



# THREAT ADVISORY

**APT 10, a state-sponsored Chinese threat group,  
conducting a global cyber espionage operation**

**TA2022089**

**Threat Level**

**RED**

**Publish Date – April 12, 2022**

A Chinese state-sponsored advanced persistent threat APT 10 group has been attacking government, legal, religious entities and non-governmental organizations (NGOs) around the world in what appears to be an espionage campaign that has been underway for several months.

The actor gained initial access by exploiting unpatched Microsoft Exchange Server vulnerabilities, and the attacker then distributed a variety of tools, including a custom loader and the **Sodamaster** backdoor. The backdoor is a fileless virus that may avoid detection in a sandbox by looking for a registry key or postponing execution; enumerating the username, hostname, and operating system of targeted computers; searching for running processes; and downloading and executing additional payloads. It may also obfuscate and encrypt traffic it delivers back to its command-and-control (C&C) server. The attackers are also seen stealing credentials, including using a custom-made Mimikatz loader. This version of Mimikatz includes mimilib.dll, which allows it to retrieve credentials in plain text for each user who connects to the compromised host and maintains persistence over reboots.

The Mitre TTPs commonly used by APT 10 are:

TA0042: Resource Development  
TA0001: Initial Access  
TA0002: Execution  
TA0003: Persistence  
TA0004: Privilege Escalation  
TA0005: Defense Evasion  
TA0006: Credential Access  
TA0007: Discovery  
TA0008: Lateral Movement  
TA0009: Collection  
TA0011: Command and Control  
TA0010: Exfiltration T1087.002: Account Discovery: Domain Account  
T1583.001: Acquire Infrastructure: Domains  
T1560: Archive Collected Data  
T1560.001: Archive via Utility  
T1119: Automated Collection  
T1059.001: Command and Scripting Interpreter: PowerShell  
T1059.003: Command and Scripting Interpreter: Windows Command Shell  
T1005: Data from Local System  
T1039: Data from Network Shared Drive  
T1074.001: Data Staged: Local Data Staging  
T1074.002: Data Staged: Remote Data Staging  
T1140: Deobfuscate/Decode Files or Information  
T1568.001: Dynamic Resolution: Fast Flux DNS  
T1190: Exploit Public-Facing Application  
T1210: Exploitation of Remote Services



# THREAT ADVISORY

T1083: File and Directory Discovery  
T1574.001: Hijack Execution Flow: DLL Search Order Hijacking  
T1574.002: Hijack Execution Flow: DLL Side-Loading  
T1070.003: Indicator Removal on Host: Clear Command History  
T1070.004: Indicator Removal on Host: File Deletion  
T1105: Ingress Tool Transfer  
T1056.001: Input Capture: Keylogging  
T1036: Masquerading  
T1036.003: Rename System Utilities  
T1036.005: Match Legitimate Name or Location  
T1106: Native API  
T1046: Network Service Scanning  
T1027: Obfuscated Files or Information  
T1588.002: Obtain Capabilities: Tool  
T1003.002: OS Credential Dumping: Security Account Manager  
T1003.003: OS Credential Dumping: NTDS  
T1003.004: OS Credential Dumping: LSA Secrets  
T1566.001: Phishing: Spearphishing Attachment  
T1055.012: Process Injection: Process Hollowing  
T1090.002: Proxy: External Proxy  
T1021.001: Remote Services: Remote Desktop Protocol  
T1021.004: Remote Services: SSH  
T1018: Remote System Discovery  
T1053.005: Scheduled Task/Job: Scheduled Task  
T1218.004: Signed Binary Proxy Execution: InstallUtil  
T1553.002: Subvert Trust Controls: Code Signing  
T1016: System Network Configuration Discovery  
T1049: System Network Connections Discovery  
T1199: Trusted Relationship  
T1204.002: User Execution: Malicious File  
T1078: Valid Accounts  
T1047: Windows Management Instrumentation

## Actor Details

Name	Origin	Target Locations	Target sectors	Motive
APT 10 (Stone Panda, menuPass Team, menuPass, Red Apollo, Potassium , Hogfish, Happyyyongzi, Cicada, Bronze Riverside, CTG- 5938, ATK 41, TA429, ITG01 )	China	Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Israel, Italy, Japan, Montenegro, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, NGOs, Pharmaceutical, Telecommunications and MSPs.	Information theft and espionage



# THREAT ADVISORY

## Indicators of Compromise (IoCs)

Type	Value
SHA256	01b610e8ffcb8fd85f2d682b8a364cad2033c8104014df83988bc3ddfac8e6ec, 056c0628be2435f2b2031b3287726eac38c94d1e7f7aa986969baa09468043b1, 062ce400f522f90909ed5c4783c5e9c60b63c09272e2ddde3d13e748a528fa88, 0b452f7051a74a1d4a544c0004b121635c15f80122dc6be54db660ceb2264d6f, 0ec48b297dd1b0d6c3ddd15ab63f405191d7a849049feedfa7e44096c6f9d42a, 20fc3cf1afc9e6f19e9abebfc9daf374909801d874c3d276b913f12d6230ec, 2317d3e14ab214f06ae38a729524646971e21b398eda15cc9deb8b00b231abc3, 2417da3adebd446b9fc8b896adb14ea495a4d923e3655e5033f78d8e648fcc8, 37f56127226ce96af501c8d805e76156ca6b87da1ba1bb5d227100912f6c52d9, 3aa54e7d99b69a81c8b25ab57aeb971644ed0a206743c9e51a80ec1852f03663, 3ff2d6954a6b62afb7499e1e317af64502570181fd49ac5a74e2f7947e2e89db, 4f6a768841595293146ca04f879efa988e4e95ce0f2bc299cb669fea55e78b65, 5269db6b19a1d758c75e58ee9bbf2f8fd684cfedbfe712d5b0182d7bbd3a1690, 5bc68df582c86c884b563b15057cc223f2e9bc1022ebb297e32a9a7e3036228b, 6b4692029f05489ecda10e11cfacf3b19097856b88647d3695f3bdc7dd83ce9, 7b581c0305c78f28bad60028c63e852dc34fc9e28f39e4b0af73d80c1d9680c9, 83030f299a776114878bcd2ade585d97836ef4ddb6943cb796be2c88bcb83a83, 90a03dabfc4e56a12cc3bac5cbe991db044b900a01ec341803c864506e467ffa, 9917a2213f114e87745867e5fea6717efd727d7c08fdc851969224be2f0e019b, 9b5f9ff82ed238bcbd83628ed3ec84988dc05f81cec9e45a512fb2c8ac45c33, adfe177ade7d9bfe4df251a69678102aec1104a4ba9f73032dd90aba76d8bdd9, b76fdf584f87c88bdd21fab613335ce7fc05788aa4bb3191d1517ec16ef4d11a, ce45af43dd2af52d6034e981515474147802efdfe036e00078fee29a01694fd6, d461347388ccf0c2008332a1674885a41f70b94b2263bdef44e796d3b1b43b5, df993dca434c3cd2da94b6a90b0ae1650d9c95ea1d5f6a5267aca640d8c6d00e, ee46e714660f7652502d5b3633fae0c08c8018f51cfb56a487afdf58d04dd551a, fe33fd5a63fee62362c9db329dde11080a0152e513ef0e6f680286a6a7b243f
IPv4	88[.]198.101[.]58, 168[.]100.8[.]38

## References

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks>