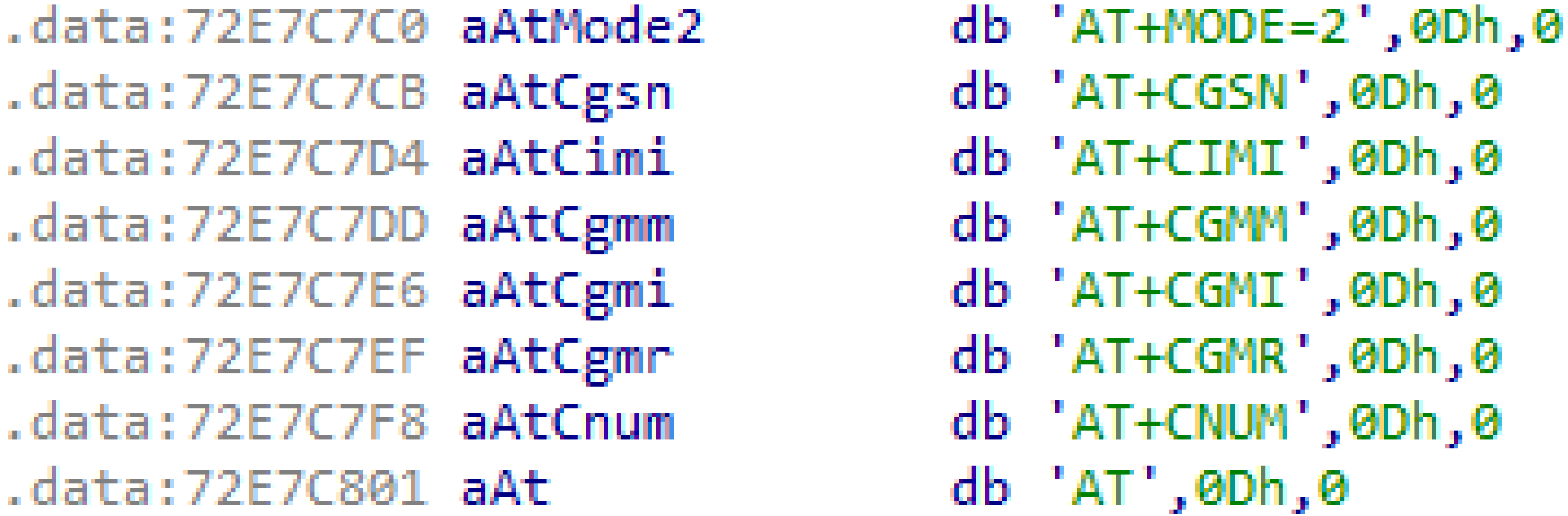
ENJOY SAFER TECHNOLOGY™

ATTOR: Spy platform with curious GSM fingerprinting

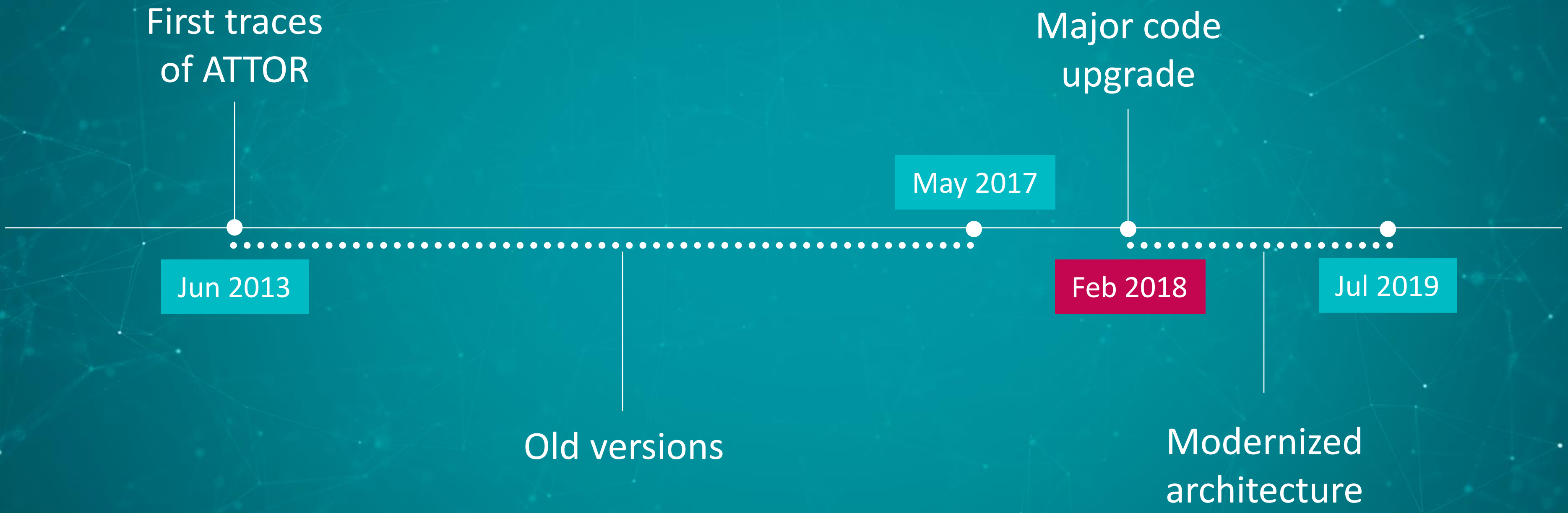
Zuzana Hromcová | Malware Analyst

AT commands?



```
.data:72E7C7C0 aAtMode2          db 'AT+MODE=2',0Dh,0
.data:72E7C7CB aAtCgsn           db 'AT+CGSN',0Dh,0
.data:72E7C7D4 aAtCimi           db 'AT+CIMI',0Dh,0
.data:72E7C7DD aAtCgmm           db 'AT+CGMM',0Dh,0
.data:72E7C7E6 aAtCgmi           db 'AT+CGMI',0Dh,0
.data:72E7C7EF aAtCgmr           db 'AT+CGMR',0Dh,0
.data:72E7C7F8 aAtCnum           db 'AT+CNUM',0Dh,0
.data:72E7C801 aAt               db 'AT',0Dh,0
```

Timeline



First traces of ATTOR

Jun 2013

Old versions

May 2017

Major code upgrade

Feb 2018

Modernized architecture

Jul 2019

Agenda

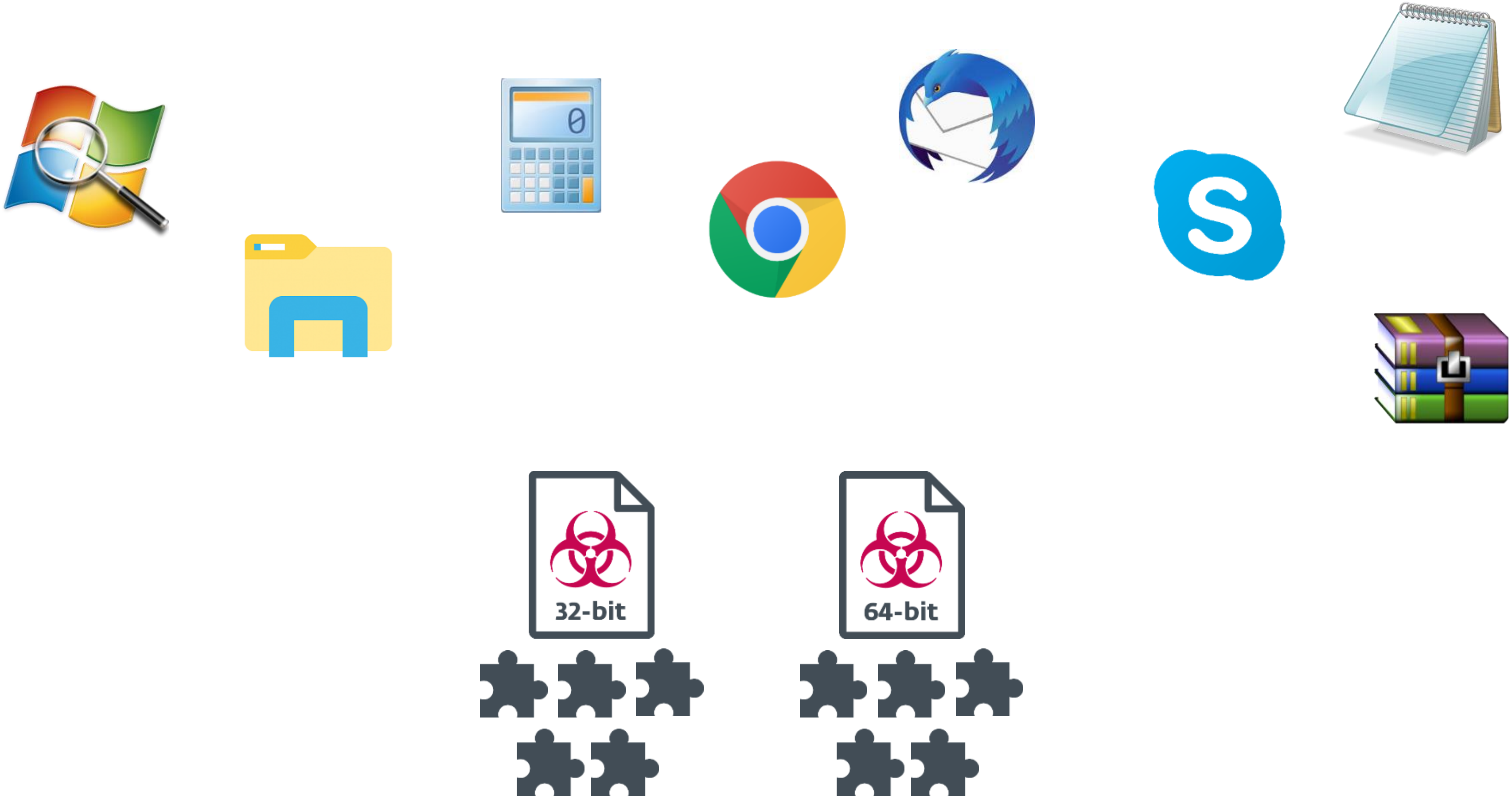
- ATTOR's targets
- Platform architecture
- ~~AT~~TOR: Network communication
- AT~~TOR~~: GSM fingerprinting

<30 targets

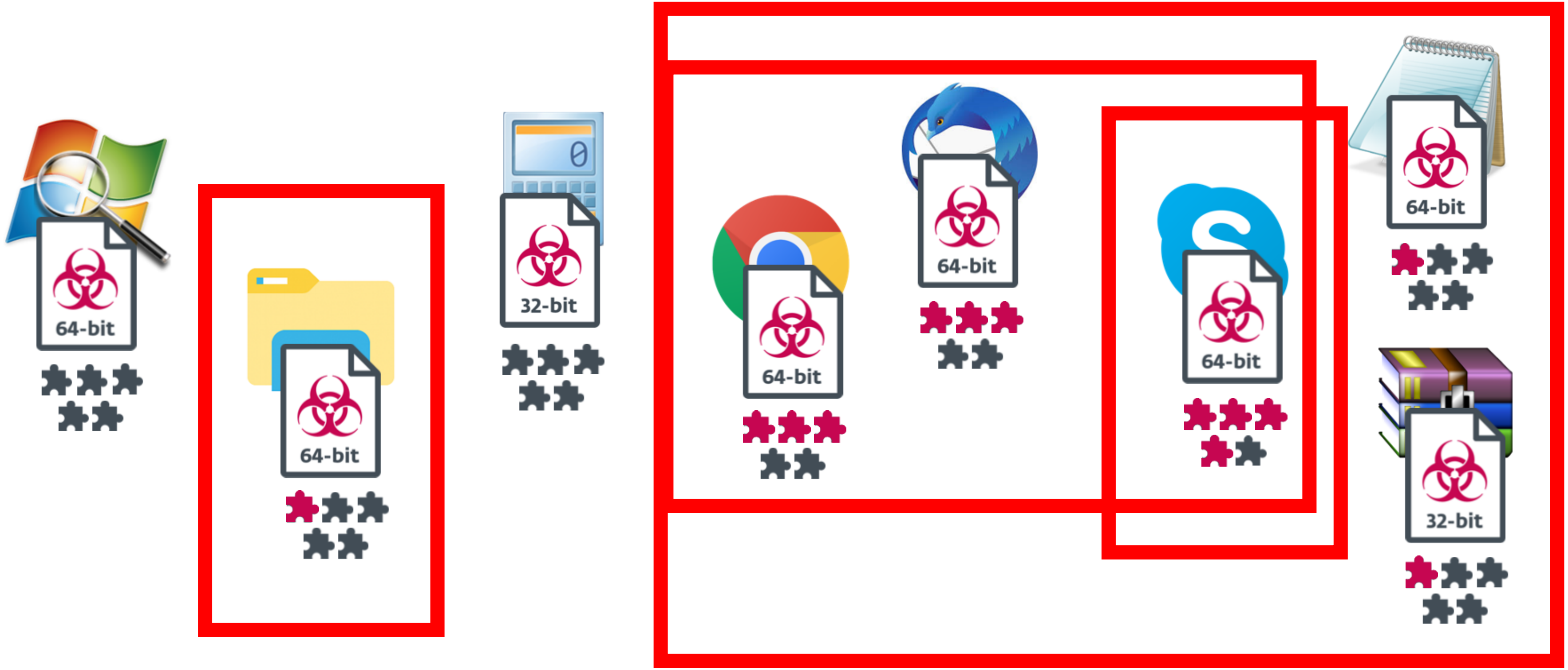
Governmental institutions

Diplomatic missions

ATTOR platform



ATTOR platform



Network communication plugins [illegible]

Targets?

Social networks

VoIP and IM applications

File sharing services

Mail services

Archiving utilities

Office software

Text editors

Blogging platforms

Russian-speaking users

ПРИГЛАШЕНИЕ ДРУЖИТЬ
ВАМ СООБЩЕНИЕ
ОДНОКЛАССНИКИ
ЯНДЕКС.ПОЧТА
POCHTA
AGENTVKONTAKTE
YANDEX.MAIL
MAILRU
QIP
WEBMONEY
RAMBLER
…

Russian search engine

Рамблер/

Rambler

Russian online payment system

WebMoney

Russian social networks

Odnoklassniki

VKontakte

QIP, Russian IM application

QIP.RU

Russian email services

Yandex.Mail

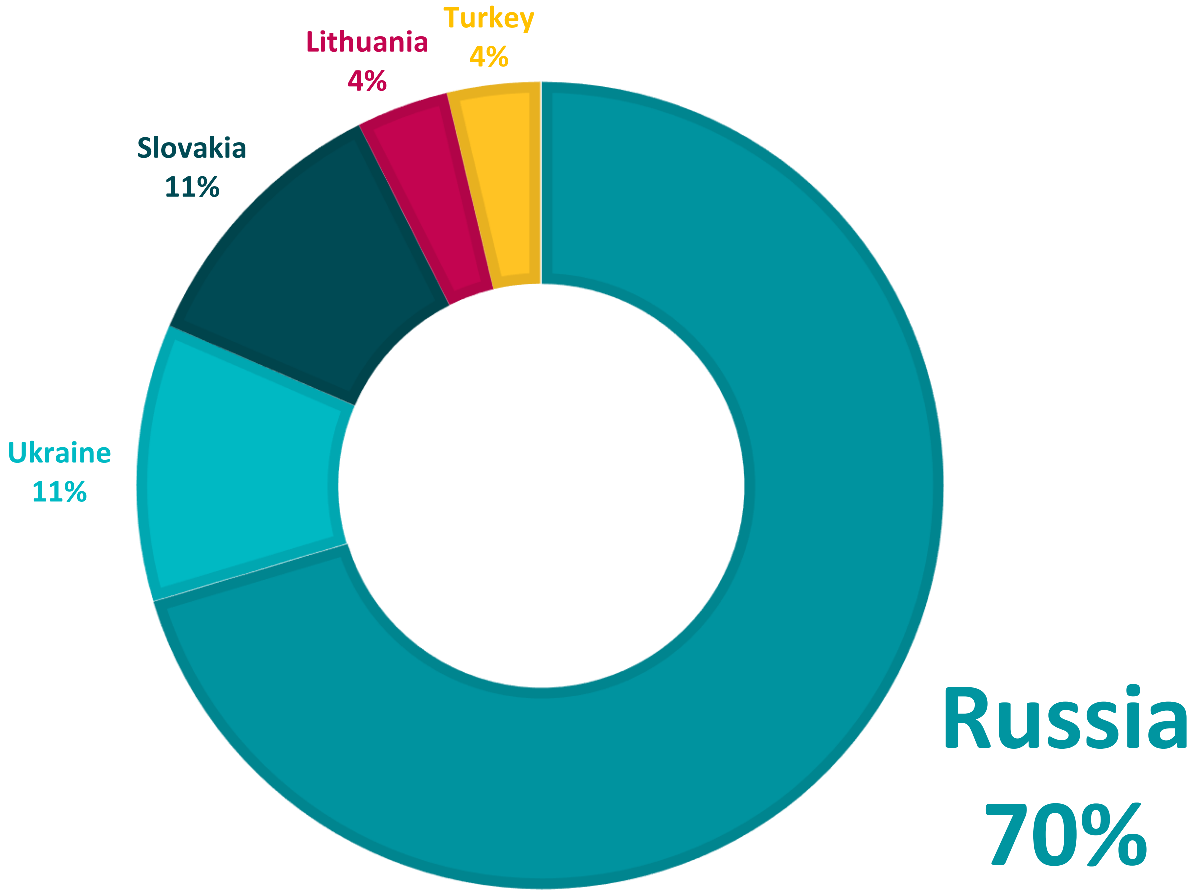
@mail

Mail.ru

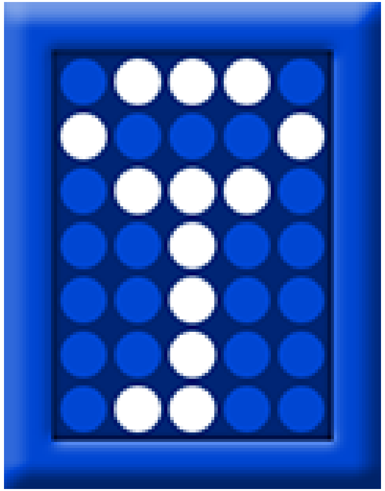
MultiFon, Russian VoIP service

MEGAFON

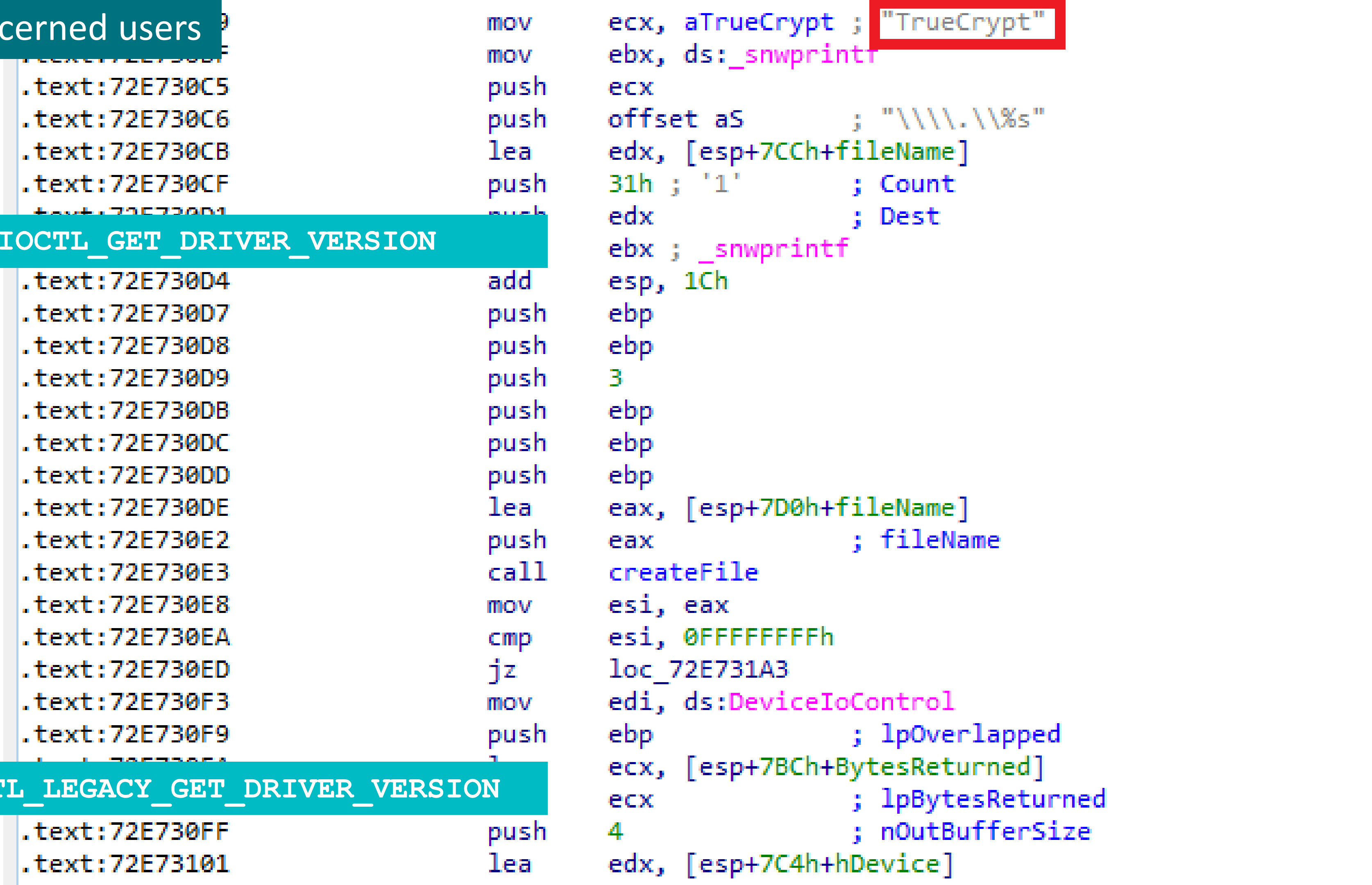
Geographical distribution



Privacy-concerned users



Privacy-concerned users



```
                          mov     ecx, aTrueCrypt ; "TrueCrypt"
                          mov     ebx, ds:_snwprintf
.text:72E730C5            push    ecx
.text:72E730C6            push    offset aS       ; "\\\\.\\%s"
.text:72E730CB            lea     edx, [esp+7CCh+fileName]
.text:72E730CF            push    31h ; '1'       ; Count
                                  edx             ; Dest
                                  ebx ; _snwprintf
.text:72E730D4            add     esp, 1Ch
.text:72E730D7            push    ebp
.text:72E730D8            push    ebp
.text:72E730D9            push    3
.text:72E730DB            push    ebp
.text:72E730DC            push    ebp
.text:72E730DD            push    ebp
.text:72E730DE            lea     eax, [esp+7D0h+fileName]
.text:72E730E2            push    eax             ; fileName
.text:72E730E3            call    createFile
.text:72E730E8            mov     esi, eax
.text:72E730EA            cmp     esi, 0FFFFFFFFh
.text:72E730ED            jz      loc_72E731A3
.text:72E730F3            mov     edi, ds:DeviceIoControl
.text:72E730F9            push    ebp             ; lpOverlapped
                                  ecx, [esp+7BCh+BytesReturned]
                                  ecx             ; lpBytesReturned
.text:72E730FF            push    4               ; nOutBufferSize
.text:72E73101            lea     edx, [esp+7C4h+hDevice]
```

TC_IOCTL_GET_DRIVER_VERSION

TC_IOCTL_LEGACY_GET_DRIVER_VERSION

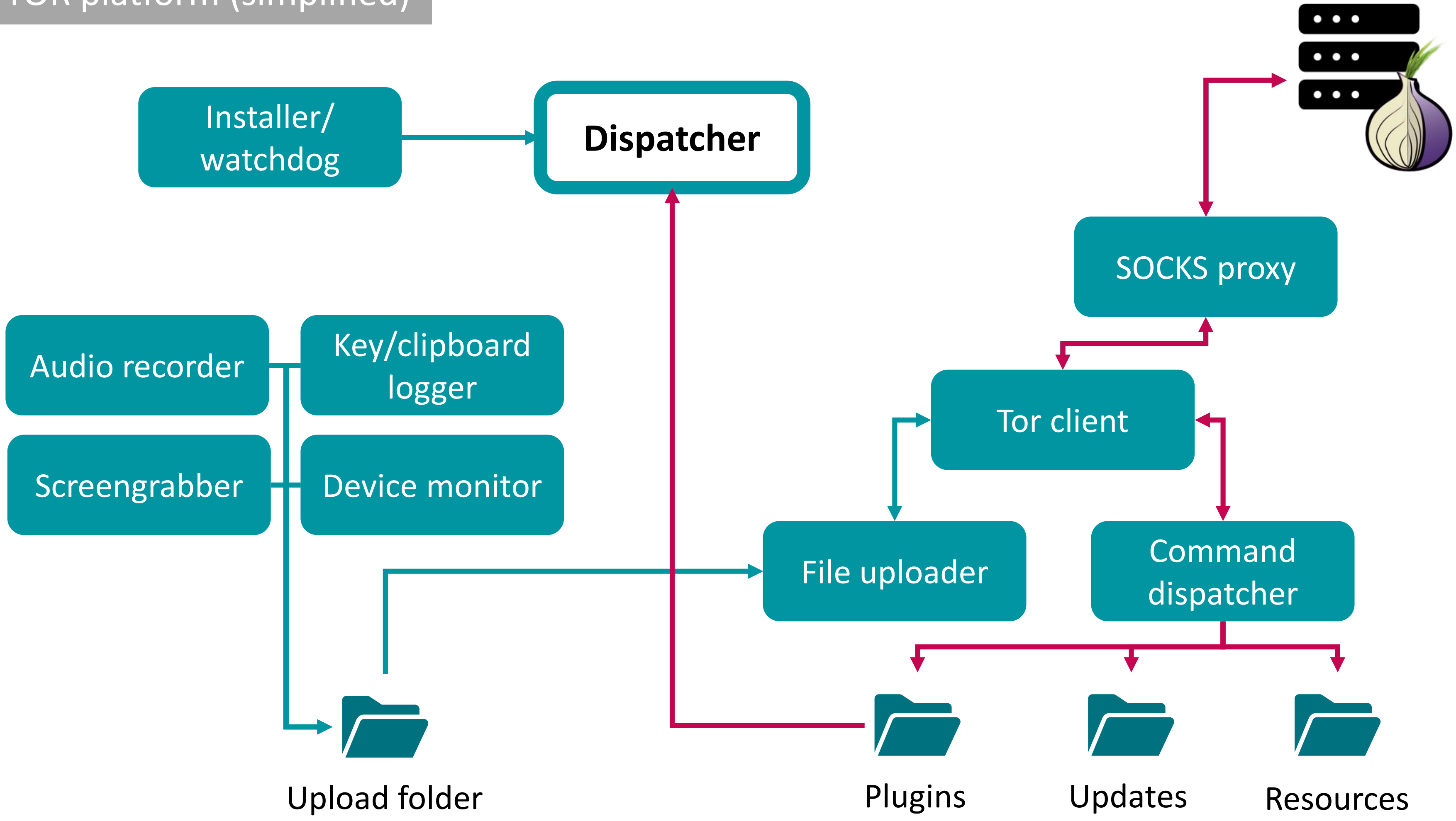
ATTOR's targets (recap)

High-profile targets in Eastern Europe

Russian-speaking, privacy-concerned users

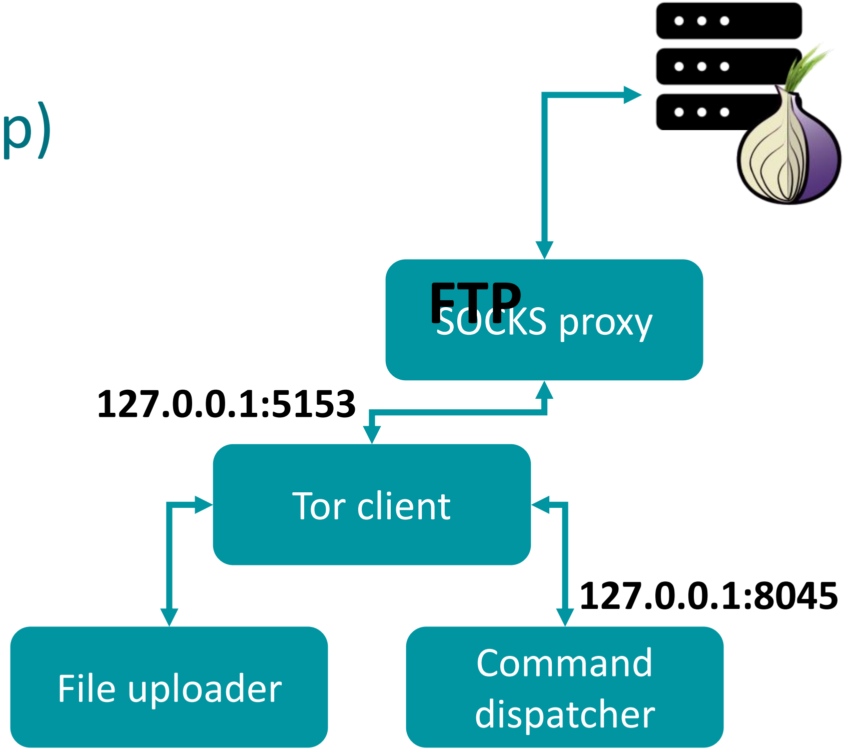
ATTOR platform

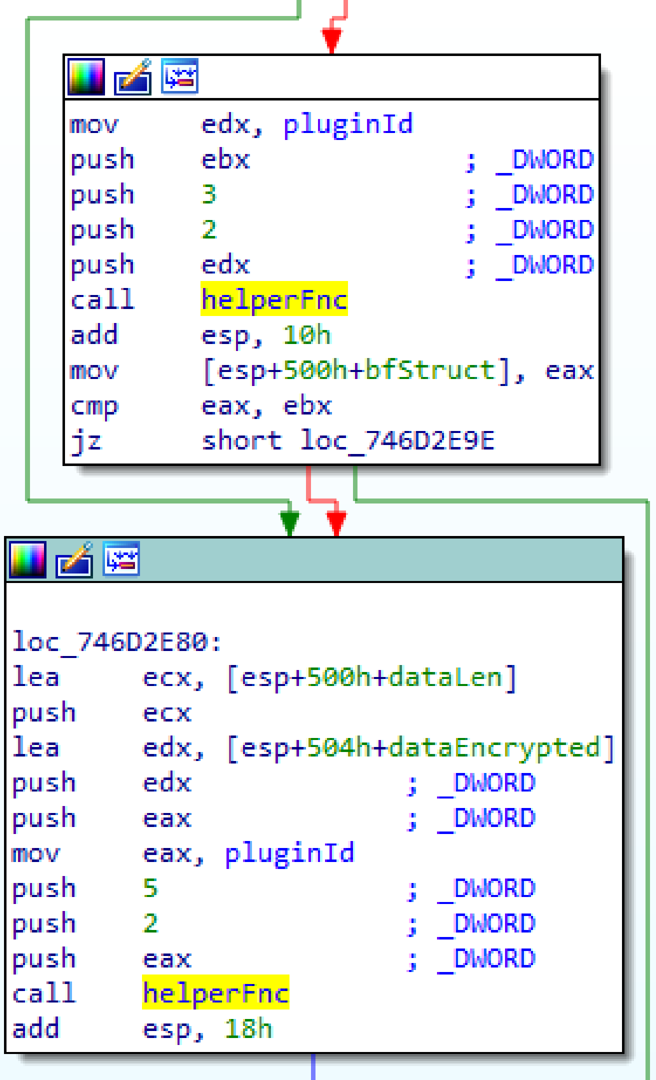
ATTOR platform (simplified)



Network communication (recap)

- Split into 4 components
- Only one component communicates with the C&C server directly
- FTP passive mode
- Selective activation of plugins
- Tor: Onion Service Protocol



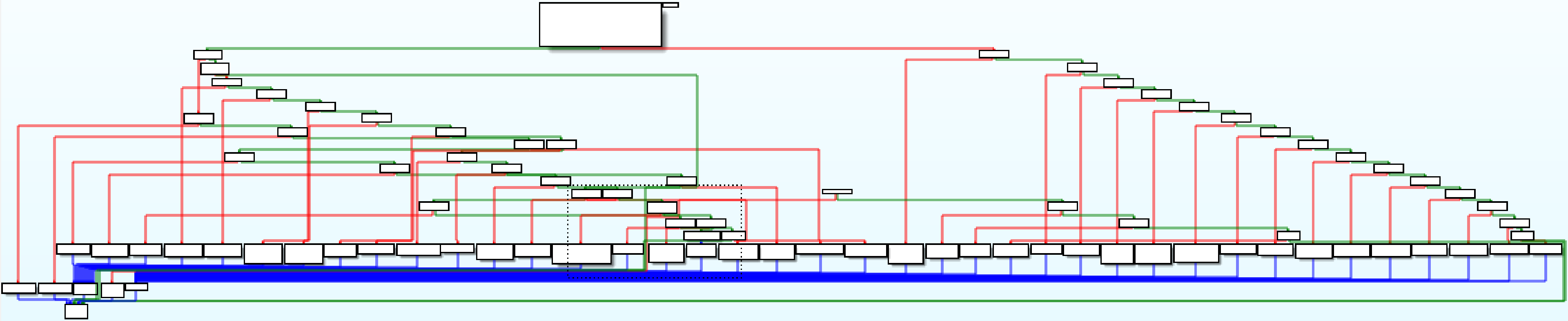


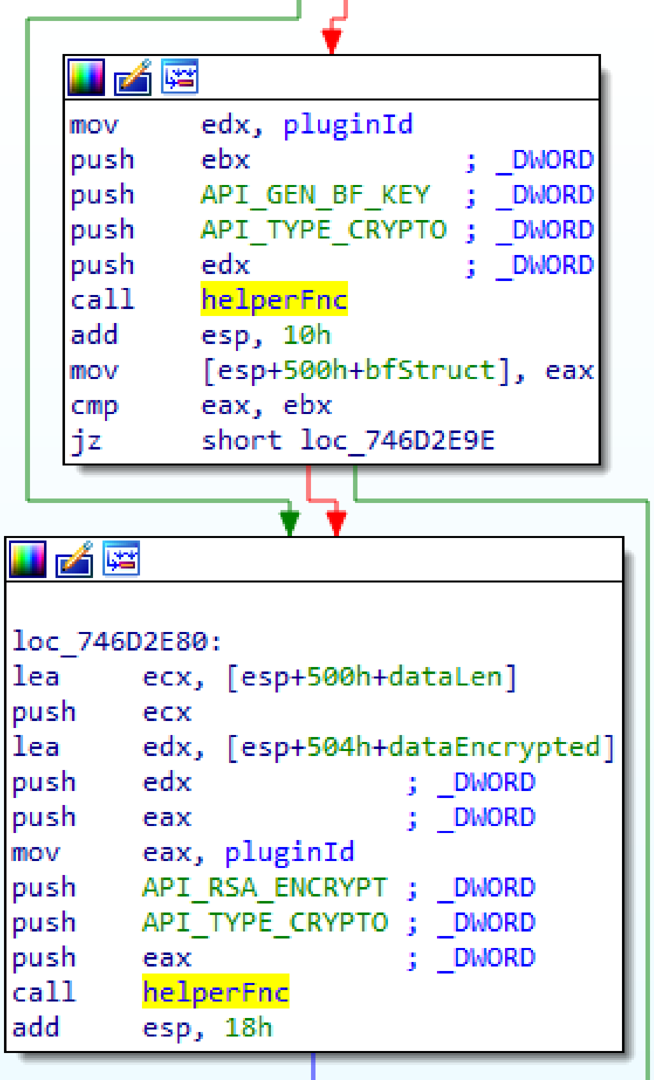
```
mov     edx, pluginId
push    ebx                  ; _DWORD
push    3                    ; _DWORD
push    2                    ; _DWORD
push    edx                  ; _DWORD
call    helperFnc
add     esp, 10h
mov     [esp+500h+bfStruct], eax
cmp     eax, ebx
jz      short loc_746D2E9E
```

```
loc_746D2E80:
lea     ecx, [esp+500h+dataLen]
push    ecx
lea     edx, [esp+504h+dataEncrypted]
push    edx                  ; _DWORD
push    eax                  ; _DWORD
mov     eax, pluginId
push    5                    ; _DWORD
push    2                    ; _DWORD
push    eax                  ; _DWORD
call    helperFnc
add     esp, 18h
```

ATTOR's plugins

ATTOR’s dispatcher





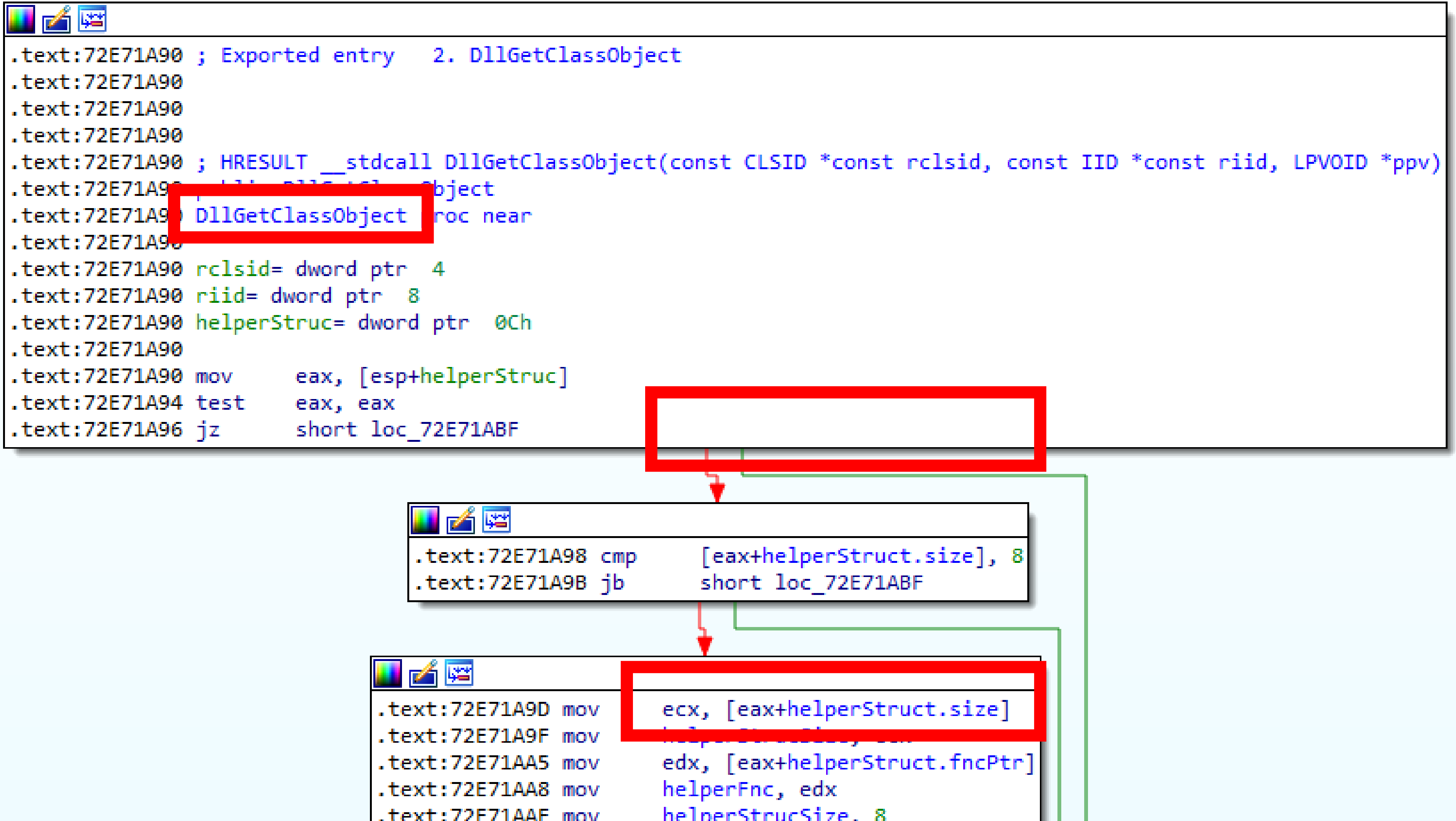
```
mov     edx, pluginId
push    ebx             ; _DWORD
push    API_GEN_BF_KEY  ; _DWORD
push    API_TYPE_CRYPTO ; _DWORD
push    edx             ; _DWORD
call    helperFnc
add     esp, 10h
mov     [esp+500h+bfStruct], eax
cmp     eax, ebx
jz      short loc_746D2E9E
```

```

loc_746D2E80:
lea     ecx, [esp+500h+dataLen]
push    ecx
lea     edx, [esp+504h+dataEncrypted]
push    edx             ; _DWORD
push    eax             ; _DWORD
mov     eax, pluginId
push    API_RSA_ENCRYPT ; _DWORD
push    API_TYPE_CRYPTO ; _DWORD
push    eax             ; _DWORD
call    helperFnc
add     esp, 18h
```

- Functions implemented by dispatcher
- Indexed by function type and function ID
- API wrappers, crypto functions, config data (30-40 functions)

- Reference passed on load



```
.text:72E71A90 ; Exported entry   2. DllGetClassObject
.text:72E71A90
.text:72E71A90
.text:72E71A90
.text:72E71A90 ; HRESULT __stdcall DllGetClassObject(const CLSID *const rclsid, const IID *const riid, LPVOID *ppv)
.text:72E71A90 public DllGetClassObject
.text:72E71A90 DllGetClassObject proc near
.text:72E71A90
.text:72E71A90 rclsid= dword ptr  4
.text:72E71A90 riid= dword ptr  8
.text:72E71A90 helperStruc= dword ptr  0Ch
.text:72E71A90
.text:72E71A90 mov     eax, [esp+helperStruc]
.text:72E71A94 test    eax, eax
.text:72E71A96 jz      short loc_72E71ABF
```

```
.text:72E71A98 cmp     [eax+helperStruct.size], 8
.text:72E71A9B jb      short loc_72E71ABF
```

```
.text:72E71A9D mov     ecx, [eax+helperStruct.size]
.text:72E71A9F mov     helperStrucSize, ecx
.text:72E71AA5 mov     edx, [eax+helperStruct.fncPtr]
.text:72E71AA8 mov     helperFnc, edx
.text:72E71AAE mov     helperStrucSize, 8
```

Collected/recovered plugins

Plugin ID	Analyzed versions	Functionality
1	14	Device monitor
2	(no version), 12	Screengrabber
3	(no version), 8, 9, 11, 12	Audio recorder
5	10	File uploader
6	10	Command dispatcher/SOCKS4 proxy
7	2, 4, 9, 10	Key/clipboard logger
13	3	TOR client
16	1	Installer/watchdog

AT~~TOR~~: GSM fingerprinting

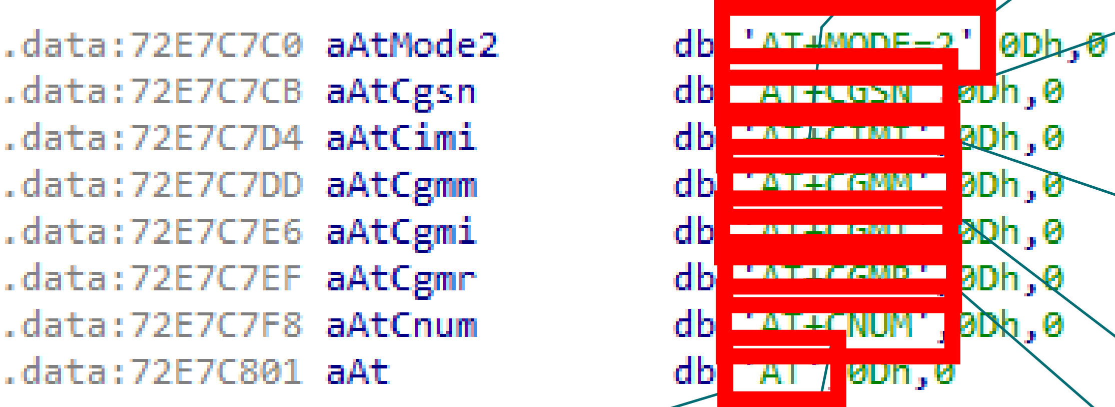
Hayes command set

1980’s

AT commands

mobile phones

GSM/GPRS modems



```
.data:72E7C7C0 aAtMode2        db 'AT+MODE=2',0Dh,0
.data:72E7C7CB aAtCgsn         db 'AT+CGSN',0Dh,0
.data:72E7C7D4 aAtCimi         db 'AT+CIMI',0Dh,0
.data:72E7C7DD aAtCgmm         db 'AT+CGMM',0Dh,0
.data:72E7C7E6 aAtCgmi         db 'AT+CGMI',0Dh,0
.data:72E7C7EF aAtCgmr         db 'AT+CGMR',0Dh,0
.data:72E7C7F8 aAtCnum         db 'AT+CNUM',0Dh,0
.data:72E7C801 aAt             db 'AT',0Dh,0
```

Request model number

Prepare for extended AT+ command set

Request IMEI number (unique device ID)

Request IMSI number (unique subscriber ID)

Request device manufacturer

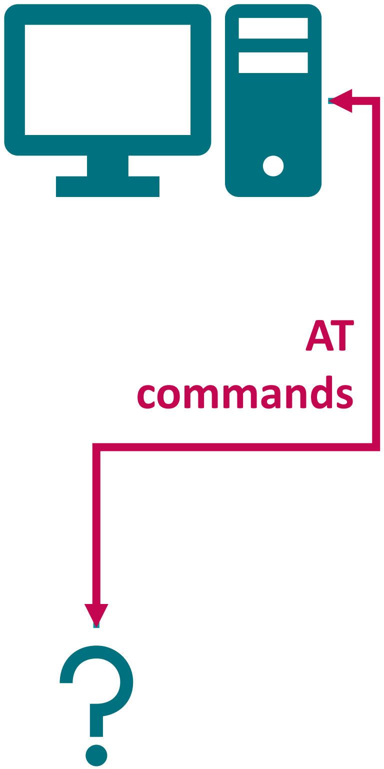
Request software version

Request MSISDN number (telephone number mapping)

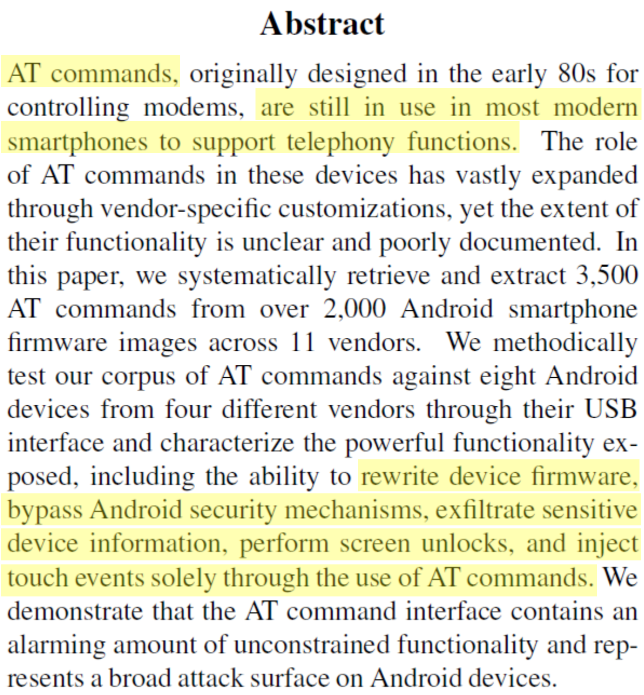
Attention! Start of communication

Device monitoring plugin (recap)

- Detects a connected device
- Communicates via AT commands
- Collects information about
  - The device: unique ID (IMEI), manufacturer, software version, model number
  - The subscriber: unique ID (IMSI), telephone number (MSISDN)

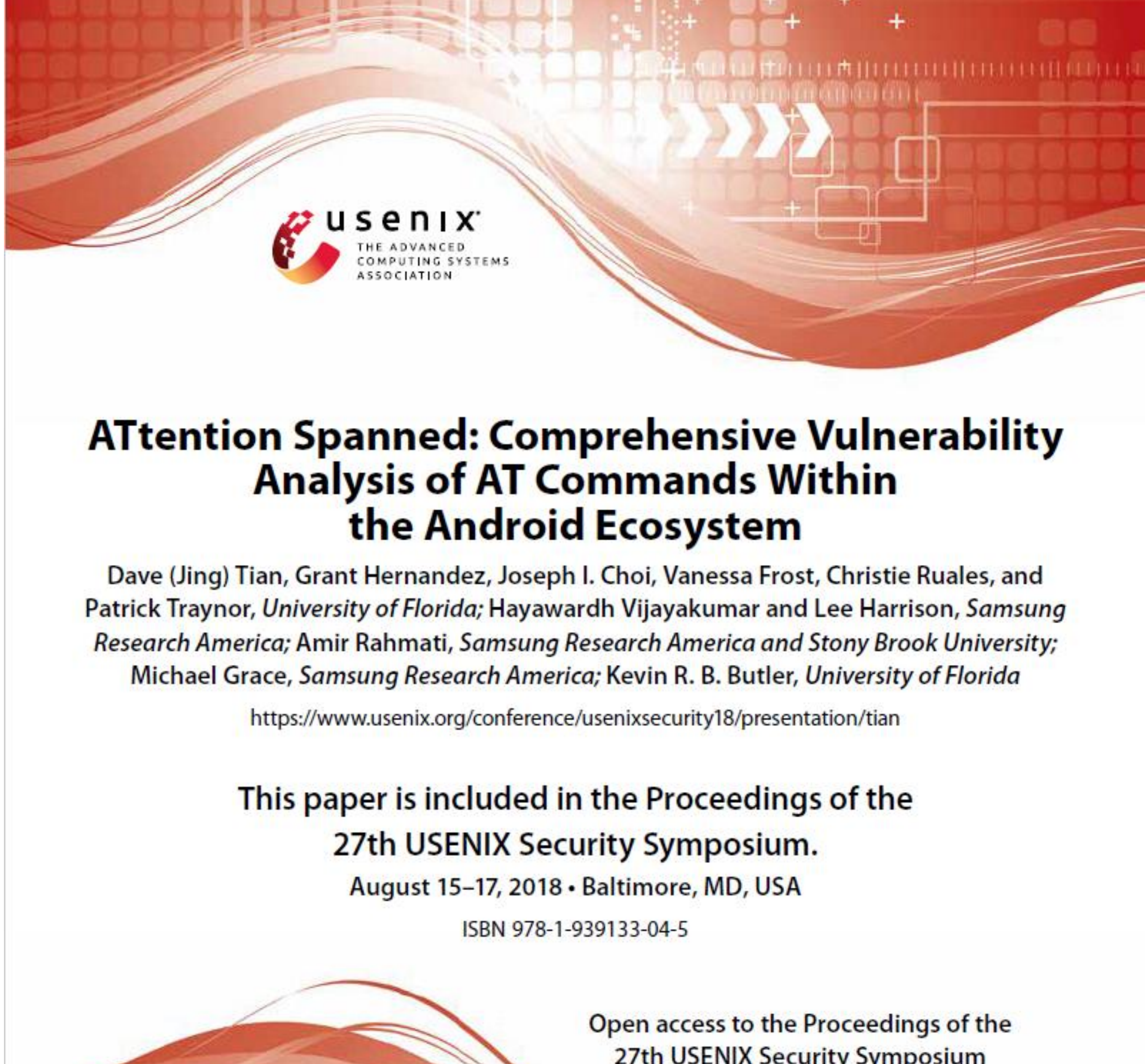


What’s ATTOR after?



Abstract

AT commands, originally designed in the early 80s for controlling modems, are still in use in most modern smartphones to support telephony functions. The role of AT commands in these devices has vastly expanded through vendor-specific customizations, yet the extent of their functionality is unclear and poorly documented. In this paper, we systematically retrieve and extract 3,500 AT commands from over 2,000 Android smartphone firmware images across 11 vendors. We methodically test our corpus of AT commands against eight Android devices from four different vendors through their USB interface and characterize the powerful functionality exposed, including the ability to rewrite device firmware, bypass Android security mechanisms, exfiltrate sensitive device information, perform screen unlocks, and inject touch events solely through the use of AT commands. We demonstrate that the AT command interface contains an alarming amount of unconstrained functionality and represents a broad attack surface on Android devices.



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem

Dave (Jing) Tian, Grant Hernandez, Joseph I. Choi, Vanessa Frost, Christie Ruales, and Patrick Traynor, *University of Florida;* Hayawardh Vijayakumar and Lee Harrison, *Samsung Research America;* Amir Rahmati, *Samsung Research America and Stony Brook University;* Michael Grace, *Samsung Research America;* Kevin R. B. Butler, *University of Florida*

https://www.usenix.org/conference/usenixsecurity18/presentation/tian

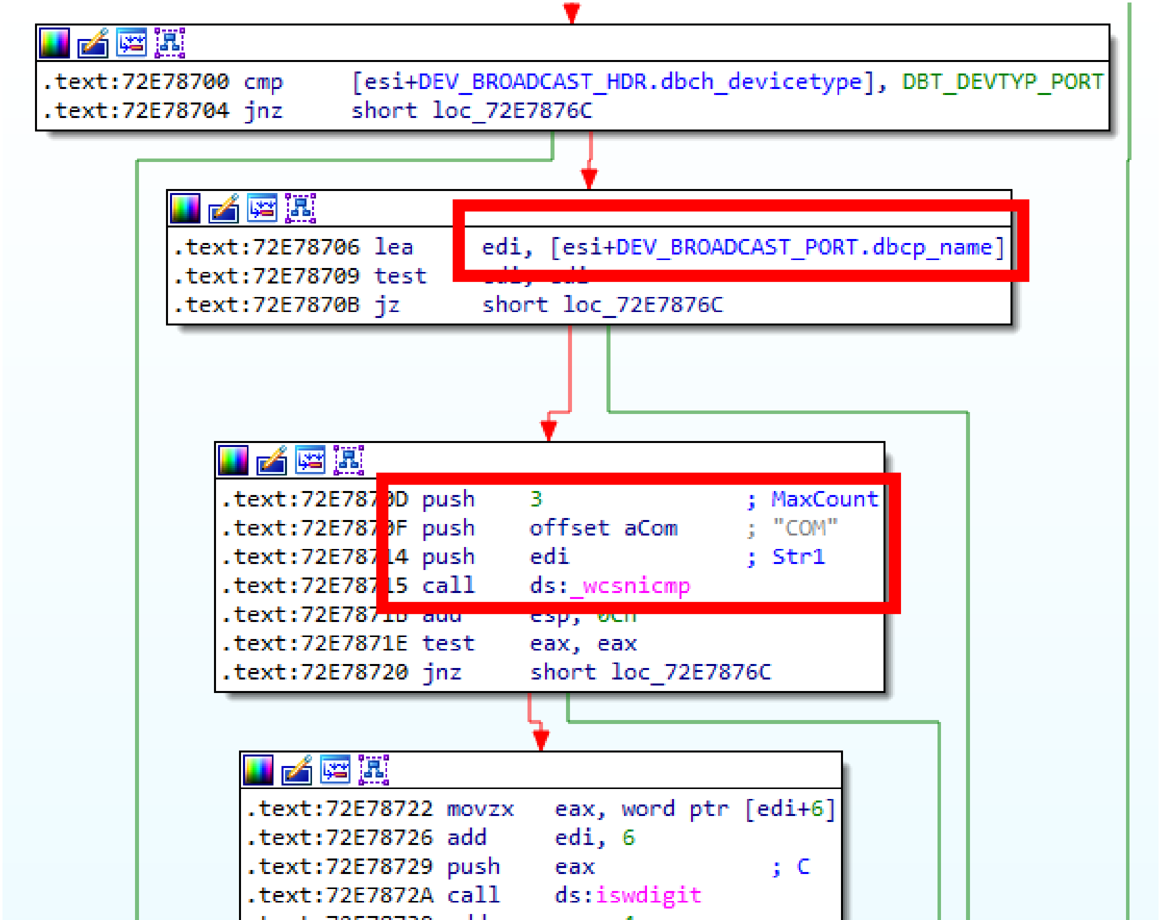
This paper is included in the Proceedings of the 27th USENIX Security Symposium.

August 15–17, 2018 • Baltimore, MD, USA

ISBN 978-1-939133-04-5

Open access to the Proceedings of the 27th USENIX Security Symposium

Smartphones fingerprinting?

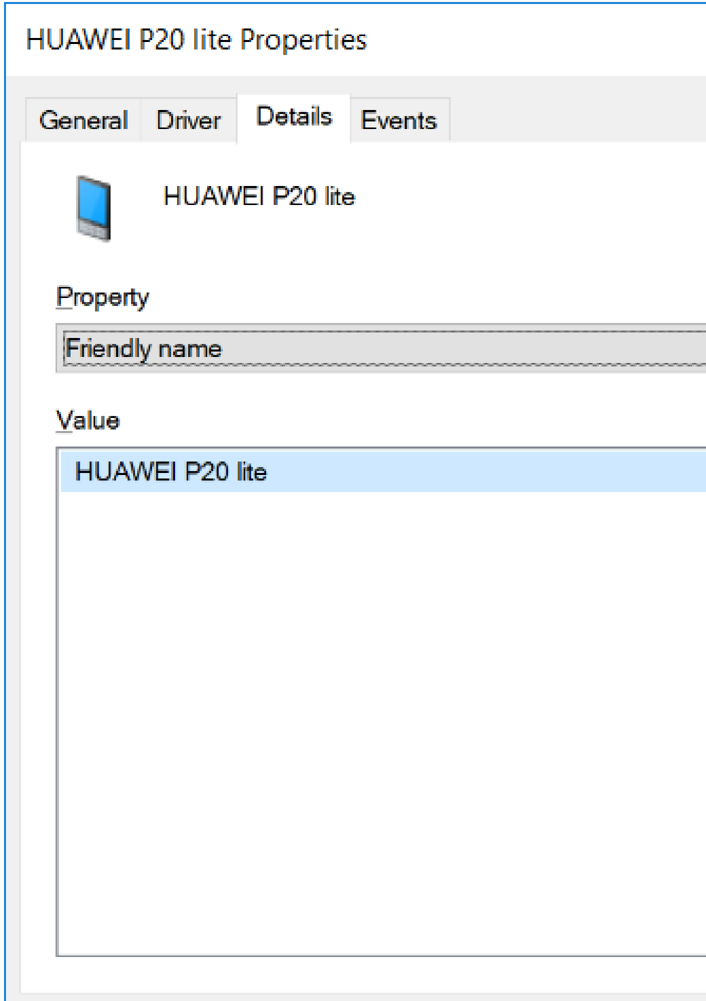


```
.text:72E78700 cmp     [esi+DEV_BROADCAST_HDR.dbch_devicetype], DBT_DEVTYP_PORT
.text:72E78704 jnz     short loc_72E7876C
```

```
.text:72E78706 lea     edi, [esi+DEV_BROADCAST_PORT.dbcp_name]
.text:72E78709 test    edi, edi
.text:72E7870B jz      short loc_72E7876C
```

```
.text:72E7870D push    3                    ; MaxCount
.text:72E7870F push    offset aCom          ; "COM"
.text:72E78714 push    edi                  ; Str1
.text:72E78715 call    ds:_wcsnicmp
.text:72E7871B add     esp, 0Ch
.text:72E7871E test    eax, eax
.text:72E78720 jnz     short loc_72E7876C
```

```
.text:72E78722 movzx   eax, word ptr [edi+6]
.text:72E78726 add     edi, 6
.text:72E78729 push    eax                  ; C
.text:72E7872A call    ds:iswdigit
```



HUAWEI P20 lite Properties

HUAWEI P20 lite

Property

Friendly name

Value

HUAWEI P20 lite

Residuum from the older ATTOR version?

- Only targets devices connected to serial port (or via USB-to-COM adaptor)
- Modems, older phones

- Plugin still included in the newest ATTOR version, first seen in 2018
- 64-bit version detected in 2019

Another hypothesis

- ATTOR targets specific devices, used in the victim’s environment/organization
- Actors behind ATTOR could learn about the devices via other reconnaissance methods

Further possibilities

- Thousands of AT commands exist – vendor-specific
- Customized plugins can be created after the initial fingerprinting
- Further data theft is possible

Conclusion

ATTOR

High profile targets in Eastern Europe

Governmental institutions

Diplomatic missions

Professionally written

Unusual functionality

Privacy-concerned, Russian-speaking targets

Read more…

ESET Research white papers

TLP: WHITE

ENJOY SAFER TECHNOLOGY™

AT COMMANDS, TOR-BASED COMMUNICATIONS: MEET ATTOR, A FANTASY CREATURE AND ALSO A SPY PLATFORM

ENJOY SAFER TECHNOLOGY™

Zuzana Hromcová

ESET Malware Analyst

@zuzana_hromcova

www.eset.com | www.welivesecurity.com | @ESETresearch