Growth and Commoditization of Remote Access Trojans

Veronica Valeros & Sebastian Garcia

Stratosphere Research Laboratory

Czech Technical University in Prague

REMOTE ACCESS SOFTWARE

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

REMOTE ACCESS TROJAN

CONSENT

Installation **without** user consent

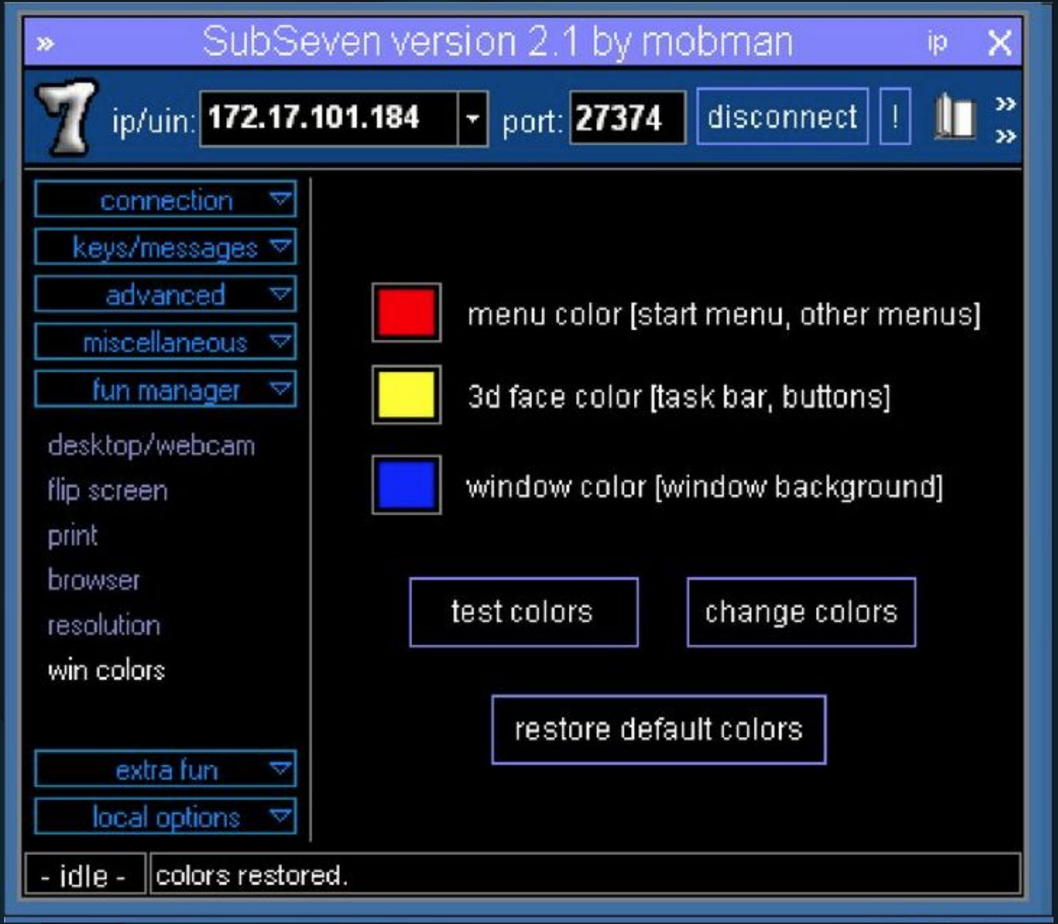
CONTROL

Remote control is performed **secretly**

EVASION

Hiding in the system to **avoid detection**

Sub7 1999



SubSeven version 2.1 by mobman

ip/uin: 172.17.101.184 port: 27374

🟥 menu color [start menu, other menus]

🟨 3d face color [task bar, buttons]

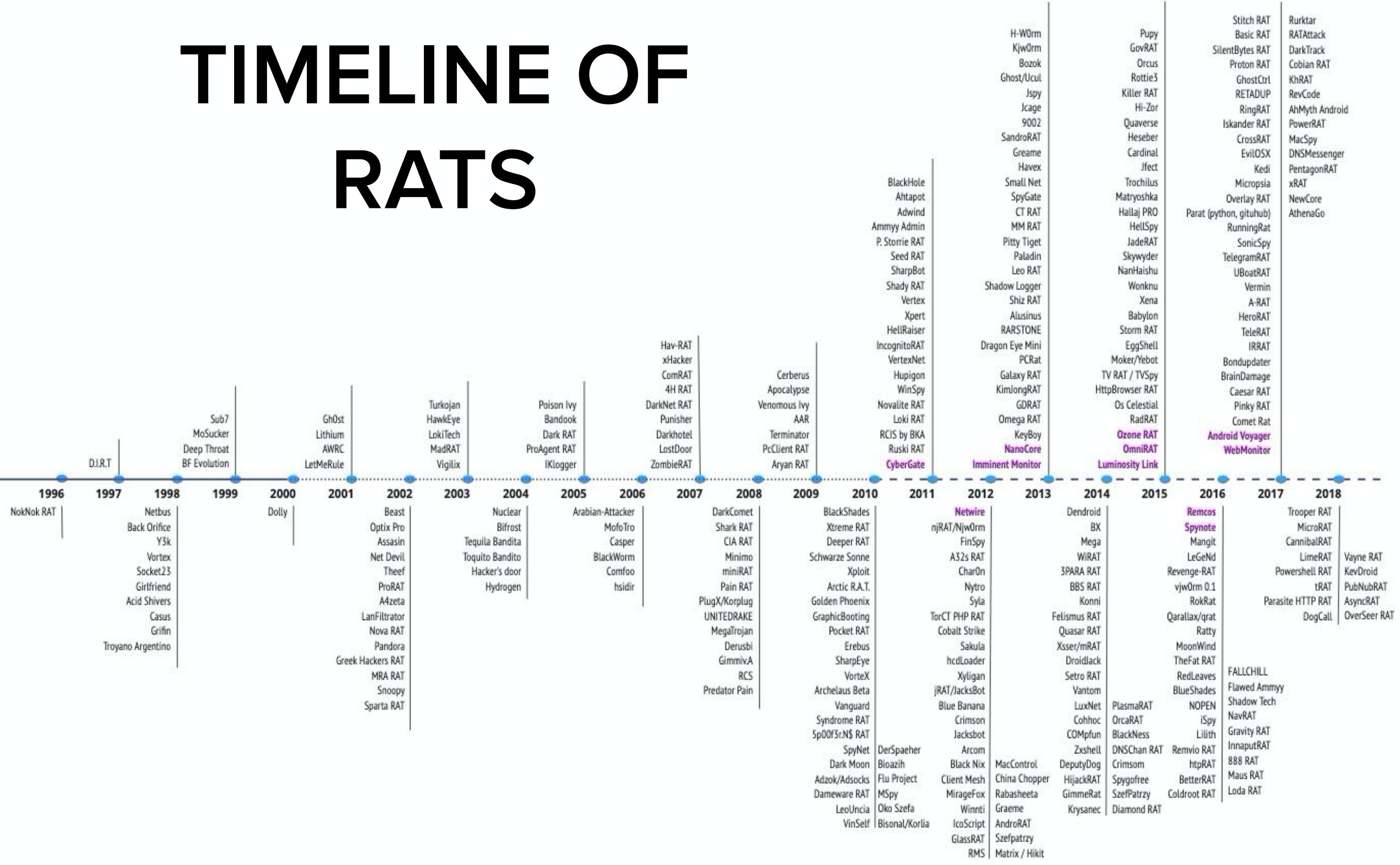
🟦 window color [window background]

- idle - colors restored.

What happened in the last 30 years?

- 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.
- Found, referenced, and documented 337 unique families of RATs.

TIMELINE OF RATS



NokNok RAT

D.I.R.T

Netbus
Back Orifice
Y3k
Vortex
Socket23
Girlfriend
Acid Shivers
Casus
Grifin
Troyano Argentino

Sub7
MoSucker
Deep Throat
BF Evolution

Dolly

Gh0st
Lithium
AWRC
LetMeRule

Beast
Optix Pro
Assasin
Net Devil
Theef
ProRAT
A4zeta
LanFiltrator
Nova RAT
Pandora
Greek Hackers RAT
MRA RAT
Snoopy
Sparta RAT

Turkojan
HawkEye
LokiTech
MadRAT
Vigilix

Nuclear
Bifrost
Tequila Bandita
Toquito Bandito
Hacker's door
Hydrogen

Poison Ivy
Bandook
Dark RAT
ProAgent RAT
IKlogger

Arabian-Attacker
MofoTro
Casper
BlackWorm
Comfoo
hsidir

Hav-RAT
xHacker
ComRAT
4H RAT
DarkNet RAT
Punisher
Darkhotel
LostDoor
ZombieRAT

DarkComet
Shark RAT
CIA RAT
Minimo
miniRAT
Pain RAT
PlugX/Korplug
UNITEDRAKE
MegaTrojan
Derusbi
Gimmiv.A
RCS
Predator Pain

Cerberus
Apocalypse
Venomous Ivy
AAR
Terminator
PcClient RAT
Aryan RAT

BlackShades
Xtreme RAT
Deeper RAT
Schwarze Sonne
Xploit
Arctic R.A.T.
Golden Phoenix
GraphicBooting
Pocket RAT
Erebus
SharpEye
VorteX
Archelaus Beta
Vanguard
Syndrome RAT
5p00f3r.N$ RAT
SpyNet
Dark Moon
Adzok/Adsocks
Dameware RAT
LeoUncia
VinSelf

DerSpaeher
Bioazih
Flu Project
MSpy
Oko Szefa
Bisonal/Korlia

BlackHole
Ahtapot
Adwind
Ammyy Admin
P. Storrie RAT
Seed RAT
SharpBot
Shady RAT
Vertex
Xpert
HellRaiser
IncognitoRAT
VertexNet
Hupigon
WinSpy
Novalite RAT
Loki RAT
RCIS by BKA
Ruski RAT
CyberGate

Netwire
njRAT/Njw0rm
FinSpy
A32s RAT
Char0n
Nytro
Syla
TorCT PHP RAT
Cobalt Strike
Sakula
hcdLoader
Xyligan
jRAT/JacksBot
Blue Banana
Crimson
Jacksbot
Arcom
Black Nix
Client Mesh
MirageFox
Winnti
IcoScript
GlassRAT
RMS

MacControl
China Chopper
Rabasheeta
Graeme
AndroRAT
Szefpatrzy
Matrix / Hikit

H-W0rm
Kjw0rm
Bozok
Ghost/Ucul
Jspy
Jcage
9002
SandroRAT
Greame
Havex
Small Net
SpyGate
CT RAT
MM RAT
Pitty Tiget
Paladin
Leo RAT
Shadow Logger
Shiz RAT
Alusinus
RARSTONE
Dragon Eye Mini
PCRat
Galaxy RAT
KimJongRAT
GDRAT
Omega RAT
KeyBoy
NanoCore
Imminent Monitor

Dendroid
BX
Mega
WiRAT
3PARA RAT
BBS RAT
Konni
Felismus RAT
Quasar RAT
Xsser/mRAT
DroidJack
Setro RAT
Vantom
LuxNet
Cohhoc
COMpfun
Zxshell
DeputyDog
HijackRAT
GimmeRat
Krysanec

PlasmaRAT
OrcaRAT
BlackNess
DNSChan RAT
Crimsom
Spygofree
SzefPatrzy
Diamond RAT

Pupy
GovRAT
Orcus
Rottie3
Killer RAT
Hi-Zor
Quaverse
Heseber
Cardinal
Jfect
Trochilus
Matryoshka
Hallaj PRO
HellSpy
JadeRAT
Skywyder
NanHaishu
Wonknu
Xena
Babylon
Storm RAT
EggShell
Moker/Yebot
TV RAT / TVSpy
HttpBrowser RAT
Os Celestial
RadRAT
Ozone RAT
OmniRAT
Luminosity Link

Remcos
Spynote
Mangit
LeGeNd
Revenge-RAT
vjw0rm 0.1
RokRat
Qarallax/qrat
Ratty
MoonWind
TheFat RAT
RedLeaves
BlueShades
NOPEN
iSpy
Lilith
Remvio RAT
htpRAT
BetterRAT
Coldroot RAT

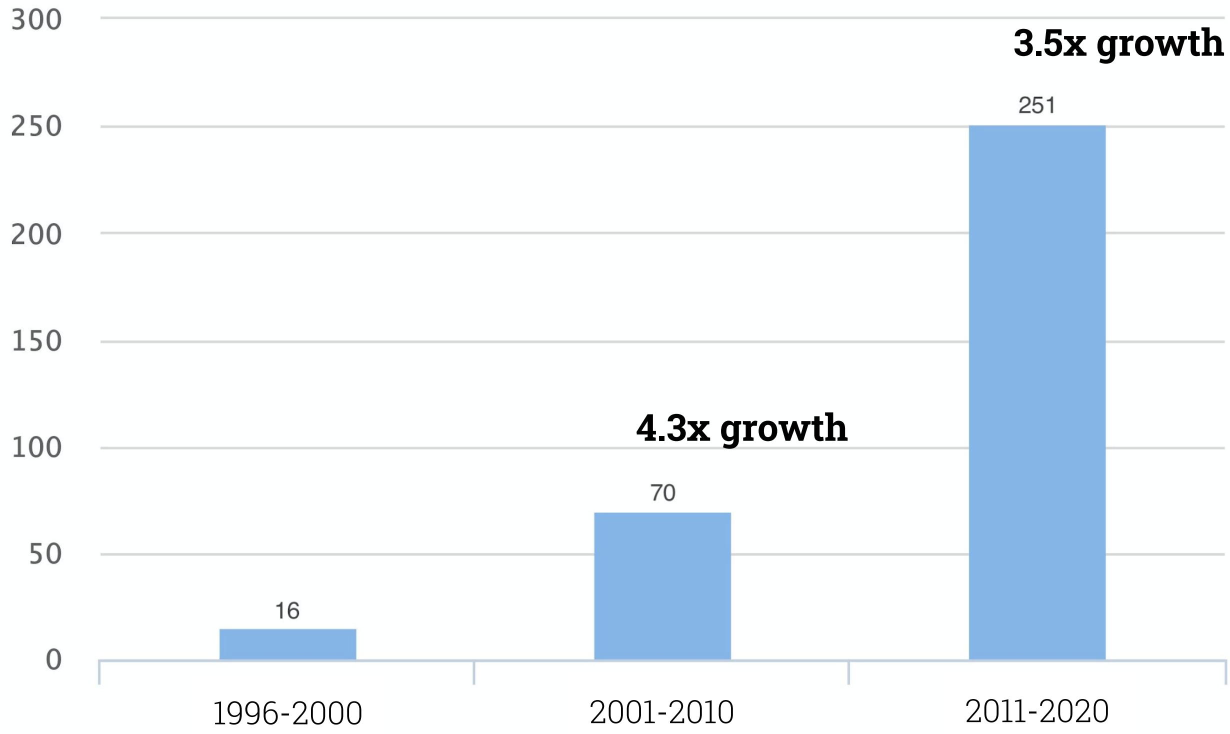
FALLCHILL
Flawed Ammyy
Shadow Tech
NavRAT
Gravity RAT
InnaputRAT
888 RAT
Maus RAT
Loda RAT

Stitch RAT
Basic RAT
SilentBytes RAT
Proton RAT
GhostCtrl
RETADUP
RingRAT
Iskander RAT
CrossRAT
EvilOSX
Kedi
Micropsia
Overlay RAT
Parat (python, gituhub)
RunningRat
SonicSpy
TelegramRAT
UBoatRAT
Vermin
A-RAT
HeroRAT
TeleRAT
IRRAT
Bondupdater
BrainDamage
Caesar RAT
Pinky RAT
Comet Rat
Android Voyager
WebMonitor

Trooper RAT
MicroRAT
CannibalRAT
LimeRAT
Powershell RAT
tRAT
Parasite HTTP RAT
DogCall

Vayne RAT
KevDroid
PubNubRAT
AsyncRAT
OverSeer RAT

Rurktar
RATAttack
DarkTrack
Cobian RAT
KhRAT
RevCode
AhMyth Android
PowerRAT
MacSpy
DNSMessenger
PentagonRAT
xRAT
NewCore
AthenaGo


300
250
200
150
100
50
0
3.5x growth
251
4.3x growth
70
16
1996-2000
2001-2010
2011-2020

1996-2000

Phase 1

2001-2010

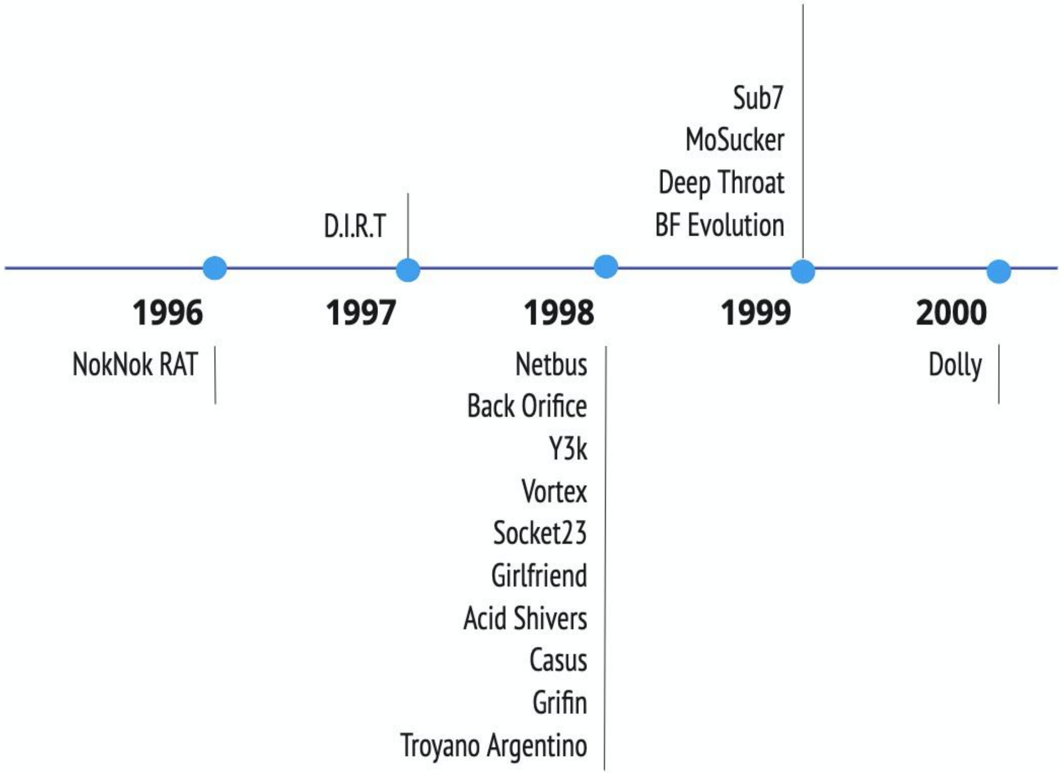
Phase 2

2011-2020

Phase 3

PHASE
01

1996-2000



1996

NokNok RAT

1997

D.I.R.T

1998

Netbus
Back Orifice
Y3k
Vortex
Socket23
Girlfriend
Acid Shivers
Casus
Grifin
Troyano Argentino

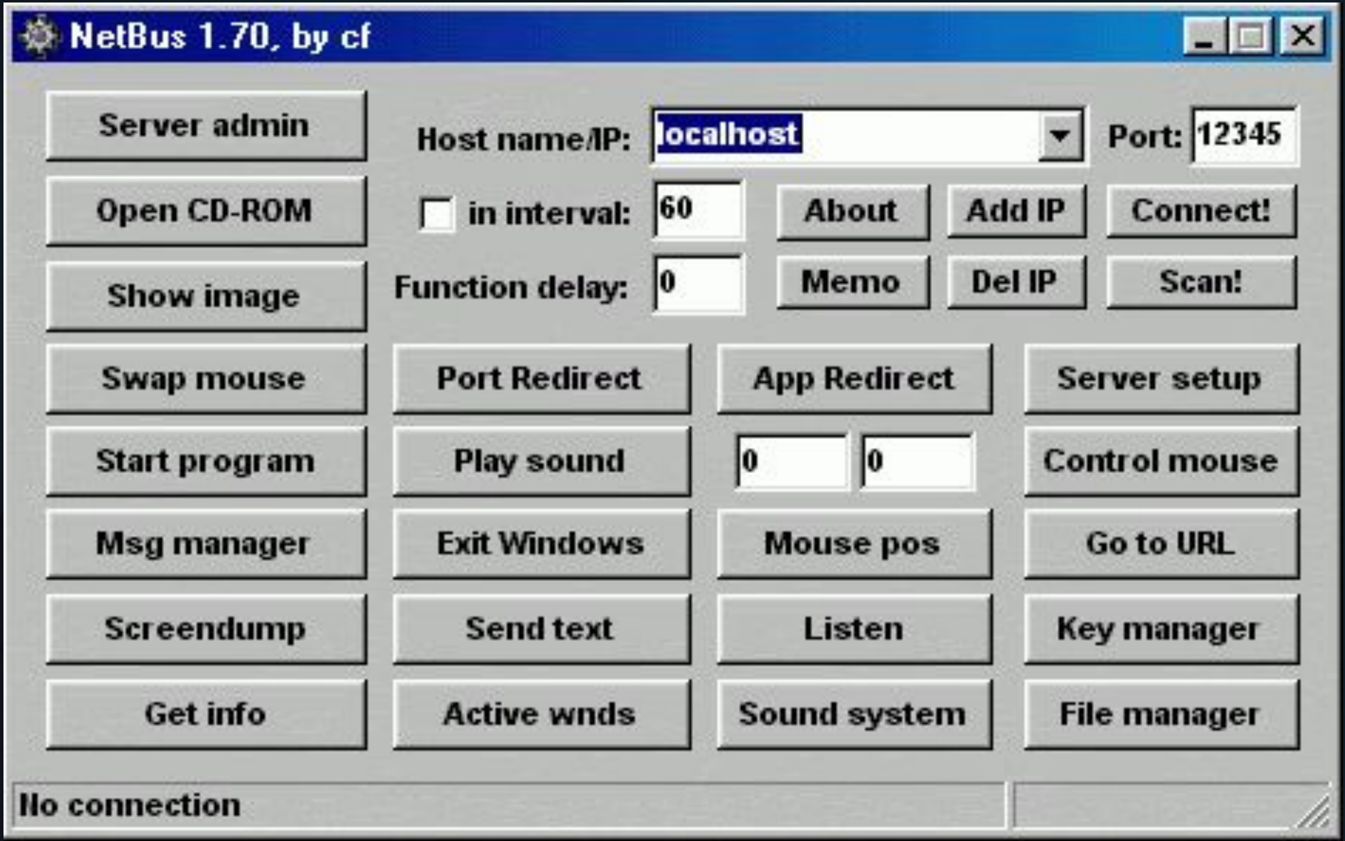
1999

Sub7
MoSucker
Deep Throat
BF Evolution

2000

Dolly

NetBus
RAT 1999



NetBus 1.70, by cf

Host name/IP: localhost

Port: 12345

□ in interval: 60

Function delay: 0

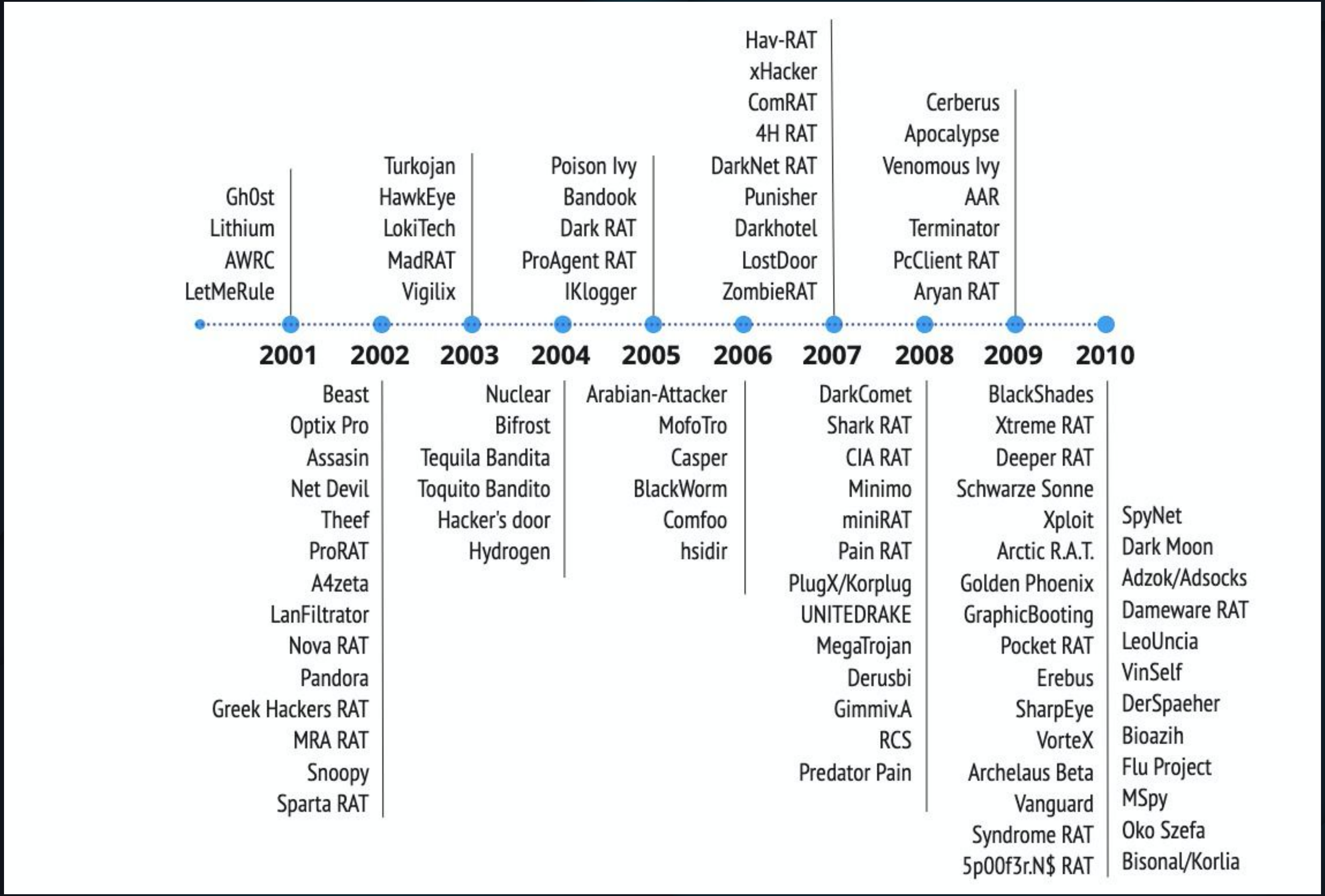
0 0

No connection

- The era of homemade RATs, for fun and amusement.
- Developers and operators were the same actor.
- Among the most prominent ones were Back Orifice, Sub7 and Netbus.
- Together they defined a generation by being innovative and disruptive.

PHASE
02

2001-2010



Gh0st
Lithium
AWRC
LetMeRule

Turkojan
HawkEye
LokiTech
MadRAT
Vigilix

Poison Ivy
Bandook
Dark RAT
ProAgent RAT
IKlogger

Hav-RAT
xHacker
ComRAT
4H RAT
DarkNet RAT
Punisher
Darkhotel
LostDoor
ZombieRAT

Cerberus
Apocalypse
Venomous Ivy
AAR
Terminator
PcClient RAT
Aryan RAT

2001 2002 2003 2004 2005 2006 2007 2008 2009 2010

Beast
Optix Pro
Assasin
Net Devil
Theef
ProRAT
A4zeta
LanFiltrator
Nova RAT
Pandora
Greek Hackers RAT
MRA RAT
Snoopy
Sparta RAT

Nuclear
Bifrost
Tequila Bandita
Toquito Bandito
Hacker's door
Hydrogen

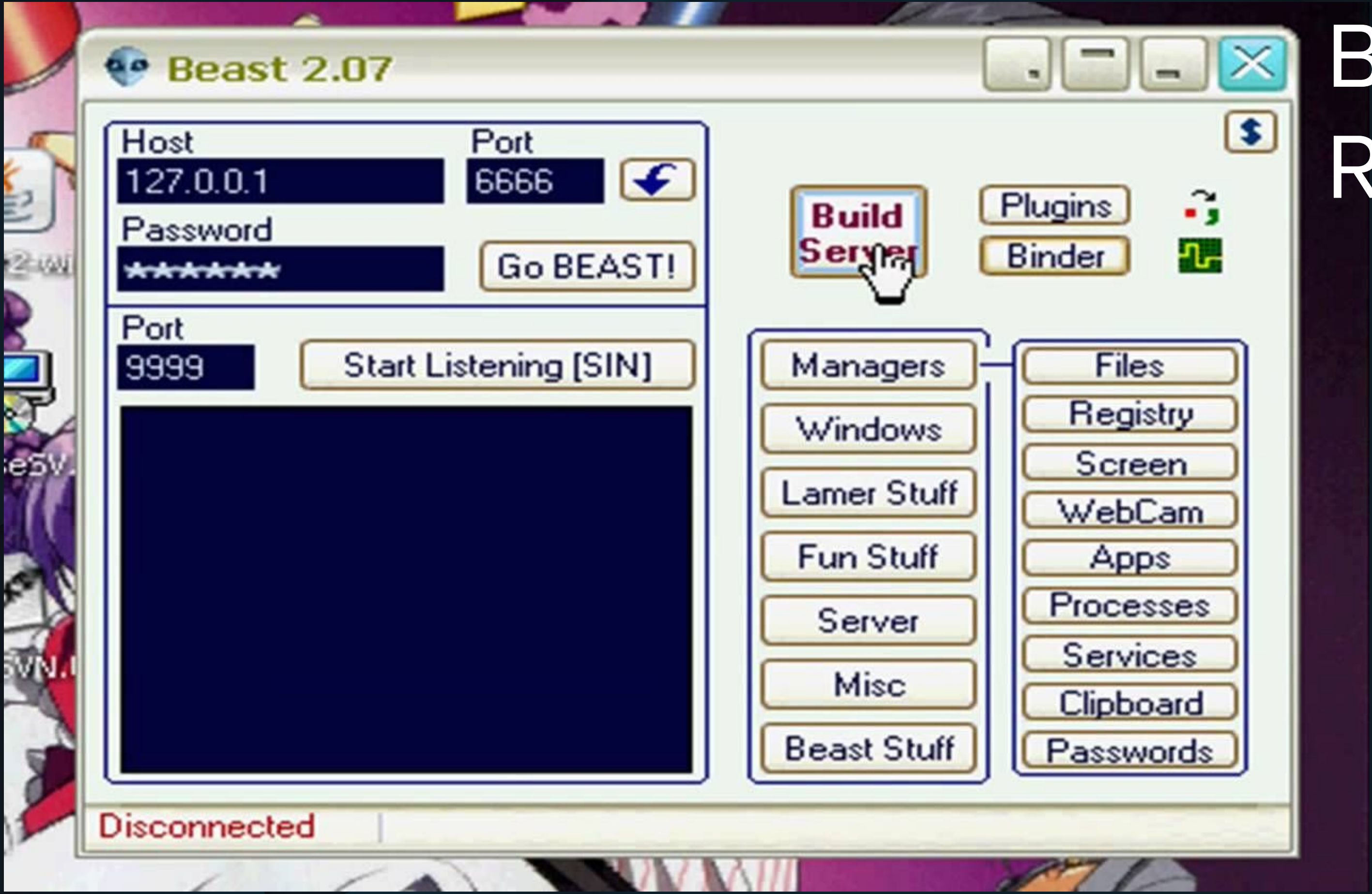
Arabian-Attacker
MofoTro
Casper
BlackWorm
Comfoo
hsidir

DarkComet
Shark RAT
CIA RAT
Minimo
miniRAT
Pain RAT
PlugX/Korplug
UNITEDRAKE
MegaTrojan
Derusbi
Gimmiv.A
RCS
Predator Pain

BlackShades
Xtreme RAT
Deeper RAT
Schwarze Sonne
Xploit
Arctic R.A.T.
Golden Phoenix
GraphicBooting
Pocket RAT
Erebus
SharpEye
VorteX
Archelaus Beta
Vanguard
Syndrome RAT
5p00f3r.N$ RAT

SpyNet
Dark Moon
Adzok/Adsocks
Dameware RAT
LeoUncia
VinSelf
DerSpaeher
Bioazih
Flu Project
MSpy
Oko Szefa
Bisonal/Korlia

Beast
RAT 2002



Host 127.0.0.1

Port 6666

Password *******

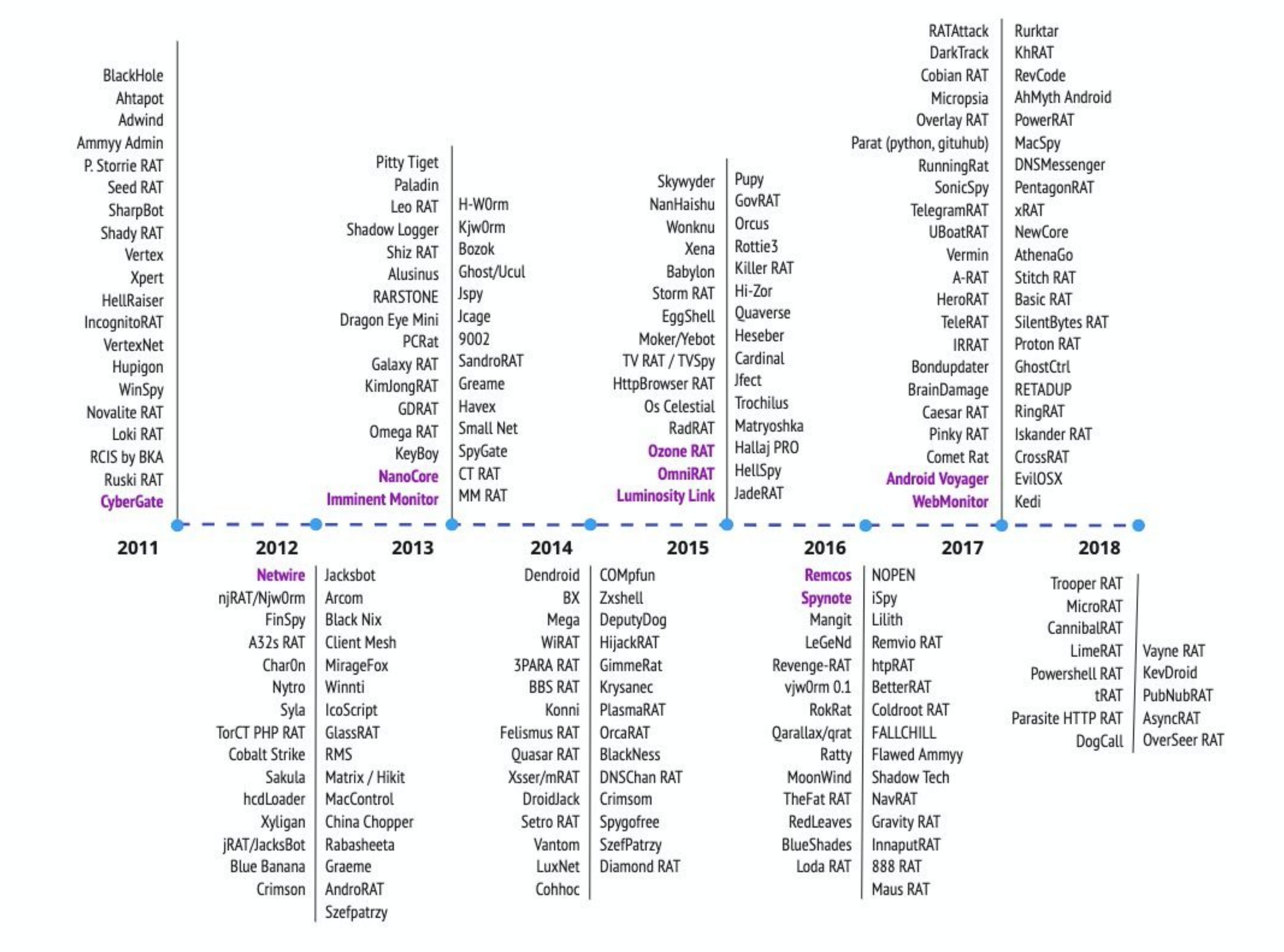
Port 9999

Disconnected

- RATs started to be used for attacks and for profit.
- Developers and operators are now different actors.
- Among the highlights of this period are Gh0st, PoisonIvy and DarkComet.
- The market started to mature.

PHASE 03

2011-2020



BlackHole
Ahtapot
Adwind
Ammyy Admin
P. Storrie RAT
Seed RAT
SharpBot
Shady RAT
Vertex
Xpert
HellRaiser
IncognitoRAT
VertexNet
Hupigon
WinSpy
Novalite RAT
Loki RAT
RCIS by BKA
Ruski RAT
CyberGate

Pitty Tiget
Paladin
Leo RAT
Shadow Logger
Shiz RAT
Alusinus
RARSTONE
Dragon Eye Mini
PCRat
Galaxy RAT
KimJongRAT
GDRAT
Omega RAT
KeyBoy
NanoCore
Imminent Monitor

H-W0rm
Kjw0rm
Bozok
Ghost/Ucul
Jspy
Jcage
9002
SandroRAT
Greame
Havex
Small Net
SpyGate
CT RAT
MM RAT

Skywyder
NanHaishu
Wonknu
Xena
Babylon
Storm RAT
EggShell
Moker/Yebot
TV RAT / TVSpy
HttpBrowser RAT
Os Celestial
RadRAT
Ozone RAT
OmniRAT
Luminosity Link

Pupy
GovRAT
Orcus
Rottie3
Killer RAT
Hi-Zor
Quaverse
Heseber
Cardinal
Jfect
Trochilus
Matryoshka
Hallaj PRO
HellSpy
JadeRAT

RATAttack
DarkTrack
Cobian RAT
Micropsia
Overlay RAT
Parat (python, gituhub)
RunningRat
SonicSpy
TelegramRAT
UBoatRAT
Vermin
A-RAT
HeroRAT
TeleRAT
IRRAT
Bondupdater
BrainDamage
Caesar RAT
Pinky RAT
Comet Rat
Android Voyager
WebMonitor

Rurktar
KhRAT
RevCode
AhMyth Android
PowerRAT
MacSpy
DNSMessenger
PentagonRAT
xRAT
NewCore
AthenaGo
Stitch RAT
Basic RAT
SilentBytes RAT
Proton RAT
GhostCtrl
RETADUP
RingRAT
Iskander RAT
CrossRAT
EvilOSX
Kedi

2011 2012 2013 2014 2015 2016 2017 2018

Netwire
njRAT/Njw0rm
FinSpy
A32s RAT
Char0n
Nytro
Syla
TorCT PHP RAT
Cobalt Strike
Sakula
hcdLoader
Xyligan
jRAT/JacksBot
Blue Banana
Crimson

Jacksbot
Arcom
Black Nix
Client Mesh
MirageFox
Winnti
IcoScript
GlassRAT
RMS
Matrix / Hikit
MacControl
China Chopper
Rabasheeta
Graeme
AndroRAT
Szefpatrzy

Dendroid
BX
Mega
WiRAT
3PARA RAT
BBS RAT
Konni
Felismus RAT
Quasar RAT
Xsser/mRAT
DroidJack
Setro RAT
Vantom
LuxNet
Cohhoc

COMpfun
Zxshell
DeputyDog
HijackRAT
GimmeRat
Krysanec
PlasmaRAT
OrcaRAT
BlackNess
DNSChan RAT
Crimsom
Spygofree
SzefPatrzy
Diamond RAT

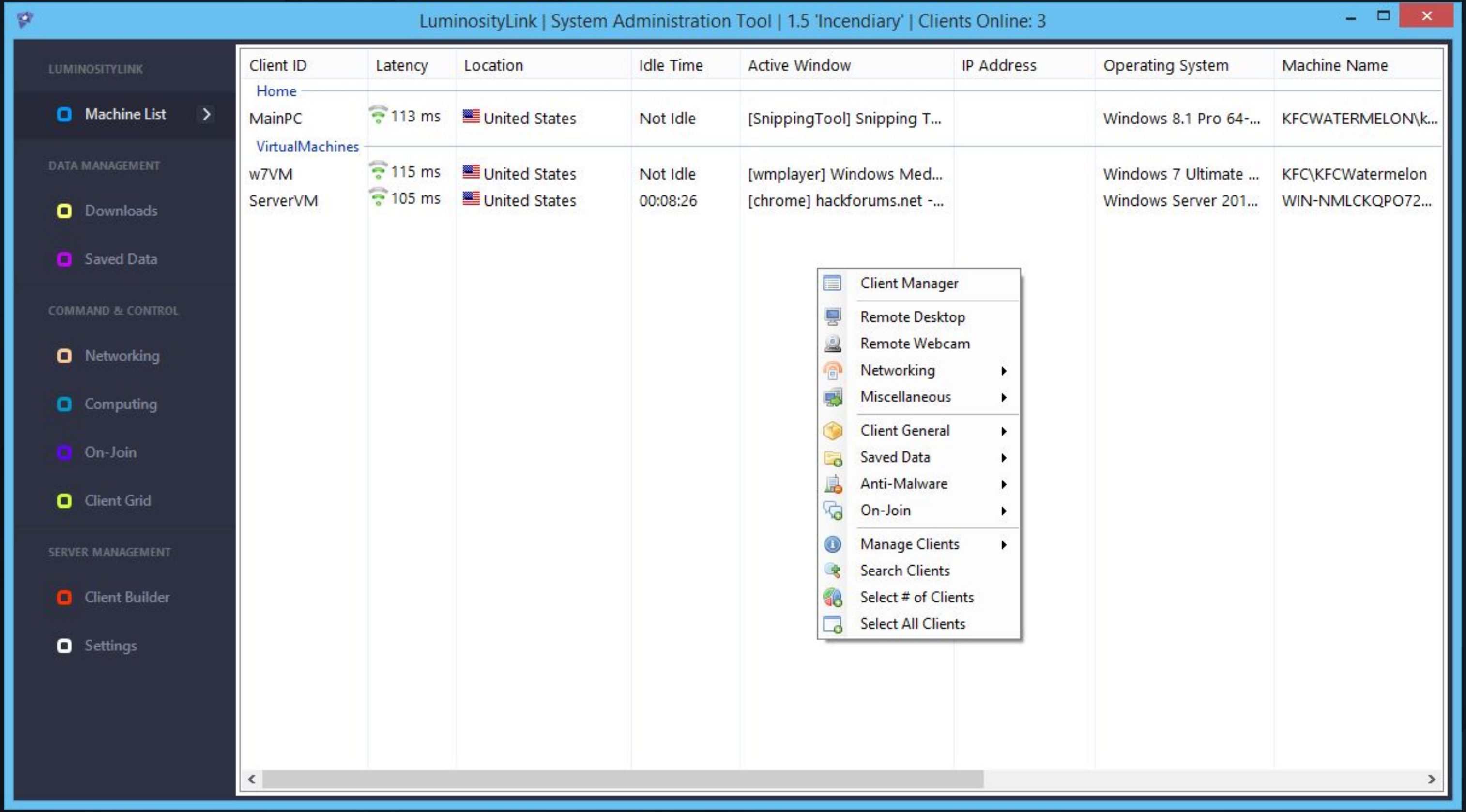
Remcos
Spynote
Mangit
LeGeNd
Revenge-RAT
vjw0rm 0.1
RokRat
Qarallax/qrat
Ratty
MoonWind
TheFat RAT
RedLeaves
BlueShades
Loda RAT

NOPEN
iSpy
Lilith
Remvio RAT
htpRAT
BetterRAT
Coldroot RAT
FALLCHILL
Flawed Ammyy
Shadow Tech
NavRAT
Gravity RAT
InnaputRAT
888 RAT
Maus RAT

Trooper RAT
MicroRAT
CannibalRAT
LimeRAT
Powershell RAT
tRAT
Parasite HTTP RAT
DogCall

Vayne RAT
KevDroid
PubNubRAT
AsyncRAT
OverSeer RAT

Luminosity RAT 2015

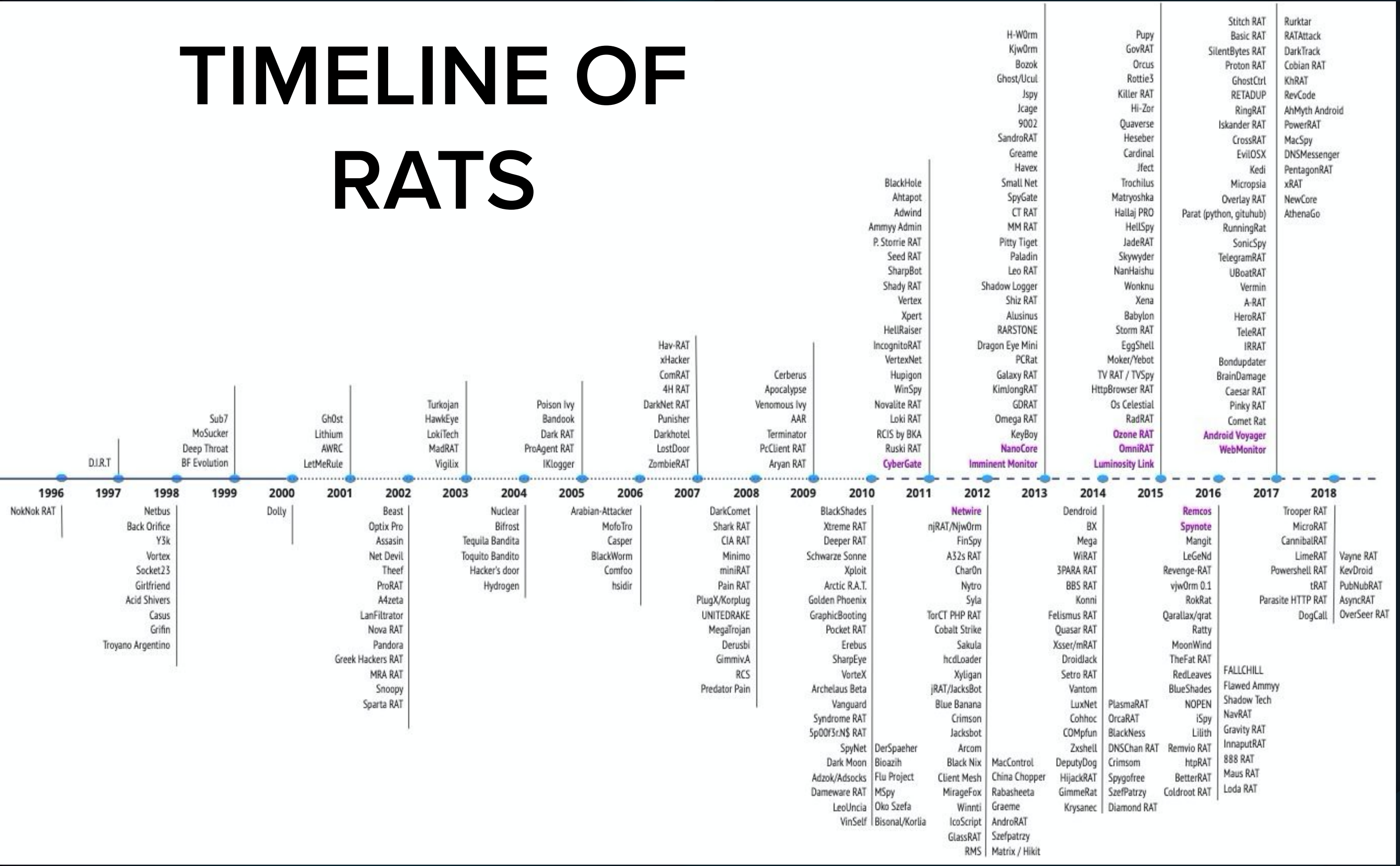


LuminosityLink | System Administration Tool | 1.5 'Incendiary' | Clients Online: 3

Client ID	Latency	Location	Idle Time	Active Window	IP Address	Operating System	Machine Name
Home							
MainPC	113 ms	United States	Not Idle	[SnippingTool] Snipping T...		Windows 8.1 Pro 64-...	KFCWATERMELON\k...
VirtualMachines							
w7VM	115 ms	United States	Not Idle	[wmplayer] Windows Med...		Windows 7 Ultimate ...	KFC\KFCWatermelon
ServerVM	105 ms	United States	00:08:26	[chrome] hackforums.net -...		Windows Server 201...	WIN-NMLCKQPO72...

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

TIMELINE OF RATS



1996
- NokNok RAT

1997
- D.I.R.T

1998
- Netbus
- Back Orifice
- Y3k
- Vortex
- Socket23
- Girlfriend
- Acid Shivers
- Casus
- Grifin
- Troyano Argentino

1999
- Sub7
- MoSucker
- Deep Throat
- BF Evolution

2000
- Dolly

2001
- Gh0st
- Lithium
- AWRC
- LetMeRule

2002
- Beast
- Optix Pro
- Assasin
- Net Devil
- Theef
- ProRAT
- A4zeta
- LanFiltrator
- Nova RAT
- Pandora
- Greek Hackers RAT
- MRA RAT
- Snoopy
- Sparta RAT

2003
- Turkojan
- HawkEye
- LokiTech
- MadRAT
- Vigilix

2004
- Nuclear
- Bifrost
- Tequila Bandita
- Toquito Bandito
- Hacker's door
- Hydrogen

2005
- Poison Ivy
- Bandook
- Dark RAT
- ProAgent RAT
- IKlogger

2006
- Arabian-Attacker
- MofoTro
- Casper
- BlackWorm
- Comfoo
- hsidir

2007
- Hav-RAT
- xHacker
- ComRAT
- 4H RAT
- DarkNet RAT
- Punisher
- Darkhotel
- LostDoor
- ZombieRAT

2008
- DarkComet
- Shark RAT
- CIA RAT
- Minimo
- miniRAT
- Pain RAT
- PlugX/Korplug
- UNITEDRAKE
- MegaTrojan
- Derusbi
- Gimmiv.A
- RCS
- Predator Pain

2009
- Cerberus
- Apocalypse
- Venomous Ivy
- AAR
- Terminator
- PcClient RAT
- Aryan RAT

2010
- BlackShades
- Xtreme RAT
- Deeper RAT
- Schwarze Sonne
- Xploit
- Arctic R.A.T.
- Golden Phoenix
- GraphicBooting
- Pocket RAT
- Erebus
- SharpEye
- VorteX
- Archelaus Beta
- Vanguard
- Syndrome RAT
- 5p00f3r.N$ RAT
- SpyNet
- Dark Moon
- Adzok/Adsocks
- Dameware RAT
- LeoUncia
- VinSelf
- DerSpaeher
- Bioazih
- Flu Project
- MSpy
- Oko Szefa
- Bisonal/Korlia

2011
- BlackHole
- Ahtapot
- Adwind
- Ammyy Admin
- P. Storrie RAT
- Seed RAT
- SharpBot
- Shady RAT
- Vertex
- Xpert
- HellRaiser
- IncognitoRAT
- VertexNet
- Hupigon
- WinSpy
- Novalite RAT
- Loki RAT
- RCIS by BKA
- Ruski RAT
- CyberGate

2012
- Netwire
- njRAT/NjwOrm
- FinSpy
- A32s RAT
- CharOn
- Nytro
- Syla
- TorCT PHP RAT
- Cobalt Strike
- Sakula
- hcdLoader
- Xyligan
- jRAT/JacksBot
- Blue Banana
- Crimson
- Jacksbot
- Arcom
- Black Nix
- Client Mesh
- MirageFox
- Winnti
- IcoScript
- GlassRAT
- RMS
- MacControl
- China Chopper
- Rabasheeta
- Graeme
- AndroRAT
- Szefpatrzy
- Matrix / Hikit

2013
- H-W0rm
- Kjw0rm
- Bozok
- Ghost/Ucul
- Jspy
- Jcage
- 9002
- SandroRAT
- Greame
- Havex
- Small Net
- SpyGate
- CT RAT
- MM RAT
- Pitty Tiget
- Paladin
- Leo RAT
- Shadow Logger
- Shiz RAT
- Alusinus
- RARSTONE
- Dragon Eye Mini
- PCRat
- Galaxy RAT
- KimJongRAT
- GDRAT
- Omega RAT
- KeyBoy
- NanoCore
- Imminent Monitor

2014
- Dendroid
- BX
- Mega
- WiRAT
- 3PARA RAT
- BBS RAT
- Konni
- Felismus RAT
- Quasar RAT
- Xsser/mRAT
- DroidJack
- Setro RAT
- Vantom
- LuxNet
- Cohhoc
- COMpfun
- Zxshell
- DeputyDog
- HijackRAT
- GimmeRat
- Krysanec
- PlasmaRAT
- OrcaRAT
- BlackNess
- DNSChan RAT
- Crimsom
- Spygofree
- SzefPatrzy
- Diamond RAT

2015
- Pupy
- GovRAT
- Orcus
- Rottie3
- Killer RAT
- Hi-Zor
- Quaverse
- Heseber
- Cardinal
- Jfect
- Trochilus
- Matryoshka
- Hallaj PRO
- HellSpy
- JadeRAT
- Skywyder
- NanHaishu
- Wonknu
- Xena
- Babylon
- Storm RAT
- EggShell
- Moker/Yebot
- TV RAT / TVSpy
- HttpBrowser RAT
- Os Celestial
- RadRAT
- Ozone RAT
- OmniRAT
- Luminosity Link

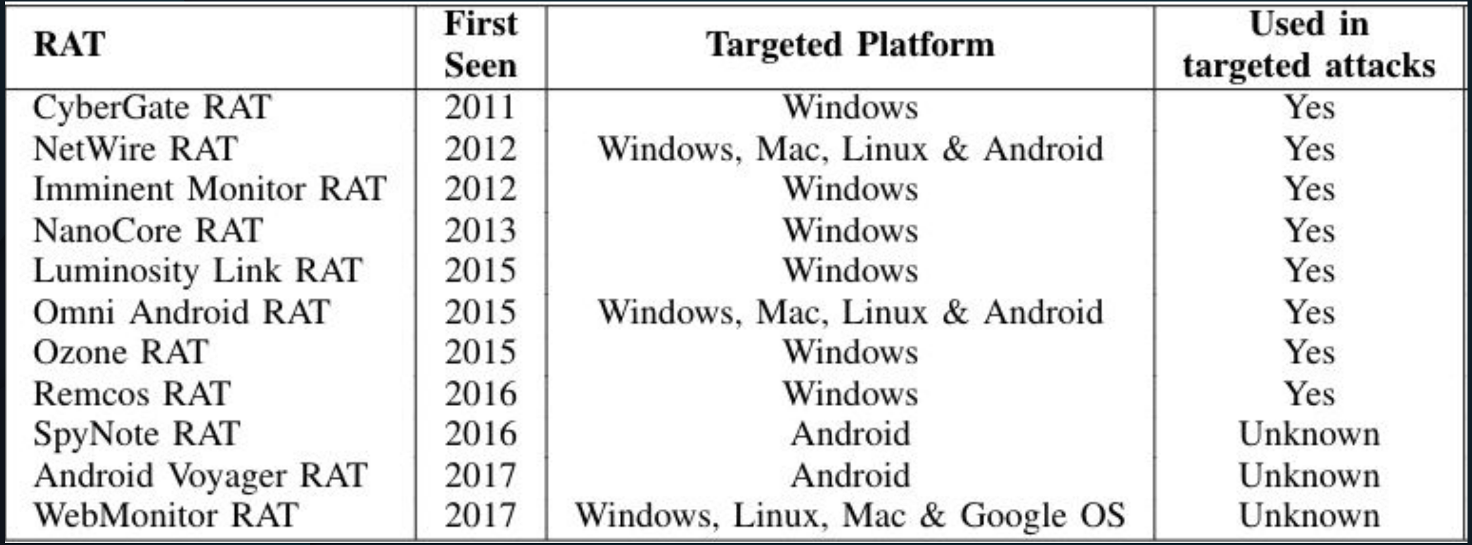
2016
- Remcos
- Spynote
- Mangit
- LeGeNd
- Revenge-RAT
- vjw0rm 0.1
- RokRat
- Qarallax/qrat
- Ratty
- MoonWind
- TheFat RAT
- RedLeaves
- BlueShades
- NOPEN
- iSpy
- Lilith
- Remvio RAT
- htpRAT
- BetterRAT
- Coldroot RAT
- FALLCHILL
- Flawed Ammyy
- Shadow Tech
- NavRAT
- Gravity RAT
- InnaputRAT
- 888 RAT
- Maus RAT
- Loda RAT

2017
- Stitch RAT
- Basic RAT
- SilentBytes RAT
- Proton RAT
- GhostCtrl
- RETADUP
- RingRAT
- Iskander RAT
- CrossRAT
- EvilOSX
- Kedi
- Micropsia
- Overlay RAT
- Parat (python, gituhub)
- RunningRat
- SonicSpy
- TelegramRAT
- UBoatRAT
- Vermin
- A-RAT
- HeroRAT
- TeleRAT
- IRRAT
- Bondupdater
- BrainDamage
- Caesar RAT
- Pinky RAT
- Comet Rat
- Android Voyager
- WebMonitor
- Rurktar
- RATAttack
- DarkTrack
- Cobian RAT
- KhRAT
- RevCode
- AhMyth Android
- PowerRAT
- MacSpy
- DNSMessenger
- PentagonRAT
- xRAT
- NewCore
- AthenaGo

2018
- Trooper RAT
- MicroRAT
- CannibalRAT
- LimeRAT
- Powershell RAT
- tRAT
- Parasite HTTP RAT
- DogCall
- Vayne RAT
- KevDroid
- PubNubRAT
- AsyncRAT
- OverSeer RAT

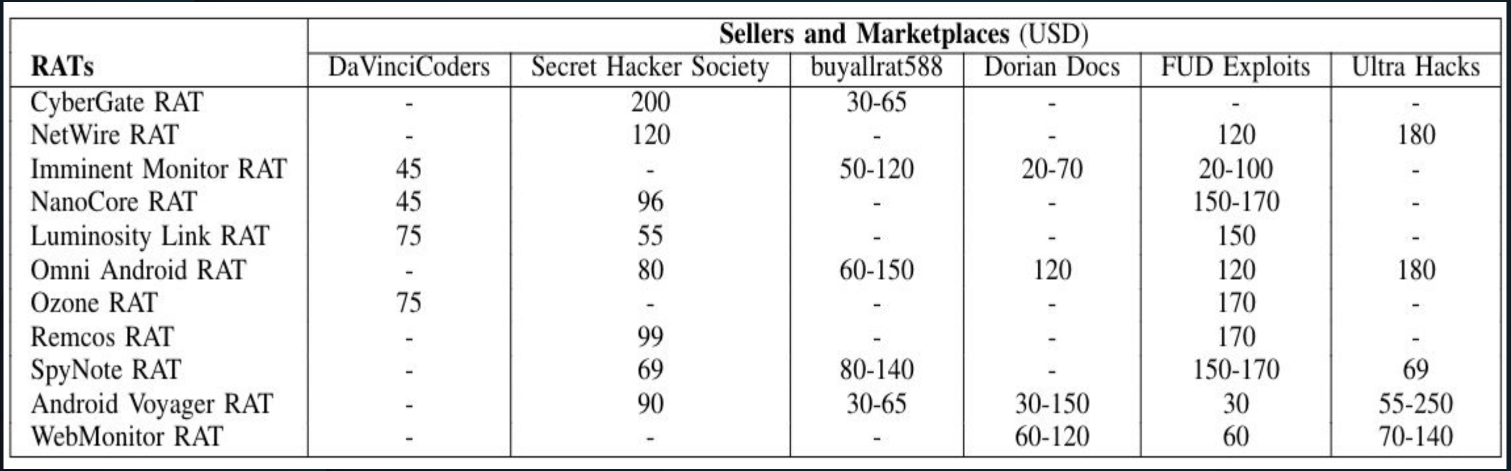
RATs in Markets

Eleven of the most common RATs in 2019-2020



RAT	First Seen	Targeted Platform	Used in targeted attacks
CyberGate RAT	2011	Windows	Yes
NetWire RAT	2012	Windows, Mac, Linux & Android	Yes
Imminent Monitor RAT	2012	Windows	Yes
NanoCore RAT	2013	Windows	Yes
Luminosity Link RAT	2015	Windows	Yes
Omni Android RAT	2015	Windows, Mac, Linux & Android	Yes
Ozone RAT	2015	Windows	Yes
Remcos RAT	2016	Windows	Yes
SpyNote RAT	2016	Android	Unknown
Android Voyager RAT	2017	Android	Unknown
WebMonitor RAT	2017	Windows, Linux, Mac & Google OS	Unknown

Commercialized prices of RATs in online marketplaces



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

BUILDER

CRYPTER

PLUGINS

Commoditization of RATs

But why?
Who is buying all these?

- Business Email Compromise
- Cyber espionage
- Targeted Attacks
- Stalkerware

RATs are essential for any type of cybercriminal activity

Where are the RATs going?

Veronica Valeros

veronica.valeros@aic.fel.cvut.cz

@verovaleros

Sebastian Garcia

sebastian.garcia@agents.fel.cvut.cz

@eldracote

THANKS!

www.stratosphereips.org