

# Dark Side of VSCode

~ How Attacker Abuse VSCode as RAT ~

Hayate Hazuru, Shuhei Sasada  
ITOCHU Cyber & Intelligence



ITOCHU Cyber & Intelligence Inc.

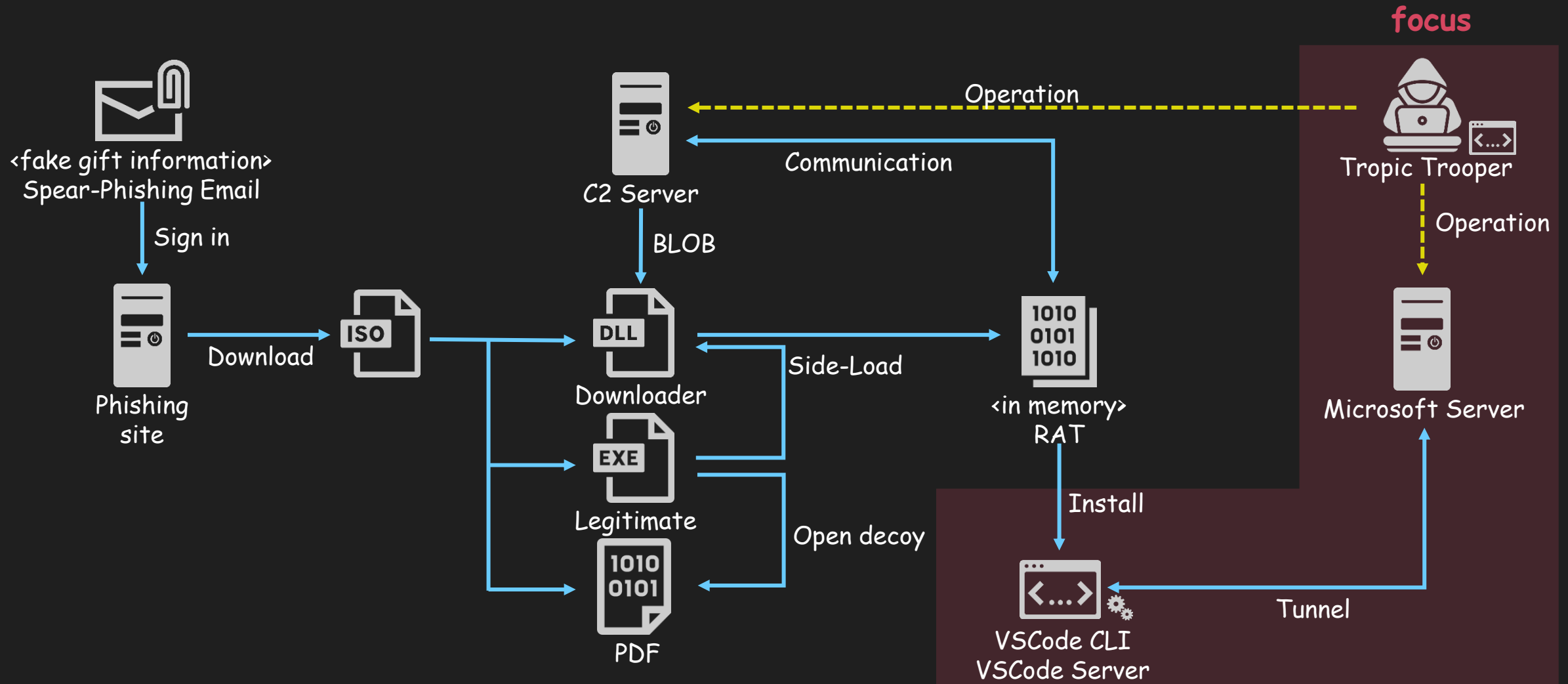
# Agenda

- 01 Introduction
- 02 What is VSCode
- 03 What is Remote Development
- 04 Artifacts Projection Only / TLP:RED
- 05 Detection and Protection
- 06 Conclusion

# 01 Introduction

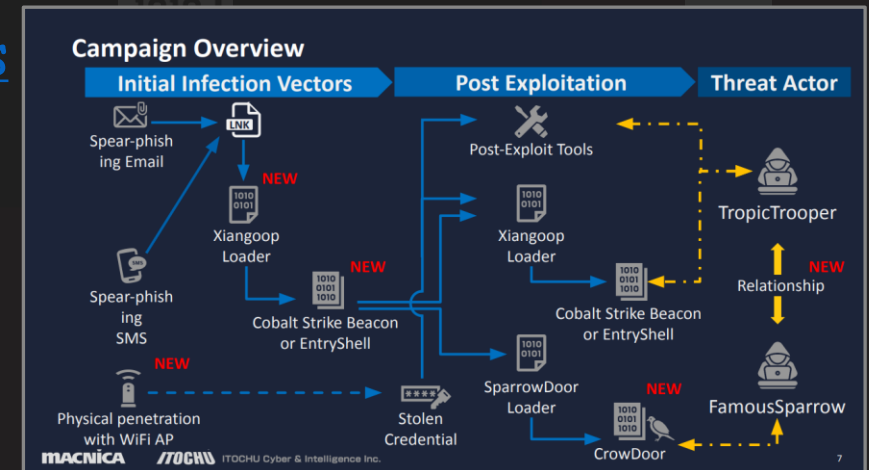
---

# Attacks overview and talk focus



# Attacks overview and talk focus

- The targeted attack was observed in late September 2023.
- VSCode abuse has been a long-standing concern, but this is the first confirmed case of APT abuse.
- Attackers used a combination of RAT and VSCode tunnels to compromise PCs through two routes.
- For complete details on Tropic Trooper(alias:Pirate Panda, KeyBoy) attack campaigns, please refer to the VB2023 London lecture material. ([Unveiling Activities of Tropic Trooper 2023: Deep Analysis for Xiangoop Loader and EntryShell payload](#))

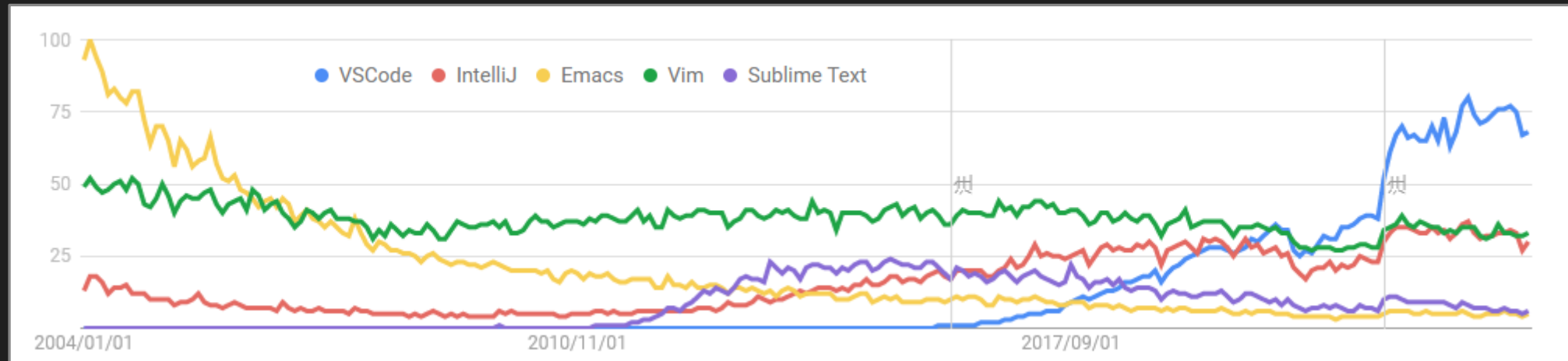


# 02 What is VSCode

---

# What is the Visual Studio Code (VSCode)

- VSCode is a code editor released by Microsoft in April 2015 (and OSS).
- It is extremely multifunctional and offers useful extensions provided by official, third-party vendors, and communities.
- Today, VSCode has become a standard in modern development, marking an end to the "editor wars".

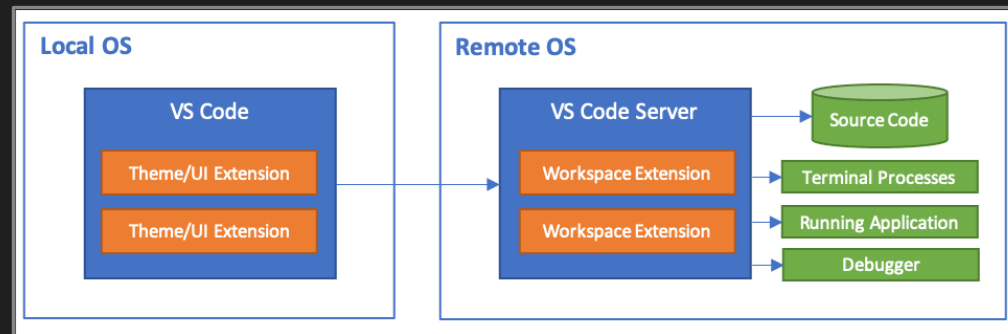


# 03 What is Remote Development

---

# VS Code Remote Development

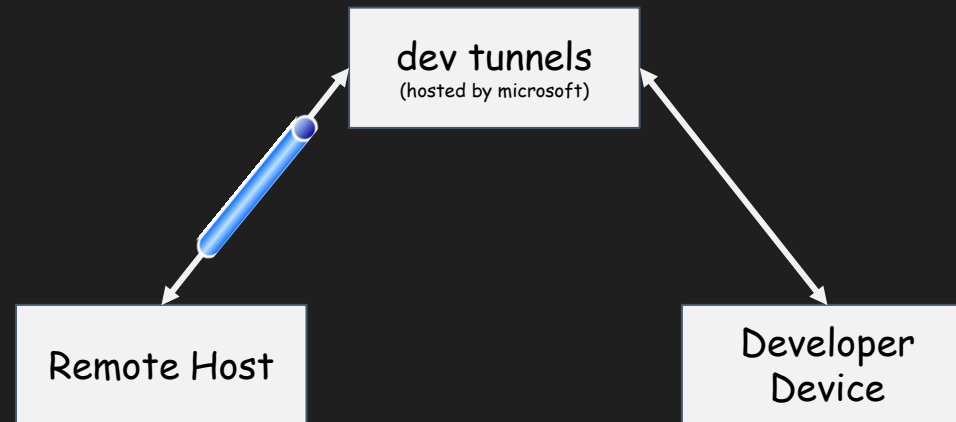
- Why we use remote development feature
  - Development on an operating system different from the host.
  - Utilization of standardized or pre-built development environments.
  - Isolation of the development environment from the host (also as protection against malicious packages/extensions).
  - Development on a more powerful host.
- How Remote Development works
  1. Connect to a remote host using methods such as SSH or tunneling.
  2. The "VS Code Server" is deployed on the remote host.
  3. By connecting from the developer's VSCode (Web/Standalone) on their device, they can edit source code on the remote host and execute commands.



[VS Code Remote Development - Microsoft](#)

# How dev tunnels work

1. Authentication using either a Github, Microsoft ID, or Entra ID establishes a connection with Microsoft's tunnel server ([dev tunnels](#)).
2. An endpoint corresponding to the Phase 1 connection is created.
3. Connect to the created endpoint using VSCode.



demo

---

# 04 Artifacts

---

# 05 Detection and Protection

---

# How to hunt vscode execution by network activity.

---

- Dev Tunnels use below hosts
  - Authentication
    - github.com
    - login.microsoftonline.com
  - Dev Tunnels
    - global.rel.tunnels.api.visualstudio.com
    - [clusterId].rel.tunnels.api.visualstudio.com
    - [clusterId]-data.rel.tunnels.api.visualstudio.com
    - \*.[clusterId].devtunnels.ms
    - \*.devtunnels.ms
    - [clusterId] list is available at <https://global.rel.tunnels.api.visualstudio.com/api/v1/clusters>
- Detect with Context
  - It would be better to detect the aforementioned communications in networks, such as business departments or production segments, where VSCode is not used.

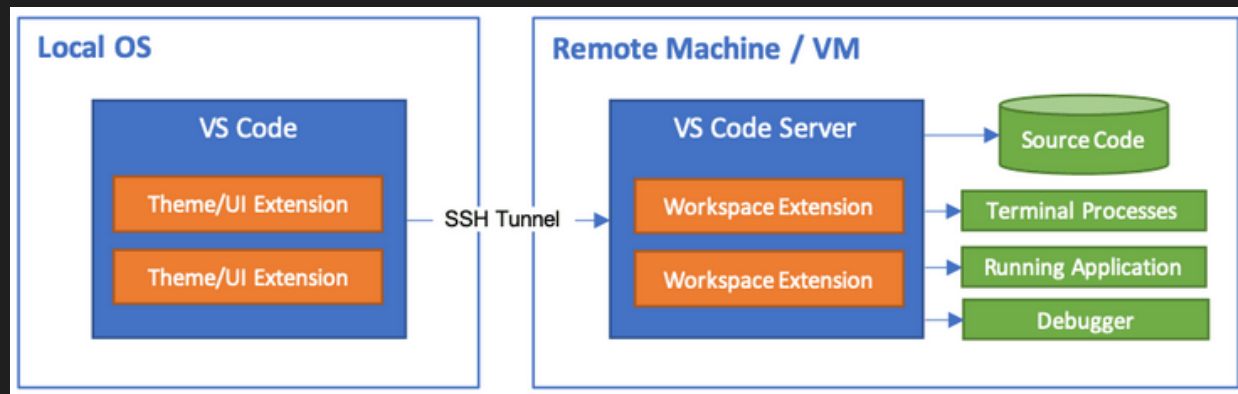
# How to hunt vscode executing by process behavior

- “node.exe” execute under vscode and Image Path is “%USERPROFILE%\%.vscode\cli\servers\Stable-[ID]\server\node.exe”
- PowerShell (pwsh.exe) is run under node.exe if actor create new terminal
- It's anomaly and you can detect VSCode tunnel by that path and process name.

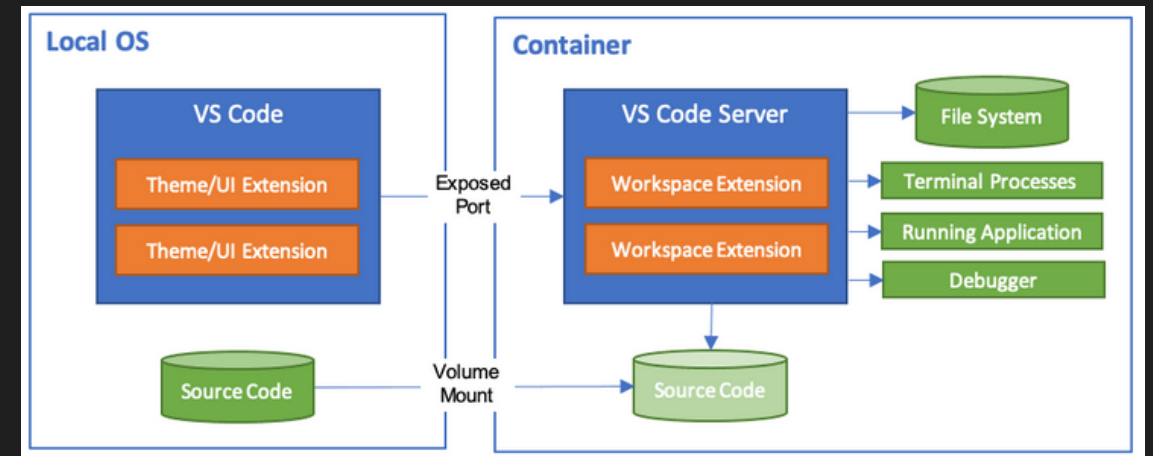
WindowsTerminal.exe	24052	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.18.3181.0_x64__8wekyb3d8bbwe\WindowsTerminal.exe
OpenConsole.exe	17928	C:\Program Files\WindowsApps\Microsoft.WindowsTerminal_1.18.3181.0_x64__8wekyb3d8bbwe\OpenConsole.exe
pwsh.exe	5852 Microsoft Corporation	C:\Program Files\PowerShell\7\pwsh.exe
code.exe	19668	C:\Users\██████\Downloads\Kentai\vscode_cli_win32_x64_cli\code.exe
cmd.exe	16056 Microsoft Corporation	C:\Windows\System32\cmd.exe
conhost.exe	11884 Microsoft Corporation	C:\Windows\System32\conhost.exe
node.exe	6100 Node.js	C:\Users\██████\%.vscode\cli\servers\Stable-0ee08df0cf4527e40edc9aa28f4b5bd38bbff2b2\server\node.exe
node.exe	3060 Node.js	C:\Users\██████\%.vscode\cli\servers\Stable-0ee08df0cf4527e40edc9aa28f4b5bd38bbff2b2\server\node.exe
node.exe	27324 Node.js	C:\Users\██████\%.vscode\cli\servers\Stable-0ee08df0cf4527e40edc9aa28f4b5bd38bbff2b2\server\node.exe
node.exe	1772 Node.js	C:\Users\██████\%.vscode\cli\servers\Stable-0ee08df0cf4527e40edc9aa28f4b5bd38bbff2b2\server\node.exe
conhost.exe	20548 Microsoft Corporation	%%?%C:\Windows\System32\conhost.exe
pwsh.exe	2684 Microsoft Corporation	C:\Program Files\PowerShell\7\pwsh.exe
PING.EXE	10764 Microsoft Corporation	C:\Windows\System32\PING.EXE

# Safe Use of VSCode Remote Development

- VSCode is essential for modern development, and the VS Code Remote Development feature itself is very useful.
- I recommend to use Dev Containers and Visual Studio Code Remote - SSH
- Dev Containers: Connect to local containers
- SSH: Establish SSH connections with remote hosts. Therefore, it can be controlled by firewall.



[VS Code Remote Development - SSH](#)



[Dev Containers](#)

# 06 Conclusion

---

# Conclusion

---

- VSCode was actually used as a RAT by APT.
- By using dev tunnels, attackers can remotely control through proxies owned by Microsoft.
- In modern development, VSCode and Remote Tunnel are very useful, but for safe use, it is recommended to use SSH or Dev Containers.
- Hunt for communications to dev tunnels and processes of the VSCode Server.
- Alternatively, deny communication to dev tunnels in segments where development communication does not occur, such as in the sales department or production network.



# Any Questions?



ITOCHU Cyber & Intelligence Inc.

# Appendix

---

# Appendix

---

- Attackers can persist tunnel process by "code tunnel service install"
- The command make auto run registry
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    - Name: Visual Studio Code Tunnel
    - Data:
      - [Path to binary]\code.exe  
--verbose  
--cli-data-dir %USERPROFILE%\vscode\cli  
tunnel service internal-run  
--log-to-file %USERPROFILE%\vscode\cli\tunnel-service.log