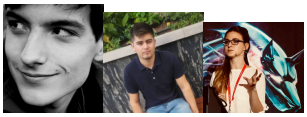
FIN8 Threat Actor Spotted Once Again with New "Sardonic" Backdoor

By Eduard BUDACA

Archived: 2026-04-06 03:10:28 UTC



August 25, 2021

Since January 2016, FIN8 has been steadily building a reputation among financially motivated advanced threat actors. Bitdefender researchers are constantly monitoring this group's activity, and previous research released in early 2021 documented the use of a new, improved version of the BADHATCH backdoor.

This whitepaper focuses on the analysis of a new backdoor component discovered during a forensic investigation, described here. As this backdoor has not been documented or referenced before, we named it "Sardonic", given that artifacts led us to believe the threat actors use this name for an entire project including the backdoor itself, the loader and some additional scripts. We believe this project is still under development, and additional updates will likely follow.

Key facts about Sardonic:

- Sardonic is a new backdoor in the FIN8 ecosystem
- Sardonic is a project still under development and includes several components
- The new components were identified in a real-life attack and seems to be compiled just before the attack
- Sardonic backdoor is extremely potent and has a wide range of capabilities that help the threat actor leverage new malware on the fly without updating components

Recommendations

FIN8 continues to strengthen its capabilities and malware delivery infrastructure. The highly skilled financial threat actor is known to take long breaks to refine tools and tactics to avoid detection before it strikes viable targets.

Bitdefender recommends that companies in target verticals (retail, hospitality, finance) check for potential compromise by applying the following IoCs to their EDR, XDR and other security defenses.

To further minimize the impact of financial malware, companies should:

- Separate the POS network from the ones used by employees or guests
- Introduce cybersecurity awareness training for employees to help them spot phishing e-mails.
- Tune the e-mail security solution to automatically discard malicious or suspicious attachments.

- Integrate threat intelligence into existing SIEM or security controls for relevant Indicators of Compromise.
- Small and medium organizations without a dedicated security team should consider outsourcing security operations to Managed Detection and Response providers.

Indicators of Compromise

An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. The currently known indicators of compromise can be found in the whitepaper below.

Download the research whitepaper
