Who is SALTY SPIDER (Sality)?| Threat Actor Profile | CrowdStrike

By AdamM

Archived: 2026-04-05 18:28:51 UTC

Common Aliases

SALTY SIDER is most commonly identified with the botnet it maintains (Sality) and it's associated pseudonyms:

- *KuKu*
- *SalLoad*
- *Kookoo*
- *SaliCode*
- *Kukacka*

SALTY SPIDER's Origins

SALTY SPIDER is an eCrime group whose actions likely indicate that it's operating out of Russia – specifically in the Republic of Bashkortostan, a region close to the Kazakhstan border. This adversary has been linked to a botnet known as Sality, which is a polymorphic file infector first discovered in 2003. Since 2008, the initial botnet has been superseded by at least three more advanced peer-to-peer (P2P) versions. Beginning in the Summer of 2017, the botnet's population grew significantly when it began exploiting the ETERNALBLUE vulnerability. **Today, the latest versions of Sality are still both prevalent and formidable.**

SALTY SPIDER's Targets

The pervasiveness of Salty Spider's attacks has resulted in a long list of victims across the globe. While it seems, for the most part, that **this adversary doesn't single out particular nations and industries**, there do appear to be a few pockets where SALTY SPIDER may be more prevalent.

Target Nations

Generally, SALTY SPIDER does not appear to be selective when it comes to the nations it targets — the group's activities have been observed worldwide. However, **CrowdStrike has observed higher volumes of Sality v3 infections in Romania and high volumes of v4 activity in Venezuela.** The reasoning for these higher pockets of activity in Romania and Venezuela remains unknown.

Target Industries

In 2017, SALTY SPIDER ceased propagation of traditional proxy and spambot payloads, and shifted its sights towards the **mining and theft of cryptocurrencies**. This shift is likely an indicator that the cryptocurrency

industry has proven to be a more lucrative area for monetizing Sality.

SALTY SPIDER's Methods

The main goal of the Sality P2P botnet is quite straightforward — infect the machine and propagate secondary payloads. This allows Sality malware to forgo extensive built-in functionality. In fact, the malware is only known to maintain the infection and manage the connection between the machine and the botnet. Once a machine has been compromised by the polymorphic file infector, which adds the malware through legitimate executables, operators can then instruct the device to download and execute payloads. Due to SALTY SPIDER's affinity for cryptocurrencies, these payloads have been observed querying the machine's clipboard for strings matching Bitcoin or Ethereum addresses. Matching strings are then replaced with the actor's own Bitcoin or Ethereum address.

Other Known "SPIDERS"

SALTY SPIDER is just one of many eCrime adversaries tracked by CrowdStrike Intelligence. Some of other cyber criminal groups that CrowdStrike monitors include the following:

- COBALT SPIDER
- DUNGEON SPIDER
- MUMMY SPIDER
- WICKED SPIDER

Curious about other eCrime, hacktivist or nation-state adversaries? Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.

Learn More About the Cyber Threat Landscape

Want more insights on the latest adversary tactics, techniques, and procedures (TTPs)? Download the CrowdStrike® 2019 Global Threat Report: Adversary Tradecraft and The Importance of Speed: **Download: CrowdStrike 2020 Global Threat Report.** To learn more about how to incorporate intelligence on threat actors like SALTY SPIDER into your security strategy, please visit the Falcon Threat Intelligence page.

Additional Resources

- *Read the report on CrowdStrike Falcon® Intelligence Automated Threat Intelligence to learn what contextualized, actionable threat intelligence can add to your security effectiveness.*
- *Learn more about comprehensive endpoint protection with the CrowdStrike Falcon®® platform by visiting the product page.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*
