Chewbacca Point-of-Sale Malware Campaign Found in 10 Countries

By Michael Mimoso

Published: 2014-01-31 · Archived: 2026-04-06 02:58:35 UTC

A criminal campaign using the Tor-based Chewbacca Trojan, which includes memory-scraping malware and a keylogger, is responsible for the theft of more than 49,000 credit card numbers in 10 countries.

Before you think that RAM scraper malware was a phenomenon specific to the Target breach, think again. A four-month-long crime spree targeting point-of-sale systems in a number of industries has been discovered; the campaign, however, is not related to the mammoth Target break-in or other recently reported hacks at Neiman Marcus or Michaels.

The malware in question is the privately sold Chewbacca Trojan, which is a two-pronged threat that uses the Tor anonymity network to hide its communication with the attackers' command and control infrastructure. Chewbacca not only infects point-of-sale terminals with the RAM scraping malware in order to steal payment card data before it is encrypted, but also drops keylogging software onto compromised systems.

Researchers at RSA Security discovered the criminal campaign and say it has found malware samples used in 10 countries, primarily in the United States and the Russian Federation. Will Gragido, senior manager at RSA FirstWatch, the company's research arm, said the command and control server they intercepted has been taken offline—likely by its Ukrainian handlers rather than law enforcement—putting a halt to the campaign. Gragido said the criminals had their hands on 49,330 credit card numbers and there were 24 million transaction records on the attackers' server.

"It's actually a mixture of industries that have been hit: some broadband providers were impacted, retailers, supermarkets, gas stations, and other associated businesses," Gragido said. "It's a sloppily put-together piece of code; it's not the most sophisticated code, but it seems effective."

The original Chewbacca samples were found in October and reported by Kaspersky Lab's Global Research and Analysis Team in December. While the original attack vector is not yet understood, Chewbacca's behaviors are pretty self-evident. Chewbacca finds running processes on compromised computers, reads process memory, drops a keylogger and is able to move that information off of infected machines, said Marco Preuss, director of research for Kaspersky Lab in Europe.

The malware is a PE32 executable compiled with Free Pascal 2.7.1; its 5 MB file includes the Tor executable, which the attackers use to move data and communication between infected POS terminals and servers, and the attackers. Once executed, Chewbacca drops as spoolsv.exe into the victim machine's startup folder and then launches its keylogger and stores all keystrokes to a log created by the malware, Preuss said. Spoolsv.exe is the same name used by the Windows Print Spooling service; the malware does so to insert itself into the startup process and maintain persistence.

Gragido said RSA FirstWatch had infiltrated the attackers' original command server, which was using a Tor .onion domain for obfuscation.

"We think we caught this campaign early on," Gragido said. "Chewbacca has not been out there very long. We've seen it established in a few small retailers and service providers."

The Target breach has elevated awareness around point of sale malware, in particular RAM scrapers. Target admitted shortly before Christmas that attackers has been on its network and stolen 40 million payment card numbers from infected point of sale systems, along with the personal information of 70 million people, putting potentially 110 million at risk for identity theft and fraud.

New details emerged this week on just how burrowed into Target's network the attackers were. Experts believe the initial compromise was a SQL injection attack that allowed the attackers access to the network. Once there, it's apparent they took advantage of hard-coded credentials on system management software used by the retailer to set up a control server on the Target network and moved data out in batches.

"We don't have anything from an evidentiary perspective that this is tied to Target, Neiman Marcus or Michaels," Gragido said. "The malware is different, the attackers' MO is different, there's no common infrastructure or common malware. The gang behind it, we think, is a newer crop of folks with activity in Eastern Europe, but it's hard to say."
