2ND WORKSHOP ON ATTACKERS AND CYBER-CRIME OPERATIONS
IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY 2020
SEPTEMBER 7 - VIRTUAL CONFERENCE

Growth and Commoditization of Remote Access Trojans

Veronica Valeros & Sebastian Garcia
Stratosphere Research Laboratory
Czech Technical University in Prague

Remote Access Trojans

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

INSTALLED WITHOUT CONSENT

SECRET REMOTE CONTROL

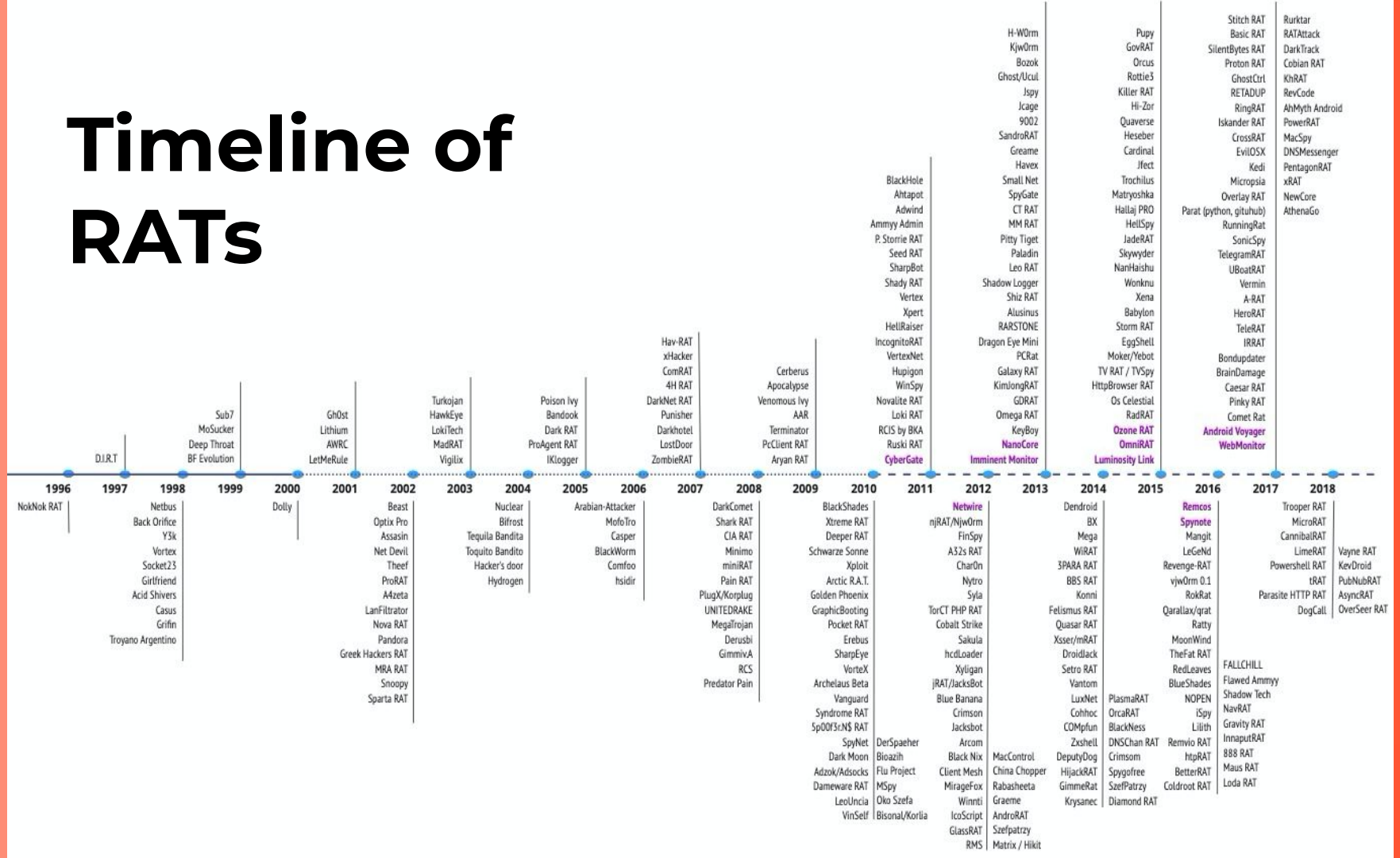
HIDES TO AVOID DETECTION

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

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.

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.

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.

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**

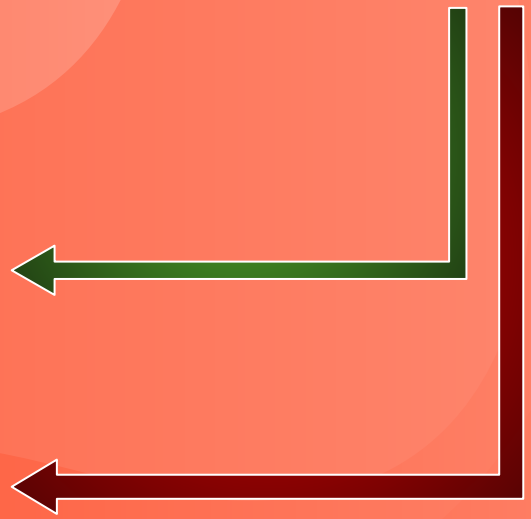
Who is using?

- 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 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