prefetch	Check the execution history of additionally downloaded malware
			Process information	Check the process of addtionally downloaded malware
			Process dump	Check the downloaded malware from the RAT process dump Magic number: MZ（0x4d 0x5a）
			Pcap	If C2 communication is unencrypted, check the downloaded malware in Pcap Magic number: MZ（0x4d 0x5a）
Exfiltration	T1041	Exfiltration Over C2 Channel	Pcap	Check C2 communication

Effective Logs

Easy

Hard

	Credential Access	
	T1552.001	T1555.003
	Credentials in Files	Credentials from Web Browsers
MFT	✓	✓
Pcap		△
Process dump		✓

Easy

Hard

	Discovery					
	T1010	T1033	T1046	T1082	T1217	T1518
	Application Window Discovery	System Owner/User Discovery	Network Service Discovery	System Information Discovery	Browser Information Discovery	Software Discovery
MFT		✓	✓			
Pcap	△			△	△	△
Process dump						

Effective Logs

Easy

Hard

	Collection				Command and Control	Exfiltration
	T1005	T1056.001	T1113	T1560	T1105	T1041
	Data from Local System	Keylogging	Screen Capture	Archvie Collected Data	Ingress Tool Transfer	Exfiltration Over C2 Channel
MFT	✓	✓			△	
Pcap			△	△	△	✓
Process dump			✓		✓	

Conclusion

Conclusion

- STARDUST: An observation platform for monitoring Post-Exploitation
    - Artifacts can be collected on-demand
- Long-term observation of RATs
    - Number of RAT samples where Post-Exploitation was observed: **10 / 41 samples**
    - ➡ Post-exploitations were observable even with scattershot-type RATs
    - Types of Post-Exploitation activities observed: **14 types**
- Logs effective for understanding Post-Exploitation: **MFT, Pcap, and Process dump**
- Future works
    - Observe Post-Exploitation activities in a large number of malware
    - Share the results with the community

Thank you!

Email: s_hiruta@nict.go.jp