


Mphasis SOC – Information Security News

Date & Time Issued: 02-JULY-2024, 3:00 IST

Title	New Unfurling Hemlock threat actor floods systems with malware	
Summary	<ul style="list-style-type: none"> A threat actor tracked as Unfurling Hemlock has been infecting target systems with up to ten pieces of malware at the same time in campaigns that distribute hundreds of thousands of malicious files. Security researchers describe the infection method as a "malware cluster bomb" that allows the threat actor to use one malware sample that spreads additional ones on the compromised machine. 	
Severity	Medium 	
Attack Vectors	<ul style="list-style-type: none"> The attacks begin with the execution of a file named 'WEXTRACT.EXE' that arrives on target devices either via malicious emails or malware loaders that Unfurling Hemlock has access to by contracting their operators. The malicious executable contains nested compressed cabinet files, with each level containing a malware sample and yet another compressed file. Each unpacking step drops a malware variant on the victim's machine. When the final stage is reached, the extracted files are executed in reverse order, meaning the most recently extracted malware is executed first. The distributed malware mainly consisted of stealers, such as Redline, RisePro and Mystic Stealer, and loaders such as Amadey and Smoke Loader While samples appeared to be distributed from various sources, a lot of them were connected to hosts within the Autonomous System 203727, an AS related to hosting services that have been widely used by Eastern European cybercriminals in the past. 	
Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	<ul style="list-style-type: none"> 229e859dda6cc0bc99a395824f4524693bdd0292b4b9c55d06b4fa38279b3ea2 8fe4d34a6a245c5acd3d1741213c1dd195468089b1a3fe80adfa6d8d8c94f2d8 fd7a9b8e52e2fbc090d5f5046a73d6e42b421abf063083210889f3fcb47dee0 35c55b402e770e25adf57ffbd408a428af9ce21a735474b5d94ccdd4123e68f8 5697652d0fd5b4a05ac00f6ec028fd3dc3e34ed7b112c4b8c6048eae72a8d326 edfb4374d5c586f0690c95ff8cacb36bda6fb4743f20dda5e6f17e7e241edd47 da4f614c983fa226d813de390937389ae4d1e043dd86524aa7a5246fd587826b 7d18c67c13ec919f3950092319d11eda129c8498e171612e681eebf1c977493d 0c48529d2979698341e89d6ea5f7e9211fa277e40d3f6a55a8996135944ebdad 80df101f1f93fa53b3dcbc315d3ec5d8c8330c08b5622ac3207f746d016b66dc 7f101603fbb2821504cf2c71fca0450689dfcd6d1f36e57e27f0392be0f2d1dd 1f224093b9557dd73caaf1c6a823028c286ddd3414bce0860e0fe084fb8c2ab 301a1c9f4e82fc8f57577ea399a2591557ff57d337472c3f8482a89c5b4105d5

Recommendations	<ul style="list-style-type: none">• Security administrators should block IOCs on all applicable security solutions post-validation.• Users should not download suspicious applications and attachments received over the internet and be alert to social engineering and phishing attacks.• Organizations are recommended to have a behavioral detection solution in place to successfully detect the presence of malware payloads.• Users are recommended to use a unique and strong password at every site with the help of a password manager and use multi factor authentication whenever possible.• Organizations are recommended to servers have a behavioral detection solution in place to successful detect the presence of malware payloads.• 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. <p>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.</p>
References	<ul style="list-style-type: none">• https://www.varutra.com/ctp/threatpost/postDetails/Unfurling-Hemlock-Threat-Actor-Floods-Systems-with-Malware/YjFTVUtVajhiSU1vRIBUSW92K2UzUT09/• https://www.bleepingcomputer.com/news/security/new-unfurling-hemlock-threat-actor-floods-systems-with-malware/• https://outpost24.com/blog/unfurling-hemlock-cluster-bomb-campaign/
<p>The information contained in this message is proprietary. It is for Mphasis and its customers only. Copyright © 2024. All rights reserved by Mphasis.</p>	