NanoCore Hunter: Track NanoCore C&C Server and Monitor RAT Operator for 180 Days

National Institute of Information and Communications Technology
Cybersecurity Laboratory, Cybersecurity Research Institute

Takashi Matsumoto

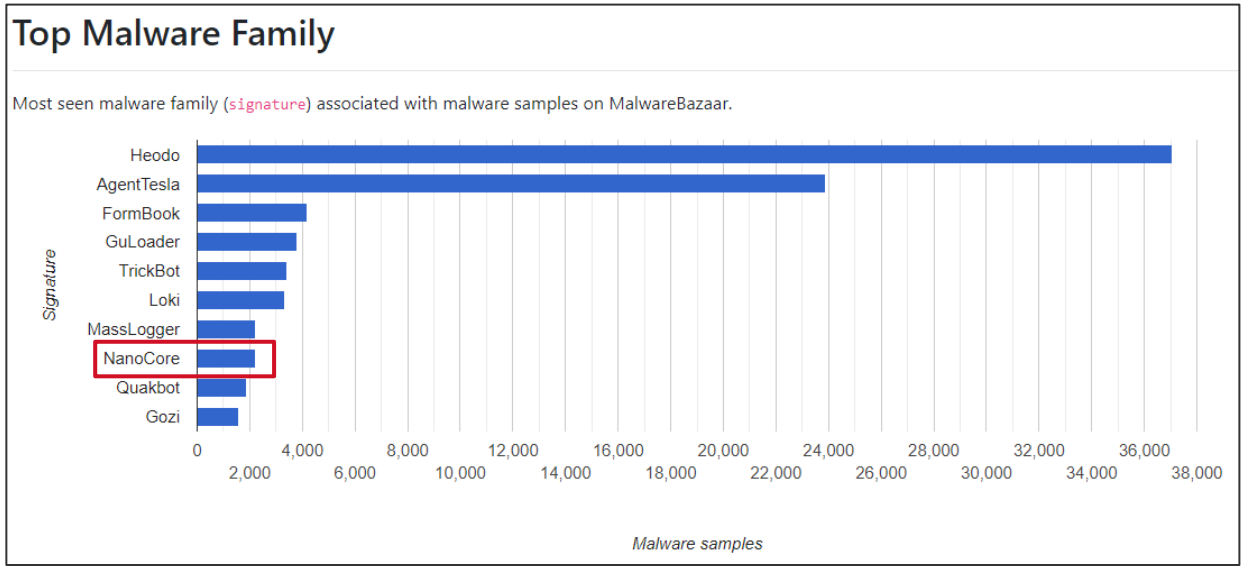
Motivation

- **New Approach to Detecting NanoCore C2 Servers**
  - We have found a way to detect the NanoCore C2 servers
- **Long-term observations of NanoCore C2 servers**
  - The USA and Europe have most of the C2 servers
  - The list of C2s is provided to the national CERTs
- **Experiments to entice NanoCore operators**
  - Many operators stole email account/passwords
  - Infected RATs other than NanoCore for a secondary infection

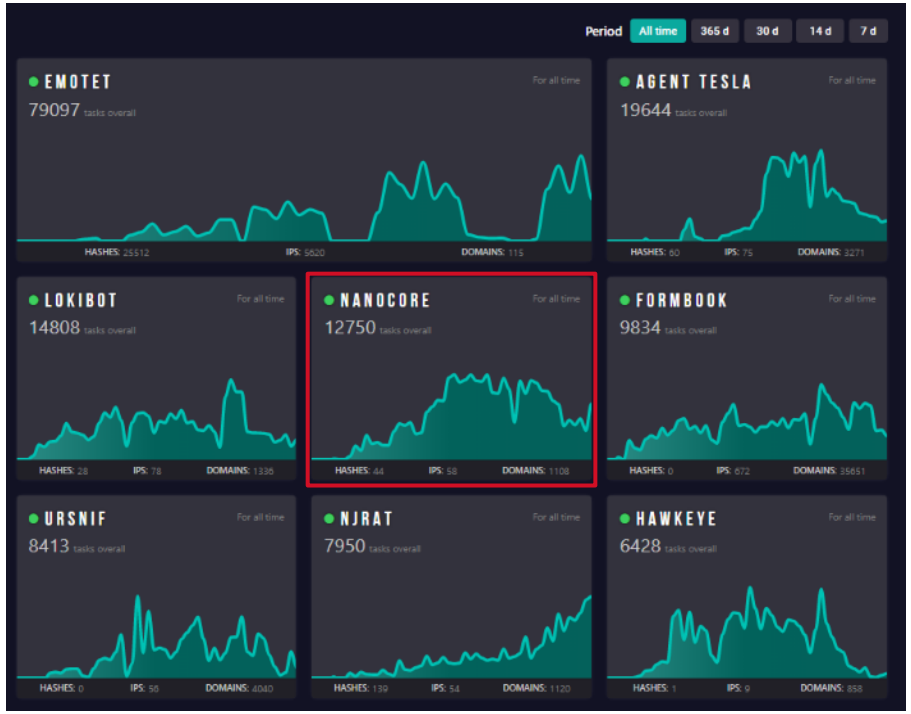
About NanoCore

Overview of NanoCore RAT

- This Remote Access Trojan (RAT) first appeared in 2013
- Still active in 2020
  - Always ranked in the top 10 among malware trends (ANY.RUN, MalwareBazaar)
  - Our organization regularly receives NanoCore-attached spams



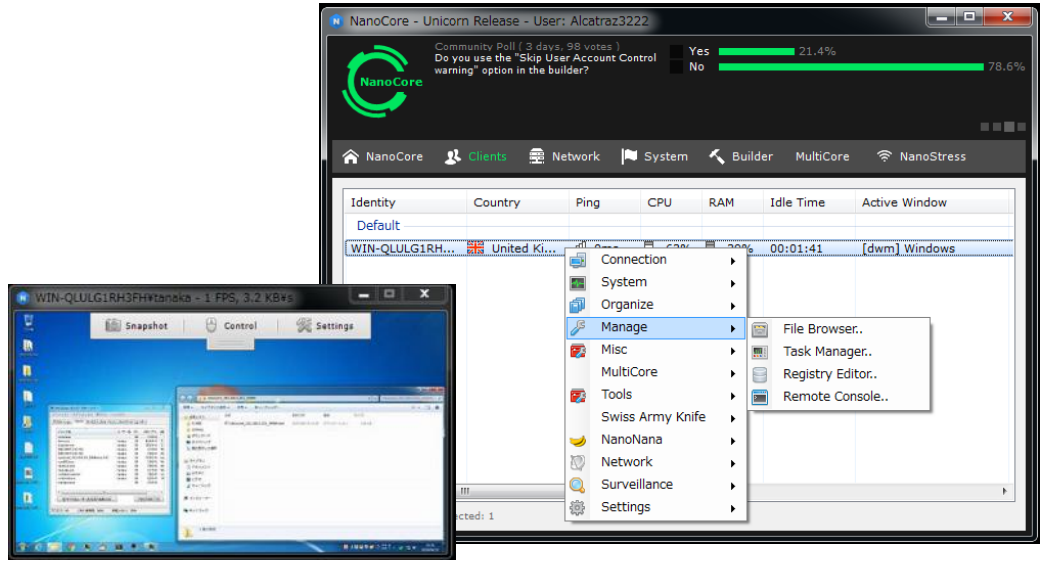
Top 10 Malware programs (MalwareBazaar by abuse.ch)



Malware Trends Tracker (ANY.RUN)

Overview of NanoCore RAT

- NanoCore Functionalities
  - Screen sharing
  - Data exfiltration (files, passwords, credentials)
  - Keylogger
  - Access to microphones and webcams, etc.



Leaked NanoCore v1.2.2.0

- NanoCore v1.2.2.0
  - Latest version
  - Widely used by RAT operators
  - A cracked version was leaked and could be easily obtained
  - We will use this version in this work

Presentation Only

Presentation Only

Presentation Only

National Institute of Information and Communications Technology

Tracking NanoCore C2 Servers

Presentation Only

NSE Script for Detecting NanoCore C2

- Custom NSE script
  - Steps to detect NanoCore C2
    1. Send **payload** that mimics NanoCore client's initial communication
    2. Decrypt returned data with DES
    3. If the decryption is successful, it is judged as a NanoCore C2
  - **Payload** (NanoCore encrypts the following data using DES)
    - GUID (used to identify the PC; could be a random value each time)
    - Identity (hostname¥username)
    - NanoCore group name (default name: Default)
    - NanoCore version (default value: 1.2.2.0)

DES encryption

```
00000000  38 00 00 00 17 f5 4b 2c  c3 65 ca 9f eb bc fd 67   8.....K, .e.....g
00000010  ad 6d 0e c4 33 7d b6 40  17 17 97 a1 d9 7c 3c b3   .m..3}.@ .....|<.
00000020  04 ea d0 16 ce 72 94 94  71 8e 87 45 32 0a 22 49   .....r.. q..E2."I
00000030  81 66 f3 8b c2 9b 2b 97  84 c8 c7 52               .f....+. ...R
```

```
function nanocore_payload(guid, identity, group, version)
    local des_key = "\x72\x20\x18\x78\x8c\x29\x48\x97"
    local des_iv = des_key

    local payload = "\x00\x00\x00\x00"
    .. "\x12" .. guid
    .. "\x0c" .. string.char(string.len(identity)) .. identity
    .. "\x0c" .. string.char(string.len(group)) .. group
    .. "\x0c" .. string.char(string.len(version)) .. version

    local enc_payload = des_encrypt(des_key, des_iv, payload)
    local payload_len = fromInt32(string.len(enc_payload))
    return payload_len .. enc_payload
end
```

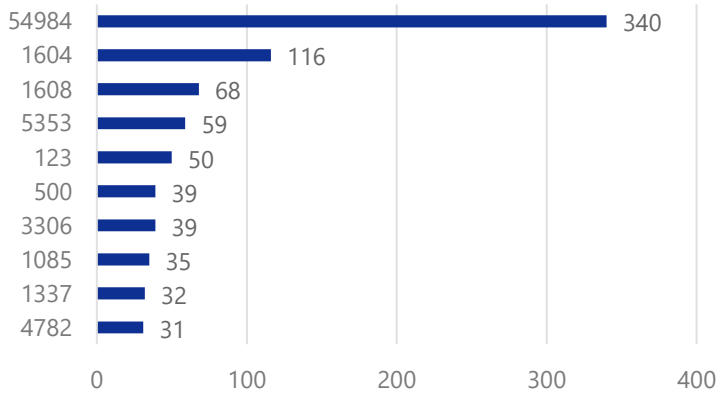
A part of nanocore.nse

Long-Term Observations of C2 Servers (1/5)

- Period
  - 05-14-2020 to 11-10-2020

Presentation Only

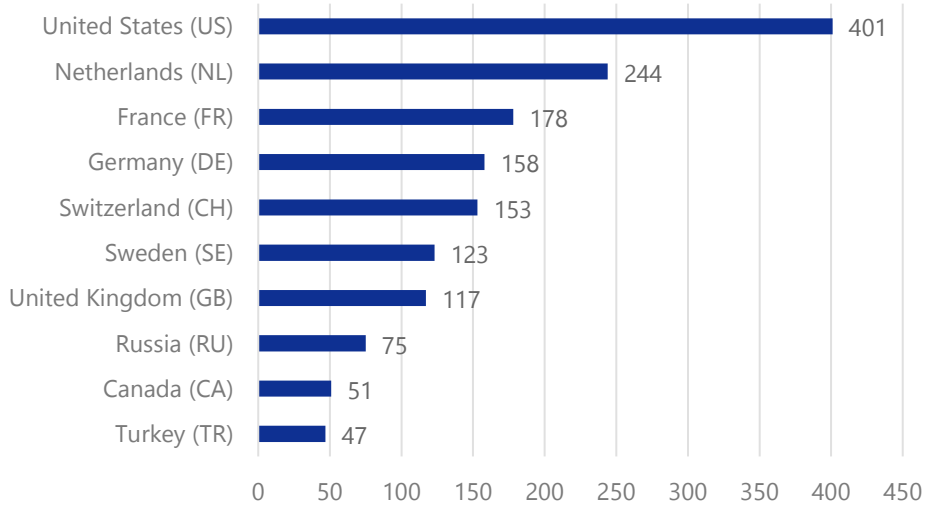
- Detected NanoCore C2 servers
  - Unique IP addresses: **2,075**
  - Unique ports: **3,671**
- Popular Port Number
  - **54984/tcp**: Default for NanoCore C2
  - **1085/tcp**: leaked NanoCore v1.2.2.0 had this port open
  - **1604/tcp**: Same as the default port of DarkComet RAT? Operators who were using DarkComet RAT have moved to use NanoCore?



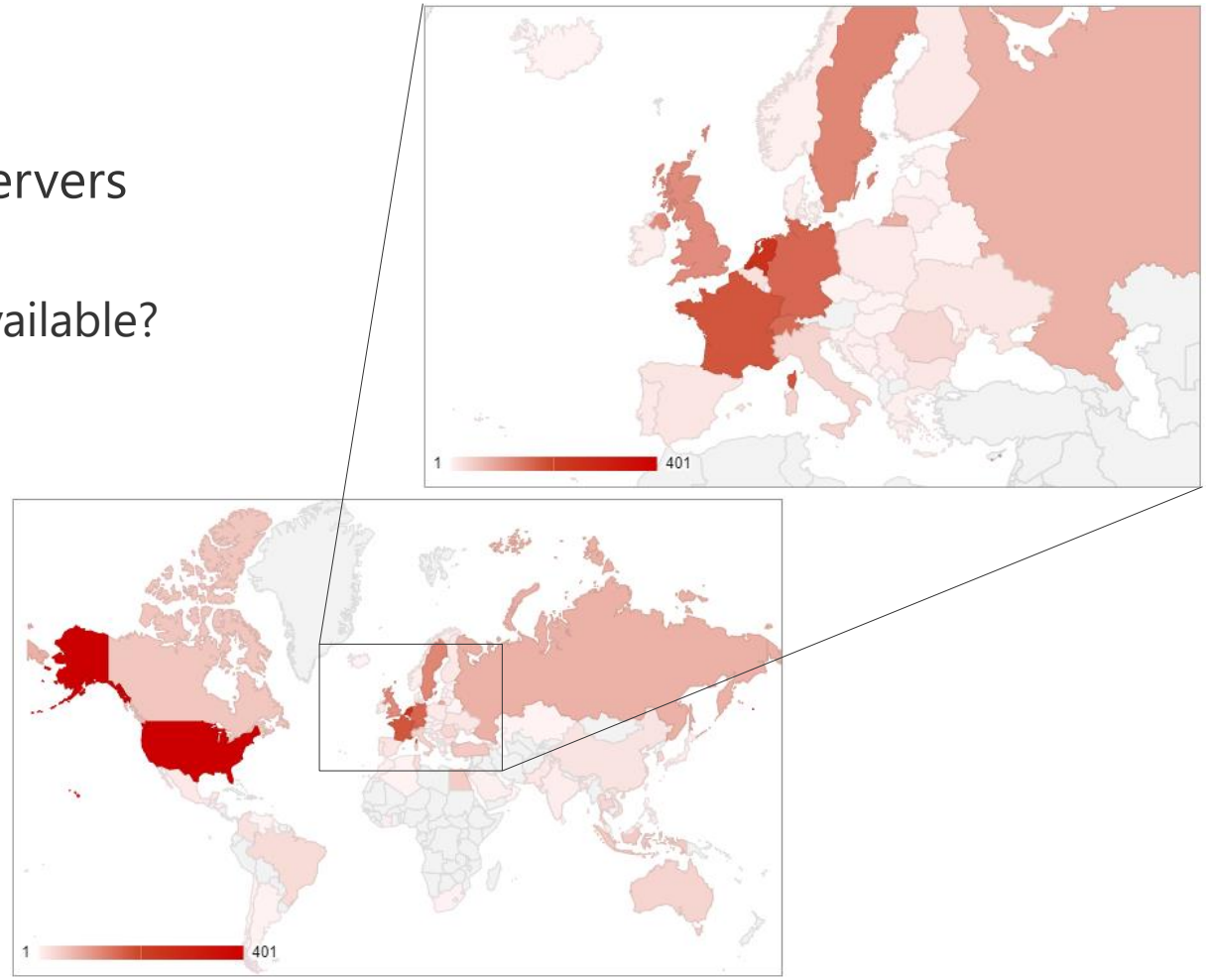
Top 10 ports

Long-Term Observations of C2 Servers (2/5)

- By country
  - **85** countries hosted NanoCore C2s
  - The **USA** and **Europe** have most of the C2 servers
    - The operator‘s hometown? Same groups?
    - The operator's favorite VPN or proxy service available?
    - Those countries are the target of the attack?



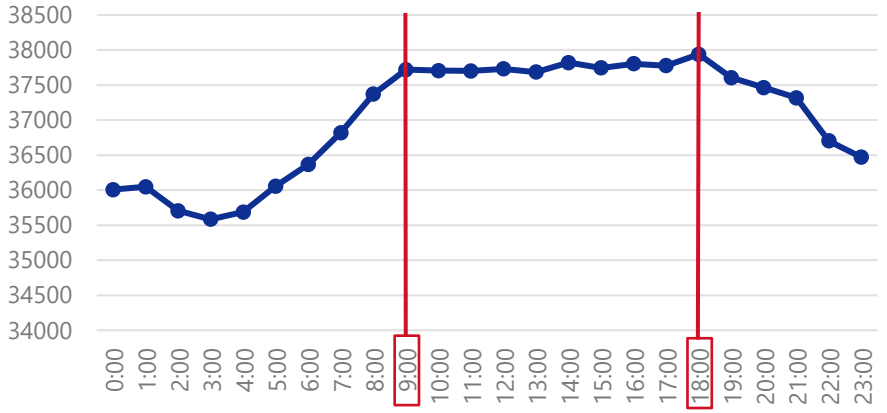
Top 10 countries



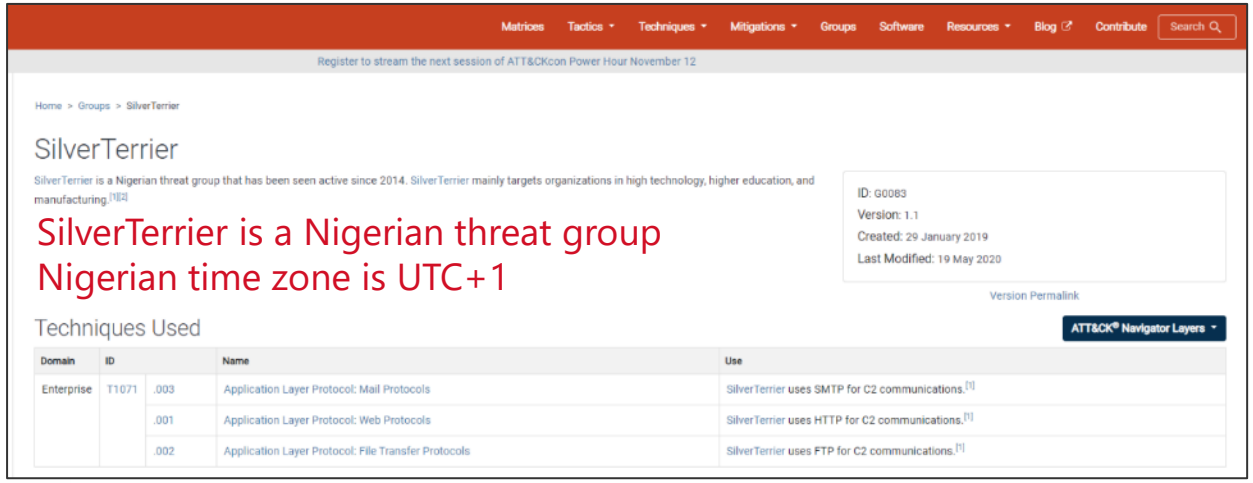
Heat map showing the number of countries where C2 servers are hosted

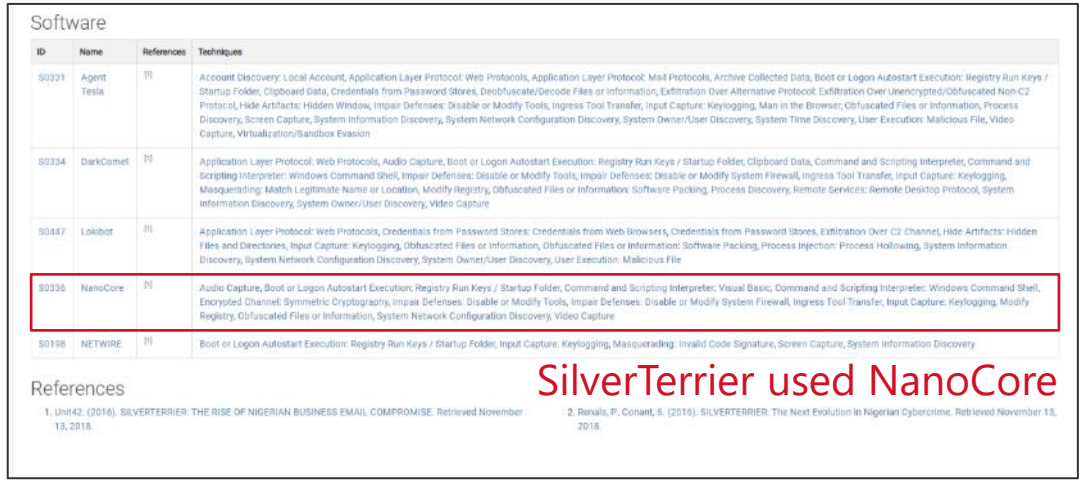
Long-Term Observations of C2 Servers (3/5)

- By time
  - Most of the servers were running **between 9:00 and 18:00**
    - RAT operator's working hours?
      - Countries where these times are during the daytime are targeted
    - Related to the Nigerian adversaries (SilverTerrier)?
      - https://attack.mitre.org/groups/G0083/
      - https://unit42.paloaltonetworks.com/silverterrier-2019-update/



Total number of open ports for every hour of every day

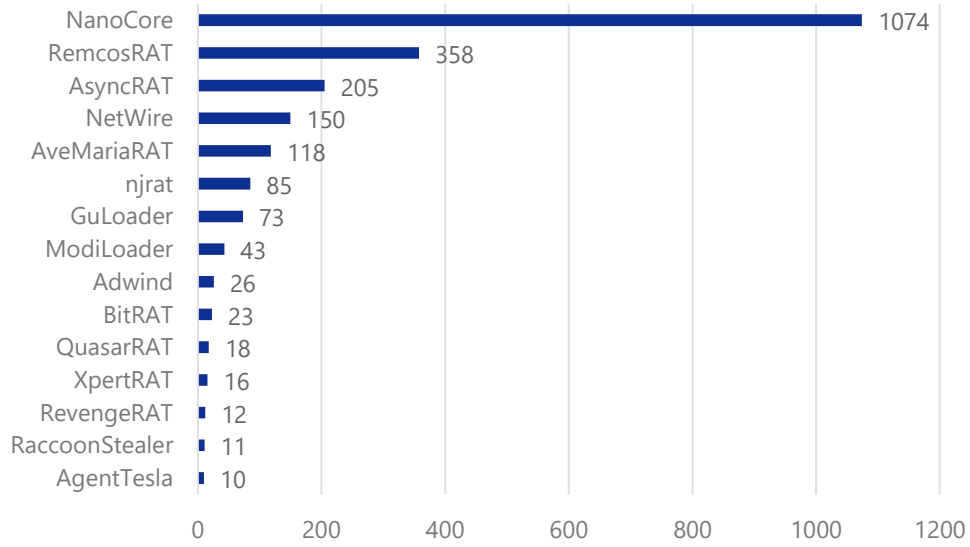




SilverTerrier, Group G0083 | MITRE ATT&CK

Long-Term Observations of C2 Servers (4/5)

- C2 addresses in VirusTotal
  - Unregistered: 480 IP addresses
  - Registered: 1,812 IP addresses
  - Malware associated with registered IP addresses
    - RATs other than NanoCore were used
    - May be using multiple RATs in conjunction?

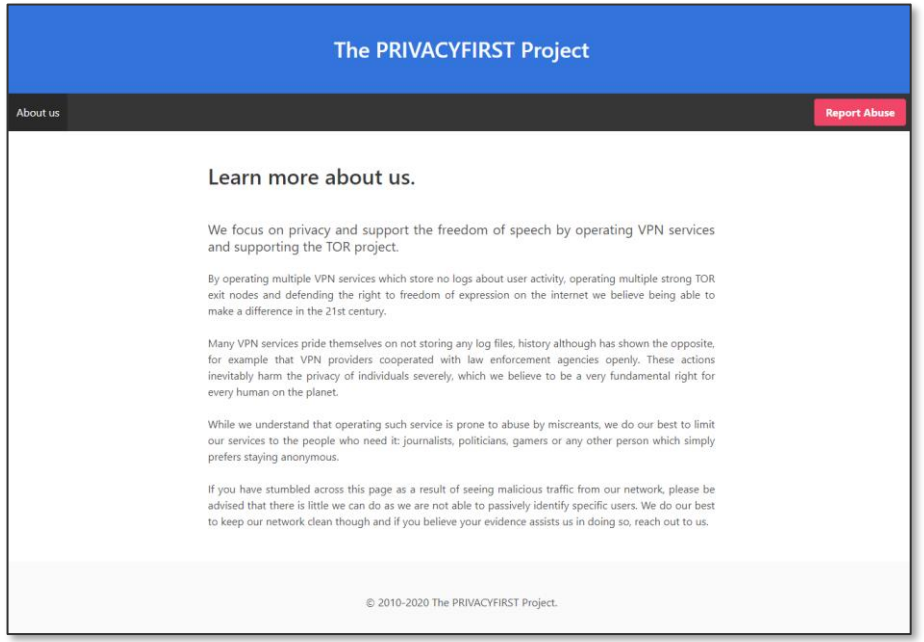


Malware associated with registered IP address
(VirusTotal and MalwareBazaar)

- Coordination
  - We have provided the list of C2s to JPCERT/CC monthly
  - JPCERT/CC has provided the C2 data to national CSIRTs:
    - United States
    - Netherlands
    - Switzerland
    - France
    - Germany
    - Sweden
    - United Kingdom
    - Russia
    - Turkey
    - Indonesia
    - Canada
    - Egypt
    - Italy
    - Romania
    - South Korea
    - Thailand
    - Colombia

Long-Term Observations of C2 Servers (5/5)

- Use of non-logging VPNs
  - About 20% of the IPs are associated “The PRIVACYFIRST Project”
  - According to GovCERT.ch, “We did inform the netblock owners in the past but to no avail.”
- Provide NanoCore IoCs using MISP
  - Add the IP address and port of the detected NanoCore C2 server daily
  - Shared to the CIRCL MISP Community



The PRIVACYFIRST Project（privacyfirst.sh）

```
organisation:   ORG-TPP6-RIPE
org-name:       The PRIVACYFIRST Project
descr:          www.privacyfirst.sh
```

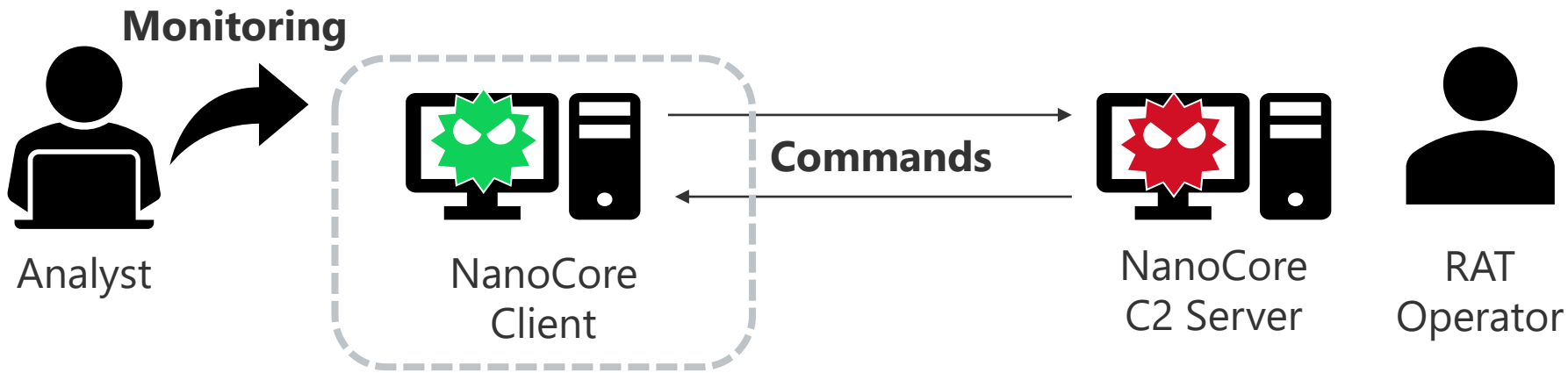
Whois results

Enticing NanoCore Operators

Revealing the Purpose of Using NanoCore

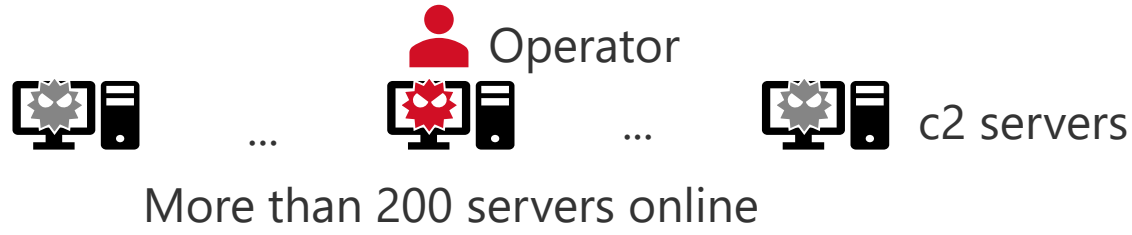
- What do they use NanoCore for?
  -> We tried revealing their purpose by enticing operators into the analysis environment

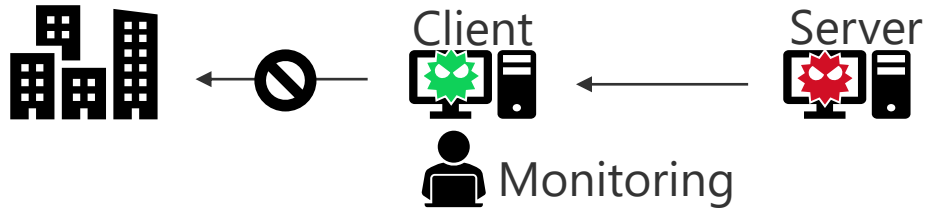
- Experiments to entice RAT operators
  - Use the IP addresses and ports of the detected NanoCore C2 servers
  - Monitor operator actions in real time



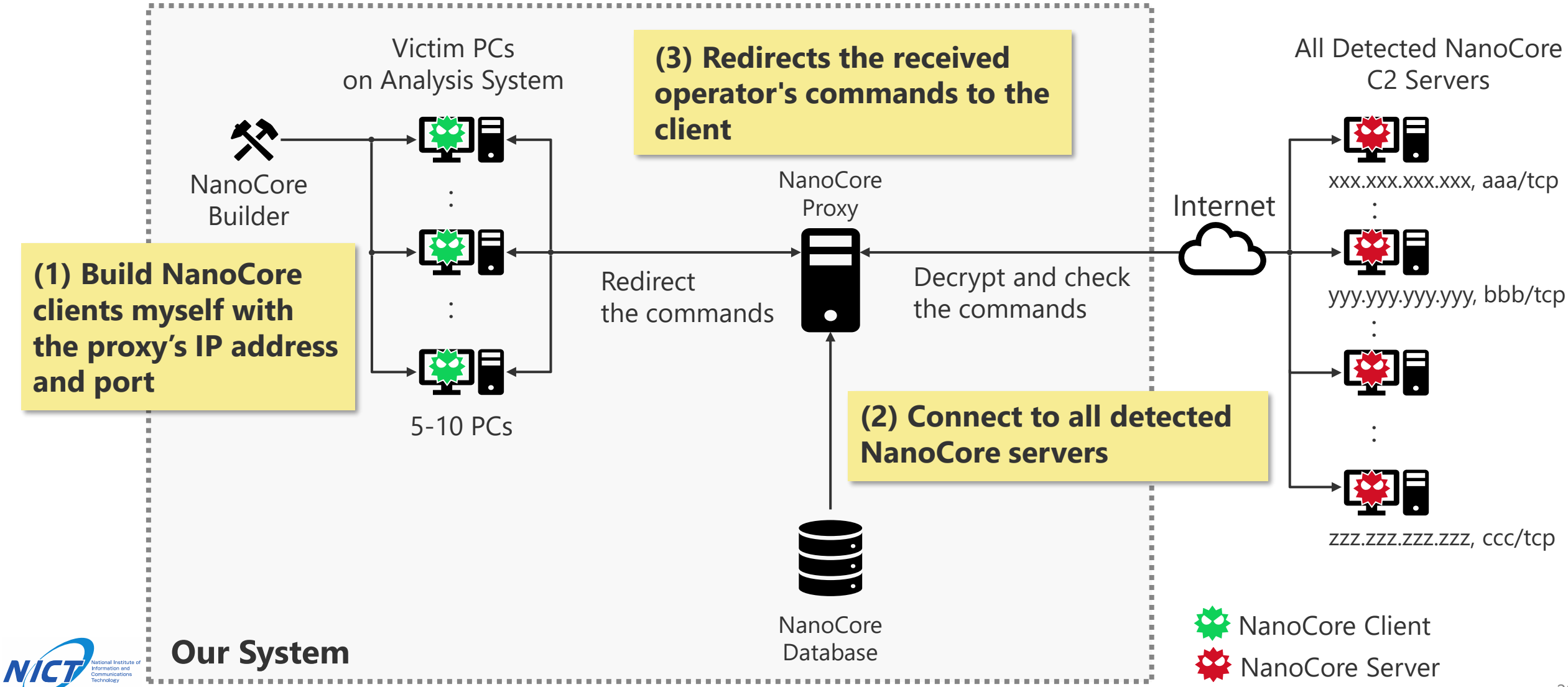
Things to Consider to Entice RAT Operators

- **Not all operators are active even if the server is online**
- **Prepare a client to connect to the C2 server**
- **Prepare an environment which is attractive to operators**
- **Never be a stepping stones for attacking others**



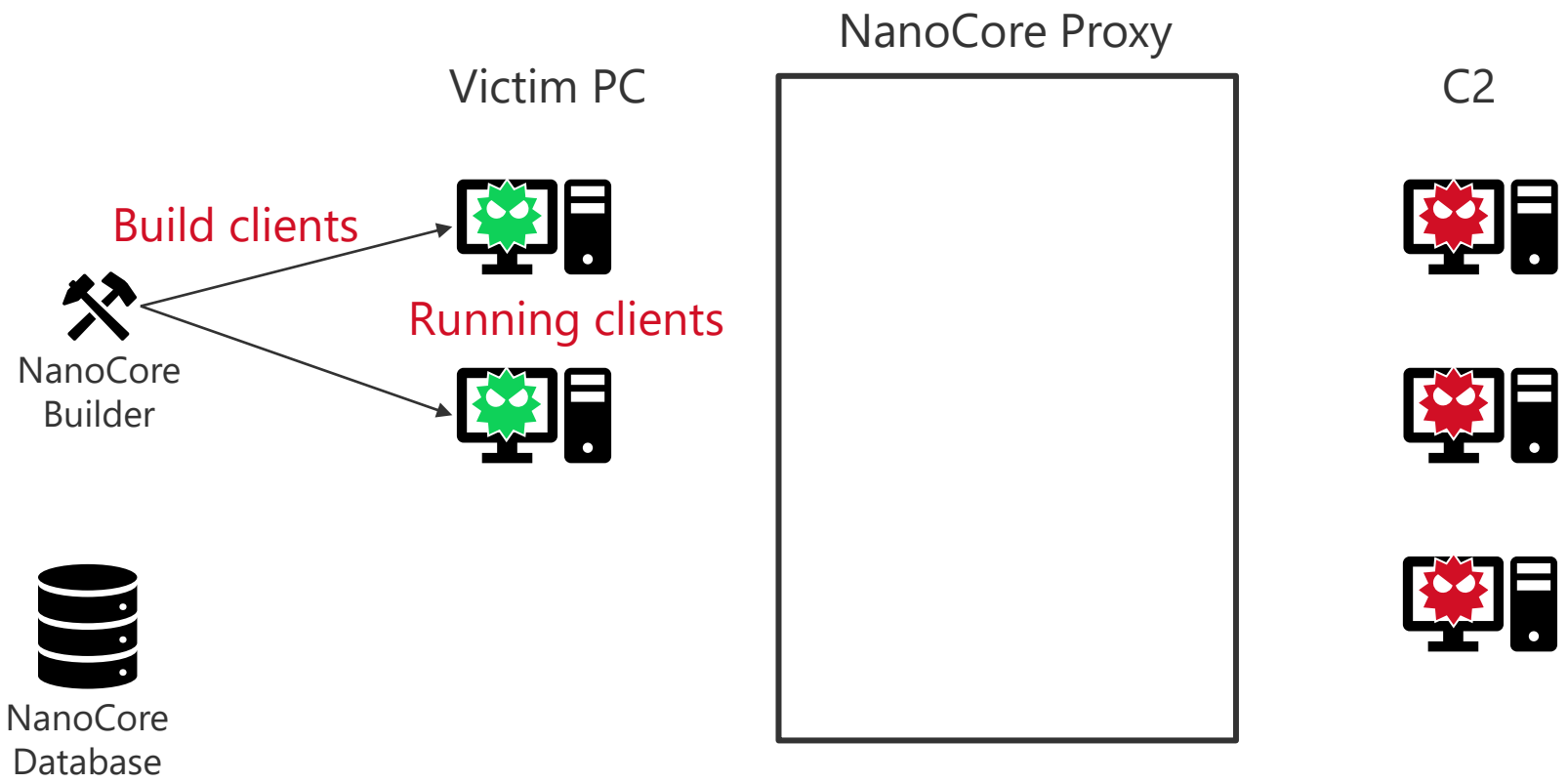


Our System to Efficiently Entice Operators



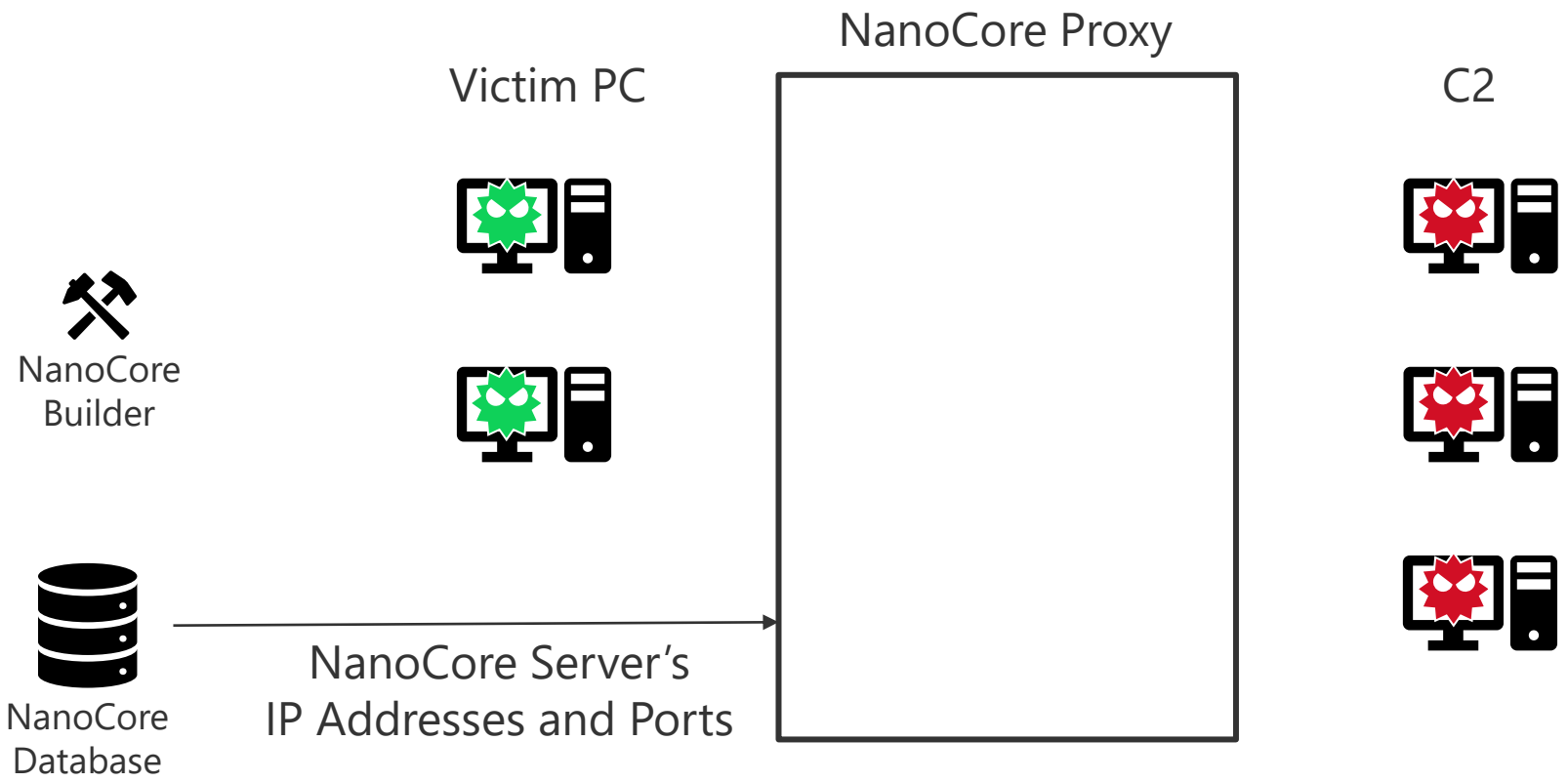
NanoCore Proxy - Procedure (1/8)

- Builds NanoCore clients with the proxy's IP address and port
- Keeps the built clients running on the Victim PCs



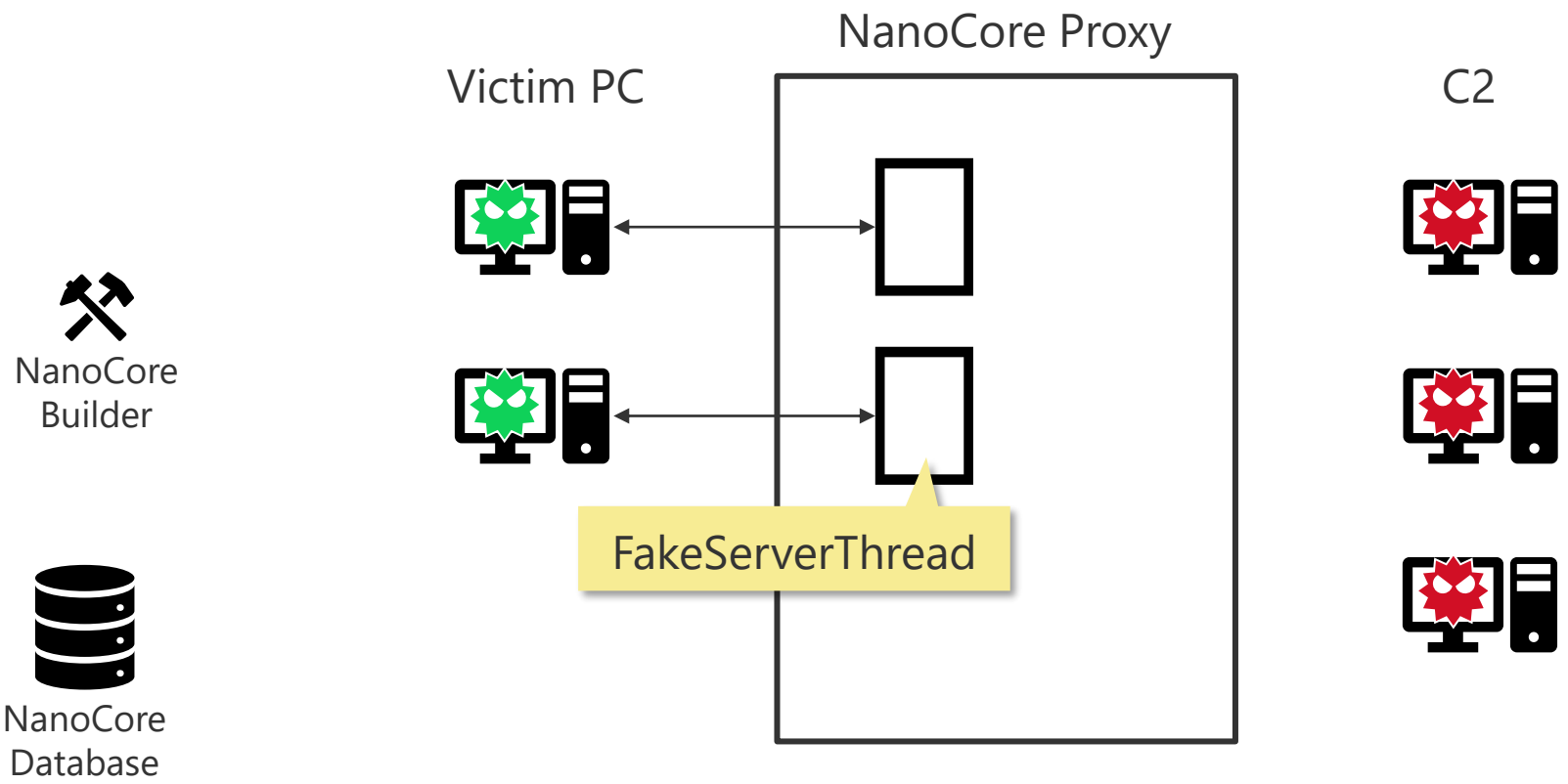
NanoCore Proxy - Procedure (2/8)

- Starts NanoCore Proxy
- Passes the NanoCore Server's IP addresses and ports to the proxy



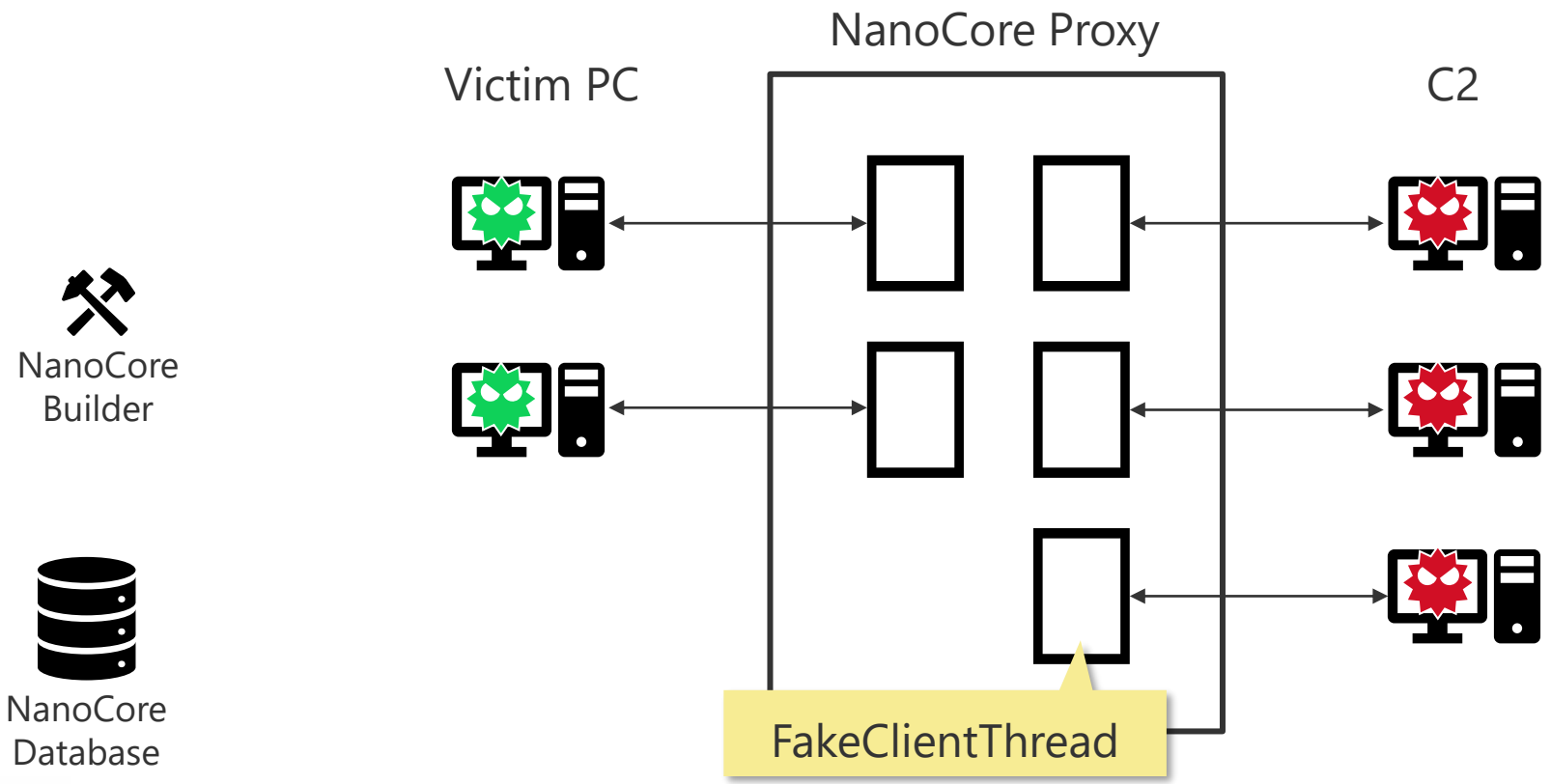
NanoCore Proxy - Procedure (3/8)

- Starts the FakeServerThreads and start communicating with the NanoCore clients



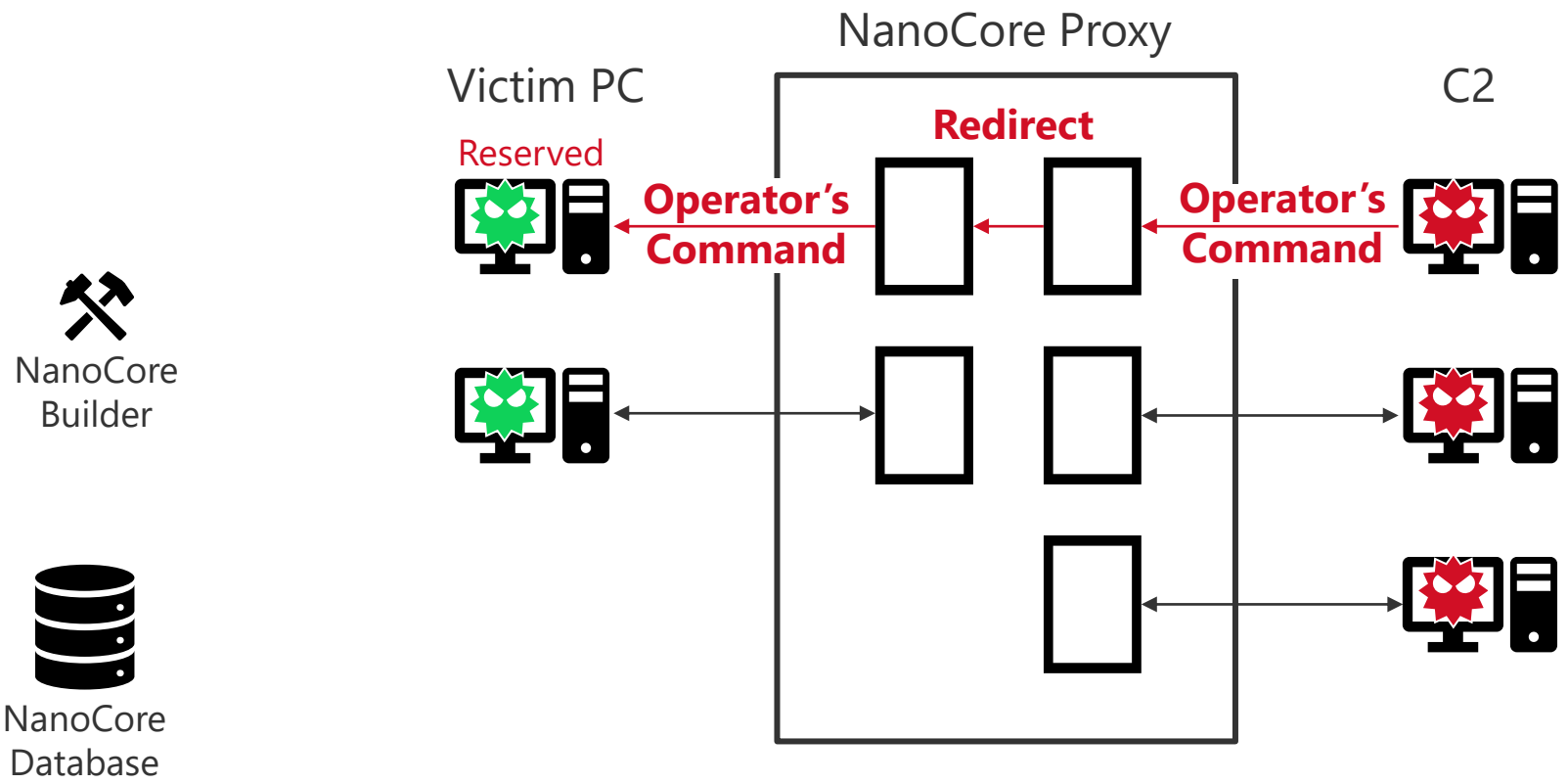
NanoCore Proxy - Procedure (4/8)

- Starts FakeClientThreads and start communicating with all the C2 servers
- Communication between the C2 server and the proxy is always decrypted



NanoCore Proxy - Procedure (5/8)

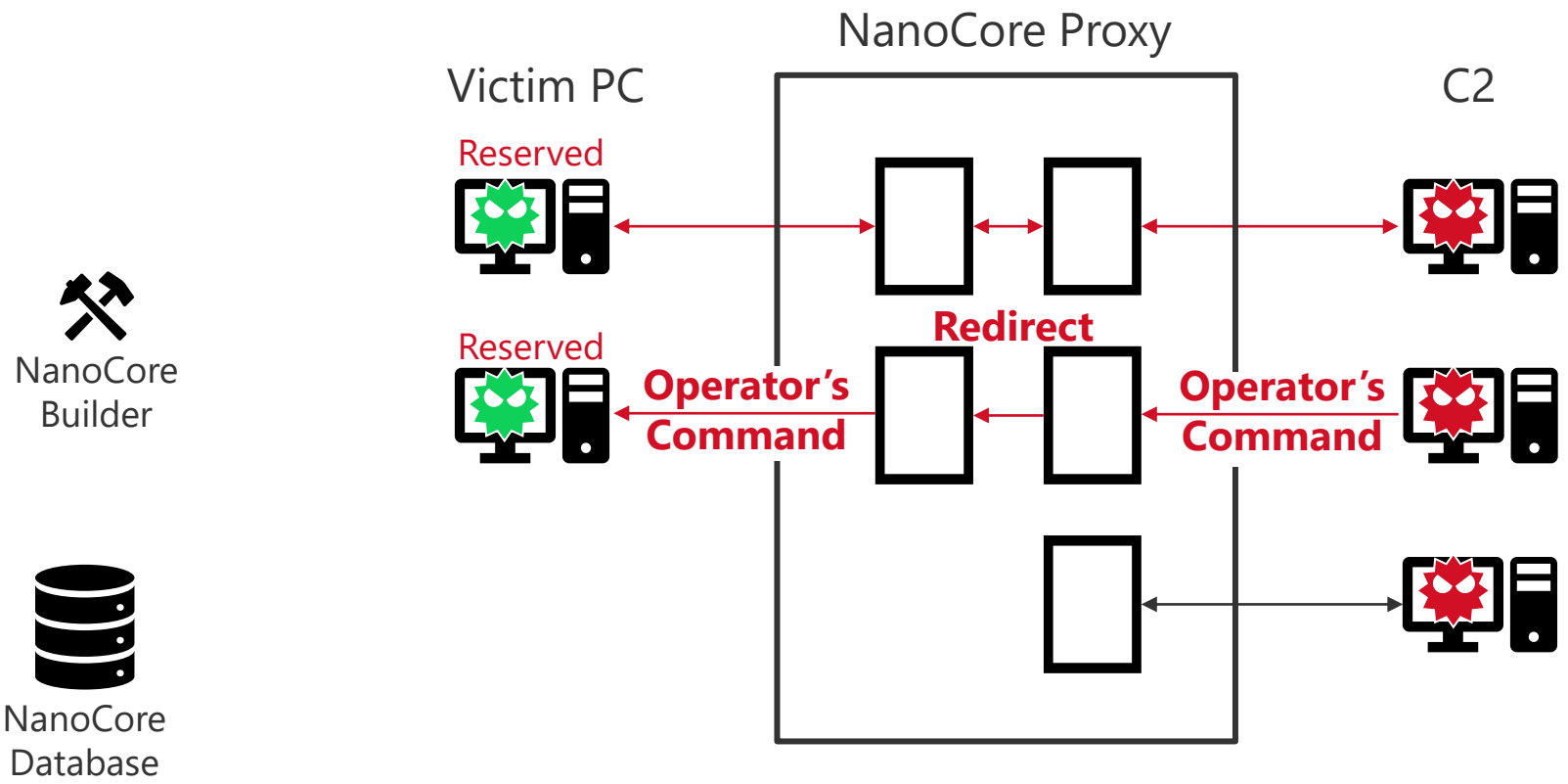
- When an operator's command is received, it is redirected to the PC targeted for be infected



Note:
'Operator's Command' is a communication other than the first communication or a periodic communication.

NanoCore Proxy - Procedure (6/8)

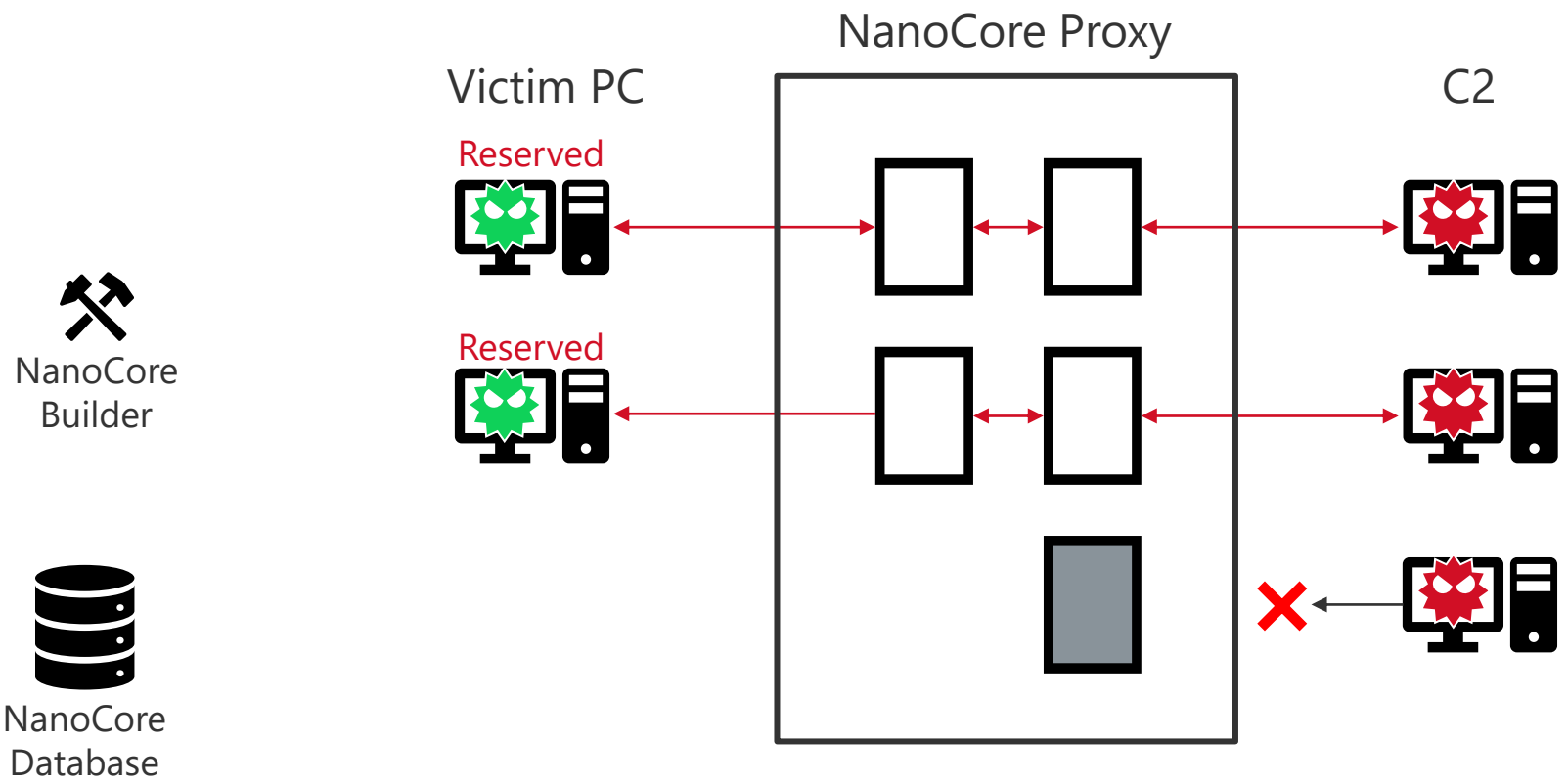
- When an operator's command is received, it is redirected to the PC targeted for be infected



Note:
'Operator's Command' is a communication other than the first communication or a periodic communication.

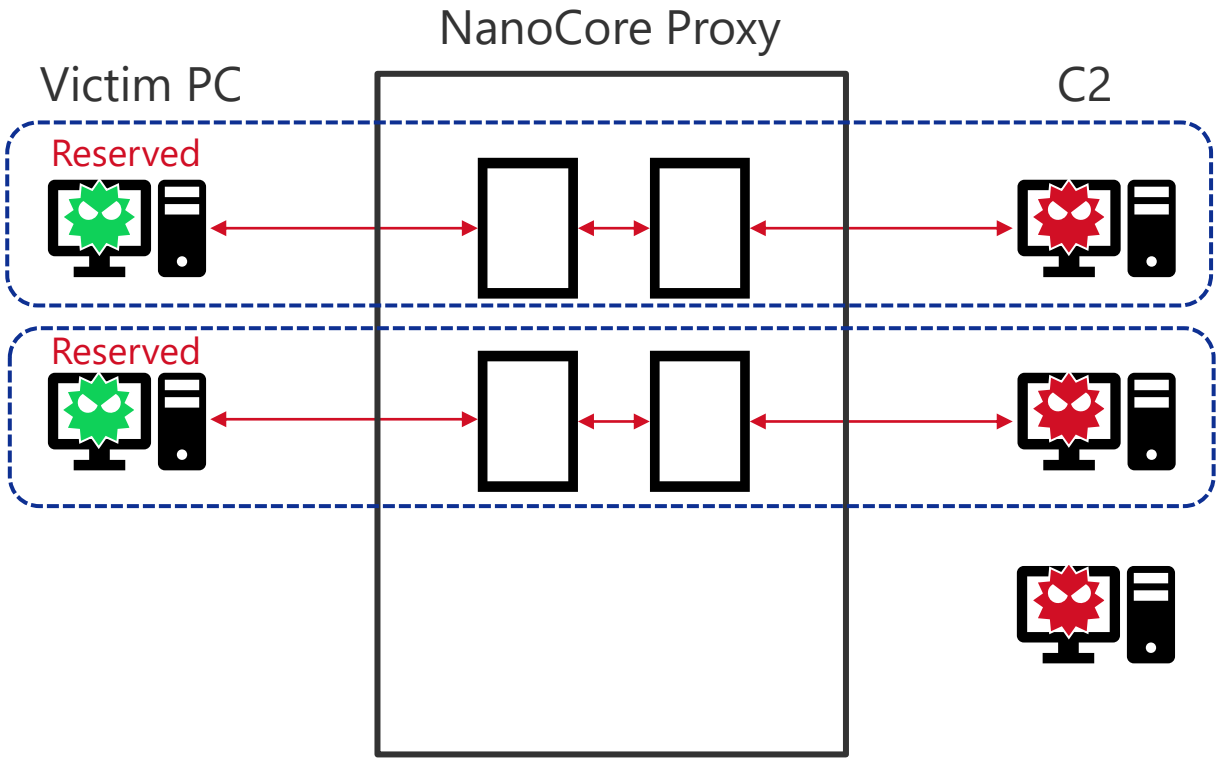
NanoCore Proxy - Procedure (7/8)

- When all the victim PCs have been reserved, the acceptance of new commands will end



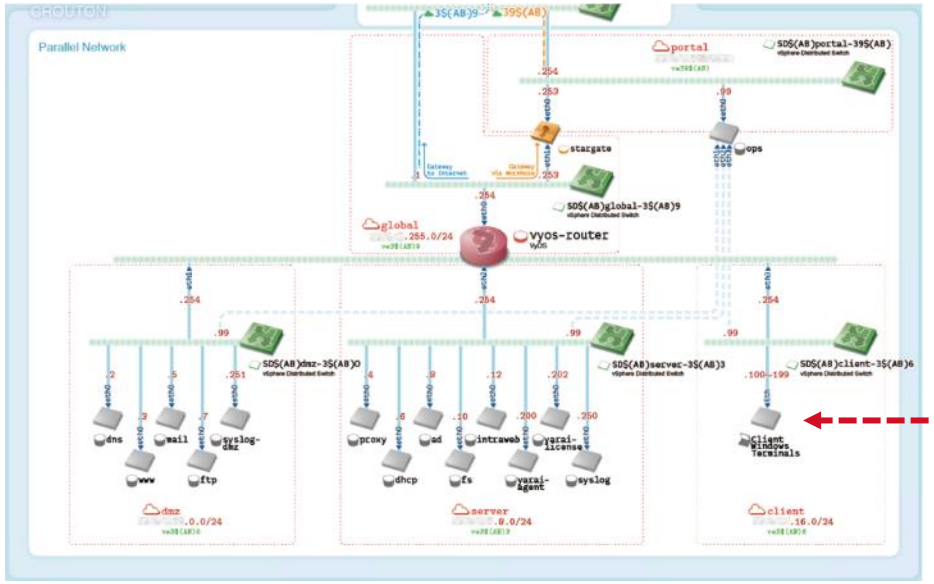
NanoCore Proxy - Procedure (8/8)

- The reserved client keeps connected to the c2 server and continues to analyze

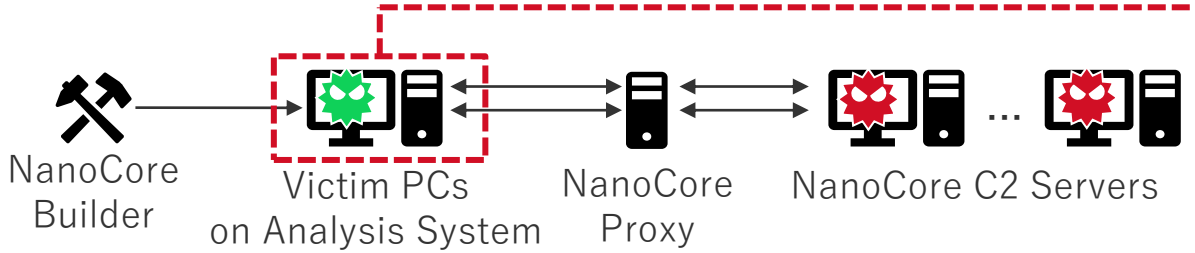


Set-up for Analyzing Actions of Operators

- Used ‘STARDUST’, a large-scale infrastructure for luring cyber attackers
  - Available Logs
    - pcap, Screenshots, Endpoint logs, Disk Forensics, etc.
  - Configuration of victim PCs
    - OS:
      - Windows7 x64
      - language: Japanese
    - Installed apps:
      - Chrome, MS Office 2013, Adobe Reader, etc.
      - Filter Driver (analysis tool)
    - Contents:
      - Mail inbox, Beacon Files (doc, xlsx, pptx, pdf), Browser History, etc



Architecture of mimetic enterprise network ‘STARDAST’
http://www.nict.go.jp/en/data/nict-news/NICT_NEWS_2018-472_E.pdf (page. 8-9)



Summary of NanoCore Operator Actions

In this experiment, we confirmed **88 intrusions**

- Operators who have achieved one or more of these objectives: **53**
  - Screen sharing and email account/passwords theft were common
  - They used built-in browser or mailer to find interested users
  - They used secondary malware occasionally

- Operators who have left: **35**
  - only screen sharing: **17**
  - screen sharing and check the browser: **8**
  - only shutdown: **3**
  - uninstall client, locked the screen, etc: **7**

Classification of operator actions

Category	Counts
SCREEN SHAREING	76
PASSWORDS	37
FILES	24
BROWSER	18
MALWARE	12
MAIL	7
UNINSTALL	6
TOOLS	5
SHUTDOWN	5
MISC	16

List of NanoCore Operator Actions

Category	Behavior
Mail	Open Outlook
	Check inbox folder
	Check for sent items
	Check draft messages
	Check user's account information
	Search for specific email
	Try to send e-mails
Browser	Open Chrome or Internet Explorer
	Check Google account login status
	Change the language setting to English
	Check user's bookmarks
	Open the bookmarked page
	Open a specific page (PayPal, Alibaba, xvideos, etc.)
	Check user's browsing history
	Download a specific tool
	Check frequently visited pages or recently closed tabs
Privilege	Request privilege escalation

Category	Behavior
File access	Open a folder or file on the desktop
	Open the recently viewed location
	Compress Files
	Check the network drive
	Upload files to the server
	Install and execute another malware
	Update NanoCore client
	Uninstall NanoCore client
	Search by "Search for programs and files"
Account Information	Steal the password stored in the browser
	Steal account information stored in Mailer
Network Connection	Right-click on the network icon in the taskbar
	Check the Network and Sharing Center in the Control Panel
Commands	run ipconfig, net view
	run systeminfo
Others	Talk to us using NjRAT chat tool
	Lock the screen to disrupt user's operation

Secondary Malware

Category	Name	Note
Classifiable Malware	AsyncRAT	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
	LimeRAT	https://github.com/NYAN-x-CAT/Lime-RAT
	Lokibot	-
	Morphine	-
	NetWire	-
	NjRAT	-
	Orcus	-
	Remcos	-
	VenomRAT	variant of https://github.com/mirkoBastianini/Quasar-RAT ?
Unknown	Unknown (worm)	Spreads using autorun.inf Tamper with the legitimate file so that it can be invoked via a worm
	Unknown	Solely execute “taskkill /f /im svchost.exe” ?

Tools and Techniques

Category	Name	Note
Tools	Disable-Windows-Defender	https://github.com/NYAN-x-CAT/Disable-Windows-Defender
	Chrome-Password-Recovery	https://github.com/0xfd3/Chrome-Password-Recovery
	LastActivityView	https://www.nirsoft.net/utils/computer_activity_view.html
	Mail PassView (NanoCore's default feature)	https://www.nirsoft.net/utils/mailpv.html
	WebBrowserPassView (NanoCore's default feature)	https://www.nirsoft.net/utils/web_browser_password.html
	AnyDesk	https://anydesk.com/
	TeamViewer	https://www.teamviewer.com/
Techniques	Microsoft AMSI (Antimalware Scan Interface) Bypass	Patch AmsiScanBuffer of amsi.dll to bypass scanning Similar code: https://github.com/rasta-mouse/AmsiScanBufferBypass/blob/master/ASBBypass/Program.cs
	HideProc	Inject taskmgr.exe and hide process name that start with asz$

NanoCore Operator Actions

- **Case1:**
  The operator shared the screen and stole the password
  (Most common action)

- **Case2:**
  The operator carefully checked the browser and mailer

- **Case3:**
  The operator attempted to infect multiple RATs

NanoCore Operator Actions – Case 1

Case 1: The operator shared the screen and stole the password (Most common action)

- Duration
  - 06-15-2020 16:32:00 ~ 16:34:00 (UTC+9)
- Actions
  - Performed screen sharing
  - Recover Passwords (NanoCore Surveillance Plugin)
    - Stole outlook 2013 credentials
    - Tried to steal browser passwords
  - Uninstalled NanoCore client

NanoCore Operator Actions – Case 1

- Took control of the screen through screen sharing ; however, did not manipulate the screen

- Recover Passwords (NanoCore Surveillance Plugin)
  - Stole outlook 2013 credentials
    - Used Nirsoft's "Mail PassView" https://www.nirsoft.net/utils/mailpv.html

```
UUID('2441ccc7-e521-6225-4a86-bbbd0ea9b98f'),
[{'type': <NanoCoreType.BYTE: 1>, 'value': b'\x00'},
 {'type': <NanoCoreType.BYTE: 1>, 'value': b'\x01'},
 {'type': <NanoCoreType.STRING: 12>, 'value': 'Outlook 2013'},
 {'type': <NanoCoreType.STRING: 12>, 'value': '[Mail address],
 {'type': <NanoCoreType.STRING: 12>, 'value': '[Password]
```

  - Tried to steal browser passwords
    - Used Nirsoft's "WebBrowserPassView" https://www.nirsoft.net/utils/web_browser_password.html
    - I did not save passwords in the browser, therefore it was not stolen

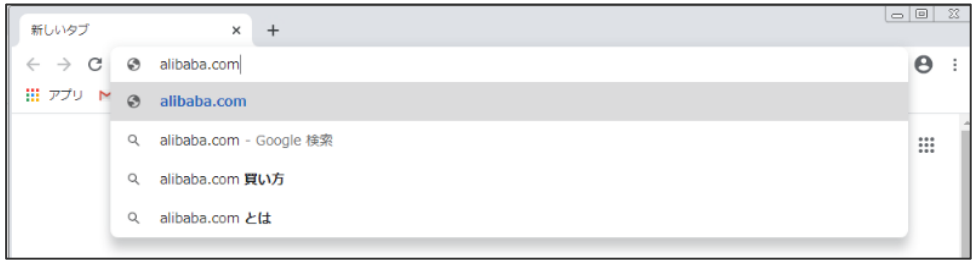
NanoCore Operator Actions – Case 2

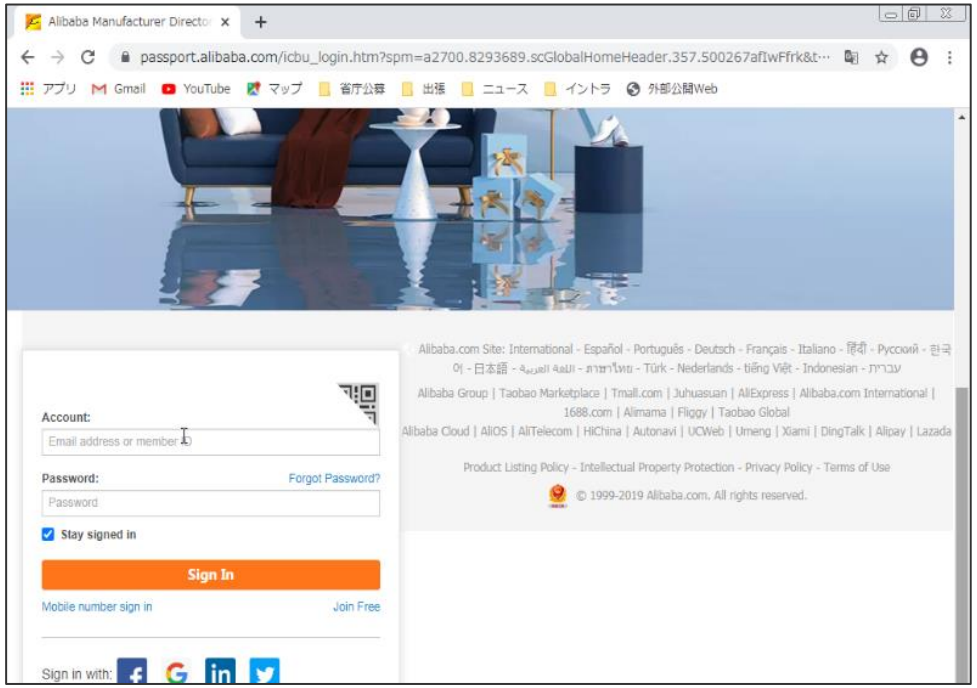
Case 2: The operator carefully checked the browser and mailer

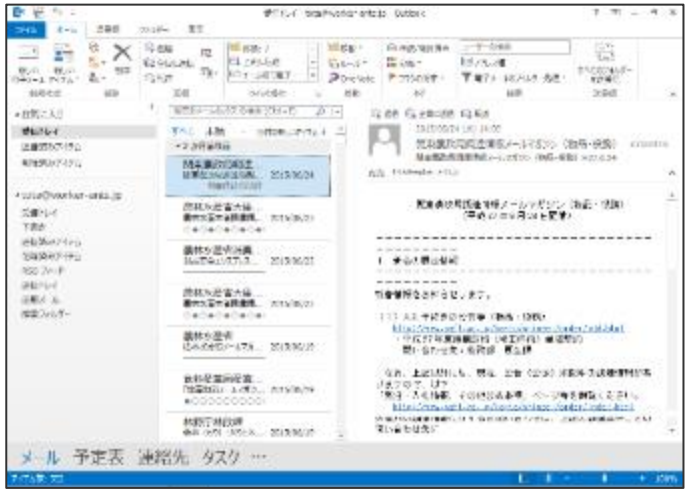
- Duration
  - 07-08-2020 16:07:10 ~ 16:56:47 (UTC+9)
- Actions
  - Performed screen sharing
    - Opened folders on the desktop
    - Checked the network connection
    - Opened Outlook again and again
      - Looked at the email list slowly
      - Checked the sender's e-mail address
      - Checked the user's Outlook account settings
      - Searched e-mails with the keywords 'AL' and 'alibaba'
      - Enlarge the mail view
    - Checked the taskbar
    - Opened Chrome again and again
      - Typed 'alibaba.com' in the address bar
      - Visited Alibaba's 'Sign In' page
      - Checked Chrome login status
      - Opened 'yelp.com' from bookmark
      - Checked installed Chrome Apps
      - Changed the language setting to English
    - Opened the start menu
      - Searched with keywords: 'al', 'english'
      - Clicked the shutdown button

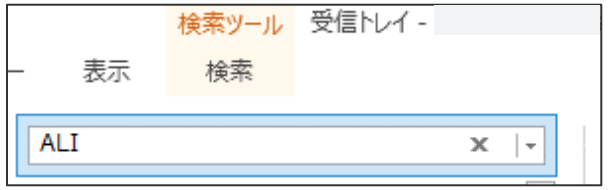
NanoCore Operator Actions – Case 2

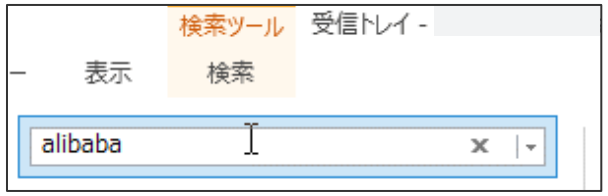
- Used Chrome and Outlook alternately
  - Opened Chrome
    -> Opened ‘alibaba.com’ page
    -> Moved to ‘Sign In’ page
    -> Opened Outlook 2013
    -> Slowly browsed the list of messages
    -> Searched e-mails with the keywords ‘ALI’ and ‘alibaba’
  - Did he/she tried to create an account using the stolen email address?











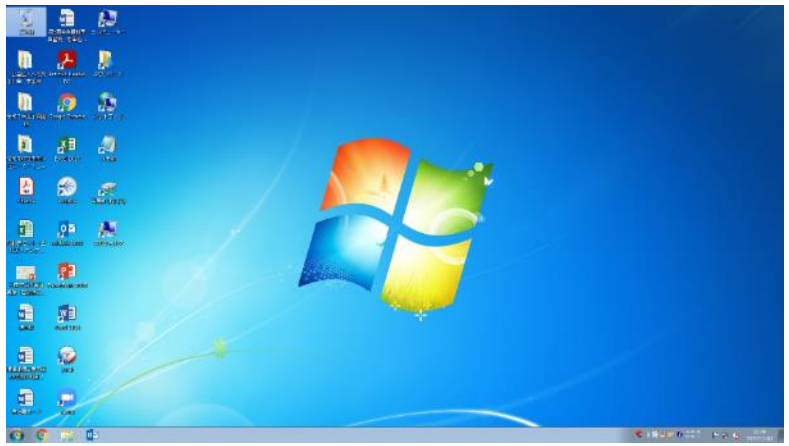
NanoCore Operator Actions – Case 3

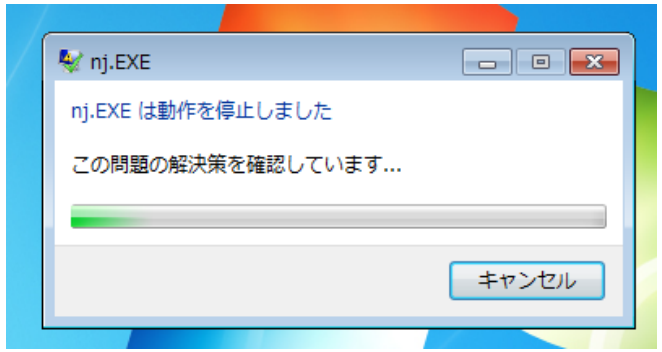
Case 3: The operator attempted to infect multiple RATs

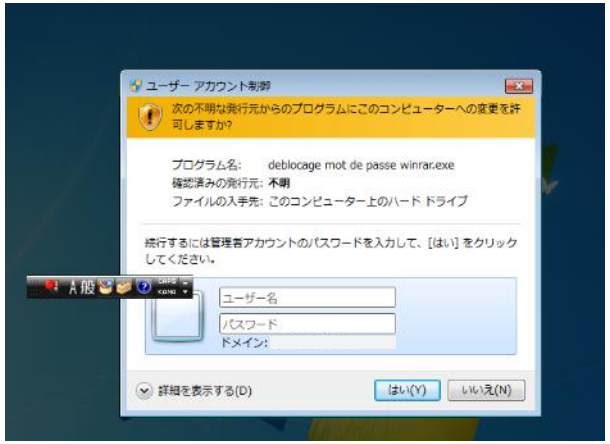
- Duration
  - 10-08-2020 15:38:44 ~ 15:44:27 (UTC+9)
  - 10-13-2020 14:52:27 ~ 15:03:54 (UTC+9)
- Actions
  - Performed screen sharing
  - Installed and executed another malware
    - NjRAT, AsyncRAT, Remcos
  - Ran a tool to disable Windows security feature
    - Disable-Windows-Defender: https://github.com/NYAN-x-CAT/Disable-Windows-Defender
  - Microsoft AMSI (Antimalware Scan Interface) Bypass

NanoCore Operator Actions – Case 3

- **FIRST DAY:** 10-08-2020 15:38:44 ~ 15:44:27 (UTC+9)
  - Took control of the screen through screen sharing ; however, did not manipulate the screen







  - Executed NjRAT and 'Disable-Windows-Defender'

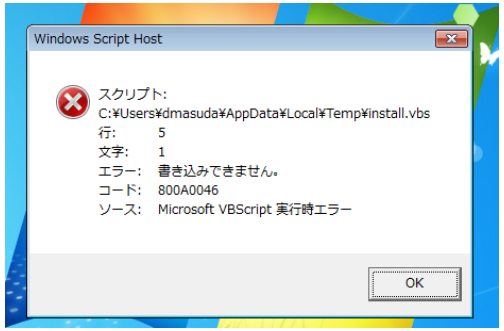
- dnshost.exe PID:2064
  - nj.EXE PID:2552
  - deblocage mot de passe winrar.exe PID:504
  - deblocage mot de passe winrar.exe PID:1964
    - powershell.exe PID:1868

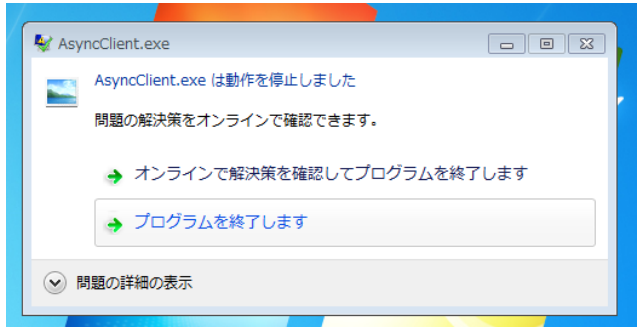
NjRAT
- Microsoft AMSI Bypass
- Win7 did not have amsi.dll, which was used for AMSI bypass; therefore, the process was abnormally terminated

Disable-Windows-Defender
- https://github.com/NYAN-x-CAT/Disable-Windows-Defender
- Require administrator privileges before running

NanoCore Operator Actions – Case 3

- **5 DAYS LATER:** 10-13-2020 14:52:27 ~ 15:03:54 (UTC+9)
  - Took control of the screen through screen sharing ; however, did not manipulate the screen





  - Executed NjRAT, AsyncRAT, Remcos
    - dnshost.exe PID:2224
      - nj.EXE PID:4260
        - timeout.exe PID:3776
      - AsyncClient.exe PID:4168
      - AsyncClient.exe PID:1108
        - timeout.exe PID:4896
      - remcos_agent.exe PID:4364
        - svchost.exe PID:4660
        - dxdiag.exe PID:4852
      - AsyncClient.exe PID:5060
      - remrem.exe PID:5792
        - timeout.exe PID:4536
        - remrem.exe PID:6428
      - remrem.exe PID:5160

→ NjRAT
→ AsyncRAT
→ Remcos

} downloaded from hastebin.com

→ Unknown (download from 000webhostapp.com failed)

NanoCore Operator Actions - Discuss

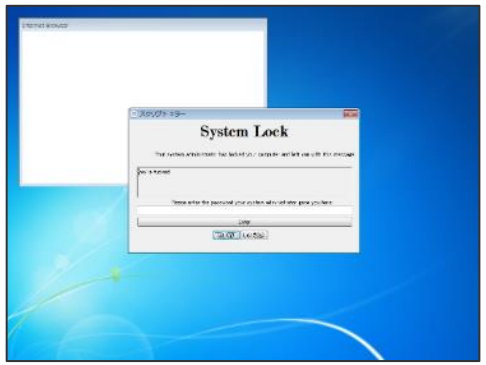
- What is the purpose of the operator?
  - **User reconnaissance**
    - 21 operators carefully **checked the browser history, bookmarks, and mailboxes in the mailer**
    - 24 operators **checked the Desktop, Documents and shared folders**
  - **Email account/passwords and the files theft**
    - 37 operators **stole email accounts and passwords**
    - 8 operators **stole the files**. Up to 221 files was stolen
  - **Backdoor installation**
    - 12 operators **were infected with malware** other than NanoCore
    - 11 different types of malware were used

NanoCore Operator Actions - Discuss

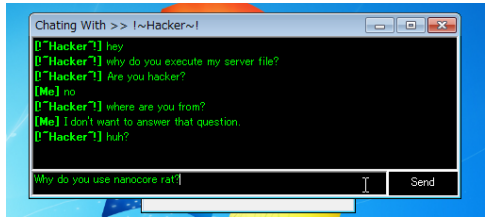
- What caused the operator to leave?
  - **Did he/she notice that it was an analysis environment?**
    - **Mailboxes (inbox, sent, draft) were empty**
    - **No browsing history**
    - Used systeminfo command to check the environment
    - VM detection
    - **Malware that only works on Windows10** has been executed
  - **Their target was different**
    - The experiment was conducted **between 9 o'clock and 18 JST (UTC+9) on weekdays**
    - **OS language setting and file contents were Japanese**
    - GeoIP of the IP address is in Japan

When they realized it was a fake user:

shutdown



locked the screen



talked to us via chat

File Creation(File System Tunneling)		scanresult.db-journal
File Creation		PING.EXE-371F41E2.pf
File Deletion		WrXE6.exe
File Creation		CMD.EXE-AC113AA8.pf
File Creation(File System Tunneling)		scanresult.db-journal

uninstalled NanoCore

Conclusion

- **Long-term observations of NanoCore C2 servers**
  - C2 servers primarily located in the USA and Europe
  - Most of the servers are running between 9:00 and 18:00
  - Running multiple RATs in combination
- **NanoCore operator attraction experiment**
  - Many operators stole email account/passwords
  - Infected RATs other than NanoCore for a secondary infection
- **Future work**
  - Setting up an environment, in which the operators are less likely to detect us
  - Scanning for VPNs and proxies commonly used by attackers may help detect RATs other than NanoCore