Hive Pro

Threat Level

Red

THREAT ADVISORY

# ACTOR REPORT

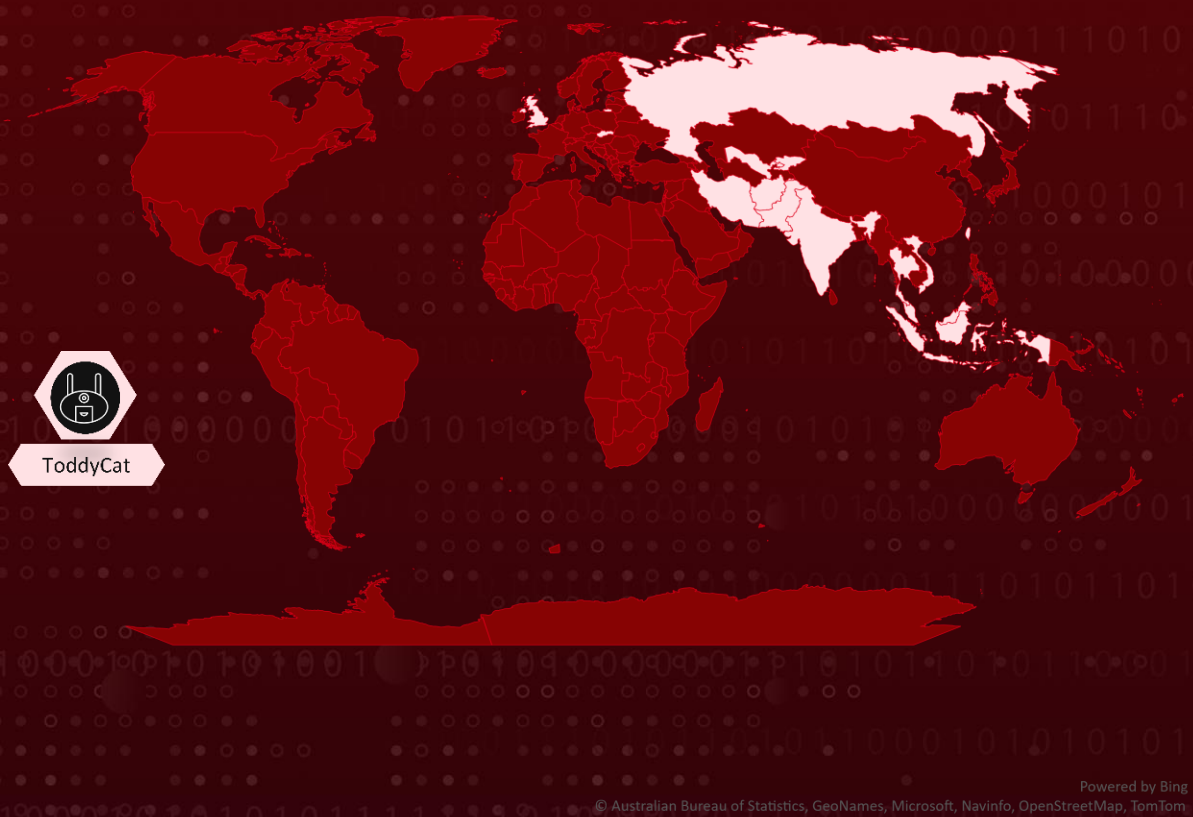
# ToddyCat exploits unknown vulnerability in Microsoft Exchange servers to targets entities in Europe and Asia

| Date of Publication | Admiralty code | TA Number |
| --- | --- | --- |
| June 22, 2022 | A2 | TA2022131 |

# Summary

ToddyCat, an APT group is deploying web shells by exploiting an unknown vulnerability in the Microsoft Exchange Servers. They are initiating a multi-stage infection that aims at governmental bodies of Europe and private companies of Asia.

## Actor Map



# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0002**<br>Execution | **T1059**<br>Command and Scripting Interpreter | **T1053**<br>Scheduled Task/Job | **TA0005**<br>Defense Evasion |
| **T1055**<br>Process Injection | **T1027**<br>Obfuscated Files or Information | **TA0010**<br>Exfiltration | **T1048**<br>Exfiltration Over Alternative Protocol |
| **T1574.002**<br>Hijack Execution Flow: DLL Side-Loading | **T1574**<br>Hijack Execution Flow | **T1037**<br>Boot or Logon Initialization Scripts | **TA0003**<br>Persistence |
| **T1071.001**<br>Application Layer Protocol: Web Protocols | **TA0011**<br>Command and Control | **T1071**<br>Application Layer Protocol | **T1090**<br>Proxy |

# Technical Details

**#1** ToddyCat starts its infection vector by exploiting vulnerable Microsoft Exchange Servers and deploying a web shell named China Chopper. The web shell is then used to drop multiple loaders which eventually executes Samurai backdoor through ports 80 & 443.

**#2** This backdoor then deploys another malware called Ninja to avoid detection and penetrate deep inside network. Both malwares are capable of taking control of the system as well as move laterally within the network.

## Actor Detail

| NAME | ORIGIN | MOTIVE | TARGET LOCATIONS | TARGET INDUSTRIES |
|---|---|---|---|---|
| ToddyCat | China (Suspected) | Information theft and espionage | Asia<br>Europe<br>Taiwan<br>Vietnam<br>Afghanistan<br>India<br>Iran<br>Malaysia<br>Pakistan<br>Russia<br>Slovakia<br>Thailand<br>United Kingdom<br>Kyrgyzstan<br>Uzbekistan<br>Indonesia | Government sectors, Private Companies |

# Indicator of Compromise (IOC)

| TYPE | VALUE |
|---|---|
| File Path | C:\inetpub\temp\debug.exe,<br>C:\Windows\Temp\debug.exe,<br>C:\Windows\Temp\debug.xml,<br>C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files\web.exe,<br>C:\Users\Public\Downloads\dw.exe,<br>C:\Users\Public\Downloads\chrome.log,<br>C:\Windows\System32\chr.exe,<br>C:\googleup.exe,<br>C:\Program Files\microsoft\exchange server\v15\frontend\httpproxy\owa\auth\googleup.log,<br>C:\google.exe,<br>C:\Users\Public\Downloads\x64.exe,<br>C:\Users\Public\Downloads\1.dll,<br>C:\Program Files\Common Files\microsoft shared\WMI\iiswmi.dll,<br>C:\Program Files\Common Files\Microsoft shared\Triedit\Triedit.dll,<br>C:\Program Files\Common Files\System\websvc.dll,<br>C:\Windows\Microsoft.NET\Framework\sbs_clrhost.dll,<br>C:\Windows\Microsoft.NET\Framework\sbs_clrhost.dat,<br>C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files\web.xml,<br>C:\Users\Public\Downloads\debug.xml,<br>C:\Users\Public\Downloads\cache.dat,<br>C:\Windows\System32\config\index.dat,<br>C:\Windows\Microsoft.NET\Framework\netfx.dat,<br>%ProgramData%\adobe\2.dll,<br>%ProgramData%\adobe\acrobat.exe,<br>%ProgramData%\git\git.exe,<br>%ProgramData%\intel\mstacx.dll,<br>%ProgramData%\microsoft\drm\svchost.dll,<br>%ProgramData%\microsoft\mf\svchost.dll,<br>%ProgramData%\microsoft\mf\svhost.dll,<br>%program files%\Common Files\services\System.Core.dll,<br>%public%\Downloads\1.dll,<br>%public%\Downloads\config.dll,<br>%system%\Triedit.dll,<br>%userprofile%\Downloads\Telegram Desktop\03.09.2021 r.zip,<br>%userprofile%\Downloads\TelegramDesktop\Тех.Инструкции.zip |

| TYPE | VALUE |
|---|---|
| File Path | %userprofile%\libraries\1.dll,<br>%userprofile%\libraries\chrome.exe,<br>%userprofile%\libraries\chrome.log,<br>%userprofile%\libraries\config.dll,<br>C:\intel\2.dll,<br>C:\intel\86.dll,<br>C:\intel\x86.dll |
| MD5 | 5cfdb7340316abc5586448842c52aabc,<br>93c186c33e4bbe2abdcc6dfea86fbbff,<br>5a912beec77d465fc2a27f0ce9b4052b,<br>f595edf293af9b5b83c5ffc2e4c0f14b,<br>5a531f237b8723396bcfd7c24885177f,<br>1ad6dccb520893b3831a9cfe94786b82,<br>33694faf25f95b4c7e81d52d82e27e7b,<br>832bb747262fed7bd45d88f28775bca6,<br>8fb70ba9b7e5038710b258976ea97c98,<br>ee881e0e8b496bb62ed0b699f63ce7a6,<br>ae5d2cef136ac1994b63c7f8d95c9c84,<br>5c3bf5d7c3a113ee495e967f236ab614,<br>bde2073dea3a0f447eeb072c7e568ee7,<br>350313b5e1683429c9ffcbc0f7aebf3b,<br>8a00d23192c4441c3ee3e56acebf64b0,<br>5e721804f556e20bf9ddeec41ccf915d |
| Registry Keys | $HKLM\System\ControlSet\Services\WebUpdate,<br>$HKLM\System\ControlSet\Services\PowerService,<br>$HKLM\SOFTWARE\Classes\Interface\{6FD0637B-85C6-D3A9-CCE9-65A3F73ADED9},<br>$HKLM\SOFTWARE\Classes\Interface\{AFDB6869-CAFA-25D2-C0E0-09B80690F21D} |
| C2 | 149.28.28[.]159,<br>eohsdnsaaojrhnqo.windowshost[.]us |

## References


https://securelist.com/toddycat/106799/

https://thehackernews.com/2022/06/new-toddycat-hacker-group-on-experts.html

https://www.kaspersky.com/about/press-releases/2022_toddycat-an-advanced-threat-actor-targets-high-profile-entities-with-new-malware

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.


At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**June 22, 2022 • 11:30 AM**



More at www.hivepro.com