Recorded Future®
Sandbox

Malware Analysis Report

2025-10-10 10:04

Sample ID	251010-lyh3watjw6
Target	IMG_0118.JPG
SHA256	b951ec03a58100ff2a8781191312af1d164646f67b7ea42f0dbc76ea15b904a9
Tags	defense_evasion execution persistence

Table of Contents

Part 1. Analysis Overview

SHA256
b951ec03a58100ff2a8781191312af1d164646f67b7ea42f0dbc76ea15b904a9

Threat Level: Likely benign

The file IMG_0118.JPG was found to be: Likely benign.

Malicious Activity Summary

defense_evasion	execution	persistence

Launch Agent

Resource Forking

Launchctl

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043		
Resource Development TA0042		
Initial Access TA0001		
Execution **TA0002**	System Services T1569	
	Launchctl	T1569.001
Persistence **TA0003**	Create or Modify System … T1543	
	Launch Agent	T1543.001
Privilege Escalation **TA0004**	Create or Modify System … T1543	
	Launch Agent	T1543.001
Defense Evasion **TA0005**	Hide Artifacts T1564	
	Resource Forking	T1564.009
Credential Access TA0006		
Discovery TA0007		
Lateral Movement TA0008		
Collection TA0009		
Command and Control TA0011		
Exfiltration TA0010		
Impact TA0040		

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-10 09:56

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-10 09:56	2025-10-10 09:59	macos-20250619-es	108s	152s

4. 2. Command Line

```
[sh -c sudo /bin/zsh -c "/Users/run/IMG_0118.jpg"]
```

4. 3. Signatures

Launch Agent

persistence

Resource Forking

defense_evasion

Description	Indicator	Process	Target
N/A	/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer	N/A	N/A
N/A	"/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater" -bgcheck	N/A	N/A
N/A	/System/Library/Frameworks/Quartz.framework/Frameworks/QuickLookUI.framework/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper	N/A	N/A
N/A	/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storeuid.app/Contents/MacOS/storeuid	N/A	N/A
N/A	/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storedownloadd	N/A	N/A

Launchctl

execution

Description	Indicator	Process	Target
N/A	/bin/launchctl load /Library/LaunchAgents/com.microsoft.update.agent.plist	N/A	N/A

4. 4. Processes

/bin/sh

```
[sh –c sudo /bin/zsh –c "/Users/run/IMG_0118.jpg"]
```

/bin/bash

```
[sh –c sudo /bin/zsh –c "/Users/run/IMG_0118.jpg"]
```

/usr/bin/sudo

```
[sudo /bin/zsh –c /Users/run/IMG_0118.jpg]
```

/System/Library/PrivateFrameworks/SpeechObjects.framework/Versions/A/SpeechDataInstallerd.app/Contents/MacOS/SpeechDataInstallerd

```
[/System/Library/PrivateFrameworks/SpeechObjects.framework/Versions/A/SpeechDataInstallerd.app/Contents/MacOS/SpeechDataInstallerd]
```

/System/Library/CoreServices/Applications/Feedback Assistant.app/Contents/Library/LaunchServices/seedusaged

```
[/System/Library/CoreServices/Applications/Feedback Assistant.app/Contents/Library/LaunchServices/seedusaged]
```

/usr/libexec/pkreporter

```
[/usr/libexec/pkreporter]
```

/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer
[/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer]

/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater
[/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater -bgcheck]

/bin/zsh
[/bin/zsh -c /Users/run/IMG_0118.jpg]

/Users/run/IMG_0118.jpg
[/Users/run/IMG_0118.jpg]

/usr/libexec/xpcproxy
[xpcproxy com.apple.quicklook.ui.helper]

/System/Library/Frameworks/Quartz.framework/Frameworks/QuickLookUI.framework/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper
[/System/Library/Frameworks/Quartz.framework/Frameworks/QuickLookUI.framework/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper]

/usr/libexec/xpcproxy
[xpcproxy com.apple.xpc.launchd.oneshot.0x10000001.Microsoft Word]

/Applications/Microsoft Word.app/Contents/MacOS/Microsoft Word
[/Applications/Microsoft Word.app/Contents/MacOS/Microsoft Word -psn_0_147492]

/usr/libexec/xpcproxy
[xpcproxy com.apple.XprotectFramework.AnalysisService 493]

/System/Library/PrivateFrameworks/XprotectFramework.framework/Versions/A/XPCServices/XprotectService.xpc/Contents/MacOS/XprotectService
[/System/Library/PrivateFrameworks/XprotectFramework.framework/Versions/A/XPCServices/XprotectService.xpc/Contents/MacOS/XprotectService]

/usr/libexec/xpcproxy
[xpcproxy com.apple.storeuid]

/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storeuid.app/Contents/MacOS/storeuid
[/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storeuid.app/Contents/MacOS/storeuid]

/usr/libexec/xpcproxy
[xpcproxy com.apple.spindump]

/usr/sbin/spindump
[/usr/sbin/spindump]

/usr/libexec/xpcproxy
[xpcproxy com.apple.spindump_agent]

/usr/libexec/spindump_agent
[/usr/libexec/spindump_agent]

/usr/libexec/xpcproxy
[xpcproxy com.apple.storedownloadd]

/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storedownloadd
[/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/storedownloadd]

/usr/libexec/xpcproxy
[xpcproxy com.apple.metadata.mdwrite]

/usr/libexec/xpcproxy
[xpcproxy com.apple.ReportMemoryException]

/usr/libexec/ReportMemoryException

```
[/usr/libexec/ReportMemoryException]
```

/usr/libexec/xpcproxy

```
[xpcproxy com.microsoft.autoupdate.fba.2660]
```

/Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS/Microsoft Update Assistant.app/Contents/MacOS/Microsoft Update Assistant

```
[/Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS/Microsoft Update Assistant.app/Contents/MacOS/Microsoft Update Assistant]
```

/bin/launchctl

```
[/bin/launchctl list]
```

/usr/libexec/xpcproxy

```
[xpcproxy com.microsoft.autoupdate.helper]
```

/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper

```
[/Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper]
```

/bin/launchctl

```
[/bin/launchctl load /Library/LaunchAgents/com.microsoft.update.agent.plist]
```

/usr/bin/codesign

```
[/usr/bin/codesign -v /Library/PrivilegedHelperTools/com.microsoft.autoupdate.helper]
```

/usr/libexec/xpcproxy

```
[xpcproxy com.apple.StreamingUnzipService 199]
```

/System/Library/PrivateFrameworks/StreamingZip.framework/Versions/A/XPCServices/com.apple.StreamingUnzipService.xpc/Contents/MacOS/com.apple.StreamingUnzipService

```
[/System/Library/PrivateFrameworks/StreamingZip.framework/Versions/A/XPCServices/com.apple.StreamingUnzipService.xpc/Contents/MacOS/com.apple.StreamingUnzipService]
```

/usr/libexec/xpcproxy

```
[xpcproxy com.apple.quicklook.QuickLookUIService 308]
```

/System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/XPCServices/QuickLookUIService.xpc/Contents/MacOS/QuickLookUIService

```
[/System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/XPCServices/QuickLookUIService.xpc/Contents/MacOS/QuickLookUIService]
```

/usr/libexec/xpcproxy

```
[xpcproxy com.apple.DictionaryServiceHelper]
```

/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/DictionaryServices.framework/Versions/A/XPCServices/com.apple.DictionaryServiceHelper.xpc/Contents/MacOS/com.apple.DictionaryServiceHelper

```
[/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/DictionaryServices.framework/Versions/A/XPCServices/com.apple.DictionaryServiceHelper.xpc/Contents/MacOS/com.apple.DictionaryServiceHelper]
```

4. 5. Network

Country	Destination	Domain	Proto
N/A	224.0.0.251:5353		udp
US	8.8.8.8:53	www.microsoft.com	udp
US	8.8.8.8:53	ecs.office.com	udp
US	52.123.129.14:443	ecs.office.com	tcp
US	8.8.8.8:53	odc.officeapps.live.com	udp
FR	52.109.68.130:443	odc.officeapps.live.com	tcp
US	8.8.8.8:53	metadata.templates.cdn.office.net	udp
GB	23.1.228.180:443	metadata.templates.cdn.office.net	tcp
US	8.8.8.8:53	binaries.templates.cdn.office.net	udp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp

IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.19:443	binaries.templates.cdn.office.net	tcp
US	8.8.8.8:53	roaming.svc.cloud.microsoft	udp
GB	52.109.28.47:443	roaming.svc.cloud.microsoft	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
IT	92.123.106.73:443	binaries.templates.cdn.office.net	tcp
US	8.8.8.8:53	messaging.engagement.office.com	udp
FR	52.111.231.13:443	messaging.engagement.office.com	tcp
US	8.8.8.8:53	ocsp.edge.digicert.com	udp
GB	104.78.173.167:80	ocsp.edge.digicert.com	tcp
US	8.8.8.8:53	itunes.apple.com	udp
GB	104.78.173.167:80	ocsp.edge.digicert.com	tcp

US	8.8.8.8:53	api2.smoot.apple.com	udp
ES	51.92.110.33:443	api2.smoot.apple.com	tcp
GB	104.78.173.167:80	ocsp.edge.digicert.com	tcp
US	8.8.8.8:53	cdn2.smoot.apple.com	udp
US	8.8.8.8:53	cdn.smoot.g.aaplimg.com	udp
DE	17.253.15.198:443	cdn2.smoot.apple.com	tcp
DE	17.253.15.198:443	cdn2.smoot.apple.com	tcp
DE	17.253.15.198:443	cdn2.smoot.apple.com	tcp
DE	17.253.15.198:443	cdn2.smoot.apple.com	tcp

4. 6. Files

/var/folders/pq/yy2b5ptn4cz739jgclj4m1wm0000gp/C/com.microsoft.Word//mds/mdsObject.db

MD5	d3a1859e6ec593505cc882e6def48fc8
SHA1	f8e6728e3e9de477a75706faa95cead9ce13cb32
SHA256	3ebafa97782204a4a1d75cfec22e15fcdeab45b65bab3b3e65508707e034a16c
SHA512	ea2a749b105759ea33408186b417359deffb4a3a5ed0533cb26b459c16bb3524d67ede5c9cf0d5098921c0c0a9313fb9c2672f1e5ba48810eda548fa3209e818

/var/folders/pq/yy2b5ptn4cz739jgclj4m1wm0000gp/C/com.microsoft.Word//mds/mdsDirectory.db

MD5	0e4a0d1ceb2af6f0f8d0167ce77be2d3
SHA1	414ba4c1dc5fc8bf53d550e296fd6f5ad669918c
SHA256	cca093bcfc65e25dd77c849866e110df72526dffbe29d76e11e29c7d888a4030
SHA512	1dc5282d27c49a4b6f921ba5dfc88b8c1d32289df00dd866f9ac6669a5a8d99afeda614bffc7cf61a44375ae73e09cd52606b443b63636977c9cd2ef4fa68a20

/Users/run/Library/Group Containers/UBF8T346G9.Office/FontCache/4/PreviewFont/hier_officeFontsPreview_4_42.ttf

MD5	fc535e45902a11516430770d47ed4183
SHA1	32ee7d71c2a7916d05f02b20e2d971198adb0c79
SHA256	4c41e4bc290496111489622fb119392b393b2a61f3b588f64c65ebd4368ed7db
SHA512	9781465e1655a72ce927615e45ef2b66001cd0946c26190b40b990bcb1f3228fc838218e69054136aa6b3cc9a0224eed1c91b81f5c4491678c6b5c127f249cce

/Users/run/Library/Containers/com.microsoft.Word/Data/Library/Application Support/Microsoft/Office/16.0/DTS/es-ES{0F56B789-596E-7847-80ED-AE95EF5455E1}/{82E84863-5012-FD41-AC7E-5A5A73719F45}mm10002086.png

MD5	2a7a2d7bfc6dd81e291517b3e023e243
SHA1	56680b5fa25e0095cf65ccd4f2a19b5ee8279115
SHA256	9b070c0a85603ec4fe95be374407d60162bd7750e9892fb5810866bb3834594b
SHA512	646b1f39bc50ff243d639e7a81b5bcfab7a284ba5f3bf682f2da58d294d0f2aaba0d0b1ba8cc93fc56a698647181ff39e580df445682ff3bcd28ceda3b967ec6

/Users/run/Library/Containers/com.microsoft.Word/Data/Library/Application Support/Microsoft/Office/16.0/DTS/es-ES{0F56B789-596E-7847-80ED-AE95EF5455E1}/{BF65623A-9FCF-9A40-9638-55FA210B0F2F}mm16382964.png

MD5	c2303ab94ae96f316a1b22de215d460b
SHA1	c4d6ccb52a967a6df17ad1b74801902f92a25f19
SHA256	dd887d16e44a4793e1b4595b7e0ada78ced622971a8d1b35bc3270dd9cda3556
SHA512	6f4834ccb081dabf3fcf5d7d38e0cba500e9e608fb963a64f4189060169fd95928583c3fd0b009485b532b3846f4170246b4473e48a9a834bd805b30853a1fa3

/Users/run/Library/Containers/com.microsoft.Word/Data/Library/Application Support/Microsoft/Office/16.0/DTS/es-ES{0F56B789-596E-7847-80ED-AE95EF5455E1}/{A54E43B3-9901-F44B-AACF-CA831E3C879E}mm16382944.png

MD5	27a6c9bfd043a91fe819853defe9dcfa
SHA1	f37ed54b242460031c469a05900c30169ed4c63e
SHA256	2f293980fa3b67beedec3ca221745c7fd9f456ea7042e1915a2054c728863dee
SHA512	8e2bf84a1fae941119b6937ddd07667fa6534a80b8e041c77cdca3373da14012dd2482f4465d3ad1b2e52d6bc92fcbe824c1fa954df9a65cd018f31829eb9911

/Users/run/Library/Containers/com.microsoft.Word/Data/Library/Application Support/Microsoft/Office/16.0/DTS/es-ES{0F56B789-596E-7847-80ED-AE95EF5455E1}/{8778E0D5-BFF3-B04B-AC19-69E5D32F8F18}mm16392740.png

MD5	5de3a142f4b2b57e117eecd14650db72
SHA1	7e2a892fe73391c9b81a895bf7e2314932758af5
SHA256	990deea80e15ceb51712509d02a1b9c1ba5bbcf8e99d65f4e8aba69943751650
SHA512	edb263ebcb7a8864b24dae58b4a0ad06d79cca70b96b778c11cf44ac133aa027420834ec37624f765960d5685ea82041a2402e5548ceaf0cade93ae09943de45

/Users/run/Library/Containers/com.microsoft.Word/Data/Library/Application Support/Microsoft/Office/16.0/microsoft word_Rules.xml

MD5	fd300ef58e2c4676ecd38ef6087d3b6a
SHA1	b8670a6bef3f1bfc084764c044087fcaf566c9c7
SHA256	cb598745eb753980f284741b4ba15dd21f225e4055173df4b83d7b45c4968d1a
SHA512	1bae225911a8f7a170ef8e5f8741dcf93f88debcb5b5e7af4da784d0eb96b391b9a28a664248127b6521d4e698a431d1e870c1c8b0a1e748e16054235acb600e

/Users/run/Library/Group Containers/UBF8T346G9.Office/Custom Dictionary

MD5	4c0026d2e0b7e24f4fe44470b563440b
SHA1	eeb842992f2a0464c356b5830997872c5b4c2b1a
SHA256	a1a4fd395f687d8656c8c452d19c76f10b58ea77419dd806b93dda03b75d6cd5
SHA512	c50fecf92c1fef0c82ae837e0ddb112381a6f7f454d0a310426f1094a2519c871736f1e26dd25ec646fe99d76eabd58086d79c8b0e5df72aed5c737430b9a00d

/Users/run/Library/Group Containers/UBF8T346G9.Office/Custom Dictionary

MD5	d00a463249b97d4de479cd6dfde36247
SHA1	442f522811b8d1d01e76053daecf12fb9aaa3a9d
SHA256	fc4a620c7f894547f21bce28d02c31e022c40cd95d5401f905b749cf934a117d
SHA512	99102ead513c6d6144a6bd2ce8f5061946f6a57bb445067cdb673c45ec52a81e6b53c401008b5c21726505d6a7e71d94e1ba775f703ee0877b47eeb75be289bf

/var/folders/pq/yy2b5ptn4cz739jgclj4m1wm0000gp/T/TelemetryUploadFilecom.microsoft.autoupdate.fba.txt

MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e