Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

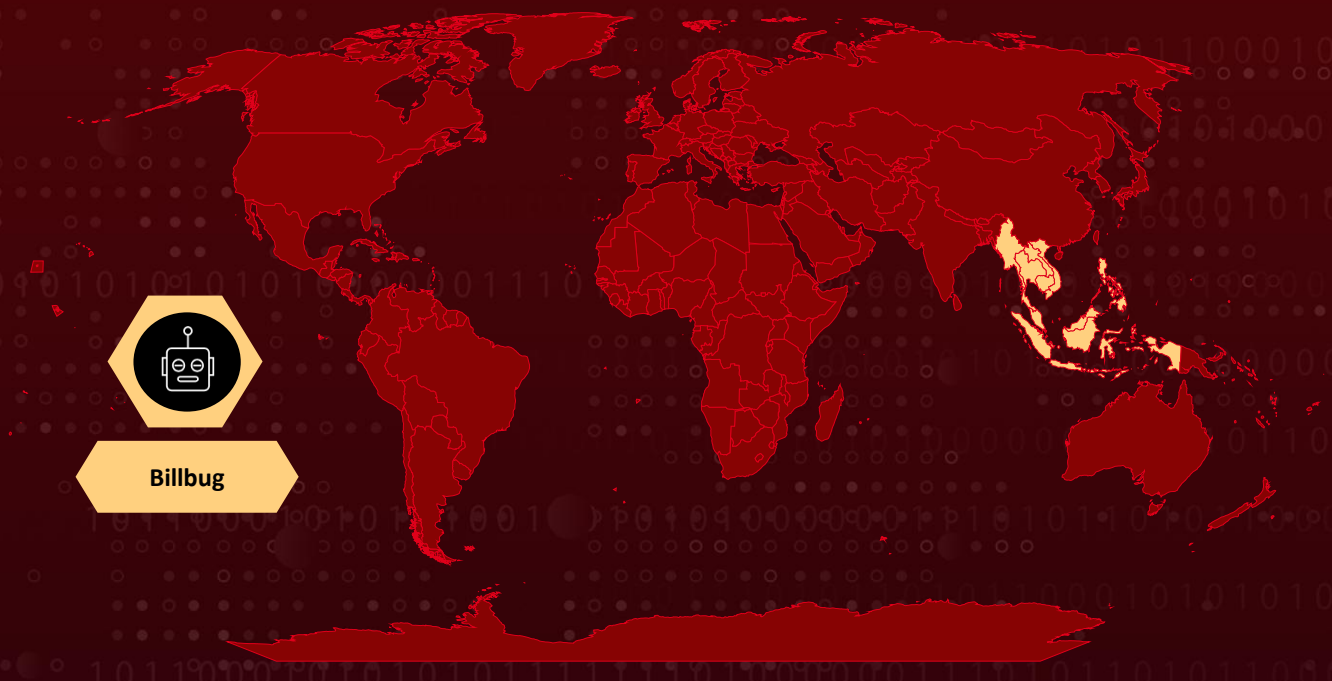
Billbug Cyberespionage Campaign Targets Southeast Asia

Date of Publication	Admiralty Code	TA Number
April 23, 2025	A1	TA2025124

Summary

Attack Commenced: August 2024 - February 2025
Targeted Region: Southeast Asia
Targeted Platform: Windows
Threat Actor: Billbug (aka Lotus Blossom, Lotus Panda, Spring Dragon, Dragonfish, Thrip, Bronze Elgin, CTG-8171, ATK 1, ATK 78, RADIUM, Raspberry Typhoon, Red Salamander)
Malware: Sagerunex, ChromeKatz, CredentialKatz
Targeted Industries: Government, Aviation, Telecommunications, and Construction
Attack: Billbug, a Chinese cyberespionage group, targeted Southeast Asian government and infrastructure sectors from August 2024 to February 2025. They used spear-phishing, custom malware like Sagerunex, and stealthy techniques such as DLL sideloading. Tools like ChromeKatz and Zrok enabled credential theft and covert remote access. Active since at least 2009, Billbug poses a significant long-term threat to national security through sustained espionage operations.

Attack Regions



Attack Details

#1

The cyberespionage group known as Billbug, also referred to as Lotus Blossom, has been implicated in a series of sophisticated attacks targeting government and critical infrastructure organizations across Southeast Asia, particularly focusing on one nation, between August 2024 and February 2025. These operations highlight the group's persistent focus on espionage and data theft.

#2

In this recent campaign, Billbug compromised several high-profile entities, including a government ministry, an air traffic control organization, a telecommunications operator, and a construction company within the targeted nation. The group also infiltrated a news agency in another country and an air freight company in a neighboring nation.

#3

Billbug's attack chain typically begins with initial access via vulnerabilities in public-facing applications, spear-phishing, or credential abuse. Once inside, the group deploys loaders to introduce custom malware, including a new variant of the Sagerunex backdoor. This malware ensures persistence by modifying Windows registry keys to run as a service, enabling long-term access.

#4

To evade detection, the group uses DLL sideloading techniques, abusing legitimate executables from vendors like Trend Micro and Bitdefender to stealthily load malicious DLLs. For credential harvesting, Billbug leverages tools like ChromeKatz and CredentialKatz to steal stored passwords and cookies from Chrome browsers. To maintain covert remote access, they deploy a custom reverse SSH tool on port 22 and use Zrok, a peer-to-peer tunneling tool, to expose internal services externally. They also use utilities like Datechanger.exe to alter file timestamps and hinder forensic analysis.

#5

Billbug's activities date back to at least 2009, with a consistent focus on government and military targets in South Asia. Their methods often include spear-phishing and watering hole attacks to deliver malware, such as Hannotog and Sagerunex. The latter is believed to be an evolution of an older tool named Evora, reflecting the group's ongoing malware development efforts. Overall, the campaign supports long-term espionage, credential theft, and unauthorized access to sensitive government and infrastructure systems, posing a serious threat to national security and critical sectors across the region.

Recommendations

Strengthen Email Security: Implement advanced email filtering solutions capable of detecting and blocking phishing attempts, especially those involving spoofed domains and deceptive content. Enable DMARC, SPF, and DKIM to validate sender authenticity.

Deploy Advanced Endpoint Protection: Utilize Endpoint Detection and Response (EDR) tools to monitor for suspicious activities, such as DLL sideloading and unauthorized registry modifications, which are tactics employed by Sagerunex. Ensure that all endpoints have up-to-date antivirus and anti-malware solutions to detect and prevent known threats.

Credential Protection: Enforce strong password policies, multi-factor authentication (MFA), and monitor for the use of credential dumping tools like ChromeKatz and CredentialKatz.

Enhance Network Monitoring: Implement continuous monitoring for unusual network traffic and suspicious activity, especially around port 22 and the use of tunneling tools like Zrok, which may indicate covert access or exfiltration attempts.

Patch Management: Ensure that all public-facing applications and systems are regularly scanned for vulnerabilities and patched promptly to prevent exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access

T1078.001 Default Accounts	T1078 Valid Accounts	T1566.001 Spearphishing Attachment	T1566 Phishing
T1134.002 Create Process with Token	T1027 Obfuscated Files or Information	T1134 Access Token Manipulation	T1082 System Information Discovery
T1021 Remote Services	T1071.001 Web Protocols	T1555 Credentials from Password Stores	T1041 Exfiltration Over C2 Channel
T1560.001 Archive via Utility	T1560 Archive Collected Data	T1555.003 Credentials from Web Browsers	T1071 Application Layer Protocol
T1573 Encrypted Channel	T1090 Proxy	T1090.002 External Proxy	T1018 Remote System Discovery
T1021.004 SSH	T1204 User Execution	T1140 Deobfuscate/Decode Files or Information	T1070.006 Timestomp
T1070 Indicator Removal	T1204.002 Malicious File	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1574.002 DLL Side-Loading	T1574 Hijack Execution Flow	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20, 788945d484b4e7da7adb438db52c35dd033869c5f43f027a5b6903b7b1dbbd7b,

TYPE	VALUE
SHA256	bf50ed2dd7a721e7c1b13b1eed0f21c3274808d5016310c52b1473530d78f34a, 47013e731b37a80e96a3523e042c23e67bfa721d3651e735307f4a1545898b11, 3d262950bf89995dce56f2c8db16938d37be5564d5e2b011ea49fe2f523f980a, 79cd6380b2cf7ca1b3e3ba386ebbd7df0104e33ac74cdb5e886fd8be207bd961, f4dd0a6594d50012b6b2e3fd578e40a2aa91dae2c2454d04df5c8c9898774da6, 8f309ffbaa532294da8d7896cdac3311e6a1ff82e86551453787ee78a94a679e, 565fbe3f1f444f79aef375678ebbe2cd08ba55bdbee737b4ed2e6d2f7bcfcc16, f88cea311efbd3aaf896dd9527b137ad2bbd29332917b5aadd4c2693b45f893f, 42b8b464147160c2f4c2722dfc222749e67384824bbbb140385271895b138c7b, ccd1f9844b00059f6e35fdff577ac93048f4d99b18162d3c56cfeb2d72b93ae4, 2b59b03e9232b83b8914ed07c6426dd53d17cfb2eba01ab13d4c6cb00466a42e, 240d3040559e6215a8931d9d8670c6eae2c1c42a9a74d260261fda22bcf0817d, e8f482dc47250eaedf8b839cdb4fd9ebffe59d47c7b48d61ad51d942fd35fa18, 0f383b8f68f3b3c3a18ec778a1150563801b8716c7114432ff51a28fff2963b4, b1c782b4a327dadf0d8db016d7556a92bae4b697b10c9282b293e24564bbef32, 5544a68a2b391c88a02f1f581ea1dde9c5cf8aeb41bb552699895283035808 46, dfdd6847579ec6d9630feeda1f5bcbf009d270cd461d30781719a9c218f33d9e, fe2046e479289b1013eb394f5b3d7a49a419cb98015add3ead0fa87614fe6e38, d67774dde98db6aca8271566fac6f3d0e8e474c40604efeedd5b1276abcc8af5, e0d969b95bd91f58b775d2c9b9190a4f7c5ee8a76d63286227885e071883fdef, fa764df857ed8f0fbf606dcbb92d64f5a72b5c1dd94b3dcb9ea02ff8a02b986b, 9e38f67fad7dfd806955c61e8b2d68084c4506227bc8c880cffb28d77612759c, 23012d0e71e40913967a511475b55690e34afcad72ca819b82c885a0df8aea79,

TYPE	VALUE
SHA256	0fd82ff1a4b4f3c55b7faa73621ecb7d11c3cde95631de841cb304a7968804df, b830fe3d5d5462bef92991dd78869a173cb56d823e7776bfa56e09642dd880ed, 776b4a7ce11d2cc9a94268c7280b652ad0d0fb33d3188cf58987e6c5c4fbb5fb, 001380aa1c1850dd603f9e1315f3b9c450e6da13686a0b6ec5c05991df46ff1a, 25df8f277074560cb899314cd649c6d937727c5cce5390a7187a6572dd2e4be1, 1cb12045c55bf2669c3573fc79f1335355defe09af64ac2f9ca495eb5f7af528, ff5a789d0df1b28a183d7f256d3d4f649a16ae4679ef803d28cd9f7443416310, 1ce0367f66a3ee2e461ccb42ae7794622aa9fb3bf9bd8926e85260ed768fb17b, 54a41f888a10e454705c5b4328c13415b0ffea3708e3e101d965883761945c67, e3292e944f3deb871d9d3c2fc28a0255ad900f067f074039dde86a55dcc7b67c, 176a34345bbd4eaf96e47bb60c866847de7cdaf315fe376427f4651c09f98e88, 710c73d806457e576a9987be60ed8676af610b7910928f9fa57fbc58f5f45d52, 4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e, 2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4, 6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61, ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7, e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1, 29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d, 461f0803b67799da8548ebfd979053fb99cf110f40ac3fc073c3183e2f6e9ced, b337a3b55e9f6d72e22fe55aba4105805bb0cf121087a3f6c79850705593d904, 54f0eaf2c0a3f79c5f95ef5d0c4c9ff30a727ccd08575e97cce278577d106f6b, b75a161caab0a90ef5ce57b889534b5809af3ce2f566af79da9184eaa41135bd, becbfc26aef38e669907a5e454655dc9699085ca9a4e5f6ccd3fe12cde5e0594,

TYPE	VALUE
IPv4	103[.]213[.]245[.]95, 103[.]224[.]80[.]102, 103[.]232[.]223[.]117, 103[.]234[.]97[.]19, 103[.]243[.]131[.]205, 103[.]74[.]192[.]105, 117[.]18[.]5[.]141, 118[.]193[.]240[.]214, 122[.]10[.]118[.]125, 122[.]10[.]91[.]36, 122[.]10[.]91[.]37, 123[.]60[.]167[.]7, 160[.]124[.]251[.]105, 185[.]243[.]42[.]80, 185[.]243[.]43[.]197, 185[.]243[.]43[.]202, 43[.]252[.]161[.]22, 43[.]254[.]217[.]138, 43[.]254[.]218[.]69, 43[.]255[.]104[.]100, 45[.]32[.]127[.]121, 45[.]32[.]127[.]212, 58[.]64[.]193[.]166, 58[.]64[.]193[.]225, 59[.]188[.]254[.]21, 59[.]188[.]254[.]79, 59[.]188[.]69[.]190, 59[.]188[.]77[.]188
Domains	cebucafe[.]net, cebucfg[.]org, davaotour[.]net, davoport[.]org, jf[.]doyourbestyet[.]com, ns1[.]poorgoddaay[.]com, www[.]acdserv[.]com, www[.]ilovekalias[.]com, www[.]sensor-data[.]online, www[.]serthk[.]com, zg[.]poorgoddaay[.]com

TYPE	VALUE
File Paths	C:\Windows\temp\TmDebug.log., C:\Windows\Temp\VT001.tmp.

References

https://www.security.com/threat-intelligence/billbug-china-espionage

https://www.picussecurity.com/resource/blog/lotus-blossom

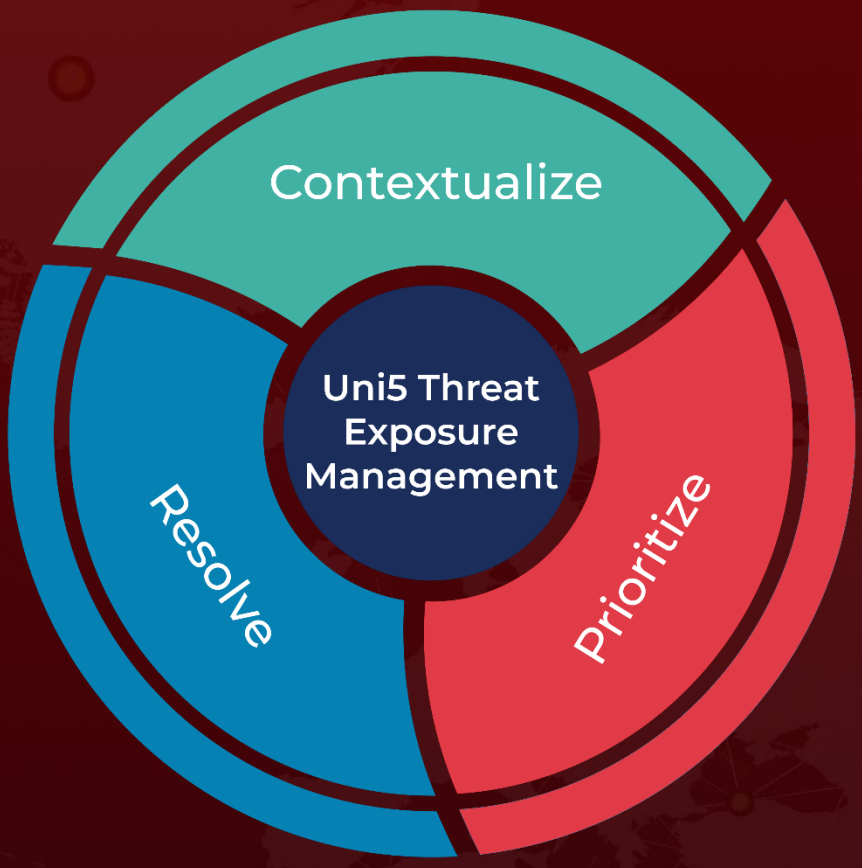
https://blog.talosintelligence.com/lotus-blossom-espionage-group/

https://www.hivepro.com/billbug-returns-after-two-years-to-conduct-an-espionage-campaign/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 23, 2025 • 5:30 AM

More at www.hivepro.com