ThreatCure

Cyber Threat Advisory

RomCom

Threat Actor Malware

Description

RomCom

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Breaches
- Financial Loss
- Reputation Damage
- Disruption of Operations

RomCom malware, also known as Storm-0978 or DEV-0978 or UAT-256, is a sophisticated cyber-espionage tool developed by a cybercriminal. Initially targeting military installations in Ukraine, RomCom has expanded its reach to English-speaking countries, including the United Kingdom. This malware employs advanced techniques such as spoofing trusted software and leveraging valid code-signing certificates to infiltrate networks and execute malicious.

RomCom functions as a Remote Access Trojan (RAT), enabling attackers to remotely control infected/compromised devices. It is primarily distributed via spear-phishing campaigns, where attackers pose as trusted software vendors to deceive users into downloading and running the malicious software. After infiltrating a system, RomCom can run various commands, download further malicious payloads, and sustain ongoing access to the compromised system. Below, we provide its updated hashes.

Infection Details

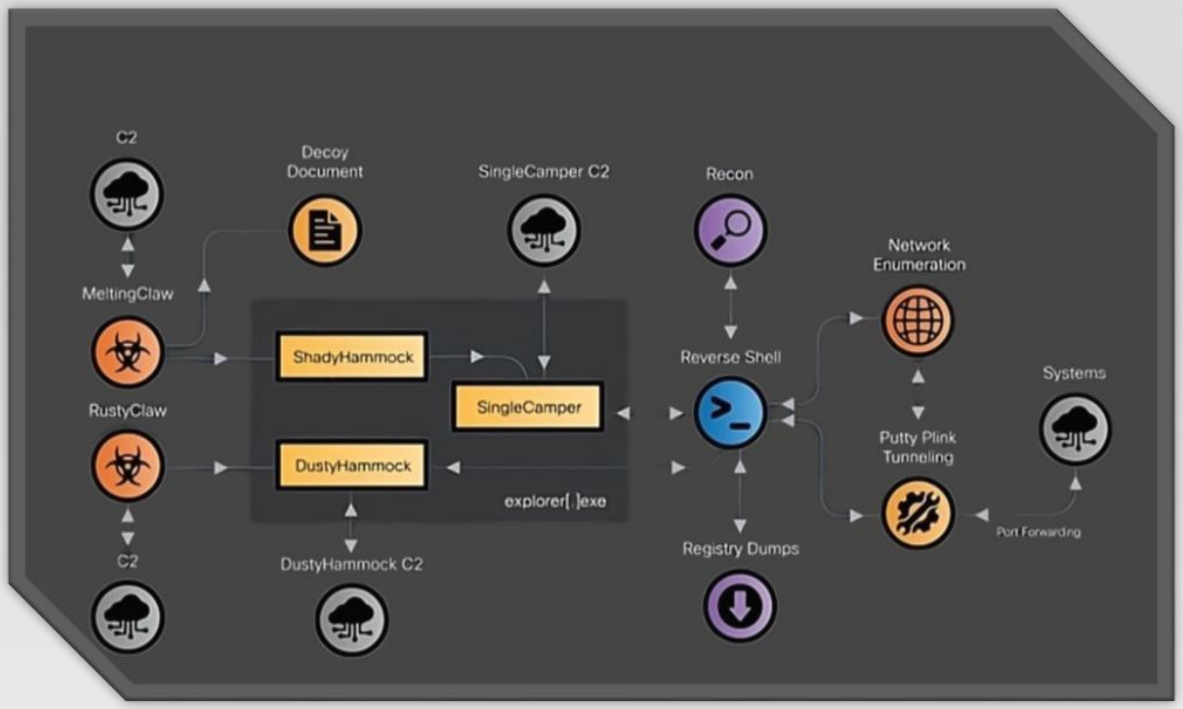

Figure 1 RomCom Infection chain

This diagram shows a sophisticated malware attack that starts with a decoy document delivered through phishing. When opened, it installs several malicious components to take control of the system.

Key actions include:

- Reverse shell for remote control.
- Registry dumps for stealing sensitive information.
- Network reconnaissance to find more systems. Putty Plink tunneling for lateral movement to other targets.

The malware constantly communicates with C2 servers (e.g., Melting Claw, Rusty Claw) to receive commands and exfiltrate data, ensuring ongoing control and adaptability during the attack.

Indicator of Compromise

SHA-256

0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501

1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed35c154

2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4

5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129

57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312

5b30a5b71ef795e07c91b7a43b3c1113894a82ddffc212a2fa71eebc078f5118

5c71601717bed14da74980ad554ad35d751691b2510653223c699e1f006195b8

60d96087c35dadca805b9f0ad1e53b414bcd3341d25d36e0190f1b2bbfd66315

92c8b63b2dd31cf3ac6512f0da60dabd0ce179023ab68b8838e7dc16ef7e363d

a2f2e88a5e2a3d81f4b130a2f93fb60b3de34550a7332895a084099d99a3d436

Remediation

- **Employee Security Training:** Train staff to recognize phishing attempts and emphasize the importance of confirming the legitimacy of email senders.
- **Ongoing System Monitoring:** Continuously monitor systems and networks to identify emerging threats and vulnerabilities.
- **Software Patch Management:** Regularly update all software to apply the latest security patches and mitigate known vulnerabilities.
- **Network Isolation:** Use network segmentation to contain malware, preventing it from spreading across systems if one is compromised.
- **Robust Access Controls:** Enforce strong password policies, multi-factor authentication, and the principle of least privilege to minimize unauthorized access.
- **Block Indicators of Compromise (IOCs):** Ensure your XDR, EDR, and other security tools are set to block all identified IOCs.

ThreatCure

Cyber Threat Advisory

Secure your byte world

RomCom

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE