Jul 06 2023

NETMANAGEIT

Intelligence Report

Welcome to New York: Exploring TA453's Foray into LNKs and Mac Malware

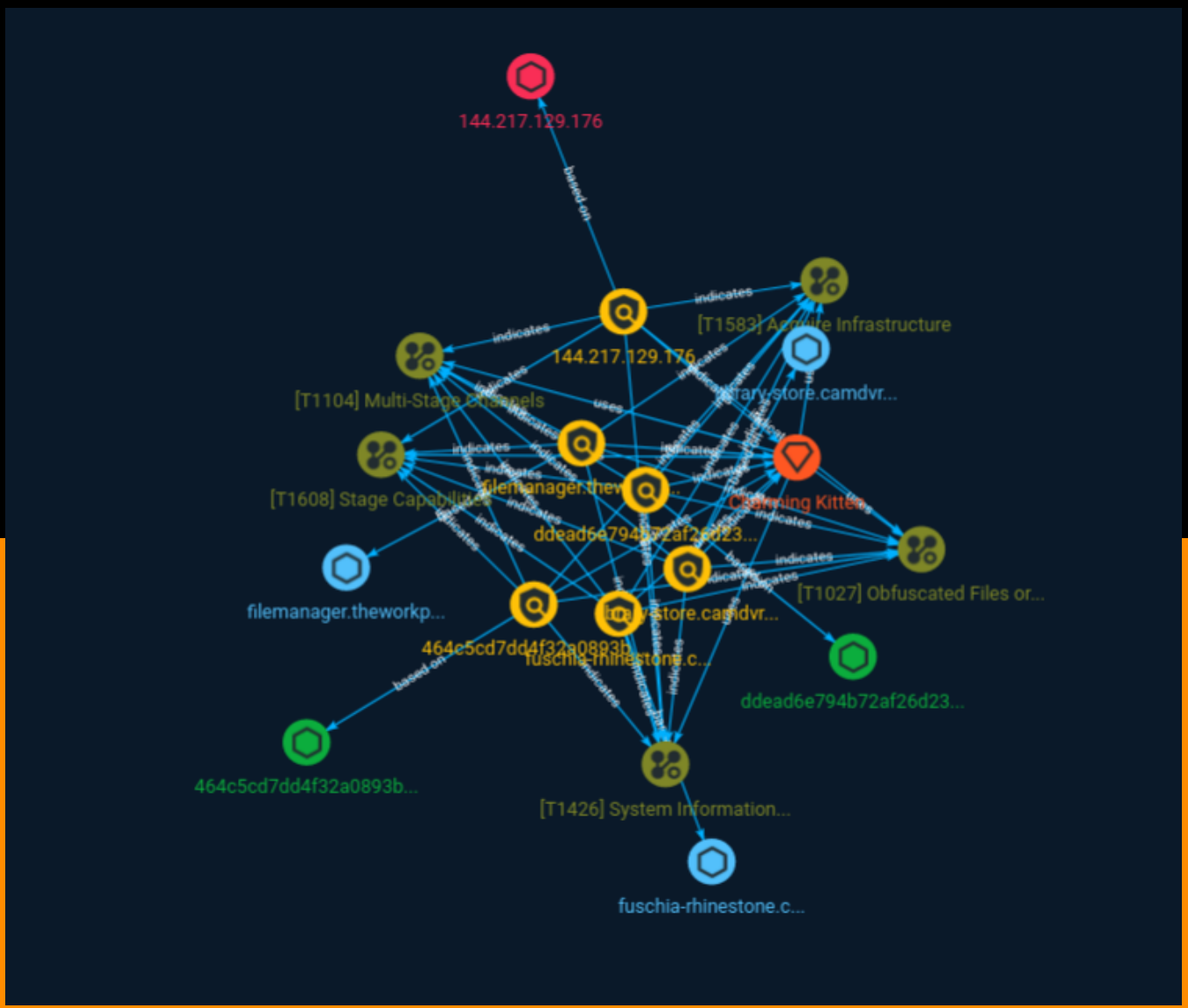

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In mid-May 2023, TA453—also known publicly as Charming Kitten, APT42, Mint Sandstorm, Yellow Garuda—sent a benign conversation lure masquerading as a senior fellow with the Royal United Services Institute (RUSI) to the public media contact for a nuclear security expert at a US-based think tank focused on foreign affairs. The email solicited feedback on a project called “Iran in the Global Security Context” and requested permission to send a draft for review. The initial email also mentioned participation from other well-known nuclear security experts TA453 has previously masqueraded as, in addition to offering an honorarium. TA453 eventually used a variety of cloud hosting providers to deliver a novel infection chain that deploys the newly identified PowerShell backdoor GorjolEcho. When given the opportunity, TA453 ported its malware and attempted to launch an Apple flavored infection chain dubbed NokNok by Proofpoint. TA453 also employed multi-persona impersonation in its unending espionage quest.

Confidence

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

15 / 100

Indicator

Name
fuschia-rhinestone.cleverapps.io
Pattern Type
stix
Pattern
[hostname:value = 'fuschia-rhinestone.cleverapps.io']
Name
filemanager.theworkpc.com
Pattern Type
stix
Pattern
[hostname:value = 'filemanager.theworkpc.com']
Name
library-store.camdvr.org

Pattern Type

stix

Pattern

[hostname:value = 'library-store.camdvr.org']

Name

ddead6e794b72af26d23065c463838c385a8fdff9fb1b8940cd2c23c3569e43b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ddead6e794b72af26d23065c463838c385a8fdff9fb1b8940cd2c23c3569e43b']

Name

144.217.129.176

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '144.217.129.176']

Name

464c5cd7dd4f32a0893b9fff412b52165855a94d193c08b114858430c26a9f1d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '464c5cd7dd4f32a0893b9fff412b52165855a94d193c08b114858430c26a9f1d']

Attack-Pattern

Name

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt

command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the

information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Intrusion-Set

Name

Charming Kitten

Description

[Charming Kitten](https://attack.mitre.org/groups/G0058) is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. [Charming Kitten](https://attack.mitre.org/groups/G0058) usually tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective. The group's TTPs overlap extensively with another group, [Magic Hound](https://attack.mitre.org/groups/G0059), resulting in reporting that may not distinguish between the two groups' activities. (Citation: ClearSky Charming Kitten Dec 2017)

StixFile

Value
464c5cd7dd4f32a0893b9fff412b52165855a94d193c08b114858430c26a9f1d
ddead6e794b72af26d23065c463838c385a8fdff9fb1b8940cd2c23c3569e43b

Hostname

Value
filemanager.theworkpc.com
library-store.camdvr.org
fuschia-rhinestone.cleverapps.io

IPv4-Addr

Value
144.217.129.176

External References

- https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware?utm_source=twitter&utm_medium=social&utm_source=social_organic&utm_social_network=twitter&utm_car cb7f-4d7a-bc5f-f4e2eeee72cb

- https://otx.alienvault.com/pulse/64a731ed59b7c34d5731ea0d