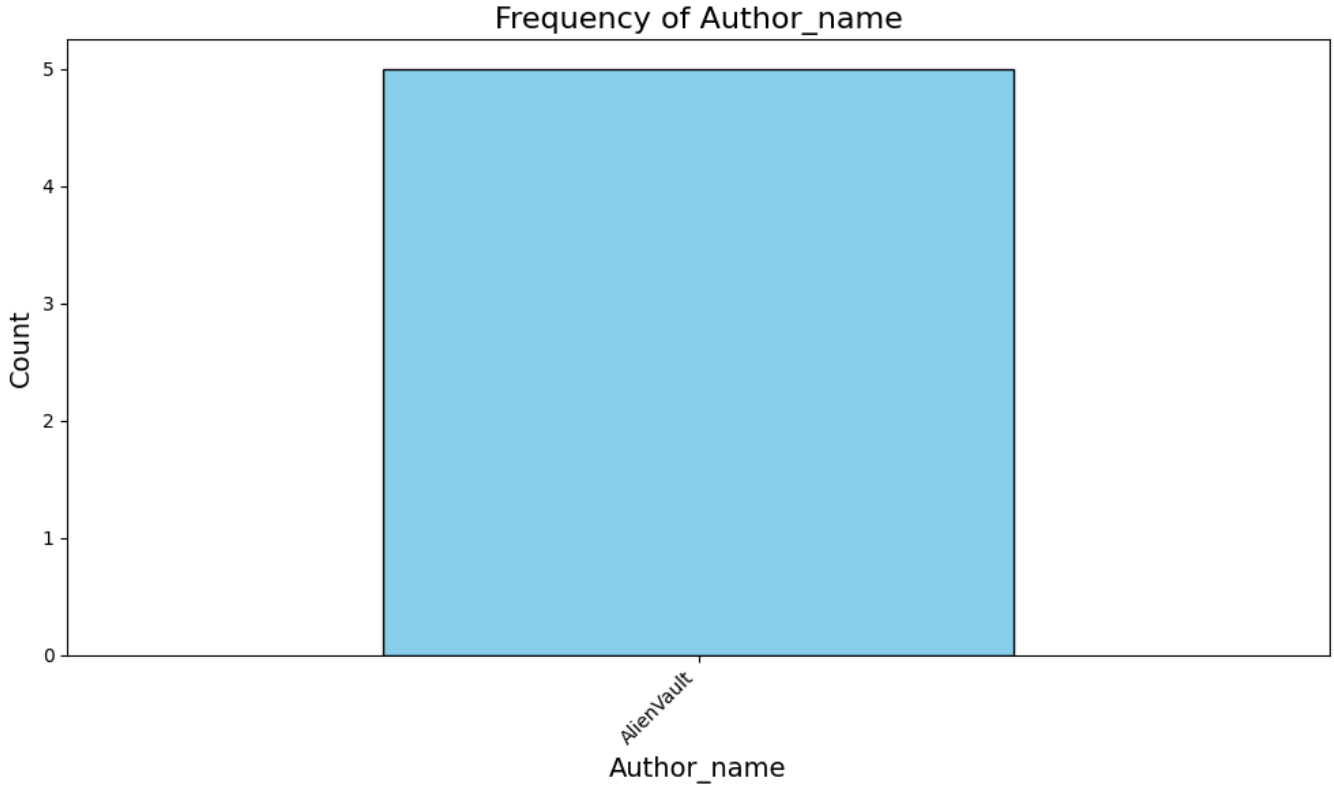
Threat Intelligence Dashboard

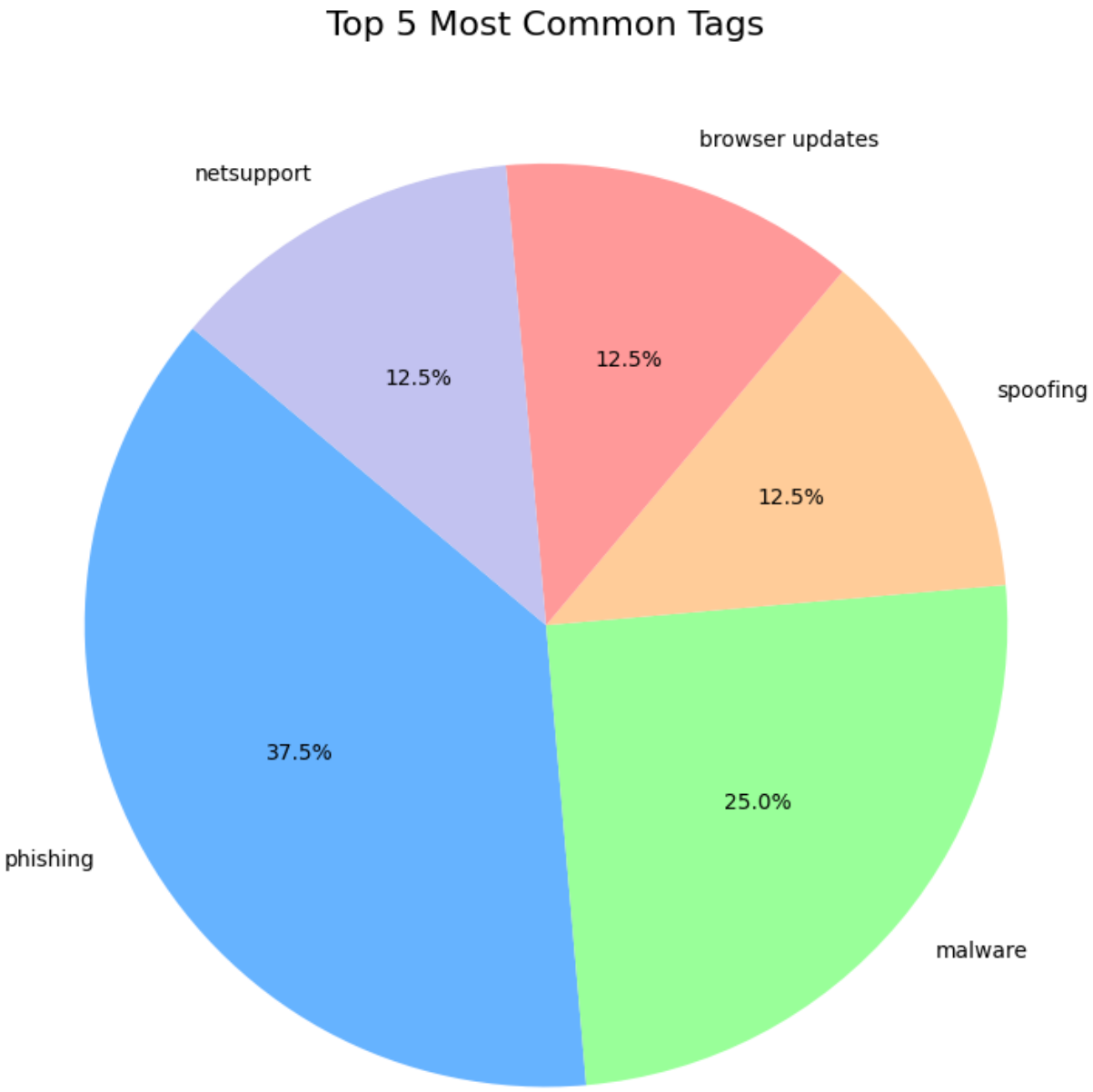
Generated on 2024-11-15 16:24:01

Threat Intelligence Dashboard

1. Bar Chart - Frequency of Authors



2. Pie Chart - Distribution of Tags



Pulse ID: 670f879377f69603fe32d425

Name: A Website Attacked

Author: AlienVault

Created: 2024-10-16 09:29:55

Modified: 2024-11-15 09:03:06

Tags:

spoofing, browser updates, netsupport, compromised websites, malware, watering hole

Description:

This report investigates a watering hole attack on a U.S. apartment website that delivered malware by spoofing a fake browser update. The investigation uncovered dozens of other compromised websites from various industries like healthcare, retail, and consumer sites. The compromised sites loaded malicious scripts from external domains, using techniques like iframes, random variable strings, and insertBefore methods. The malware spoofed Chrome, Mozilla, and Edge browser updates to deliver NetSupport malware. Domain registration analysis revealed the actor utilized various registrars, ISPs, and nameservers, prioritizing volume and speed over operational security. The activity shares similarities with the Socgholish threat group.

Pulse ID: 670f86c5b38b1037dd8353e4

Name: The New Malware Distribution Service

Author: AlienVault

Created: 2024-10-16 09:26:29

Modified: 2024-11-15 09:03:06

Tags:

injection, lv, ekans, snakehose, keylogger, distribution, bladabindi, malware, agenttesla, njrat, njw0rm, remcos, evasion

Description:

This analysis uncovers a novel malware distribution mechanism utilizing VBE scripts stored in archive files to spread various malware families, including AgentTesla, Remcos, Snake, and NjRat. It details the infection chain, which involves downloading encoded files from a command-and-control server, storing data in the registry, creating scheduled tasks, and employing techniques like process hollowing for payload injection. The final payload is revealed to be the SNAKE Keylogger, known for stealing sensitive data like keystrokes, screenshots, and clipboard contents.

Pulse ID: 6736b74edca101b2488c6c9a

Name: Fake North Korean IT Worker Linked to BeaverTail Video Conference App Phishing Attack

Author: AlienVault

Created: 2024-11-15 02:51:58

Modified: 2024-11-15 08:55:19

Tags:

supply chain, beavertail, north korea, contagious interview, insider threat, phishing, fake it workers, invisibleferret, wagemole

Description:

Unit 42 researchers identified a North Korean IT worker activity cluster, CL-STA-0237, involved in phishing attacks using malware-infected video conference apps. The cluster likely operates from Laos and exploited a U.S.-based SMB IT services company to apply for other jobs, securing a position at a major tech company in 2022. This cluster is part of a broader network of North Korean IT workers supporting illicit activities. The article highlights the shift from stable income-seeking to aggressive malware campaigns and illustrates the global reach of these workers. Organizations are advised to strengthen hiring processes, implement robust monitoring, evaluate outsourced services, and ensure employees don't use corporate machines for personal activities.

Pulse ID: 673653d6415530884c3d27ef

Name: Financially Motivated Chinese Threat Actor SilkSpecter Targeting Black Friday Shoppers

Author: AlienVault

Created: 2024-11-14 19:47:34

Modified: 2024-11-15 08:53:21

Tags:

oemapps, chinese threat actor, black friday, financial fraud, google translate, stripe, e-commerce, phishing

Description:

A Chinese financially motivated threat actor, dubbed SilkSpecter, has been uncovered targeting e-commerce shoppers in Europe and USA with a phishing campaign leveraging Black Friday discounts. The actor uses fake discounted products as lures to steal Cardholder Data, Sensitive Authentication Data, and Personally Identifiable Information. SilkSpecter exploits the legitimate payment processor Stripe to complete genuine transactions while covertly exfiltrating sensitive data. The phishing sites use Google Translate to dynamically adjust the language based on the victim's IP location. The campaign is linked to a Chinese SaaS platform, oemapps, which enables the creation of convincing fake e-commerce sites. The phishing domains primarily use .top, .shop, .store, and .vip TLDs, often typosquatting legitimate e-commerce organizations.

Pulse ID: 67364be4eea4a69c8055ab06

Name: Malware Spotlight: A Deep-Dive Analysis of WezRat

Author: AlienVault

Created: 2024-11-14 19:13:40

Modified: 2024-11-15 08:51:13

Tags:

backdoor, iran, phishing, modular, wezrat, infostealer, c&c, espionage

Description:

Check Point Research provides a comprehensive analysis of WezRat, a custom modular infostealer attributed to the Iranian cyber group Emennet Pasargad. The malware has been active for over a year, targeting organizations in multiple countries. WezRat's capabilities include executing commands, taking screenshots, uploading files, keylogging, and stealing clipboard content and cookie files. The analysis reveals the malware's evolution, its modular architecture, and the threat actors' infrastructure. The latest version was distributed through a phishing campaign impersonating the Israeli National Cyber Directorate, demonstrating the group's ongoing development and refinement of this versatile cyber espionage tool.