Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 01-JULY-2024, 4:30: IST

Title	**Russian Power Companies, IT Firms, and Govt Agencies Hit by Decoy Dog Trojan**
Summary	• HellHounds was first documented by the firm in late November 2023 following the compromise of an unnamed power company with the Decoy Dog trojan. It's confirmed to have infiltrated 48 victims in Russia to date, including IT companies, governments, space industry firms, and telecom providers.
Severity	Medium
Attack Vectors	• The Hellhounds group compromises organizations they select and gain a foothold on their networks, remaining undetected for years," security researchers Aleksandr Grigorian and Stanislav Pyzhov said. "In doing so, the group leverages primary compromise vectors, from vulnerable web services to trusted relationships." • In May 2024, cybersecurity researchers reported that a Windows version of Decoy Dog had been distributed by the HellHounds threat group in a campaign that targeted Russian organizations. During this campaign, Operation Lahat, the threat actors gained initial system access using compromised SSH login credentials and installed Decoy Dog while disguising it as ISO images. The attackers-maintained access for a long time, stealing credentials on Linux-based hosts using a modified version of the 3snake utility. • Details about Decoy Dog, a custom variant of the open-source Pupy RAT, emerged in April 2023, when Infoblox uncovered the malware's use of DNS tunneling for communications with its command-and-control (C2) server to remotely control infected hosts. A notable feature of the malware is its ability to move victims from one controller to another, allowing the threat actors to maintain communication with compromised machines and remain hidden for extended periods of time. • The latest findings from Positive Technologies all but confirm the presence of an identical version of Decoy Dog for Windows, which is delivered to mission-critical hosts by means of a loader that employs dedicated infrastructure to get the key for decrypting the payload. Further analysis has uncovered Hellhounds' use of a modified version of another open-source program known as 3snake to obtain credentials on hosts running Linux. • Positive Technologies said that in at least two incidents, the adversary managed to gain initial access to victims' infrastructure via a contractor using compromised Secure Shell (SSH) login credentials. "The attackers have long been able to maintain their presence inside critical organizations located in Russia," the researchers said." Although virtually all the Hellhound's toolkit is based on open-source projects, the attackers have done a fairly good job modifying it to bypass malware defenses and ensure prolonged covert presence inside compromised organizations."

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	Domain	• beacon[.]net[.]eu[.]org • c[.]glb-ru[.]info • claudfront[.]net • maxpatrol[.]net • nsdps[.]cc • rcsmf100[.]net • wmssh[.]com • dw-filter[.]com • net-sensors[.]net • mvs05[.]zyns[.]com
	IP address	• 31[.]184[.]204[.]42
	File Hash	• 9a977571296ae1548c32df94be75eec2a414798bee7064b0bf44859e886a0cfa • 4d30fd05c3bdac792e0a011892e2cad02818436484e81b6de6a02928149bc92d • e27d1bab901c1bb414d0849c5c132faa8c7c6a61357d9627a7d2785270034793 • 31b21de71f2162e8da1be8483f3a5d019b0c817832bc11a9f307b6b36821ca54 • 18d4a3a92b24b2ad75115a44fe2727081316eca346499a4aa00aa13713cf00cb • 9a96c7b0595f628027c4f4caeece475ef742c420adf2fde8df934c6ce6481fb5 • d9a8151aff9d1c061826a9812ed9a6600805c74a519df333513fd4a79d2d4e61 • 07fe71b256c1c913b0f3e3fa67e53d21a3d1f499beb4e550597f5743797a77c4

Recommendations	• 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.**
References	• https://thehackernews.com/2024/06/russian-power-companies-it-firms-and.html • https://varutra.com/ctp/threatpost/postDetails/Decoy-Dog-Trojan-Targets-Russian-Power-Companies,-IT-Firms,-and-Government-Agencies/TDdFMDBGd1lUR1hnazl0QWZUM3pGQT09