Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

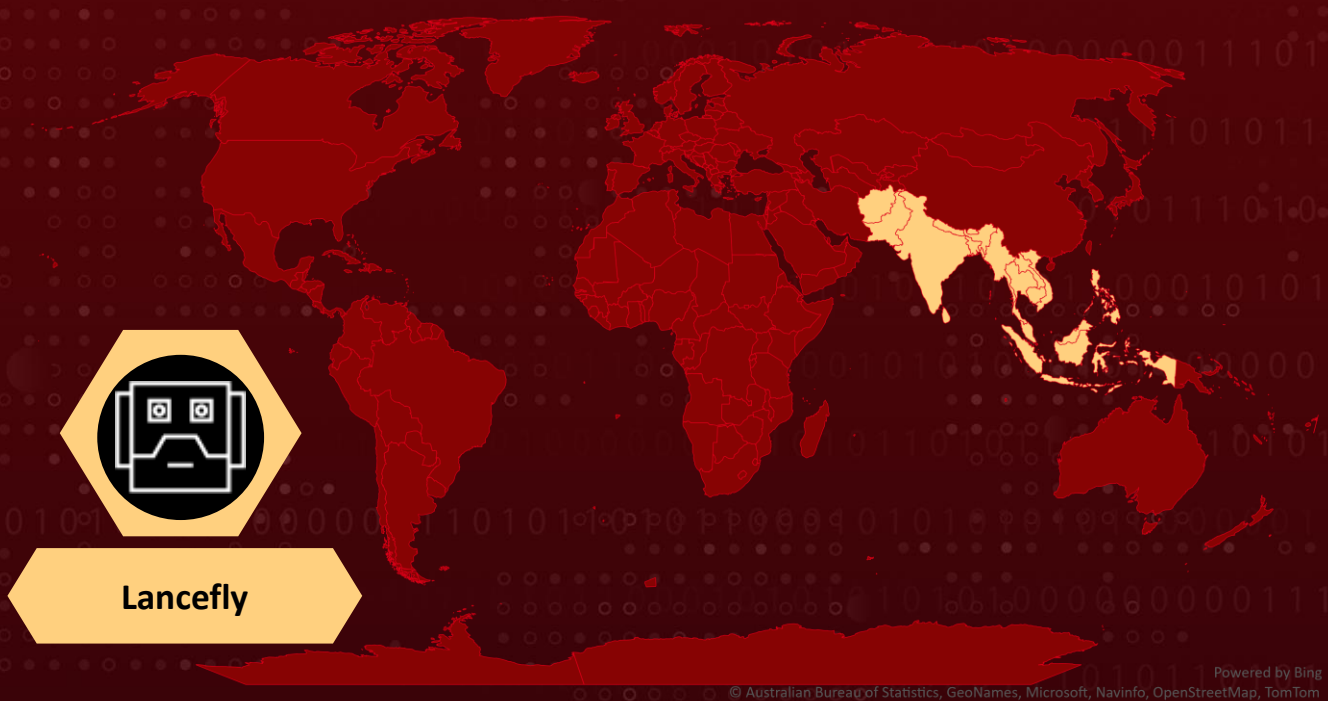
Lancefly APT Group Deploys Custom Backdoor 'Merdoor' in Targeted Attacks

Date of Publication	Admiralty code	TA Number
May 16, 2023	A1	TA2023229

Summary

First Appearance: 2018
Actor Name: Lancefly
Target Region: South and Southeast Asia
Target Sectors: Government, aviation, education, and telecoms
Malware: Merdoor backdoor, ZXShell rootkit

Actor Map



Actor Details

#1

The Lancefly advanced persistent threat (APT) group has been conducting targeted attacks in South and Southeast Asia for several years. They utilize a custom-written backdoor called Merdoor, which is a powerful and fully-featured malware that has been in existence since 2018. Merdoor is used selectively, appearing on only a few networks and machines, indicating highly targeted attacks for intelligence gathering purposes. The attackers also have access to an updated version of the ZXShell rootkit. The recent targets of Lancefly's activity include government, aviation, education, and telecom sectors.

#2

The attack chain involves various tools and techniques, including credential theft using non-malware techniques like PowerShell, Reg.exe, and Avast's legitimate tool. The attackers also utilize Impacket Atexec for lateral movement, suspicious SMB activity, WinRAR for staging and encrypting files, and the LSSAS Dumper for credential theft.

#3

The ZXShell rootkit used by Lancefly is an updated version of a previously known tool, and it is used to disable antivirus software and provide additional functions. The rootkit includes a loader that drops a malicious Windows Kernel driver and creates a service. Lancefly's attack chain often includes Merdoor being injected into legitimate processes like perfhost.exe or svchost.exe, followed by suspicious SMB activity and the connection to the command-and-control server. A masqueraded WinRAR file is used to stage and encrypt files before possible exfiltration.

#4

The installation and update utility associated with Lancefly's activity shares code fragments with the Merdoor loader. It attempts to read and delete a configuration file, performs antivirus tampering, decompresses a file, and appends content from a configuration file to the decompressed file. The utility also handles installation and update functionality by decompressing a file, replacing certain system files, modifying registry values, and restarting services.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Lancefly APT	China **MOTIVE** Information theft and espionage	South and Southeast Asia	Government, aviation, education, and telecoms

Recommendations

Regularly back it up offline to protect critical data and install reliable anti-virus and internet security software on all connected devices. Enable automatic software updates whenever possible and practical. Additionally, consider implementing proactive security measures, such as blocking indicators of compromise (IoCs), to stay ahead of potential threats.

Deploy robust endpoint protection solutions, including next-generation antivirus (NGAV) and behavioral analysis tools.Implement network segmentation to limit lateral movement within the infrastructure and restrict access to critical systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0005 Defense Evasion	TA0011 Command and Control	TA0007 Discovery
TA0009 Collection	TA0001 Initial Access	TA0002 Execution	T1057 Process Discovery
T1014 Rootkit	T1219 Remote Access Software	T1059 Command and Scripting Interpreter	T1112 Modify Registry
T1021 Remote Services	T1003 OS Credential Dumping	T1056 Input Capture	T1574 Hijack Execution Flow
T1055 Process Injection	T1090 Proxy	T1056.001 Keylogging	T1574.001 DLL Search Order Hijacking
T1218 System Binary Proxy Execution	T1027 Obfuscated Files or Information	T1566 Phishing	T1110 Brute Force
T1059.001 PowerShell	T1218.011 Rundll32	T1003.001 LSASS Memory	T1036 Masquerading
T1560.001 Archive via Utility	T1021.002 SMB/Windows Admin Shares		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA 256	13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead 8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38 89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744 5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075 ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740 14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3 db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03 e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2 dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6 fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949 fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104 341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200 f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4 750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3 9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774 a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0 d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7 f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57 139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4

TYPE	VALUE
SHA 256	11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5 0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75 eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b 1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fc1a109b9ae092a5d7492b7dd fae713e25b667f1c42ebbea239f7b1e13ba5dc99b225251a82e65608b3710be7 1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221 592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae 929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798 009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4 ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8 ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28 32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849 a1f9b76ddfdafc47d4a63a04313c577c0c2ffc6202083422b52a00803fd8193d 3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e 210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92 530c7d705d426ed61c6be85a3b2b49fd7b839e27f3af60eb16c5616827a2a436 5018fe25b7eac7dd7bc30c7747820e3c1649b537f11dbaa9ce6b788b361133bf efa9e9e5da6fba14cb60cba5dbd3f180cb8f2bd153ca78bbacd03c270aefd894 a5a4dacddfc07ec9051fb7914a19f65c58aad44bbd3740d7b2b995262bd0c09e

TYPE	VALUE
SHA 256	10b96290a17511ee7a772fcc254077f62a8045753129d73f0804f3da577d2793 0dcfcdf92e85191de192b4478aba039cb1e1041b1ae7764555307e257aa566a7 415f9dc11fe242b7a548be09a51a42a4b5c0f9bc5c32aeffe7a98940b9c7fc04 947f7355aa6068ae38df876b2847d99a6ca458d67652e3f1486b6233db336088 8d77fe4370c864167c1a712d0cc8fe124b10bd9d157ea59db58b42dea5007b63 d8cc2dc0a96126d71ed1fce73017d5b7c91465ccd4cdcff71712381af788c16d e94a5bd23da1c6b4b8aec43314d4e5346178abe0584a43fa4a204f4a3f7464b9 5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e 19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169 41d174514ed71267aaff578340ff83ef00dbb07cb644d2b1302a18aa1ca5d2d0 67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675 f92cac1121271c2e55b34d4e493cb64cdb0d4626ee30dc77016eb7021bf63414 859e76b6cda203e84a7b234c5cba169a7a02bf028a5b75e2ca8f1a35c4884065 fcdec9d9b195b8ed827fb46f1530502816fe6a04b1f5e740fda2b126df2d9fd5 9584df964369c1141f9fc234c64253d8baeb9d7e3739b157db5f3607292787f2 711a347708e6d94da01e4ee3b6cdb9bcc96ebd8d95f35a14e1b67def2271b2e9 f040a173b954cdeadede3203a2021093b0458ed23727f849fc4c2676c67e25db 90edb2c7c3ba86fecc90e80ac339a42bd89fbaa3f07d96d68835725b2e9de3ba b0d25b06e59b4cca93e40992fa0c0f36576364fcf1aca99160fd2a1faa5677a2 4c55f48b37f3e4b83b6757109b6ee0a661876b41428345239007882993127397 3e1c8d982b1257471ab1660b40112adf54f762c570091496b8623b0082840e9f 9830f6abec64b276c9f327cf7c6817ad474b66ea61e4adcb8f914b324da46627 79ae300ac4f1bc7636fe44ce2faa7e5556493f7013fc5c0a3863f28df86a2060

References

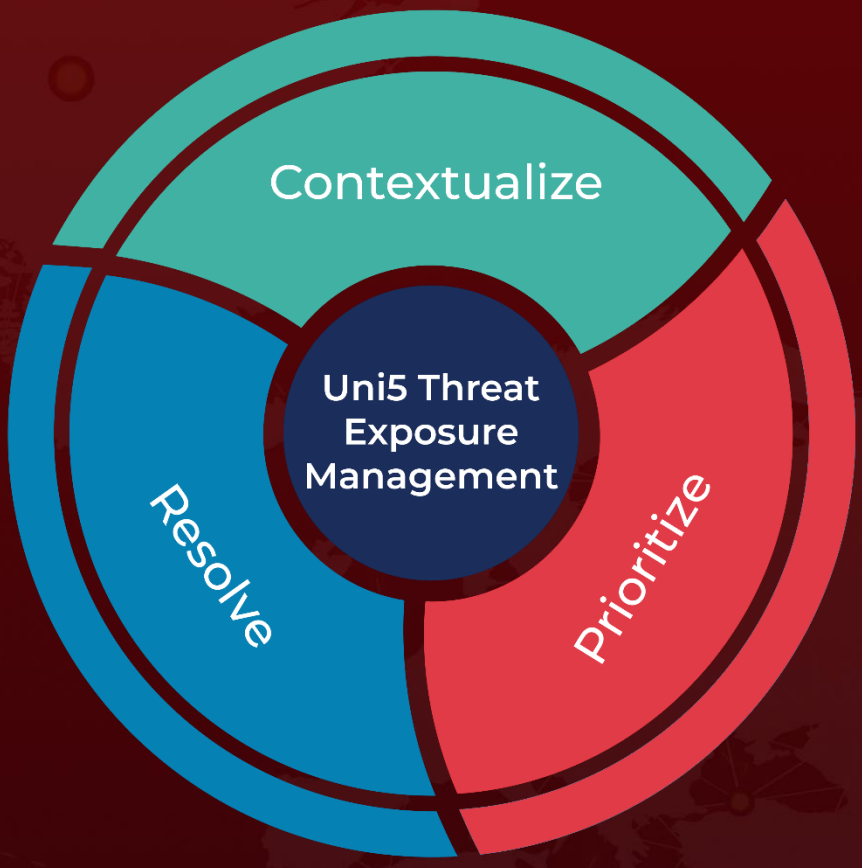
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

https://www.bleepingcomputer.com/news/security/stealthy-merdoor-malware-uncovered-after-five-years-of-attacks/

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

May 16, 2023. 4:00 AM

More at www.hivepro.com