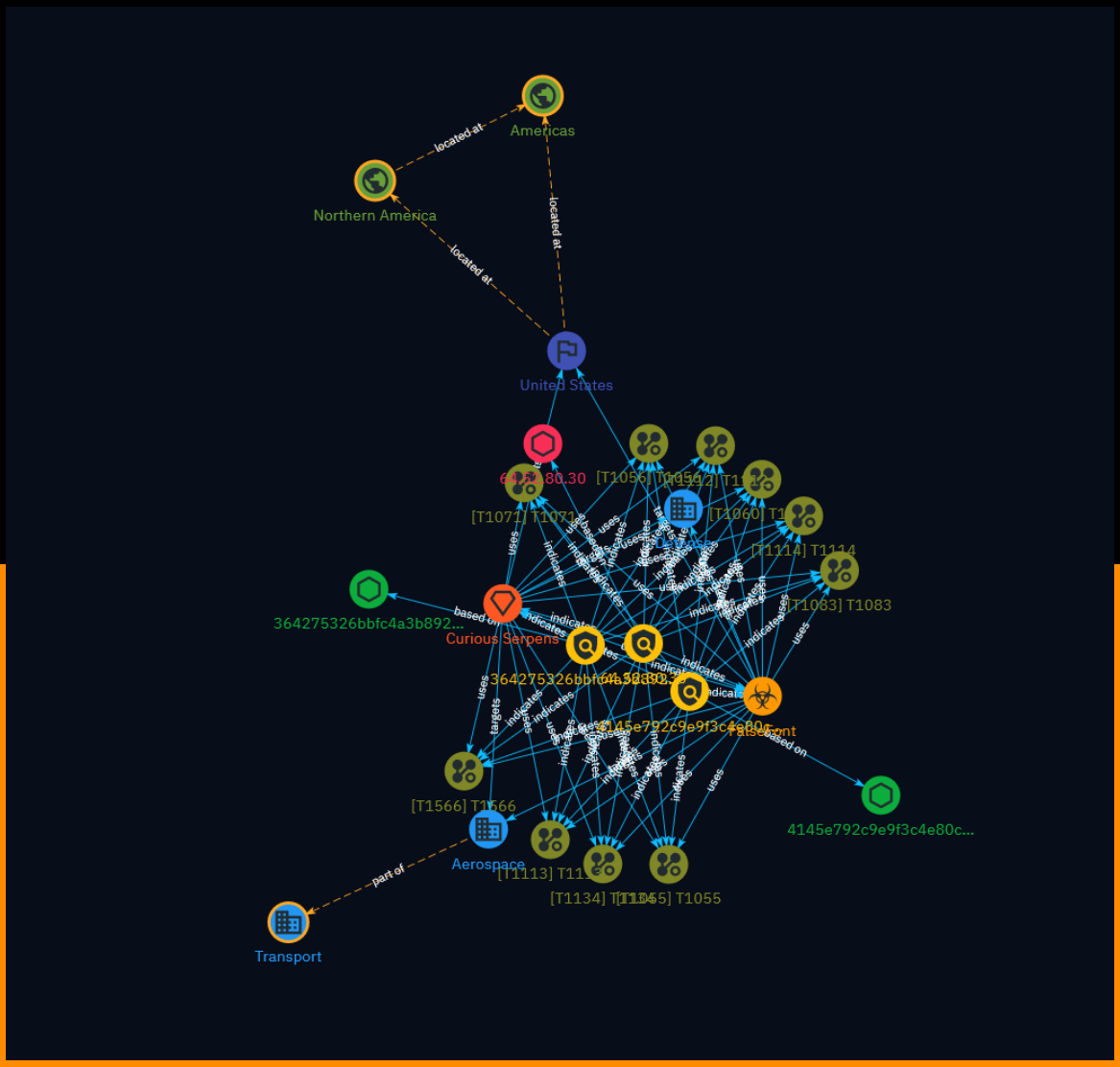
Mar 21 2024

NETMANAGEIT

# Intelligence Report

# Curious Serpens' Backdoor: Technical Analysis, Detection and Prevention



# Table of contents

## Overview


- Description 4
- Confidence 4
- Content 5


## Entities


- Indicator 6
- Malware 8
- Intrusion-Set 9
- Attack-Pattern 10
- Country 16
- Region 17
- Sector 18

## Observables


- StixFile 19
- IPv4-Addr 20


## External References


- External References 21

# Overview

## Description

This report provides a technical analysis of FalseFont, a backdoor used by the suspected Iranian threat actor Curious Serpens to target aerospace and defense sectors. The malware disguises itself as job recruitment software to trick victims into installing it. Analysis focuses on FalseFont's architecture, functionality, command and control, and credential theft capabilities. The report also discusses detection and prevention controls.

## Confidence

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

100 / 100

# Content

N/A

# Indicator

| Name |
| --- |
| 4145e792c9e9f3c4e80ca0e290bd7568ebcef678affd68d9b505f02c6acaab12 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '4145e792c9e9f3c4e80ca0e290bd7568ebcef678affd68d9b505f02c6acaab12'] |
| **Name** |
| 364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614 |
| **Pattern Type** |
| stix |
| **Pattern** |
| [file:hashes.'SHA-256' = '364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614'] |
| **Name** |

64.52.80.30

## Description

- **Zip Code:** N/A - **ISP:** BLNWX - **ASN:** 399629 - **Organization:** BLNWX - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 64.52.80.30 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Los Angeles - **Latitude:** 34.05 - **Longitude:** -118.24

## Pattern Type

stix

## Pattern

[ipv4-addr:value = '64.52.80.30']

# Malware

| Name |
| --- |
| FalseFont |

# Intrusion-Set

| Name |
| --- |
| Curious Serpens |

# Attack-Pattern

| Name |
| --- |
| T1060 |
| **ID** |
| T1060 |
| **Name** |
| T1134 |
| **ID** |
| T1134 |
| **Description** |
| Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) |

to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

**Name**

T1056

**ID**

T1056

**Description**

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

**Name**

T1083

**ID**

T1083

**Description**

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

**Name**

T1566

**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**

T1112

**ID**

T1112

**Description**

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

**Name**

T1055

**ID**

T1055

**Description**

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

**Name**

T1071

**ID**

T1071

**Description**

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

**Name**

T1114

**ID**

T1114

**Description**

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

**Name**

T1113

**ID**

T1113

**Description**

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

# Country

| Name |
| --- |
| United States |

# Region

| Name |
| --- |
| Northern America |

| Name |
| --- |
| Americas |

# Sector

| Name |
| --- |
| Defense |
| **Description** |
| Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations. |
| **Name** |
| Aerospace |
| **Description** |
| All entities transporting people or goods by plane, managing or exploiting airports and structures, traffic authorities and plane manufacturers. Includes all civilian space activities. |
| **Name** |
| Transport |
| **Description** |
| All entities involved in the movement of people or goods from one place to another. |

# StixFile

| Value |
| --- |
| 4145e792c9e9f3c4e80ca0e290bd7568ebcef678affd68d9b505f02c6acaab12 |
| 364275326bbfc4a3b89233dabdaf3230a3d149ab774678342a40644ad9f8d614 |

# IPv4-Addr

| Value |
| --- |
| 64.52.80.30 |

# External References

- https://unit42.paloaltonetworks.com/curious-serpens-falsefont-backdoor/#post-133071-_re5lfhtpycch
- https://otx.alienvault.com/pulse/65fc13c6c2ca6974d1ee78ea