Malware Brief: A malware foursome working together

By Barracuda Networks

Published: 2025-07-21 · Archived: 2026-04-05 22:33:54 UTC

In today's Malware Brief we'll take a quick look at four different examples of malware that have all emerged at about the same time. They demonstrate the complex chain of threats being used together, sometimes by different groups for disparate purposes.

In this case, all four — RomCom RAT, TransferLoader, MeltingClaw and DustyHammock — were identified in the early 2020s following the Russian invasion of Ukraine. They were, and are, extensively used by Russian-speaking groups against Ukrainian, Polish and some Russian targets.

RomCom RAT

Type: Remote Access Trojan (RAT)

Distribution: Phishing campaigns, compromised URLs, fake software downloads

Variant: SingleCamper

First identified: 2022

Common targets: Primarily deployed against targets in Ukraine

Known operators: TA829, UAT-5647

RomCom RAT is used by threat actors to create a backdoor for remotely controlling endpoint computers. The Russian-linked TA829 group uses this and other tools for intelligence-gathering as well as financial fraud. This group typically exploits vulnerabilities in Mozilla Firefox and Microsoft Windows to spread RomCom RAT.

Once a system is compromised with RomCom RAT, the threat actor typically inserts a stealthy loader such as TransferLoader or SlipScreen into it. These are then used to load ransomware into the target system.

It was initially used primarily against Ukrainian and Polish targets by Russian-speaking groups, prior being adapted to financial crimes.

TransferLoader

Type: Malware loader

Distribution: job-application-themed phishing campaigns, RAT compromise

First identified: February 2025

Known operator: UNK_GreenSec, RomCom

TransderLoader combines a downloader, a backdoor, and a backdoor loader to enable threat actors to make changes to compromised systems and insert ransomware or other malware.

It was first discovered when it was used to load Morpheus ransomware into an American law firm's system. It has since been used to drop malware such as MeltingClaw and DustyHammer.

TransferLoader has been designed for stealth, using a variety of techniques to avoid detection. When executing downloaded malicious code, it masks its activity by opening decoy PDF files.

MeltingClaw

Type: Downloader

Variant: RustyClaw

First identified: 2024

Known operators/creators: RomCom — aka Storm-0978, UAC-0180, Void Rabisu, UNC2596, and Tropical Scorpius

Advanced spear-phishing campaigns have been used to deliver the downloaders MeltingClaw and its cousin RustyClaw. These then download and install the backdoors DustyHammock or ShadyHammock.

These stealthy backdoors allow for long-term access to target systems, finding and exfiltrating data or performing other malicious tasks. It was used for espionage and sabotage against systems in Ukraine during the Russian invasion.

DustyHammock

Type: Backdoor

Variant: ShadyHammock

First identified: 2024

DustyHammock is designed to communicate with a command-and-control server, perform initial reconnaissance on targeted systems, and allow threat actors to run arbitrary commands and download and place malicious files.

Meant to enable long-term access while evading detection, DustyHammock has been used for data exfiltration and espionage, as well as for sabotage.
