New ‘Domino’ Malware Linked to FIN7 Group, Ex-Conti Members



Distribution campaigns for a recently identified backdoor have revealed a partnership between former members of the Conti ransomware group and developers for the FIN7 advanced persistent threat (APT), IBM reports.

Dubbed ‘Domino’, the backdoor has been active since at least October 2022 and is capable of gathering basic system information, sending data to its command-and-control (C&C) server, and executing a loader to deploy the final payload on the compromised systems.

Domino’s code, IBM has discovered, overlaps with the Lizar malware, which was previously attributed to the FIN7 group. The two malware families also share similarities in functionality, configuration structure, and bot ID formats.

Lizar, also known as Tirion and DiceLoader, was used in

attacks between March 2020 and late 2022, but appears to have been replaced by Domino in more recent campaigns, IBM's security researchers say.

Starting February 2023, Domino attacks were seen using the Dave loader, which has been linked to the Conti/TrickBot group, and which former members of the criminal enterprise continue to maintain.

This, IBM says, shows that ex-Conti members likely collaborated with current or former FIN7 developers to buy or use Domino.

The Dave loader has been used in association with Cobalt Strike in attacks that can be attributed to former Conti members, and was also seen deploying IcedID and Emotet, both used by ex-Conti affiliates to deploy ransomware.

The FIN7 developers, IBM believes, shared with the ex-Conti threat actors not only the Domino backdoor, but also the Project Nemesis infostealer, which Domino has been deploying since at least October 2022.

Advertised on the dark web since December 2021, Project Nemesis has not been frequently used in attacks and is relatively unknown, but can collect a broad range of data, which operators can access using a web-based control panel.

IBM provides a technical analysis of the Domino backdoor, Dave loader, and Project Nemesis.

Related: Number of Ransomware Attacks on Industrial Orgs Drops Following Conti Shutdown

Related: FIN7 Cybercrime Operation Continues to Evolve Despite Arrests

Related: Malware Trends: What's Old Is Still New

New 'Domino' Malware Linked to FIN7 Group, Ex-Conti Members