IMPORTANT CYBERSECURITY NEWS: LOTUS BLOSSOM HACKERS TARGET SOUTHEAST ASIA WITH SAGERUNEX BACKDOOR

Vairav Cyber Security News Report

Date: 2025-03-03

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident involving the Lotus Blossom espionage group has led to sophisticated cyber-espionage campaigns targeting multiple industries in Southeast Asia. Attackers employed the Sagerunex backdoor, exploiting legitimate cloud services for command-and-control (C2) communications, resulting in potential data exfiltration and prolonged unauthorized access. Security experts advise organizations to implement robust monitoring and enhance security measures to mitigate such threats.

DETAILS OF THE INCIDENT

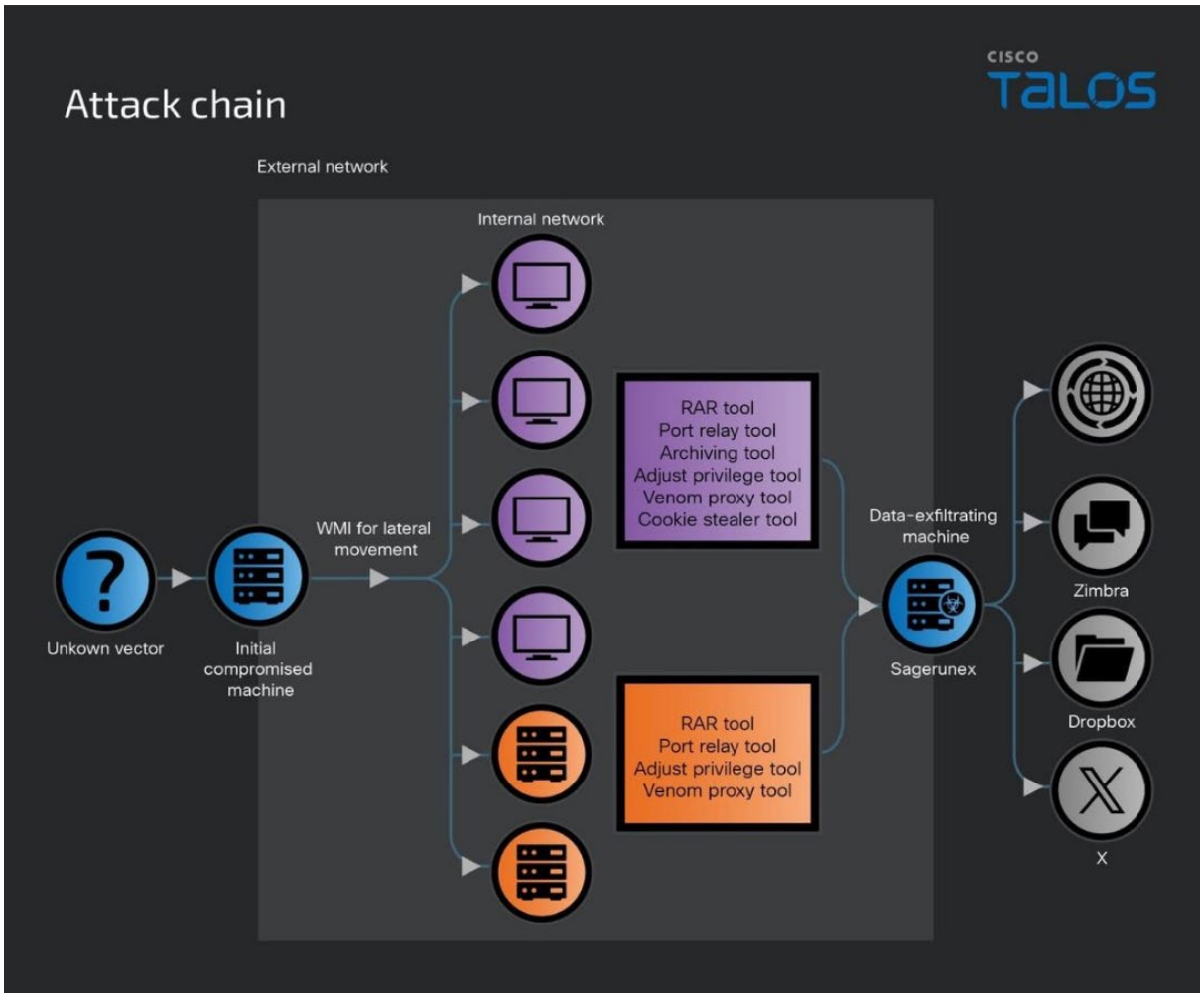

Figure 1: Attack Chain of Sagerunex backdoor

Description of the Cyber Threat: The Lotus Blossom group conducted cyber-espionage operations using the Sagerunex backdoor, a sophisticated Remote Access Trojan (RAT). Recent variants of Sagerunex leverage legitimate cloud services such as Dropbox, Twitter,

and Zimbra for C2 communications, enabling the attackers to blend malicious traffic with legitimate service usage, thereby evading detection. Active since at least 2012, Lotus Blossom (also known as Spring Dragon, Billbug, or Thrip) is a state-backed espionage group. They have developed multiple variants of the Sagerunex backdoor, employing advanced techniques like memory-only execution and the use of legitimate cloud services for C2 channels.

Identification: The campaigns were identified through Talos Intelligence's cybersecurity investigations that uncovered the use of new Sagerunex variants during attacks on telecommunications and media companies. The shift to using third-party cloud services for C2 communications was a notable finding.

Threat Actor: The attacks are attributed to the Lotus Blossom group, a state-backed Advanced Persistent Threat (APT) group known for cyber-espionage activities targeting Southeast Asia.

Affected Entities/Industries: The targeted sectors include government, manufacturing, telecommunications, and media industries across regions.

Potential Impact: Risks posed by the attack encompass data exfiltration, prolonged unauthorized access, operational disruptions, and significant reputational damage to the affected organizations

Exploitation Methods: The attackers utilized the Sagerunex backdoor to establish persistent access, executed remote commands, and exfiltrated data. They exploited legitimate cloud services (Dropbox, Twitter, Zimbra) for C2 communications, making detection challenging. Additional tools included credential stealers and proxy tools to facilitate deeper network infiltration.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 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

Suspicious 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

Malware Hashes (SHA256/MD5)

- 3fb81913c2daf36530c9ae011feebeb5bc61432969598e2dfaa52fc2ce839f20
- 788945d484b4e7da7adb438db52c35dd033869c5f43f027a5b6903b7b1dbbd7b
- bf50ed2dd7a721e7c1b13b1eed0f21c3274808d5016310c52b1473530d78f34a
- 47013e731b37a80e96a3523e042c23e67bfa721d3651e735307f4a1545898b11
- 3d262950bf89995dce56f2c8db16938d37be5564d5e2b011ea49fe2f523f980a
- 79cd6380b2cf7ca1b3e3ba386ebbd7df0104e33ac74cdb5e886fd8be207bd961
- f4dd0a6594d50012b6b2e3fd578e40a2aa91dae2c2454d04df5c8c9898774da6
- 8f309ffbaa532294da8d7896cdac3311e6a1ff82e86551453787ee78a94a679e
- 565fbe3f1f444f79aef375678ebbe2cd08ba55bdbee737b4ed2e6d2f7bcfcc16
- f88cea311efbd3aaf896dd9527b137ad2bbd29332917b5aadd4c2693b45f893f
- 42b8b464147160c2f4c2722dfc222749e67384824bbbb140385271895b138c7b
- ccd1f9844b00059f6e35fdff577ac93048f4d99b18162d3c56cfeb2d72b93ae4
- 2b59b03e9232b83b8914ed07c6426dd53d17cfb2eba01ab13d4c6cb00466a42e
- 240d3040559e6215a8931d9d8670c6eae2c1c42a9a74d260261fda22bcf0817d
- e8f482dc47250eaedf8b839cdb4fd9ebffe59d47c7b48d61ad51d942fd35fa18
- 0f383b8f68f3b3c3a18ec778a1150563801b8716c7114432ff51a28fff2963b4
- b1c782b4a327dadf0d8db016d7556a92bae4b697b10c9282b293e24564bbef32

- 5544a68a2b391c88a02f1f581ea1dde9c5cf8aeb41bb55269989528303580846
- dfdd6847579ec6d9630feeda1f5bcbf009d270cd461d30781719a9c218f33d9e
- fe2046e479289b1013eb394f5b3d7a49a419cb98015add3ead0fa87614fe6e38
- d67774dde98db6aca8271566fac6f3d0e8e474c40604efeedd5b1276abcc8af5
- e0d969b95bd91f58b775d2c9b9190a4f7c5ee8a76d63286227885e071883fdef
- fa764df857ed8f0fbf606dcbb92d64f5a72b5c1dd94b3dcb9ea02ff8a02b986b
- 9e38f67fad7dfd806955c61e8b2d68084c4506227bc8c880cffb28d77612759c
- 23012d0e71e40913967a511475b55690e34afcad72ca819b82c885a0df8aea79
- 0fd82ff1a4b4f3c55b7faa73621ecb7d11c3cde95631de841cb304a7968804df
- b830fe3d5d5462bef92991dd78869a173cb56d823e7776bfa56e09642dd880ed
- 776b4a7ce11d2cc9a94268c7280b652ad0d0fb33d3188cf58987e6c5c4fbb5fb
- 001380aa1c1850dd603f9e1315f3b9c450e6da13686a0b6ec5c05991df46ff1a
- 25df8f277074560cb899314cd649c6d937727c5cce5390a7187a6572dd2e4be1
- 1cb12045c55bf2669c3573fc79f1335355defe09af64ac2f9ca495eb5f7af528
- ff5a789d0df1b28a183d7f256d3d4f649a16ae4679ef803d28cd9f7443416310
- 1ce0367f66a3ee2e461ccb42ae7794622aa9fb3bf9bd8926e85260ed768fb17b
- 54a41f888a10e454705c5b4328c13415b0ffea3708e3e101d965883761945c67
- e3292e944f3deb871d9d3c2fc28a0255ad900f067f074039dde86a55dcc7b67c
- 176a34345bbd4eaf96e47bb60c866847de7cdaf315fe376427f4651c09f98e88
- 710c73d806457e576a9987be60ed8676af610b7910928f9fa57fbc58f5f45d52

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Monitor network traffic for unusual patterns, especially involving cloud services like Dropbox, Twitter, and Zimbra.
- Update and patch systems to address known vulnerabilities exploited by the Sagerunex backdoor.
- Isolate affected systems to prevent further spread and conduct thorough forensic analysis.

Security Best Practices

- Implement multi-factor authentication (MFA) to enhance access security.
- Conduct regular security awareness training to educate staff on recognizing phishing attempts and other attack vectors.
- Maintain up-to-date antivirus and endpoint detection and response (EDR) solutions.

For Advanced Security Teams

- Deploy advanced threat detection systems capable of identifying memory-only malware execution.
- Utilize threat intelligence feeds to stay informed about emerging threats and Indicators of Compromise (IOCs).
- Perform regular threat hunting exercises focusing on detecting lateral movement and unauthorized persistence mechanisms.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://securityonline.info/lotus-blossom-hackers-target-southeast-asia-with-sagerunex-backdoor/
- https://blog.talosintelligence.com/lotus-blossom-espionage-group/
- https://github.com/Cisco-Talos/IOCs/blob/main/2025/02/lotus-blossom-espionage-group.txt

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com