2020 CERT-EU ANNUAL CONFERENCE

Remote Access Trojans in the Cyber Crime World: Past, Present, and Future

Veronica Valeros & Sebastian Garcia
{ @verovaleros, @eldracote, @StratosphereIPS }
Stratosphere Research Laboratory
Czech Technical University in Prague

Remote Access Software

A computer program that allows an individual to have **full remote control** of the device where the software is installed.

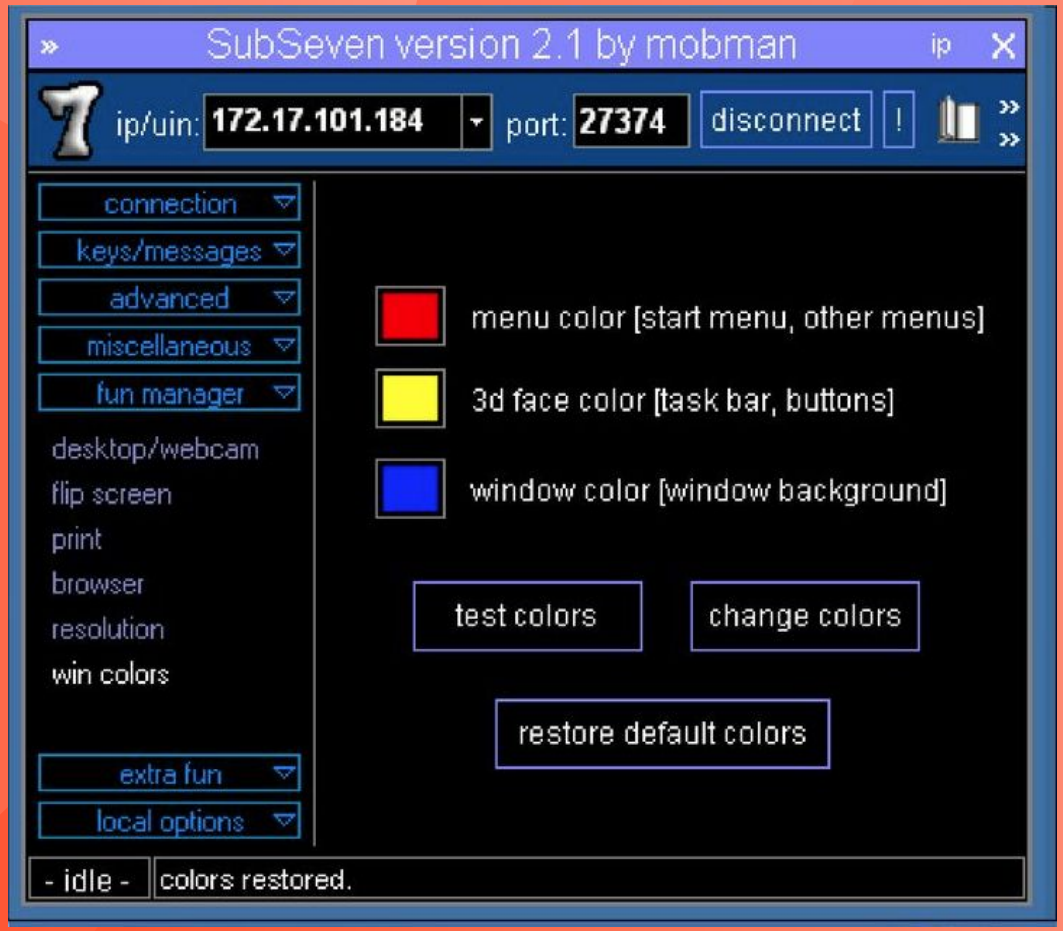
Remote Access Trojans

INSTALLED **WITHOUT** CONSENT

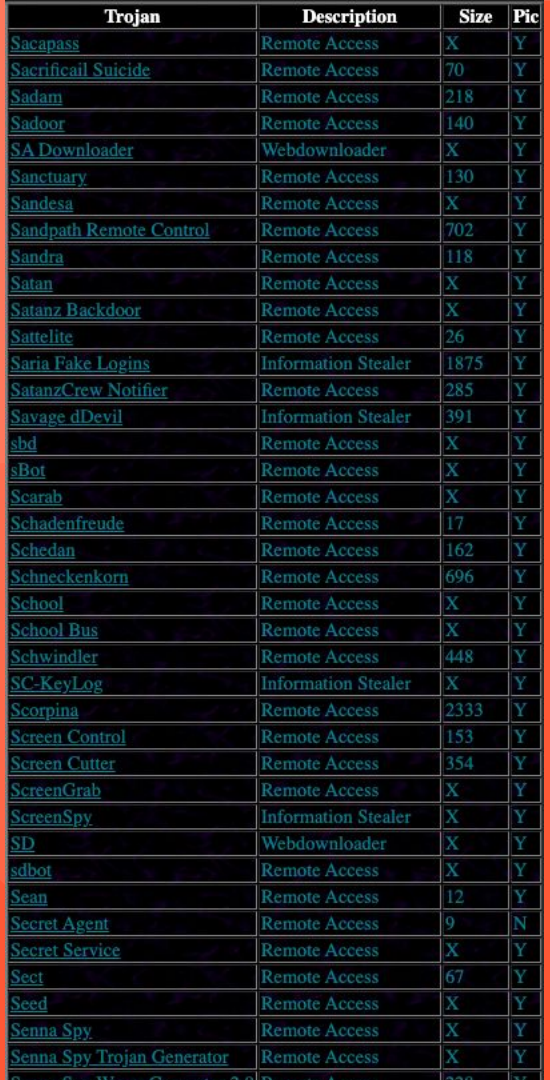
SECRET REMOTE CONTROL

HIDES TO **AVOID** DETECTION

Sub7 1999


SubSeven version 2.1 by mobman
ip
ip/uin: 172.17.101.184
port: 27374
disconnect
!
connection
keys/messages
advanced
miscellaneous
fun manager
desktop/webcam
flip screen
print
browser
resolution
win colors
extra fun
local options
menu color [start menu, other menus]
3d face color [task bar, buttons]
window color [window background]
test colors
change colors
restore default colors
- idle -
colors restored.

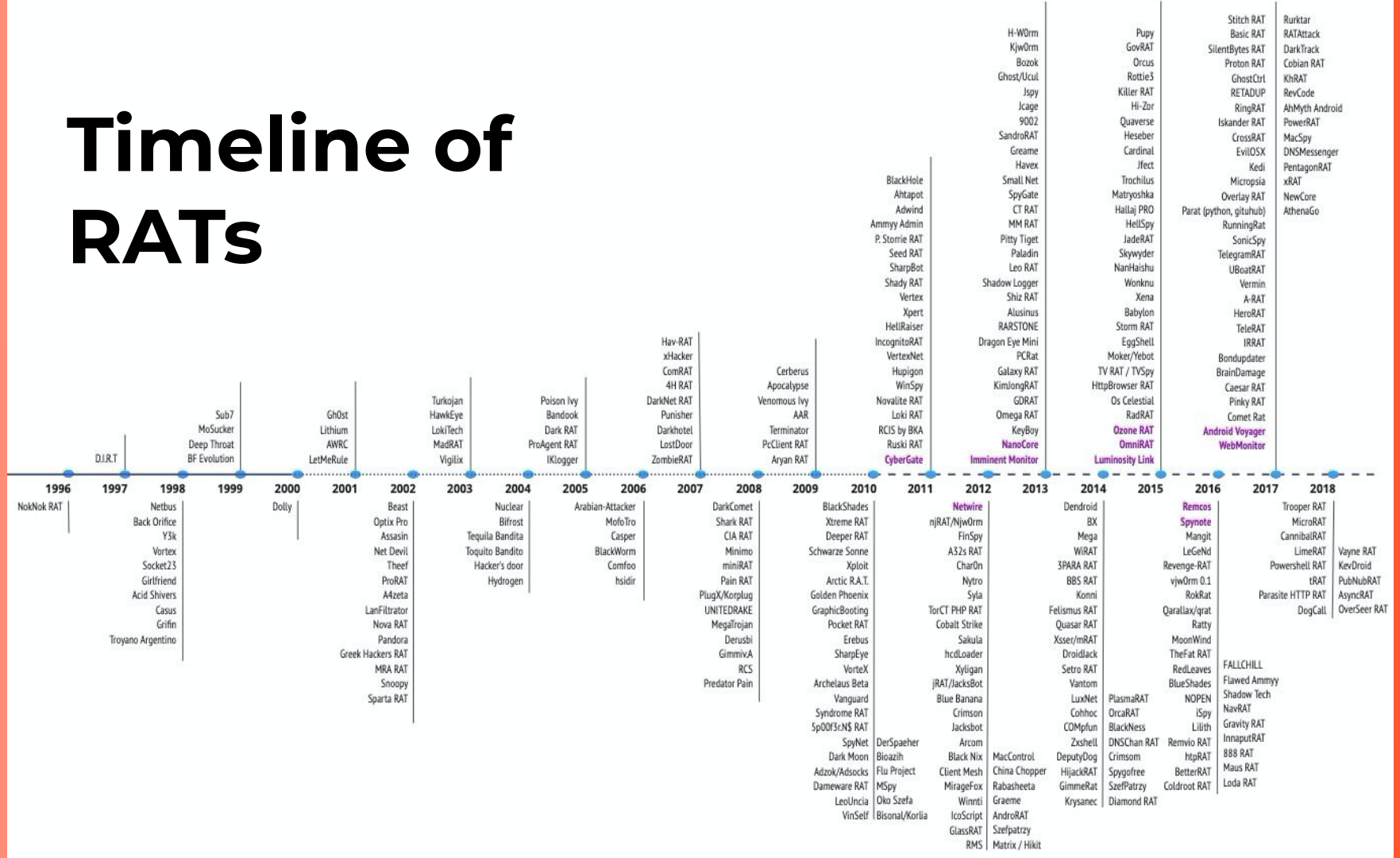
PAST:
What happened in the last 30 years?



Trojan	Description	Size	Pic
Sacapass	Remote Access	X	Y
Sacrificail Suicide	Remote Access	70	Y
Sadam	Remote Access	218	Y
Sadoor	Remote Access	140	Y
SA Downloader	Webdownloader	X	Y
Sanctuary	Remote Access	130	Y
Sandesa	Remote Access	X	Y
Sandpath Remote Control	Remote Access	702	Y
Sandra	Remote Access	118	Y
Satan	Remote Access	X	Y
Satanz Backdoor	Remote Access	X	Y
Sattelite	Remote Access	26	Y
Saria Fake Logins	Information Stealer	1875	Y
SatanzCrew Notifier	Remote Access	285	Y
Savage dDevil	Information Stealer	391	Y
sbd	Remote Access	X	Y
sBot	Remote Access	X	Y
Scarab	Remote Access	X	Y
Schadenfreude	Remote Access	17	Y
Schedan	Remote Access	162	Y
Schneckenkorn	Remote Access	696	Y
School	Remote Access	X	Y
School Bus	Remote Access	X	Y
Schwindler	Remote Access	448	Y
SC-KeyLog	Information Stealer	X	Y
Scorpina	Remote Access	2333	Y
Screen Control	Remote Access	153	Y
Screen Cutter	Remote Access	354	Y
ScreenGrab	Remote Access	X	Y
ScreenSpy	Information Stealer	X	Y
SD	Webdownloader	X	Y
sdbot	Remote Access	X	Y
Sean	Remote Access	12	Y
Secret Agent	Remote Access	9	N
Secret Service	Remote Access	X	Y
Sect	Remote Access	67	Y
Seed	Remote Access	X	Y
Senna Spy	Remote Access	X	Y
Senna Spy Trojan Generator	Remote Access	X	Y

- We collected, investigated, and built a corpus of the most well-known **RATs in history**.
- RATs are grouped in **families**, with slight variations of the same RATs grouped together.
- Documented **337** unique families of RATs.

Timeline of RATs



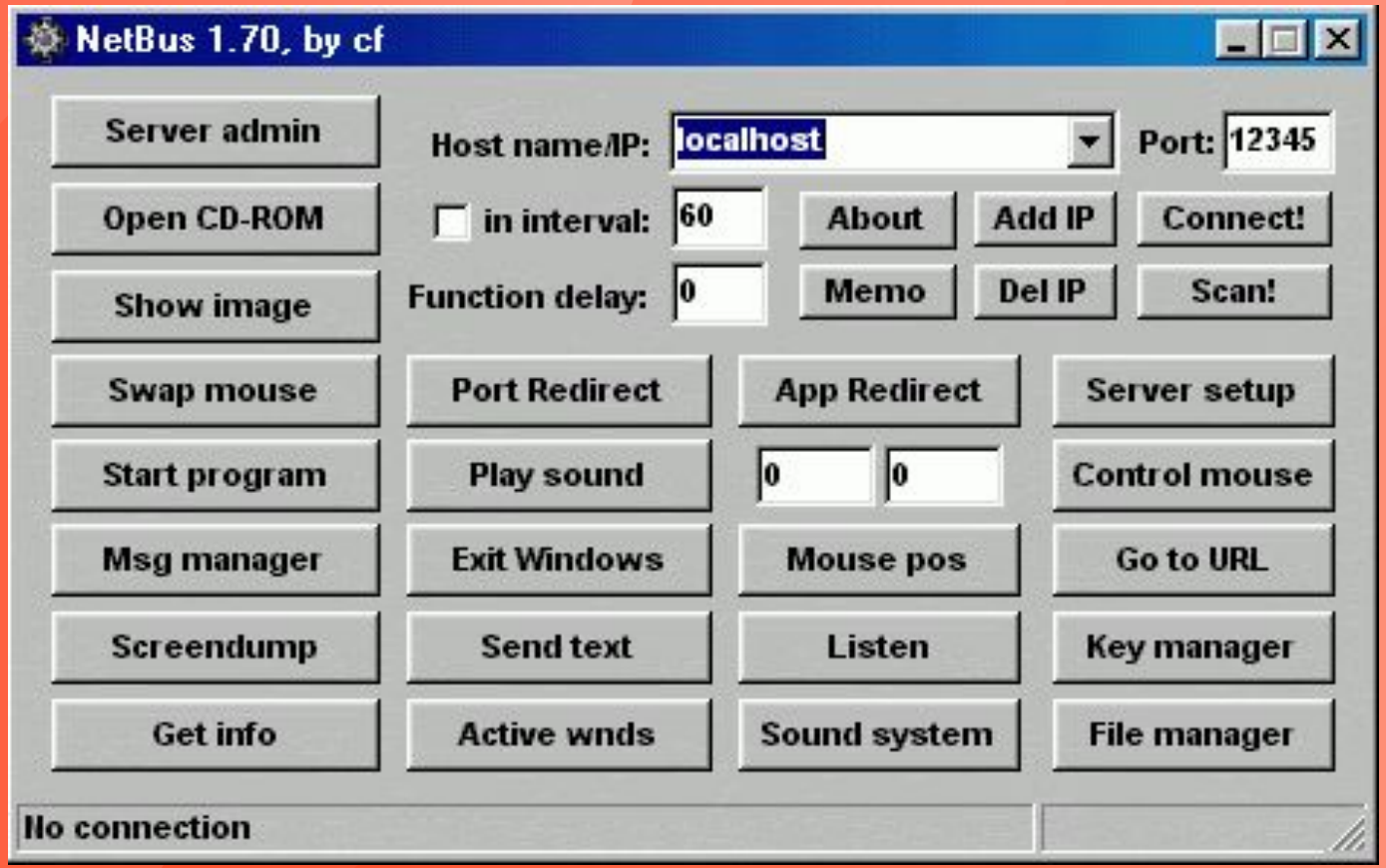
1996-2000	2001-2010	2011-2020
Phase 1	**Phase 2**	**Phase 3**
16 RAT families	70 RAT families	251 RAT families
	4.3x growth	3.5x growth

1996-2000

Phase 1

16 RAT families

NetBus RAT 1999



Phase 1: 1996 - 2000

- Era of homemade RATs: **fun and amusement**.
- Developers and operators were the **same actor.**
- Most prominent RATs: Back Orifice, Sub7 and Netbus.
- **Innovative** and disruptive.

2001-2010

Phase 2

70 RAT families

4.3x growth

Beast RAT 2002

Phase 2: 2001 - 2010

- RATs started to be used for **attacks and profit.**
- Developers and operators are **different** actors.
- Most prominent RATs: Gh0st, PoisonIvy and DarkComet.
- The **market** started to mature.

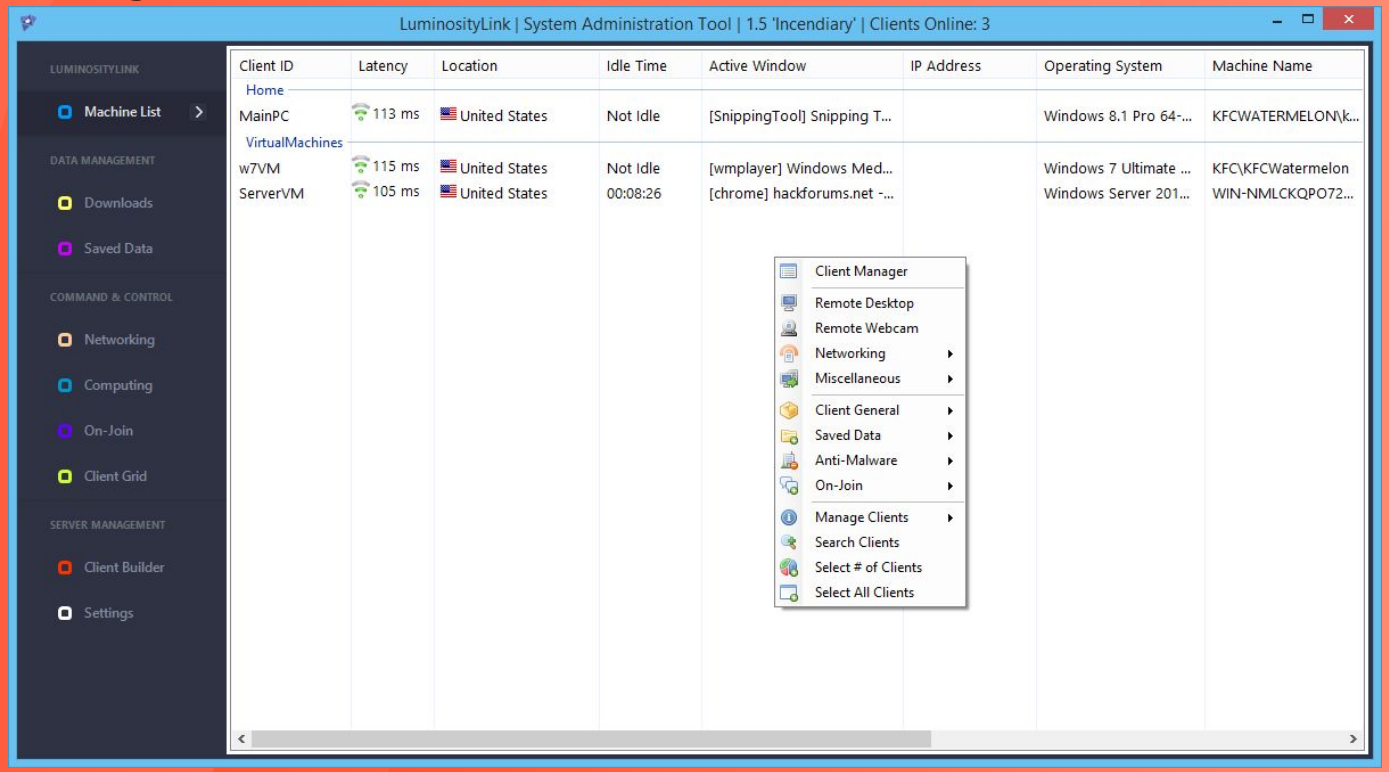
2011-2020

Phase 3

251 RAT families

3.5x growth

Luminosity RAT 2015



Phase 3: 2011 - 2020

- Developers became **entrepreneurs**.
- Multi-tiered operators driving the market.
- Prominent RATs: NanoCore, NjRAT, and Imminent Monitor.
- Sellers provide support, new features, and host part of the infrastructure.

PRESENT:
RATs in Markets

RATs	Sellers and Marketplaces (USD)					
	DaVinciCoders	Secret Hacker Society	buyallrat588	Dorian Docs	FUD Exploits	Ultra Hacks
CyberGate RAT	-	200	30-65	-	-	-
NetWire RAT	-	120	-	-	120	180
Imminent Monitor RAT	45	-	50-120	20-70	20-100	-
NanoCore RAT	45	96	-	-	150-170	-
Luminosity Link RAT	75	55	-	-	150	-
Omni Android RAT	-	80	60-150	120	120	180
Ozone RAT	75	-	-	-	170	-
Remcos RAT	-	99	-	-	170	-
SpyNote RAT	-	69	80-140	-	150-170	69
Android Voyager RAT	-	90	30-65	30-150	30	55-250
WebMonitor RAT	-	-	-	60-120	60	70-140

BUILDERS **CRYPTERS** **PLUGINS**

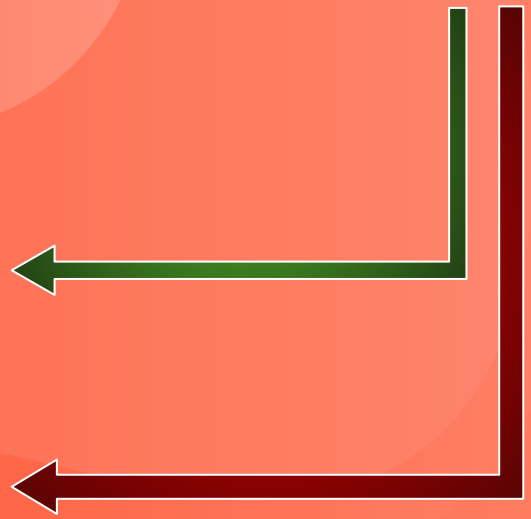
Who is using?

- Newbies to learn
- ‘Hackers’ for fun
- State-sponsored attackers
- Cybercrime groups for financial profit

Who is using?

- ~~Newbies to learn~~
- ~~‘Hackers’ for fun~~
- State-sponsored attackers
- Cybercrime groups for financial profit

Who is buying?



For what purpose?

- Business Email Compromise
- Cyber espionage
- Targeted Attacks
- Stalkerware
- **RATs are essential for most cybercriminal activities**

FUTURE: Where are RATs going?

Why new RATs appear?

- Attackers fear **backdoored** RATs
- Lack of **trust** in the underground markets
- Safer to create **your own**
- “**Real** hackers code their own RATs”

- RATs will continue to appear and get better
- New and more mature markets
- Adaptation to new attacks and technologies

Future work

- Analysis of RATs features
- Expand market research
- Evaluate change in RAT prices over time
- Stalkerware, Spyware, Children monitoring apps

Thanks!

www.stratosphereips.org

Veronica Valeros
veronica.valeros@aic.fel.cvut.cz
@verovaleros

Sebastian Garcia
sebastian.garcia@agents.fel.cvut.cz
@eldracote