Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

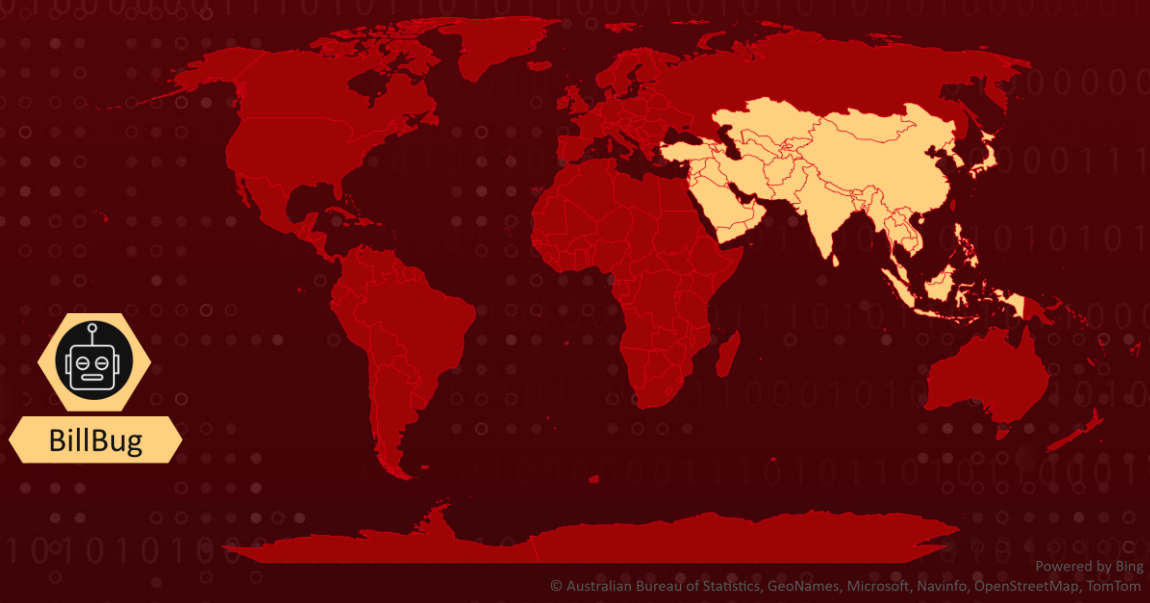
Billbug returns after two years to conduct an espionage campaign

Date of Publication	Admiralty code	TA Number
November 16, 2022	A1	TA2022258

Summary

First Appearance: 2009
Actor Name: Billbug
Target Region: Asia
Target Sectors: Government, Defense and Certificate Authority

Actor Map



Actor Details

#1 After being widely active in the year 2018-2019, Billbug, a Chinese state-sponsored group, is back after almost two years. They have been attacking multiple government agencies in an Asian country since March 2022 as part of a campaign targeting digital certificate authorities.

#2 In this recent attack chain, attackers exploit public-facing applications to gain access to victim networks. The attackers use multiple dual-use tools, such as AdFind, Winmail, WinRAR, Ping, Tracert, Route, NBTscan, Certutil, and Port Scanner, as well as custom malware, such as Hannotog backdoor, Stowaway Proxy Tool, and Sagerunex backdoor in this recent activity.

#3 Considering Billbug's ability to compromise multiple targets at once, this threat group is a high-skilled and well-resourced operator capable of conducting sustained and extensive campaigns.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Billbug (Lotus Blossom, Spring Dragon, Dragonfish, Thrip, Bronze Elgin, CTG-8171, ATK 1, ATK 78)	China	Asia	Government, Defense and Certificate Authority
	MOTIVE		
	Information theft and espionage		

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0040** Impact	**T1190** Exploit Public-Facing Application	**T1090** Proxy
T1134 Access Token Manipulation	**T1027** Obfuscated Files or Information	**T1046** Network Service Discovery	**T1560** Archive Collected Data
T1543 Create or Modify System Process	**T1489** Service Stop	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell
T1562 Impair Defenses	**T1562.004** Disable or Modify System Firewall	**T1587** Develop Capabilities	**T1587.001** Malware
T1018 Remote System Discovery	**T1016** System Network Configuration Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1553** Subvert Trust Controls
T1553.004 Install Root Certificate	**T1105** Ingress Tool Transfer		

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	d1b36aee7dc8cefe6101fe2fb7b9c544, cfa7954722d4277d26e96edc3289a4ce, 8334f346585aa27ac6ae86e5adcaefa2, 585fa6ba755facc1c3e2960f1c3f2c41, 550f2d43320bbc8cf6e2faf71ae37c2e, 415b5faf53231dee903f2b8c0a5b8e19, 23f361930d778a1f63c53dc36cd62d6c, 03fa6a2e8e779644dfd612d61e1e8769

TYPE	VALUE
SHA256	072022b54085690001ff9ec546051b2f60564ffbf5b917ac1f5a0e3abe7254a5, 0cc6285d4bfcb5de4ebe58a7eab9b8d25dfcfeb12676b0c084e8705e69f6f281, 148145b9a2e3f3abdc6c2d3de340eabc82457be67fb44cfa400a5e7bd2f88760, 2a4302e61015fdf5f65fbd456249bafe96455cd5cc8aefe075782365b9ae3076, 3585a5cbbf1b8b3206d7280355194d5442ed997f61e061fd6938a93163c79507, 37fe8efe828893042e4f1db7386d20fec55518a3587643f54d4c3ec82c35df6d, 3c35514b27c57a46a5593dbbbfceddbc49979b20fddc14b68bf4f0ee965a7c59, 3dd7b684024941d5ab26df6730d23087037535783e342ee98a3934cccddb8c3e, 64c546439b6b2d930f5aced409844535cf13f5c6d24e0870ba9bc0cf354d8c11, 79f9f25b15e88c47ce035f15dd88f18ecc11e1319ff6f88568fdd0d327ad7cc1, 7fe67567a5de33166168357d663b85bd452d64a4340bdad29fe71588ad95bf6f, 80a8a9a2e91ead0ae5884e823dca73ef9fce59ff96111c632902d6c04401a4fe, 861d1307913d1c2dbf9c6db246f896c0238837c47e1e1132a44ece5498206ec2, 8f7c74a9e1d04ff116e785f3234f80119d68ae0334fb6a5498f6d40eee189cf7, a462085549f9a1fdeff81ea8190a1f89351a83cf8f6d01ecb5f238541785d4b3, adb61560363fcda109ea077a6aaf66da530fcbbb5dbde9c5923a59385021a498, bcc99bc9c02e1e2068188e63bc1d7ebe308d0d12ce53632baa31ce992f06c34a, b631abbfbbc38dac7c59f2b0dd55623b5caa1eaead2fa62dc7e4f01b30184308, c4a7a9ff4380f6b4730e3126fdaf450c624c0b7f5e9158063a92529fa133eaf2, e4a460db653c8df4223ec466a0237943be5de0da92b04a3bf76053fa1401b19e, f7ea532becda13a1dcef37b4a7ca140c56796d1868867e82500e672a68d029e4, f969578a0e7fe90041d2275d59532f46dee63c6c193f723a13f4ded9d1525c6b, fea2f48f4471af9014f92026f3c1b203825bb95590e2a0985a3b57d6b598c3ff

TYPE	VALUE
SHA1	da3f6926c2c7ef05334f5da2769cffb4631bfde7, a3d91de52447cba8fafb57e0679566fc0665401b, 90b73ba3433b68f5038c5150723cde4083acfe71, 5ddce7c83d7ef1bee41cb66e147993ea08aea6f7, 2e1b8f65bf87430b736cf1e7fbc58b1a95be23d3, 26144e553b64ba64bfe8a3446de0f110f6b718db, 17502da3da751ee7e3f777d859c5d142ca113fcc, 0e26f2b3d70b5153ea10ef513a4211a6a8a8f6ba

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments-cert-authority

https://thehackernews.com/2022/11/researchers-say-china-state-backed.html

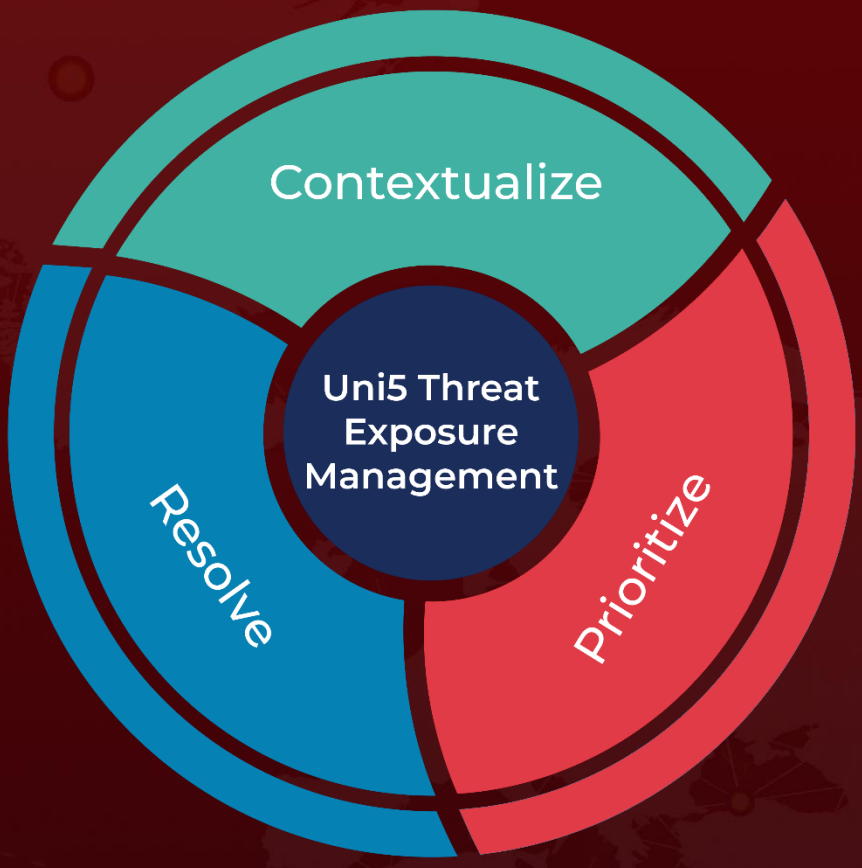
https://www.bleepingcomputer.com/news/security/chinese-hackers-target-government-agencies-and-defense-orgs/

https://otx.alienvault.com/pulse/6373c57769f0990a421696db

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 16, 2022 . 4:00 AM

More at www.hivepro.com