OBTS v5 2022

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ATT&CKing Pandas

Drawing out ATT&CK® Techniques in the Wild

Cat Self

- Former Artist
- Military Intelligence Veteran
- Red Teamer, Threat Hunter @Target
- Lead macOS & Linux ATT&CK @MITRE
- ATT&CK Evaluations TPM

What we are going to cover…

- Fun analogy
- Procedure focused
- What's Apple expects to happen
- A panda's workaround

What is ATT&CK?

A knowledge base of adversary behavior

- ***Based on real-world observations***
- ***Free, open, and globally accessible***
- ***A common language***
- ***Community-driven***

ATT&CK TACTICS: THE ADVERSARY’S TECHNICAL GOALS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	
e-by npromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Accoun Discove
loit lic-Facing lication	Exploitation for Client Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Debugger Evasion	Brute Force	Applica Window
ernal note Services	Inter-Process Communication	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Credentials from Password Stores	Browse Discove
dware itions	Native API	Browser Extensions	Create or Modify System Process	Execution Guardrails	Exploitation for Credential Access	Debugg
shing	Scheduled Task/Job	Compromise Client Software Binary	Event Triggered Execution	Exploitation for Defense Evasion	Forge Web Credentials	File and Discove
ply in Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Input Capture	Networl Discove
sted ationship	System Services	Create or Modify System Process	Hijack Execution Flow	Hide Artifacts	Modify Authentication Process	Networl Share D
d Accounts	User Execution	Event Triggered Execution	Process Injection	Hijack Execution Flow	Multi-Factor Authentication Interception	Networl
		External Remote Services	Scheduled Task/Job	Impair Defenses	Multi-Factor Authentication Request Generation	Passwo Policy D
		Hijack Execution Flow	Valid Accounts	Indicator Removal on Host	Network Sniffing	Periphe Device
		Modify			OS Credential	Permiss

ATT&CK TECHNIQUE: HOW THE GOALS ARE ACHIEVED

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Accou Disco
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Debugger Evasion	Brute Force	Applic Windo
External Remote Services	Inter-Process Communication	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Credentials from Password Stores	Brows Disco
Hardware Additions	Native API	Browser Extensions	Create or Modify System Process	Execution Guardrails	Exploitation for Credential Access	Debu
Phishing	Scheduled Task/Job	Compromise Client Software Binary	Event Triggered Execution	Exploitation for Defense Evasion	Forge Web Credentials	File a Disco
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	File and Directory Permissions Modification	Input Capture	Netw Disco
Trusted Relationship	System Services	Create or Modify System Process	Hijack Execution Flow	Hide Artifacts	Modify Authentication Process	Netw Share
Valid Accounts	User Execution	Event Triggered Execution	Process Injection	Hijack Execution Flow	Multi-Factor Authentication Interception	Netw
		External Remote Services	Scheduled Task/Job	Impair Defenses	Multi-Factor Authentication Request Generation	Passw Policy
		Hijack Execution Flow	Valid Accounts	Indicator Removal on Host	Network Sniffing	Periph Devic
		Modify				

MITRE

ATT&CK SUB-TECHNIQUE: MORE SPECIFIC TECHNIQUE

Initial Access	Execution	Persistence	Privilege Escalation	
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Contro
Exploit Public-Facing Application	AppleScript	SSH Authorized Keys	Elevated Execution with Prompt	El wi
External Remote Services	JavaScript	Boot or Logon Autostart Execution	Setuid and Setgid	Se ar
Hardware Additions	Python	Kernel Modules and Extensions	Sudo and Sudo Caching	Su ar
Phishing	Unix Shell	Login Items	Boot or Logon Autostart Execution	Debug
Spearphishing Attachment	Visual Basic	Re-opened Applications	Kernel Modules and Extensions	Deobfu Files o
Spearphishing Link	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Login Items	Execut Guard
Spearphishing via Service	Inter-Process Communication	Login Hook	Re-opened Applications	E K
Supply Chain Compromise	XPC Services	RC Scripts	Boot or Logon Initialization Scripts	Exploit Defens
Compromise Hardware Supply Chain	Native API	Startup Items	Login Hook	File an Permis
Compromise Software Dependencies and Development Tools	Scheduled Task/Job	Browser Extensions	RC Scripts	Li M P

ATT&CK: PROCEDURES

Boot or Logon Autostart Execution: Login Items

Other sub-techniques of Boot or Logon Autostart Execution (14)

ID: T1547.015

Adversaries may add login it
applications, documents, fol
items can be added via a sh
using scripting languages su
`SMLoginItemSetEnabled`.

Login items installed using t
Preferences, and can only be removed by the application that created them. Login items created using a shared file list are visible in System Preferences, can hide the application when it launches, and are executed through LaunchServices, not launchd, to open applications, documents, or URLs without using Finder.[4] Users and applications use login items to configure their user environment to launch commonly used services or applications, such as email, chat, and music applications.

Adversaries can utilize AppleScript and Native API calls to create a login item to spawn malicious executables.[5] Prior to version 10.5 on macOS, adversaries can add login items by using AppleScript to se
Events" process, which has an AppleScript dictionary for manipulating login items.[6]
such as `tell application "System Events" to make login item at end with`
`/path/to/executable`.[7][8] This command adds the path of the malicious executab
in `~/Library/Application Support/com.apple.backgroundtaskmanagementagent`
Adversaries can also use login items to launch executables that can be used to contr
as a means to gain privilege escalation by prompting for user credentials.[10][11][12]

Version Permalink

Procedure Examples

ID	Name	Description
S0281	Dok	Dok uses AppleScript to install a login Item b
S0690	Green Lambert	Green Lambert can add Login Items to establish persistence.[13][14]

Objective-See
a non-profit 501(c)(3) foundation.

Made In America: Green Lambert for OS X

by: Runa Sandvik / October 1, 2021

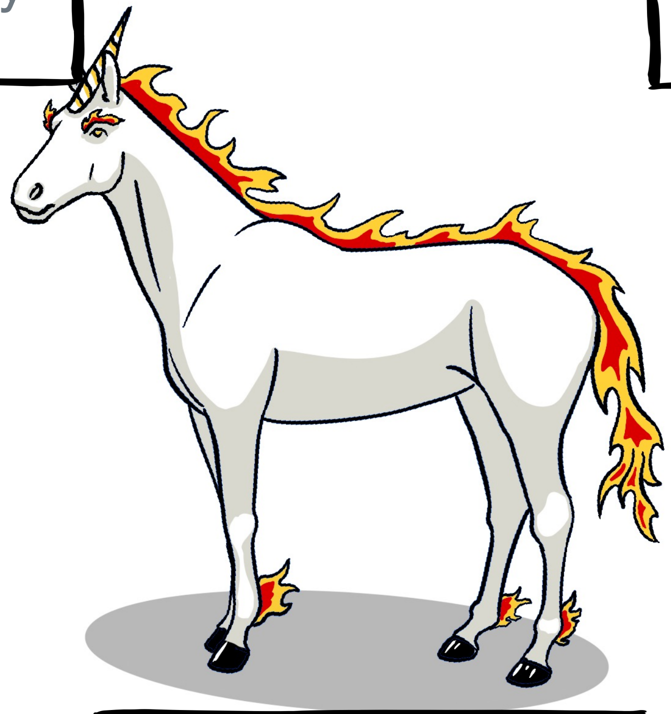
Cast of Characters

Ninja Panda & threads

Drunken Monkey Master

Kung Fu Master

A Pure Unicorn App



Helper Daemons

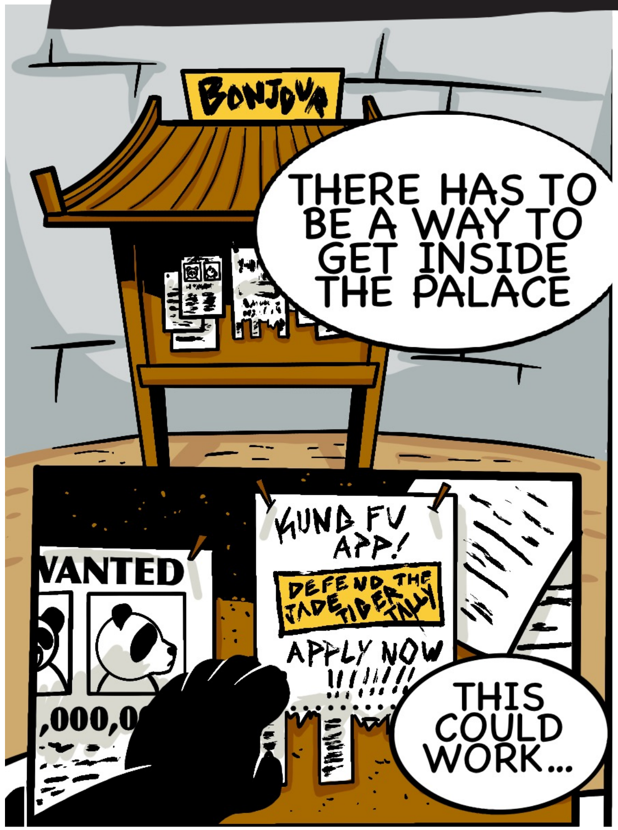
Artwork powered by
@MiscreantsHQ
@coolestcatiknow

MITRE

Discovery

Network Service Discovery - T1046

"Adversaries can use a mDNS query, `dns-sd -B _ssh._tcp .`, to find other systems broadcasting the ssh service."



Artwork powered by
@MiscreantsHQ
@coolestcatiknow

MITRE

Discovery

File and Directory Discovery – T1083

"XCSSETs uses `mdfind` to enumerate a list of apps known to grant screen sharing permissions."

```
set appId to do shell script "mdfind kMDItemCFBundleIdentifier = '" & bundleId & "'"
```

To be continued…

DISCLAIMER
Techniques presented are in draft state for the October ATT&CK release and subject to change.

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

Discovery

File and Directory Discovery – T1083

DISCLAIMER
Techniques presented are in draft state for the October ATT&CK release and subject to change.

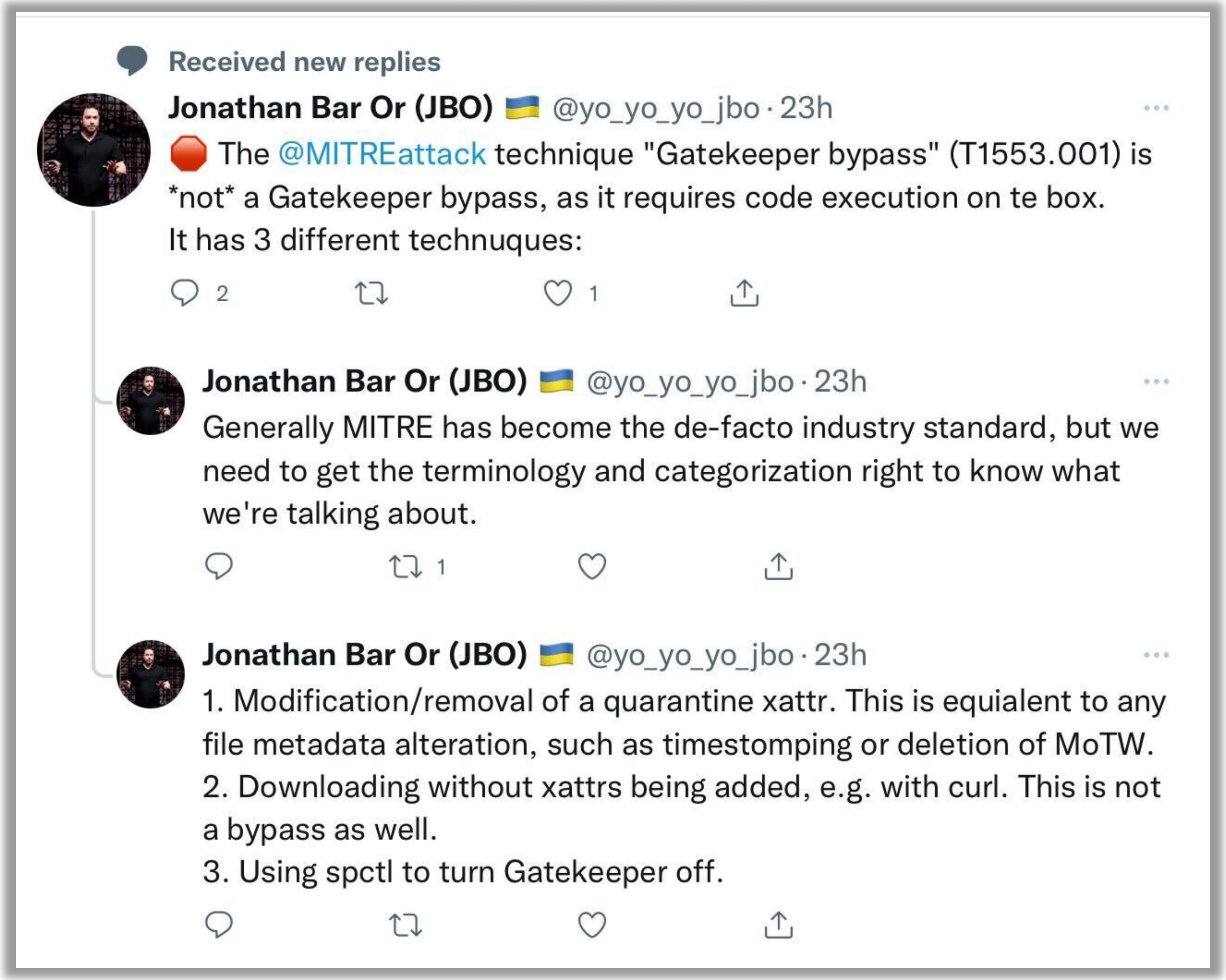
To be continued…

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

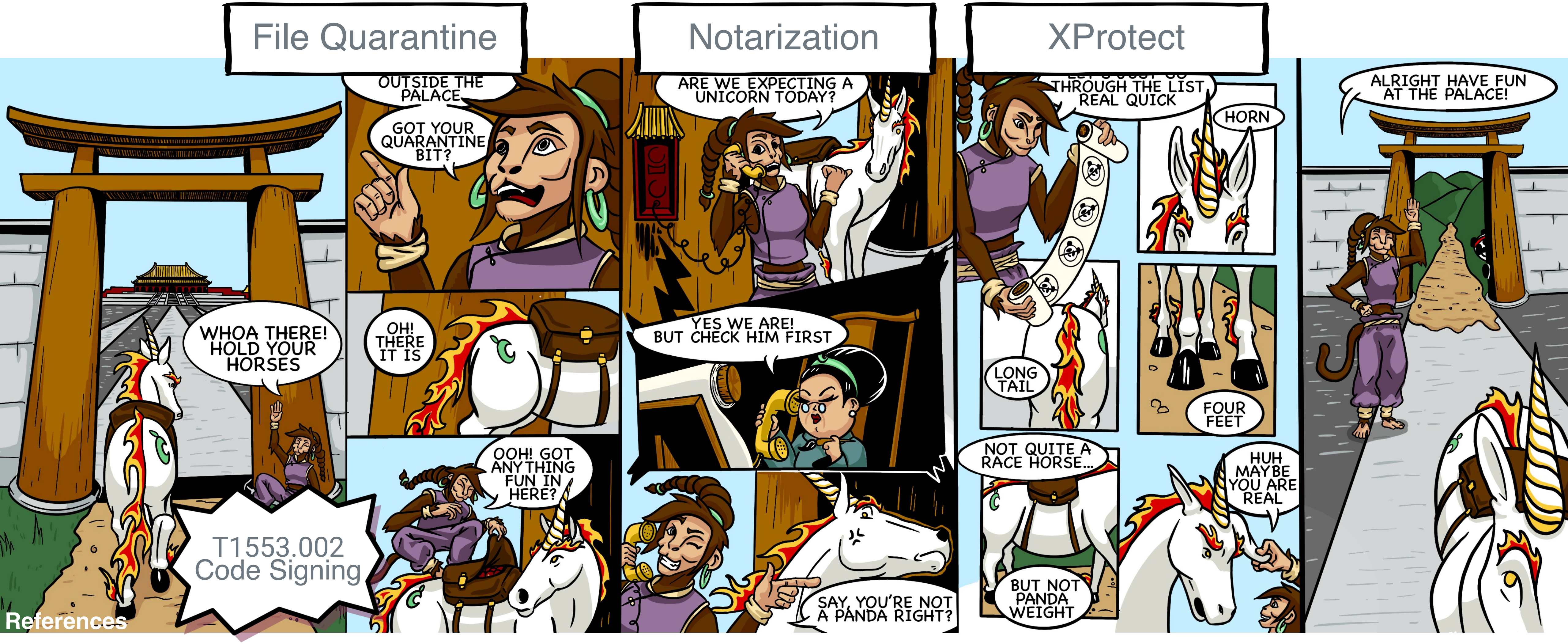
MITRE

Conversations in the Wild - Quarantine

Thank you! 😻



Defense Evasion – From Gatekeeper to XProtect



References

Quarantine process, data locations

Code Signing process, data locations

Notarization process, data locations

Xprotect process, data locations

Artwork powered by @MiscreantsHQ @coolestcatiknow

MITRE

Evading Pandas in the Wild - Quarantine

Gatekeeper Bypass - T1553.001

Subvert Trust Controls: Gatekeeper Bypass

Other sub-techniques of Subvert Trust Controls (6)

Adversaries may modify file attributes that signify programs are from untrusted sources to subvert Gatekeeper controls in macOS. When documents, applications, or programs are downloaded an extended attribute (xattr) called `com.apple.quarantine` can be set on the file by the application performing the download. T s attribute, also known as a quarantine flag, is read by Apple's

ID: T1553.001

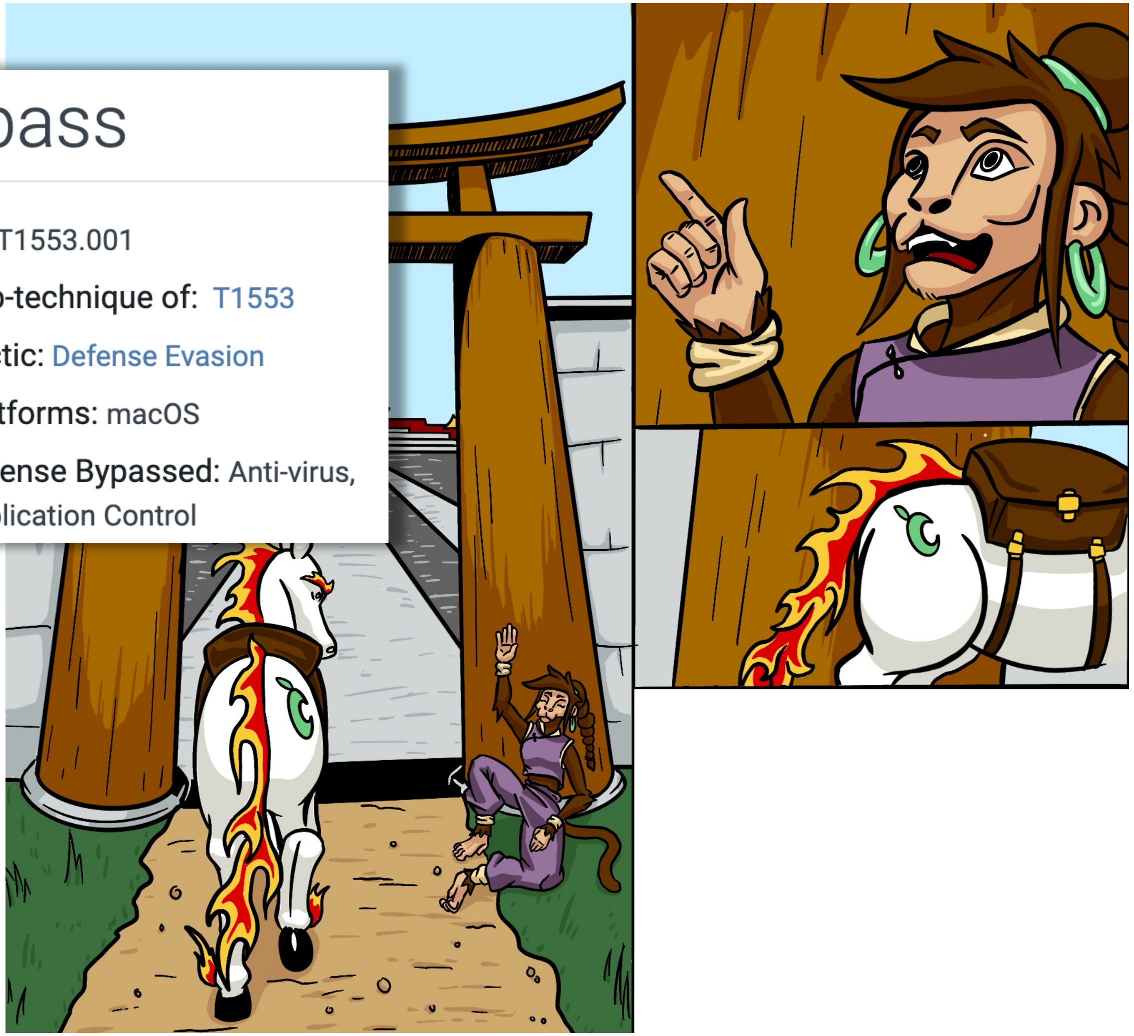
Sub-technique of: T1553

ⓘ Tactic: Defense Evasion

ⓘ Platforms: macOS

ⓘ Defense Bypassed: Anti-virus, Application Control

Focus on Extended Attributes

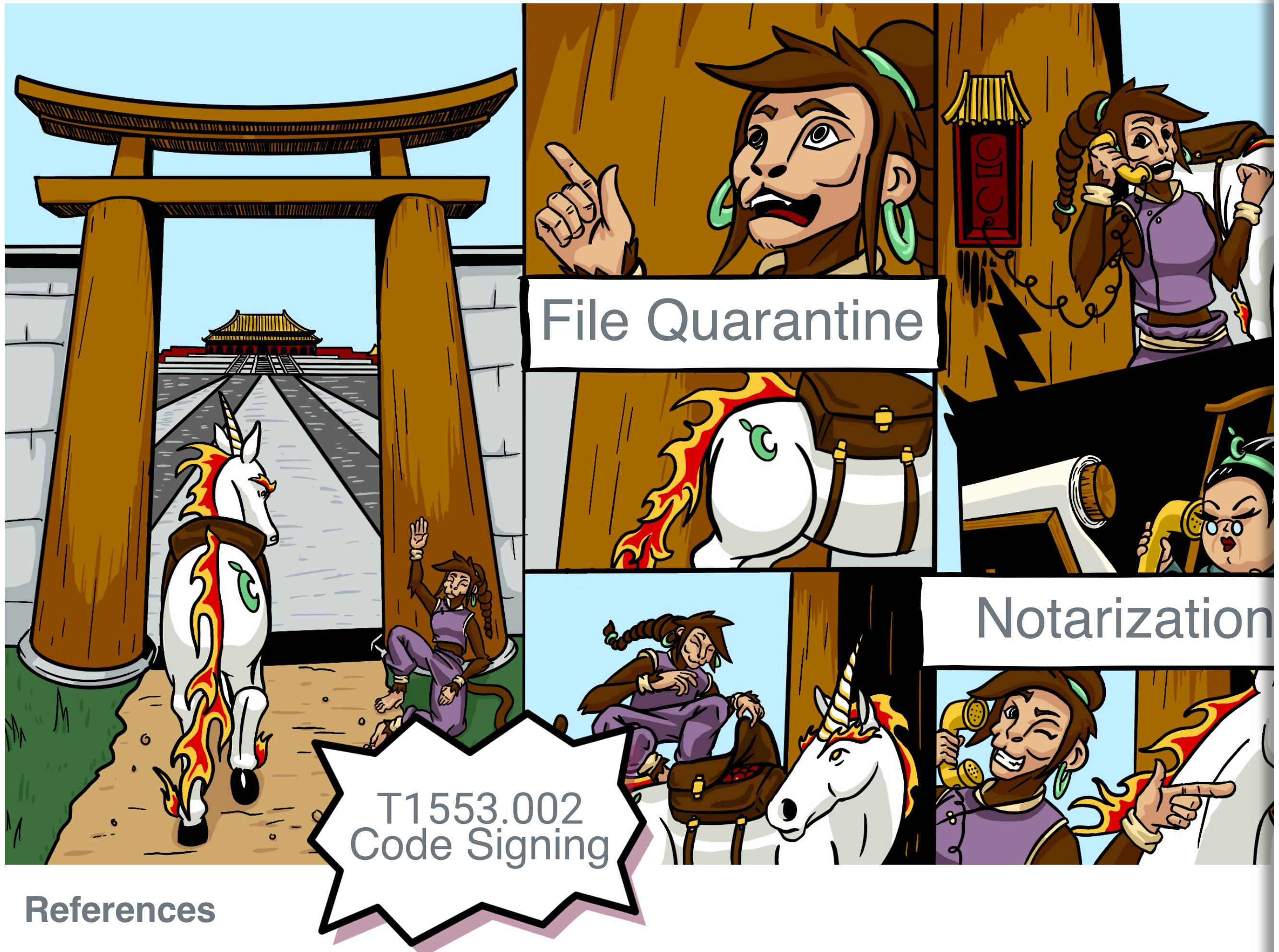


References

Quarantine Breakdown, DB locations and Executables , Adversary Usage

Evading Pandas in the Wild – Gatekeeper Bypass

Gatekeeper Bypass - T1553.001



Subvert Trust Controls: Gatekeeper Bypass

Other sub-techniques of Subvert Trust Controls (7)

Adversaries may modify file attribu... user prompts and gain execution... of Apple's security model to ensu... Gatekeeper was built on top of F... grown to include Code Signing, s... Gatekeeper treats applications... applications.[1][2]

Based on an opt-in system, when ...nded attribute (xattr) called com.apple.quarantine can be set on the file... performing the download, also known as a quarantine flag. La...ens the application in a suspended state. For first run applications with ...antine flag set, Gatekeeper executes the following functions:

1. Checks extended attribute – ...eeper checks for the quarantine flag, then provides an alert prompt to the user to allow or deny execution.[3][4]
2. Checks System Policies - Checks the Gatekeeper's security policy, Allow app... downloaded from, (options are App Store or App Store and identified developers`).
3. Code Signing – Checks for a valid code signature from an Apple Developer ID.
4. Notarization - Using the api.apple-cloudkit.com API, Gatekeeper reaches out to Apple servers to verify or pull down the notarization ticket and ensure it's not revoked. User can override notarization which will result in a prompt of executing an "unauthorized app" and the security policy will be modified.

ID: T1553.001
Sub-techniqu...
Tactic: Defen...
Platforms: m...
Defense Byp...
Application C...
Contributors...
@PartyD0lphi...
Version: 2.0
Created: 05 F...
Last Modifie...

Focus on components

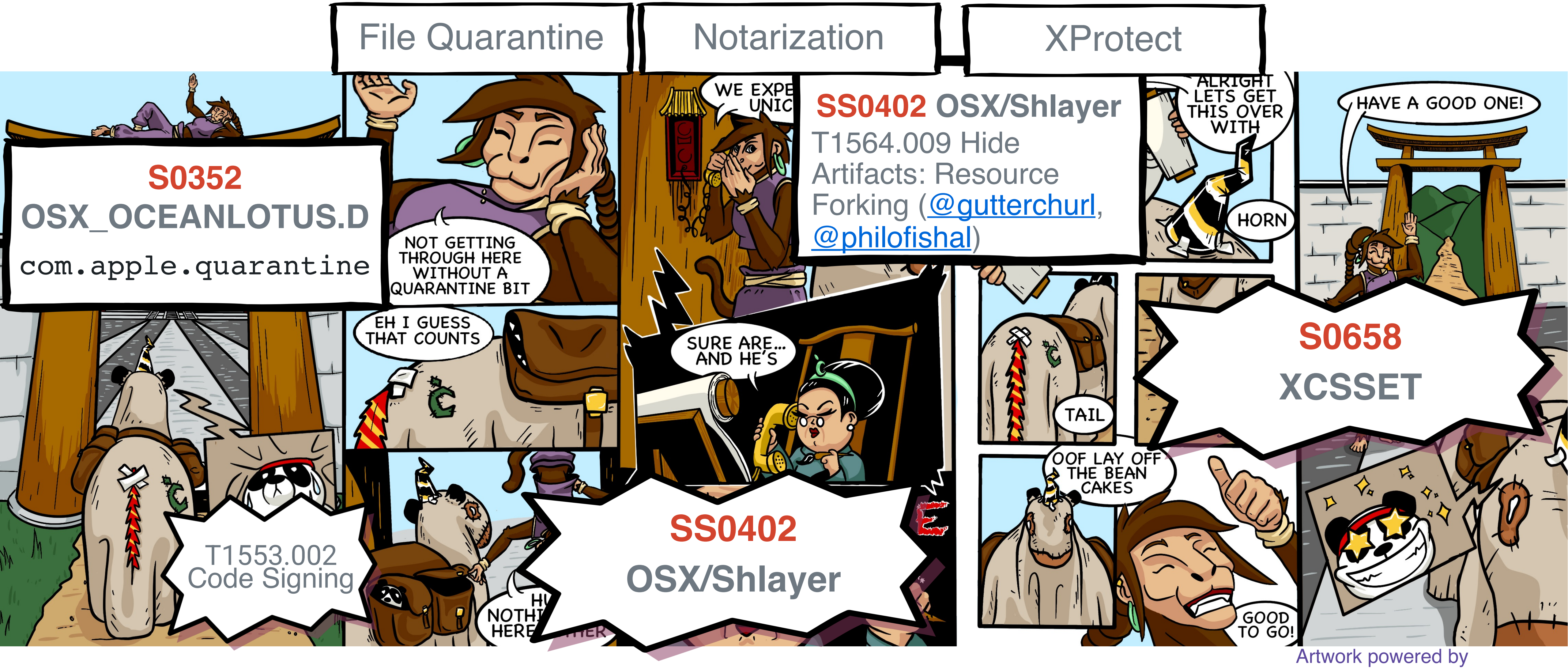
DISCLAIMER
Techniques presented are in draft state for the October ATT&CK release and subject to change.

References

Quarantine Breakdown, DB locations and Executables , Adversary Usage

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

Quarantine Evading Pandas in the Wild



Artwork powered by
@MiscreantsHQ
@coolestcatiknow

MITRE

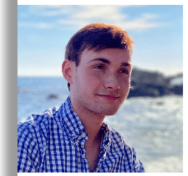
Quarantine Evading Pandas in the Wild

File Quarantine	Notarization	XProtect

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

Conversations in the Wild – Application Bundle Manipulation

Thank you!



RESOURCES • BLOG

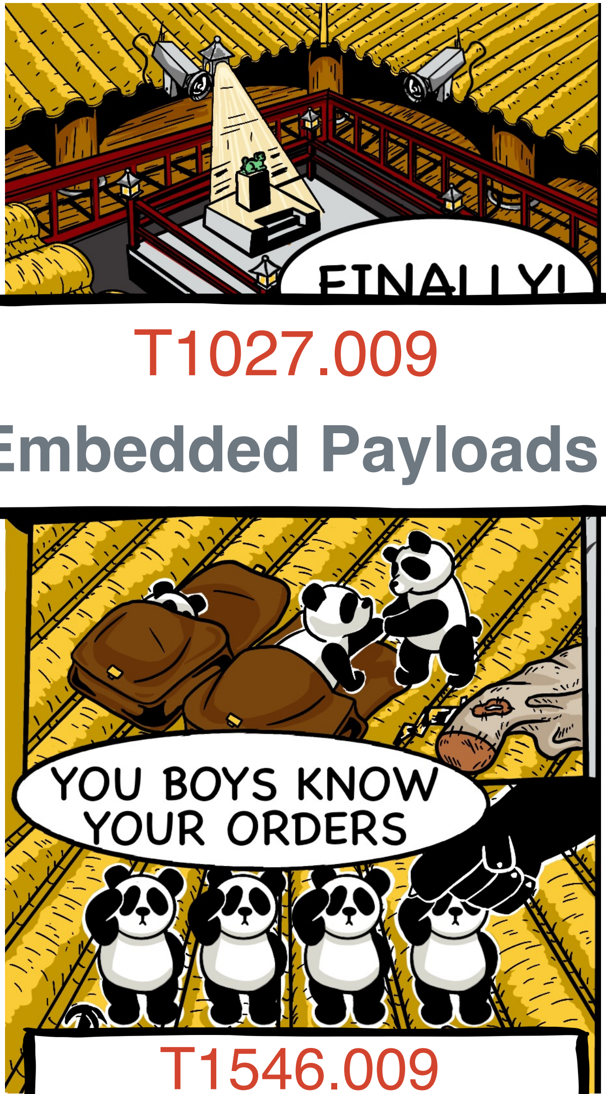
THREAT DETECTION

A bundle of nerves: Tweaking macOS security controls to thwart application bundle manipulation

Adversaries commonly manipulate application bundles to subvert security controls, elevate privileges, and install malware on macOS devices. Here's what you can do about it.

BRANDON DALTON

Evading Pandas in the Wild



T1027.009
Embedded Payloads

T1546.009
Stripped Payloads

DISCLAIMER
Techniques presented are in draft state for the October ATT&CK release and subject to change.

Obfuscated Files or Information: Embedded Payloads

Other sub-techniques of Obfuscated Files or Information (9)

Adversaries may embed payloads within files to conceal malicious content from defensive and analysis tools. By embedding payloads in otherwise seemingly benign files (such as scripts and executables), adversaries may obfuscate their malicious conte… Embedded payloads may also allow adversaries to Subvert Trust Controls without impacting digital signatures, notarization ticke… or other execution controls.[1]

ID: T1027.0…
Sub-techni…
T1027
ⓘTactic: Defe…
ⓘPlatforms:

S1048
macOS.OSAMiner

References

[SentinelLABS FADE DEAD]()

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

Evading Pandas in the Wild

T1027.009
Embedded Payloads

T1546.009
Stripped Payloads

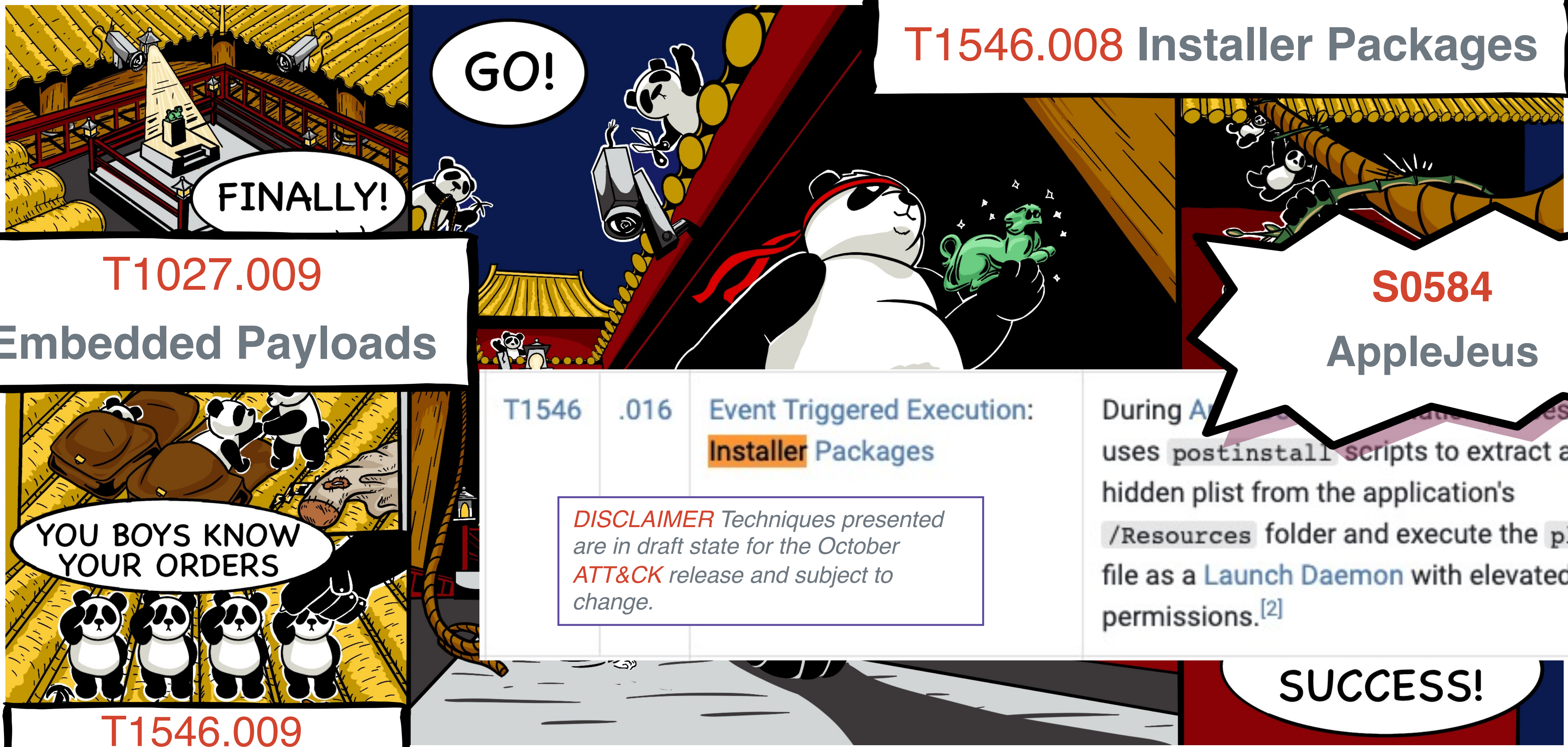
T1546.008
Installer Packages

DISCLAIMER Techniques presented are in draft state for the October ATT&CK release and subject to change.

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

MITRE

Evading Pandas in the Wild



T1546.008 Installer Packages

T1027.009 Embedded Payloads

S0584 AppleJeus

T1546	.016	Event Triggered Execution: Installer Packages	During A ... ess, it uses `postinstall` scripts to extract a hidden plist from the application's `/Resources` folder and execute the `plist` file as a Launch Daemon with elevated permissions.[2]

DISCLAIMER Techniques presented are in draft state for the October ATT&CK release and subject to change.

T1546.009 Stripped Payloads

References

[Cybersecurity and Infrastructure Security Agency (CISA) Report]

Artwork powered by
@MiscreantsHQ
@coolestcatiknow

Takeaways

- ATT&CK == Community Driven
- not in ATT&CK != not in the wild
- Pattern of cross-platform languages
- 🍎 Roadmap for Gatekeeper 🙏
- 🙏 Howard Oakley, Phil Stokes, & many more

Cat Self

@coolestcatiknow

attack@mitre.org