Multistage Attack Hijacking Systems with SSLoad, Cobalt Strike

Date: 29th April 2024 | Severity: High

Summary

Cybersecurity researchers have discovered an ongoing attack campaign that's leveraging phishing emails to deliver a malware called SSLoad. The campaign, codenamed FROZEN#SHADOW, also involves the deployment of Cobalt Strike and the ConnectWise Screen Connect remote desktop software.

Attack Vectors

- The attack starts with phishing emails targeting organizations, these emails contain links leading to the retrieval of a JavaScript file, initiating the infection process. Palo Alto Networks discovered two different distribution methods for SSLoad: one using website contact forms with booby-trapped URLs and the other employing macro-enabled Microsoft Word documents. These methods have been observed delivering another malware called Latrodectus, possibly a successor to IcedID.
- The obfuscated JavaScript file, when executed, retrieves an MSI installer file, "slack.msi," from a network share and runs it to download and execute the SSLoad malware payload. SSLoad then beacons to a command-and-control (C2) server, providing information about the compromised system. Subsequently, Cobalt Strike is deployed to download and install ConnectWise Screen Connect, enabling remote access to the compromised host. The attackers then proceed to acquire credentials and gather critical system details, scanning for stored credentials and sensitive documents.
- The attackers pivot to other systems in the network, including the domain controller, creating their domain administrator account to infiltrate the victim's Windows domain fully. This level of access allows them to access any connected machine within the domain, posing a significant challenge for organizations to remediate. Meanwhile, AhnLab Security Intelligence Center (ASEC) reported infections of Linux systems with the Pupy RAT open-source remote access trojan.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• bjSdg0[.]pintaexoticfashion[.]co[.]in • l1-03[.]winupdate[.]us[.]to • 23-95-209-148-host[.]colocrossing[.]com • mmtixmm[.]org

	• wireoneinternet[.]info • skinnyjeanso[.]com • titnovacrion[.]top • simplyfitphilly[.]com • kasnackamarch[.]info • sokingscrosshotel[.]com • danteshpk[.]com • stratimasesstr[.]com • winarkamaps[.]com • globalsolutionunlimitedltd[.]com • maramaravilha[.]com • krd6[.]com
Hashes	• F8FC9B40B946B742D6044F291914439727E1A7F53EA87562446F682B26CCE65A • E8979741F0355A47DAE575EAD8C829DF47F282B4533EC1BE4D63086515F9C449 • 08E82F1C0A033AB295B4D342C53970E4528E20933C614BDA3BBC5D57BAB20651 • 4F52B4A2A781F366ED534D8C4B2FAFEF48A7848C4C20B4229B98747CA8AB06D3 • 68E1CAF530366B1890993185157C01161B3D625063D75A41C88D2D1BB8EDFE02 • 6D7A94B7551F15732E193A07357375B98B463F0DCE6B1FED871A42FCBDDE9F48 • 2B026343214C3D2C10FDFA9B04B7694E57EE8D3605FBF9A2E127FE6FA9A58309 • 96212917B7B0DC881332DB7ECE0BACFE21D9AC713AF1ABE078F6D3E74BAACD01 • 9785231ebf3d00216aa979f8c705e2513568802e • 93cb0fa81ed42d4c44fac49dd0354d0b • 4a2ee1666e2e9c40d372853e2203a7f2336b6e03 • BA3FA920708DB856737A66F70E2C7E86BBA73C73836F7F30C2CE42CD70D0C5BD • 7DBEBB7C76511FC063B5ACE0A9359B655F66A55A494200B8FD11905C78B5FB90 • 6E892AA13CBD4B71A1C476207ABDDB1EF830BE04999809B4EF569488A37E47E0 • 7DFF08656413A737483ECEE2A50E412338EBFEE3D36A1A5C04E74B25949B2306 • 75DB4709428310C76656BF76F5DE267AB490E43284312B374BAF7582108300A9 • C172ABD808CC6216B309BC307FE69B821C7EAED35F874FD4684AB33B4291F95A • 5FB093A9348FCF4A81BEFDA978C948796A8319FCABE7899C2CF5BA1419EC9D35 • 9FC48724CB9F70F774F7ED9E809E49979BD089DFD641896D8D5E3026F049B0AF • C122596E25A4DAD1D46D4AB983F4EF15BFA7B65582B7C311F404036766498105 • E8E76B851FC78D87FE58AD7D29BC6356A8965236D1B96C5F572334DD695D5DE9 • 791C28D4201E8B9EA5162FBEE3908FEB34793B1C51F5AAEDC43916E86068248D • CAF8295570E8A8244C7099A8EABFD1BD55EA50F026B4461E9F0F5425D54703E8 • 092962BC268390DEBF17CD148D03147CDF919E442E61C92DE01EAC3BDB34B1C1 • 24CB279EEBCD49E1327905AB2BD19B9B2E09EFA3E0A5E1875F3989C398A5DA81 • 8F7A90B540F38712C9C1A5359C6333BBE1091102D6F621B22321E08352C84CFC • 7DFF08656413A737483ECEE2A50E412338EBFEE3D36A1A5C04E74B25949B2306 • 0737FA0B403FAB17331C9835497A4F3B2955543E2FAC85009DCC66DF41A015F8 • 2118C5B95D5D57492B2E8B8C0403E23B21ACC4FF50282F8B6007BA89ADFAA992 • A557F891F4D50E458D745C7EAF7D0BE3ECEEA36F0398097E977CD3F6EC463875 • 4D9274CFE7A2BD9A125352271D1634708E1F9B1D70B056D1C1950CB98B8F91FF • 3584CA9C1E7E0A38E47F59BB16C21203A60833D0F826294D535A98E7CA76D9C1 • 63283E012F067A3FFB27ED4FE6803F740C80F6F65213FE5507F0CD1EE0019B96 • 828EF3E4CA064891836913015C48AC9807ECD43B32F6E7E4BFF29B9FD2E218C9 • 780B970DAD15835D138546BE9B615FC1B4124C1060A8EFD91B9C52F9C3160D5B
IPs	• 85[.]239.54[.]190 • 23[.]159[.]160[.]88 • 23[.]95[.]209[.]148 • 45[.]95[.]11[.]134

Recommendation

- Security administrators should block the IOCs on all applicable security solutions post-validation.
- Organizations should conduct a periodic security assessment, hardening, and architecture review of critical assets exposed over the Internet.
- Users should not download suspicious applications and attachments received over the internet and are alert to social engineering attacks.
- Users should not download, accept, or execute files and do not visit websites or follow links provided by unknown or untrusted sources.
- Security administrators should apply the Principle of Least Privilege to all systems and services.
- Keep AV signatures, operating systems, and third-party applications up to date on all systems, mobile devices, and servers.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/researchers-detail-multistage-attack.html
- https://varutra.com/ctp/threatpost/postDetails/Multistage-Attack-Leveraging-SSLoad-and-Cobalt-Strike-Detailed-by-Researchers/SGY4c0YveTFLTm1FSWxRMEFRS0c3dz09
- https://blog.bughunters.am/en/researchers-detail-multistage-attack-hijacking-systems-with-ssload/
- https://www.cistck.com/uncategorized/researchers-detail-multistage-attack-hijacking-systems-with-ssload-cobalt-strike/