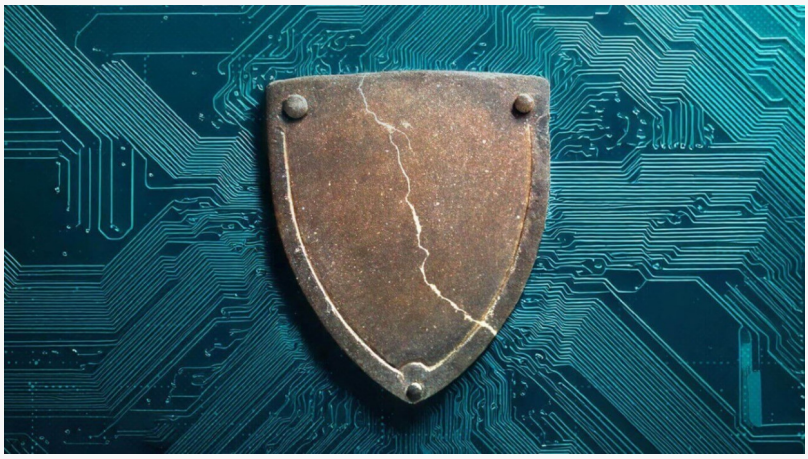
New ransomware group Embargo uses toolkit that disables security solutions, ESET Research discovers



DUBAI, DUBAI, UNITED ARAB EMIRATES, October 29, 2024 /EINPresswire.com/ -- ESET researchers have discovered new tooling leading to the deployment of Embargo ransomware. Embargo is a relatively new group in the ransomware scene, first observed by ESET in June 2024. The new toolkit consists of a loader and an endpoint detection and response killer (EDR), which ESET has named respectively. MS4Killer is particularly noteworthy as it is custom-compiled for each victim's environment, targeting only selected security solutions. The malware abuses Safe Mode and a vulnerable driver to disable the security products running on the victim's machine. Both tools are written in Rust, the Embargo group's language of choice for developing its ransomware.

Based on its modus operandi, Embargo seems to be a well-resourced group. It sets up its own infrastructure to communicate with victims. Moreover, the group pressures victims into paying by using double extortion: the operators exfiltrate victims' sensitive data and threaten to publish it on a leak site, in addition to encrypting it. In an interview with an alleged group member, an Embargo representative mentioned a basic payout scheme for affiliates, suggesting that the group is providing RaaS (ransomware as a service). "Given the group's sophistication, the existence of a typical leak site, and the group's claims, we assume that Embargo indeed operates as a RaaS provider," says ESET researcher Jan Holman, who analyzed the threat along with fellow researcher Tomáš Zvara.

Differences in deployed versions, bugs, and leftover artifacts suggest that these tools are under active development. Embargo is still in the process of building its brand and establishing itself as a prominent ransomware operator.

Developing custom loaders and EDR removal tools is a common tactic used by multiple

ransomware groups. Besides the fact that MDeployer and MS4Killer were always observed deployed together, there are further connections between them. The strong ties between the tools suggest that both are developed by the same threat actor, and the active development of the toolkit suggests that the threat actor is proficient in Rust.

With MDeployer, the Embargo threat actor abuses Safe Mode to disable security solutions. MS4Killer is a typical defense evasion tool that terminates security product processes using the technique known as Bring Your Own Vulnerable Driver (BYOVD). In this technique, the threat actor abuses signed, vulnerable kernel drivers to gain kernel-level code execution. Ransomware affiliates often incorporate BYOVD tooling in their compromise chain to tamper with security solutions protecting the infrastructure being attacked. After disabling the security software, affiliates can run the ransomware payload without worrying whether their payload gets detected.

The main purpose of the Embargo toolkit is to secure the successful deployment of the ransomware payload by disabling the security solution in the victim's infrastructure. Embargo puts a lot of effort into that, replicating the same functionality at different stages of the attack. "We have also observed the attackers' ability to adjust their tools on the fly, during an active intrusion, for a particular security solution," adds ESET researcher Tomáš Zvara.

For a more detailed analysis and technical breakdown of Embargo's tools, check out the latest ESET Research blogpost "Embargo ransomware: Rock'n'Rust" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
