Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:45:26 UTC

APT group: Tortilla

Names	Tortilla *(TG Soft)*
Country	[Unknown]
Motivation	Financial gain
First seen	2021
Description	(Talos) Cisco Talos recently discovered a malicious campaign deploying variants of the Babuk ransomware predominantly affecting users in the U.S. with smaller number of infections in U.K., Germany, Ukraine, Finland, Brazil, Honduras and Thailand. The actor of the campaign is sometimes referred to as Tortilla, based on the payload file names used in the campaign. This is a new actor operating since July 2021. Prior to this ransomware, Tortilla has been experimenting with other payloads, such as the PowerShell-based netcat clone Powercat, which is known to provide attackers with unauthorized access to Windows machines. We assess with moderate confidence that the initial infection vector is exploitation of ProxyShell vulnerabilities in Microsoft Exchange Server through the deployment of China Chopper web shell.
Observed	Countries: Brazil, Finland, Germany, Honduras, Thailand, UK, Ukraine, USA.
Tools used	Babuk Locker, China Chopper.
Information	<https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html>

Last change to this card: 04 November 2021

Download this actor card in PDF or JSON format