



ENJOY SAFER TECHNOLOGY™

ATTOR: Spy platform with curious GSM fingerprinting

Zuzana Hromcová | Malware Researcher



Hayes command set

AT commands

1980's

```
.data:72E7C7C0 aAtMode2  
.data:72E7C7CB aAtCgsn  
.data:72E7C7D4 aAtCimi  
.data:72E7C7DD aAtCgmm  
.data:72E7C7E6 aAtCgmi  
.data:72E7C7EF aAtCgmr  
.data:72E7C7F8 aAtCnum  
.data:72E7C801 aAt
```

```
db 'AT+MODE=2',0Dh,0  
db 'AT+CGSN',00h,0  
db 'AT+CIMI',00h,0  
db 'AT+CGMM',00h,0  
db 'AT+CGMI',00h,0  
db 'AT+CGMR',00h,0  
db 'AT+CNUM',00h,0  
db 'AT',0Dh,0
```

GSM/GPRS modems

Mobile phones

Extended AT+ set

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.



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

ATTOR

32/64-bit
espionage platform
targeting Windows



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

ATTOR operation timeline

First traces
of ATTOR

Jun 2013

May 2017

Major code
upgrade

Feb 2018

Jul 2019

Old versions

Modernized
architecture

Agenda

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

<30 TARGETS

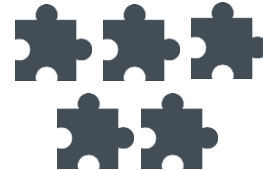
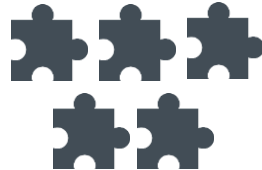


Government
organizations

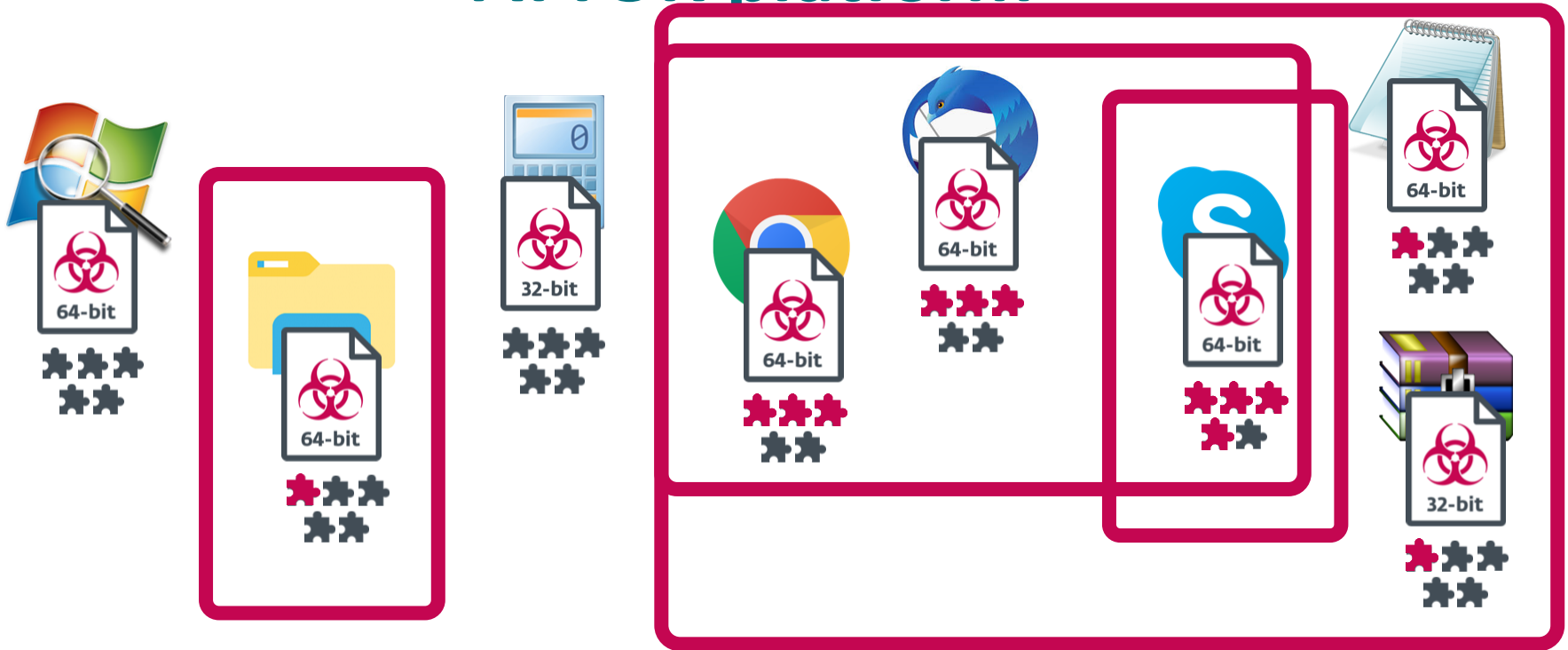


Diplomatic
missions

ATTOR platform



ATTOR platform



Network logging plugin
Serial logging plugin

The background is a solid teal color with a subtle, intricate pattern of white lines and dots, resembling a network or molecular structure. The lines connect various points, some of which are highlighted with small white dots. The overall effect is a complex, interconnected web of light against the darker teal background.

Targets?



Social networks



VoIP and IM applications



File sharing services



Mail services



WinZip®



Archiving utilities



Office software



Text editors



LIVEJOURNAL



Blogging platforms

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

Рамблер/

Rambler

**Russian search
engine**



QIP

**Russian IM
application**



WebMoney

**Russian online
payment system**



Yandex



Mail.ru

**Russian email
services**



Odnoklassniki



VKontakte

**Russian social
networks**



MEGAFON

MultiFon

**Russian VoIP
service**

Turkey

4%

Lithuania

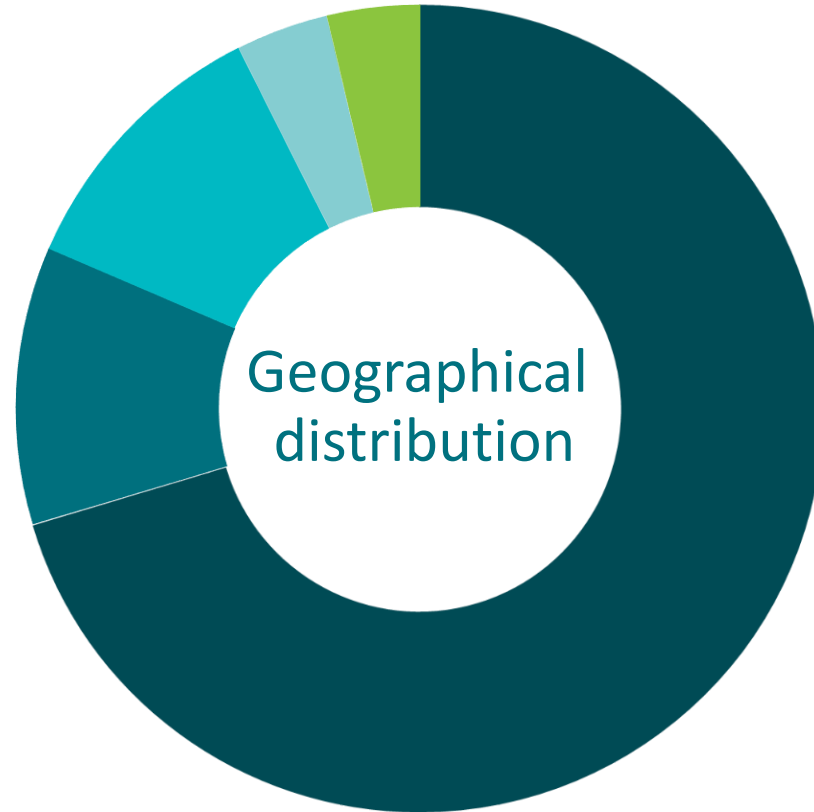
4%

Slovakia

11%

Ukraine

11%

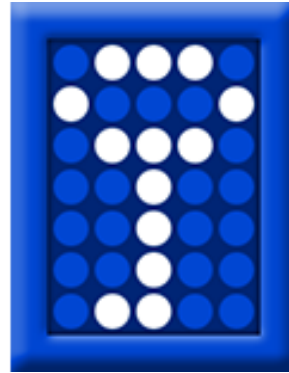


Geographical
distribution

Russia

70%

Privacy-concerned users



```

.text:72E730B9      mov     ecx, aTrueCrypt ; "TrueCrypt"
.text:72E730BF      mov     ebx, ds:_snprintf
.text:72E730C5      push   ecx
.text:72E730C6      push   offset aS        ; "\\\\.\\%s"
.text:72E730CB      lea    edx, [esp+7CCCh+fileName]
.text:72E730CF      push   31h ; '1'        ; Count
.text:72E730D1      push   edx              ; Dest
                    ebx ; _snprintf
.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)



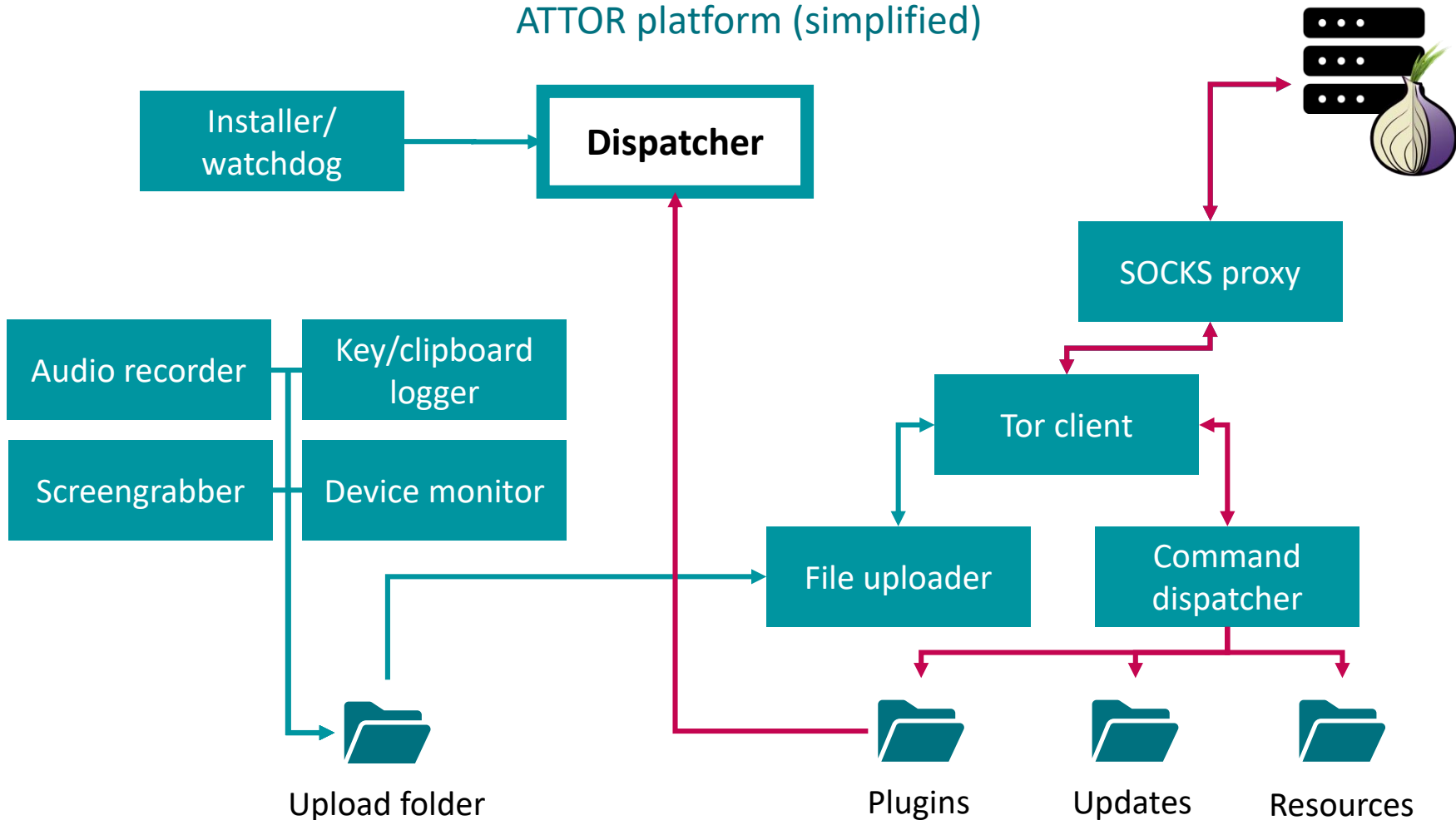
High-profile users
in Eastern Europe



Russian-speaking,
privacy-concerned users

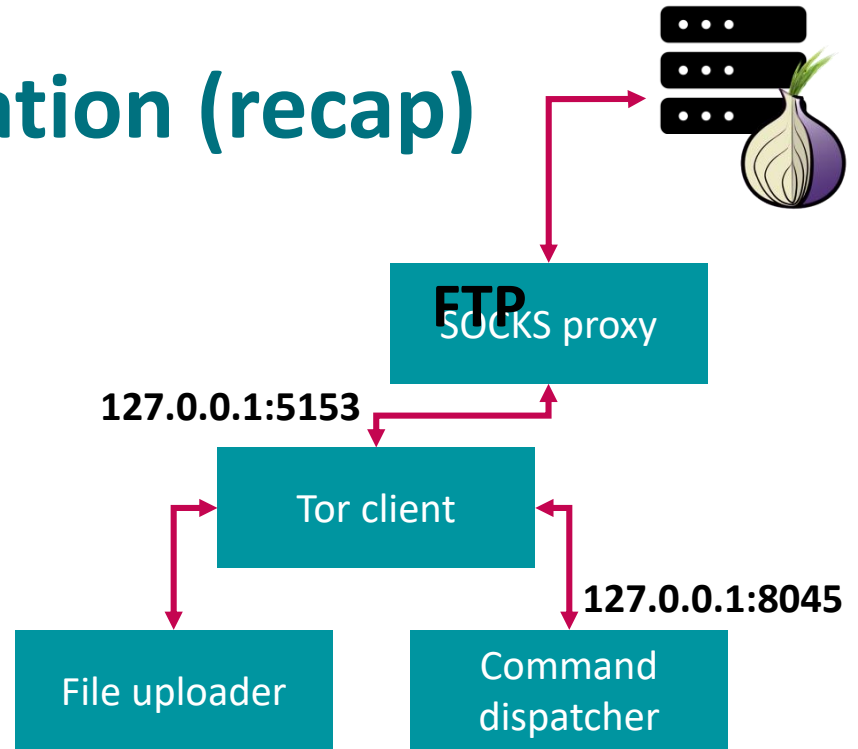
ATTOR platform

ATTOR platform (simplified)



Network communication (recap)

- Split into 4 components
- Selective activation of plugins
- Tor: Onion Service Protocol
- Customized Tor for anonymity and untraceability

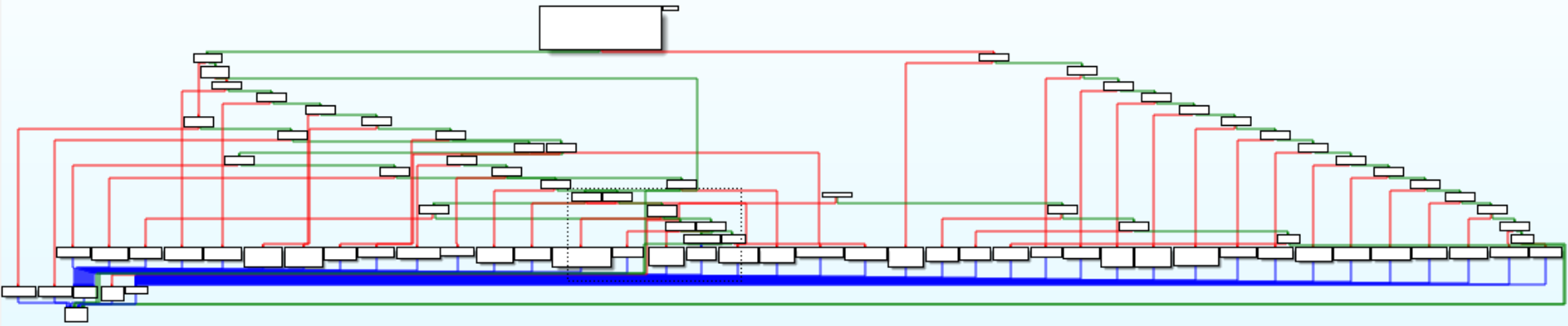


```
mov     edx, pluginId
push   ebx           ; _DWORD
push   3             ; _DWORD
push   2             ; _DWORD
push   edx           ; _DWORD
call   helperFnc
add    esp, 10h
mov    [esp+500h+bfStruct], eax
cmp    eax, ebx
jz     short loc_746D2E9E
```

```
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_CRYPT0 ; _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_CRYPT0 ; _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 ; 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
```

DllGetClassObject

[Redacted]

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

```
.text:72E71A9D mov     ecx, [eax+helperStruc.size]
.text:72E71A9F mov     helperStruc.rclsid, ecx
.text:72E71AA5 mov     edx, [eax+helperStruc.fncPtr]
.text:72E71AA8 mov     helperFnc, edx
.text:72E71AAF mov     helperStrucSize, 8
```

[Redacted]

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/SOCKS proxy
7	2, 4, 9, 7, 10	Key/clipboard logger
10	3	Privilege escalation
13	3	TOR client
15	3	Alternative network communication
16	1	Installer/watchdog

ATTOR: GSM fingerprinting

Request model number

```
.data:72E7C7C0 aAtMode2  
.data:72E7C7CB aAtCgsn  
.data:72E7C7D4 aAtCimi  
.data:72E7C7DD aAtCgmm  
.data:72E7C7E6 aAtCgmi  
.data:72E7C7EF aAtCgmr  
.data:72E7C7F8 aAtCnum  
.data:72E7C801 aAt
```

Request IMEI unique device ID

Request device manufacturer

```
db 'AT+MODE=2' 0Dh,0  
db 'AT+CGSN' 0Dh,0  
db 'AT+CIMI' 0Dh,0  
db 'AT+CGMM' 0Dh,0  
db 'AT+CGMI' 0Dh,0  
db 'AT+CGMR' 0Dh,0  
db 'AT+CNUM' 0Dh,0  
db 'AT' 0Dh,0
```

Request IMSI unique subscriber ID

Request software version

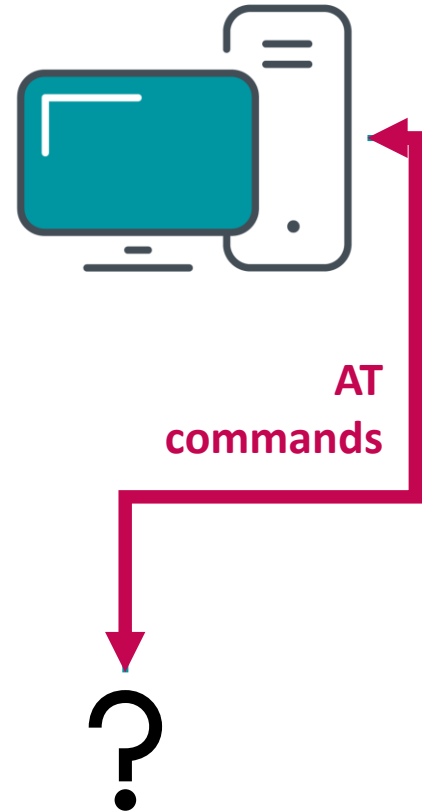
ATTENTION!
start of communication

Prepare for extended
AT+ set

Request MSISDN phone number mapping

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?



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: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

General Driver Details Events



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)
- GSM modems, older phones
- Plugin still included in the newest ATTOR version, first seen in 2018
- 64-bit version detected in 2019

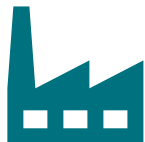


GSM/GPRS
modems, phones



Smartphones

Affected devices



ICS devices



Specialized GSM
communication devices



Device fingerprinting



Data theft

Implications



Device
compromise



Geolocation

Conclusion



High profile targets
in Eastern Europe



Professionally
written

ATTOR



Unusual
functionality




Privacy-concerned,
Russian-speaking targets

Full white paper:



Zuzana Hromcová
ESET Malware Researcher

 @ESETresearch
@zuzana_hromcova



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