Sep 18 2023

NETMANAGEIT

Intelligence Report

Guarding Against the Unseen: Investigating a Stealthy Remcos Malware Attack on Colombian Firms

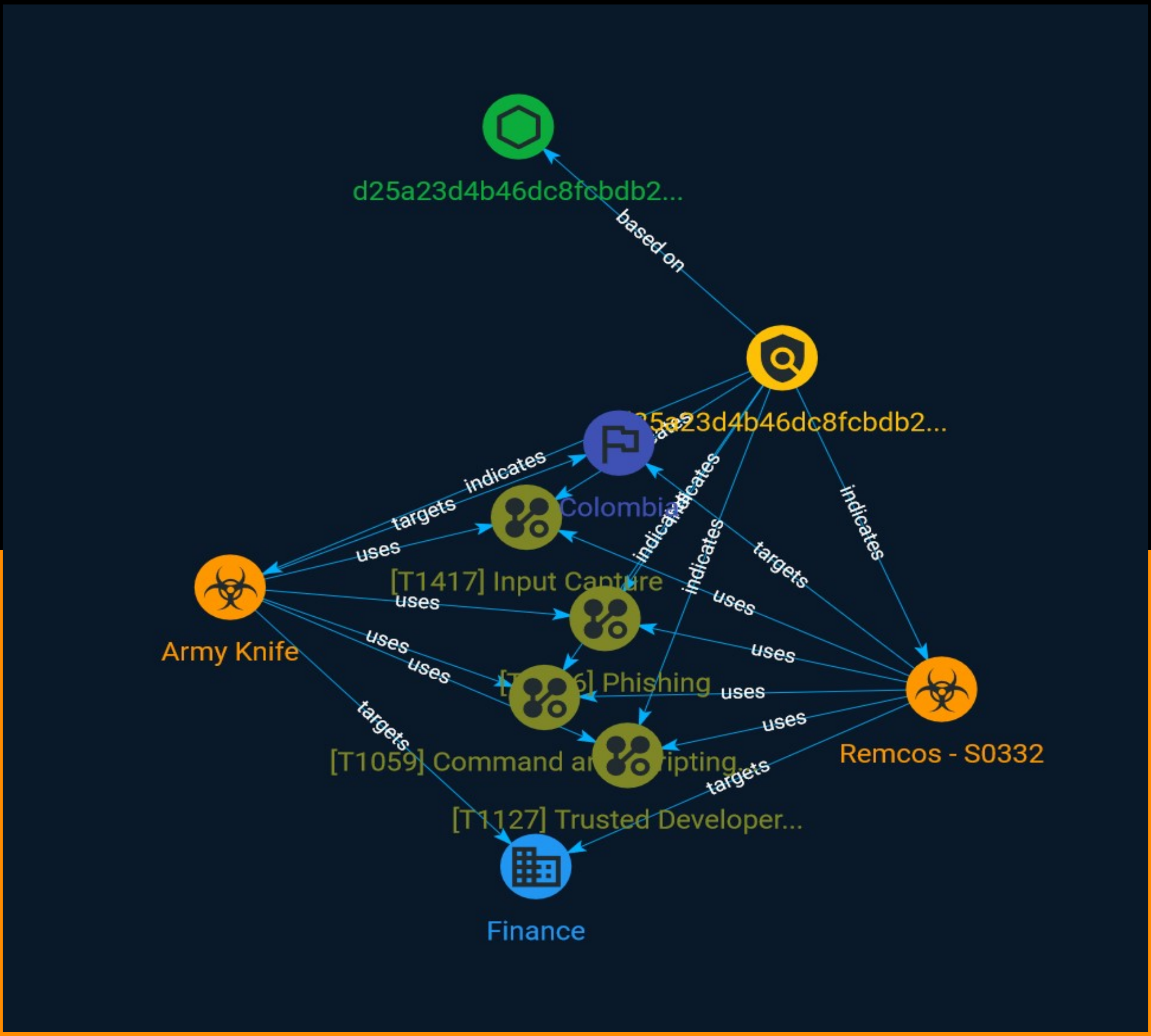

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In the last two months, researchers encountered a new large-scale phishing campaign that recently targeted more than 40 prominent companies across multiple industries, in Colombia. The attackers' objective was to discreetly install the notorious "Remcos" malware on victims' computers. Remcos, a sophisticated "Swiss Army Knife" RAT, grants attackers full control over the infected computer and can be used in a variety of attacks. Common consequences of a Remcos infection include data theft, follow-up infections, and account takeover. In our report, we delve into the attack intricacies and highlight the stealthy techniques employed by the malicious actors.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name
Command and Scripting Interpreter
ID
T1059
Description
Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)
Name
Input Capture
ID
T1417

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal device usage, users often provide credentials to various locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Keylogging](https://attack.mitre.org/techniques/T1417/001)) or rely on deceiving the user into providing input into what they believe to be a genuine application prompt (e.g. [GUI Input Capture](https://attack.mitre.org/techniques/T1417/002)).

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Sector

Name
Finance

Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Indicator

Name
d25a23d4b46dc8fcbdb233c6c96b9d438033cba0fc10452fdffe69ebafdfea8f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd25a23d4b46dc8fcbdb233c6c96b9d438033cba0fc10452fdffe69ebafdfea8f']

Country

Name
Colombia

Malware

Name
Remcos - S0332

Name
Army Knife

StixFile

Value
d25a23d4b46dc8fcbdb233c6c96b9d438033cba0fc10452fdffe69ebafdfea8f

External References

- https://otx.alienvault.com/pulse/6508105ac11655dac290989a
- https://research.checkpoint.com/2023/guarding-against-the-unseen-investigating-a-stealthy-remcos-malware-attack-on-colombian-firms/