Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 22-06-2024, 12:30 IST

Title	**Void Arachne Targets Chinese-Speaking Users with the Winos 4.0 C&C Framework**
Summary	• Chinese-speaking users are the target of a never-before-seen threat activity cluster codenamed Void Arachne that employs malicious Windows Installer (MSI) files for virtual private networks (VPNs) to deliver a command-and-control (C&C) framework called Winos 4.0.
Severity	Medium
Attack Vectors	• A new threat actor group that we dubbed Void Arachne. This group targets Chinese-speaking users with malicious Windows Installer (MSI) files in a recent campaign. These MSI files contain legitimate software installer files for AI software and other popular software but are bundled with malicious Winos payloads. • The campaign also promotes compromised MSI files embedded with nudifiers and deepfake pornography-generating software, as well as AI voice and facial technologies. • The campaign uses SEO poisoning tactics and social media and messaging platforms to distribute malware. • The malware installs a Winos backdoor during the installation process, which could lead to a full system compromise. • Due to strict government control in China, VPN services and public interest in this technology have notably increased. And in this Void Arachne campaign, we've observed how threat actors are exploiting the heightened public interest in software that can evade the Great Firewall and online censorship.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	cdceea00a5f53e49063c455eea3f6a62c0713d01813a55a2427ad758d11a15bf b330ccb0877b27bd67966bb9ad86d3f2ce3d59c67493f9ce152f13d92f4b3de6 cdf8a481d305d87661b440c717c6095154cd519b3ec302eea32279de28162044 f18896c3016ea675f092502604dd85a61b990c5d6c1eba40f34ef57e4315cdab ffafc11d8569f1df18da1bf41571870ca84e8f59b193d85631bbad8dfbf7334b 9ca14ae3d4324847a0903f11dcee74164f823bc635f80861e1033af27cb4a1c4 611341e64eb6864e3b3b9cd0cb433bb5ff185a8158174ee02aea9307216ee96d 342dbf7c84e35622f680d65e15a82ccd0f0938fa38ef29292db81d71f9f4de45 6776a4680f26756100f4b65e326e726bbdb4f35a8b906069b0489ebae7955160 eecc00360b0a0649d954da34ef1b8212dc6a9bf74b8624882aaa97209b97b582 5bf7821b32bf188e0890f56dc5c832651c7cb35328029f6b87d47328376d4d13 8fc1931fd9206ba78f348a14317cd8be8f135810787b6555a8439fdd65da81a0 e5ae87f46ff88c819ff236f0f290c7c6bda3e80019db093d35cae6b087d528ae a12cb2d529a95798160114bdb6fb389553d3cc1d8bd10a5c8295d5a0c74e257c bd462515ea9ffe66fc27d9baa0fcc4bf733385829c2fc5676129aaeeb2e0af88 44abf0cadee82f049bbc3dfeb8277529d3650f6f76fb76e00ec65228b8ec21e6 d555bc8a99c7ae22302201f1bae997aa9539502728a419e63c03f329c364a32c 29097fab695ba54082d64fd31a511d93ee16ee94039282afd7e63dd661f5654b 437d6223c13675c1824bc4b17cd0986cbffb1f87cd1cf6a72560bef1e51eb62b fae4f96beda54a1ed4914537b0542182d3a020dd9db9d9995df37d303b88e6df 4e54ddbfcbbf78d031d9743be4229171554fbca5aafb5f2a924e59435b79e858 aa7cc08e0b29cd9022cde6b0c9307cb2f93365d098f71fb37478339daff80714 8444b6066e4171f49ea18a2cf8992226f1ad683eb2a1828c9f63557156a22d99 84d888ff8691635682c7f612189ac0fd77d13810301fca31c4a1336c1ed8876a acd98cfbe4cc1c19441eac76e7bba60a57eb1d68634b1f912fdc519fb1e0fdf1 5a98acbd41f0dd445fc60246be9738f73a090379e5d320b06801bb3cb5b75a7f 1e8e2dbac76dd41afd990949059832467b425521147ca4281e8958076daf2c83
	Domains	hm[.]webcamcn[.]xyz 103[.]214[.]147[.]14[.]webcamcn[.]xyz hm2[.]webcamcn[.]xyz 98[.]159[.]98[.]114[.]webcamcn[.]xyz 103[.]214[.]147[.]101[.]webcamcn[.]xyz 156[.]248[.]54[.]11[.]webcamcn[.]xyz

Recommendations	• Block all threat indicators at your respective controls. • Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls. • Be cautious when downloading and installing software, especially from untrusted sources. • Regularly update your security software and keep your operating system patched. • Educate users about the risks associated with downloading and running MSI files from unknown origins. **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.**
References	• https://thehackernews.com/2024/06/void-arachne-uses-deepfakes-and-ai-to.html • https://www.trendmicro.com/en_sg/research/24/f/behind-the-great-wall-void-arachne-targets-chinese-speaking-user.html • https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/6673ea92cd693f17848763c7