MAC İşletim Sisteminde Olay Müdahale

Olay Müdahale Nedir?

- Olay müdahale, bir güvenlik ihlali veya olay meydana geldiğinde bu olayı tespit etme, yanıt verme ve olayın etkilerini en aza indirerek sistemi normale döndürme süreçlerini kapsar. Bu süreç, yalnızca olay anında yapılan müdahalelerle sınırlı değildir. Aynı zamanda olay sonrası analizleri ve gelecekte benzer olayların önlenmesi için alınacak önlemleri de içerir.

Mac İşletim Sisteminde Olay Müdahalesinin Önemi

- Statcounter'ın son verilerine göre, Apple macOS, masaüstü bilgisayarların yaklaşık %15'ini oluşturuyor.

- Mac işletim sistemleri, uzun süre güvenli kabul edilse de, artan kullanıcı sayısı ve popülaritesi nedeniyle artık daha fazla siber tehditlere maruz kalıyor. Zararlı yazılımlar, fidye yazılımları ve diğer siber tehditler Mac kullanıcıları için ciddi riskler oluşturuyor. Bu nedenle, Mac kullanıcıları ve sistem yöneticileri güvenlik olaylarına karşı hazırlıklı olmalı ve etkin bir müdahale planıyla bu tehditlere karşı koymalıdır.

Olay Müdahale Süreci

- Olay müdahale süreci, bir güvenlik olayının tespit edilmesinden kurtarma aşamasına kadar bir dizi adımdan oluşur. Bu süreç, olayın etkilerini en aza indirmeyi ve gelecekte benzer olayların yaşanmasını önlemeyi amaçlar.

- Olay müdahalesinin ilk adımı, güvenlik olaylarının tespit edilmesidir. MacOS'ta, anormal aktiviteleri ve potansiyel tehditleri erken tespit etmek için Activity Monitor ve Console gibi yerleşik araçlar kullanılabilir. Bu araçlar, sistem performansını izleyerek şüpheli süreçleri ve olayları hızlıca tespit etmeye yardımcı olur.

- Bir güvenlik olayı tespit edildiğinde, olayın ciddiyetinin ve etkilediği sistem bileşenlerinin hızlıca değerlendirilmesi gerekir. Ciddi bir tehdit durumunda, etkilenen sistemin izole edilmesi ve ağ bağlantısının kesilmesi gibi önlemler alınmalıdır.

- Olayın izolasyonu sonrasında, derinlemesine analiz yapılır. Bu analiz, olayın kök nedenini ve etkilediği tüm dosya ve sistem bileşenlerini belirler. Terminal komutları ve log incelemeleri bu aşamada önemli rol oynar. Ayrıca, üçüncü parti güvenlik yazılımları da zararlı yazılımların tespiti ve temizlenmesine yardımcı olabilir.

- Olay müdahalesinin son aşaması, müdahale ve kurtarma sürecidir. Bu süreçte, güvenlik açıkları kapatılır, etkilenen sistemler temizlenir ve gerekirse yedeklerden geri yükleme işlemleri gerçekleştirilir. Sistem normale döndürülerek, gelecekte benzer olayların yaşanmaması için gerekli önlemler alınır.
- Olay müdahalesi, sürekli bir öğrenme ve gelişim sürecidir. Bu süreçte elde edilen bilgiler, gelecekteki olaylara karşı hazırlıklı olunmasını sağlar ve kullanıcıların güvenlik farkındalığını artırır.
- Sonuç olarak, MacOS'ta olay müdahalesi, sistem güvenliğinin temel taşlarından biridir. Proaktif güvenlik önlemleri almak, düzenli güncellemeler yapmak ve etkin bir olay müdahale planı oluşturmak, kullanıcıların ve sistem yöneticilerinin güvenlik tehditlerine karşı daha hazırlıklı olmalarını sağlar. Güvenli bir dijital ortam yaratmak için, bu süreçlerin düzenli olarak gözden geçirilmesi ve güncellenmesi kritik önem taşır.

Kullanılan Araçlar ve Komutlar

Olay müdahalesi sürecinde, çeşitli araçlar ve komutlar kullanılır. İşte bu süreçte kullanabileceğiniz bazı önemli araçlar ve komutlar:

Activity Monitor: Sistem kaynaklarını izlemek ve anormal aktiviteleri tespit etmek için kullanılır. CPU, bellek ve disk kullanımını izleyerek şüpheli süreçleri belirler.

Console: Sistem loglarını ve hataları incelemek için kullanılır. Güvenlik olaylarının zaman çizelgesini çıkarmak ve analiz etmek için önemlidir.

Terminal Komutları:

- ps aux: Aktif süreçleri listeler.
- lsof -i: Ağ bağlantılarını listeler.
- netstat: Ağ istatistiklerini gösterir.
- sudo fs_usage: Dosya sistemini izler.
- sudo lsof: Açık dosyaları ve ağ bağlantılarını gösterir.

Örnek Olaylar

Örnek Olay 1: Wirenet Zararlı Yazılımı

- **Tespit:** Şüpheli plist dosyası ve işlem.
- **Analiz:** Dosya ve ağ bağlantılarının incelenmesi.
- **İçeri Alma:** İşlemin durdurulması ve ağ bağlantısının kesilmesi.
- **Ortadan Kaldırma:** Zararlı dosyaların ve plistlerin silinmesi.
- **Kurtarma:** Sistemin yedekten geri yüklenmesi ve güncellemeler.

Örnek Olay 2: Mokes Zararlı Yazılımı

- **Tespit:** Şüpheli süreç ve ağ bağlantısı.
- **Analiz:** Dosya izinleri ve ağ bağlantılarının incelenmesi.
- **İçeri Alma:** İşlemin durdurulması.
- **Ortadan Kaldırma:** Zararlı yazılımın manuel olarak temizlenmesi.
- **Kurtarma:** Güvenlik yamalarının uygulanması.

Wirenet

- Wirenet, macOS için tasarlanmış kötü amaçlı yazılımdır. Bu zararlı yazılım, bilgisayar korsanlarının macOS işletim sistemine sahip cihazları hedef almak için kullandığı bir araçtır.
- Wirenet, diğer adıyla NetWire veya NetWeird, genellikle bir backdoor olarak bilinir. Bu zararlı yazılım, 2019 yılında Firefox'un Zero-Day saldırısı sırasında Coinbase'i hedef alan saldırılar ile birlikte yeniden ortaya çıkmıştır.
- Wirenet, kullanıcıların klavye girişlerini izleyerek ve bu bilgileri uzak bir sunucuya ileterek hassas verileri çalabilir. Ayrıca, ekran görüntülerini çekebilir ve sistem bilgilerini toplayabilir.

Şüpheli Davranışların Belirlenmesi

Bu adımda, sistemde çalışan işlemleri ve bu işlemlerin kaynağını belirleyin. Özellikle şüpheli görünen işlemleri ve Launch Agents'ları inceleyin.

NOT:
"Launch Agents" macOS işletim sisteminde, belirli uygulamaların veya komutların kullanıcı oturumu açıldığında otomatik olarak çalışmasını sağlayan küçük yapılandırma dosyalarıdır. Bu dosyalar, sistem ve kullanıcı düzeyinde otomatik başlatma işlemlerini düzenler.

- suspicious_behaviors.txt
  - Process with PID 529 running from a hidden folder
  - Launch agent named com.mac.host.plist
  - Are these related? 🤔

```
Suspicious processes
----------------------------
  529 /Users/test/.defaults/
Finder.app/Contents/MacOS/Finder

Suspicious agents & daemons
----------------------------
/Users/test/Library/LaunchAgents/
com.mac.host.plist
```

Şüpheli İşlemler ve Launch Agents:
PID 529 ile Çalışan İşlem:
•Bu işlem, /Users/test/.defaults/Finder.app/Contents/MacOS/Finder yolunda çalıştırılıyor. Bu, normalde Finder uygulamasının çalıştırılmaması gereken bir yoldur, bu yüzden şüphelidir.

Launch Agents:
•com.mac.host.plist isimli launch agents, şüpheli bir konumda bulunuyor: /Users/test/Library/LaunchAgents/com.mac.host.plist. Bu plist dosyası, zararlı yazılımın sistem başlatıldığında otomatik olarak çalışmasını sağlar.

Dosya ve İşlem İncelemesi

Dosya Bilgileri:

•**Finder.app:** Bu uygulama, şüpheli bir dizinde (.defaults) bulunuyor ve normalde burada bulunmaması gerekiyor.

com.mac.host.plist: Launch Agents sistem yeniden başlatıldığında otomatik olarak çalışacak şekilde yapılandırılmıştır. Bu ajan, Finder.app uygulamasını gizli bir klasörden başlatmaktadır ve bu sayede zararlı yazılımın sürekli çalışmasını sağlamaktadır.

- artifacts/Users/test/Library/LaunchAgents/com.mac.host.plist
  - Responsible for launching the Finder process

```
<dict>
    <key>Label</key>
    <string>com.mac.host</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/
test/.defaults/Finder.app/Contents/
MacOS/Finder</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>KeepAlive</key>
    <false/>
</dict>
```

- fileinfo.txt
  - both Finder.app and com.mac.host.plist created June 29, 2019 @ 20:26:17

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	40755	2019-06-29T 20:26:17	2019-06-29T 20:26:17	2019-06-29T 20:29:29	/Users/test/.defaults/Finder.app
0	501	20	100750	2019-06-29T 20:26:17	2019-06-29T 20:26:17	2019-06-29T 20:29:29	/Users/test/Library/LaunchAgents/com.mac.host.plist

Ağ Bağlantılarının İncelenmesi

- processes_network.txt
  - Finder process has a network connection open to 89.34.111.113

```
COMMAND   PID  USER  FD   TYPE             DEVICE SIZE/OFF   NODE
NAME

Finder    529  test   3u  IPv4 0x2888275a1e50e0d5      0t0    TCP
192.168.1.13:49219->89.34.111.113:https (ESTABLISHED)
```

Finder, 89.34.111.113 IP adresine bir ağ bağlantısı açmıştır. Bu bağlantı, sistemin saldırgan tarafından uzaktan kontrol edilmesi için kullanılmaktadır.

- system_logs.logarchive
  - log show --start "2019-06-29 20:26:15+0000" --end "2019-06-29 20:26:20+0000" --timezone "00:00:00" --info --archive system_logs.logarchive

```
2019-06-29 20:26:17.237182+0000 0x1a04     Info        0x51cf              319    0
Finder: (LaunchServices) [com.apple.launchservices:cas] LaunchApplication:
appToLaunch={ "ApplicationType"="UIElement", "CFBundleExecutablePath"="/Users/test/
Downloads/Finder.app/Contents/MacOS/Finder", "CFBundleExecutablePathDeviceID"=16777220,
"CFBundleExecutablePathINode"=921876, "CFBundleName"="Finder", "CFBundlePackageType"="APPL",
"LSBundlePath"="/Users/test/Downloads/Finder.app", "LSBundlePathDeviceID"=16777220,
"LSBundlePathINode"=921873, "LSExecutableFormat"="LSExecutableMachOFormat" } modifiers:
{ "AddPSNArgument"=true, "LSAdditionalEnvironmentVars"={  }, "LSLaunchAsync"=true,
"LSLaunchStoppedTemporarily"=true } args=[ NULL ]
```

Çıkarımlar

Uygulama Başlatma

- **Başlatma Bilgisi**: Finder uygulamasının /Users/test/Downloads/Finder.app/Contents/MacOS/Finder yolundan başlatıldığı belirtiliyor. Bu yol, uygulamanın sıradan bir Finder uygulaması olmadığını, kullanıcı indirme klasöründe gizlenmiş olabileceğini gösterir.
- **Uygulama Türü**: Log kaydında ApplicationType olarak UIElement tanımlanmış. Bu, kullanıcı arayüzü olmayan arka planda çalışan bir uygulama olduğunu gösterir.

Değerlendirme

Bu log kaydı, kullanıcı indirilenler klasöründe gizlenmiş bir uygulamanın (Finder.app) başlatıldığını ve bu sürecin bazı alışılmadık parametrelerle (örneğin, eşzamansız başlatma) gerçekleştirildiğini göstermektedir. Bu durum, özellikle sistemdeki meşru Finder uygulaması yerine başka bir yerde bulunan ve zararlı olma ihtimali yüksek bir uygulamanın başlatıldığını düşündürmektedir.

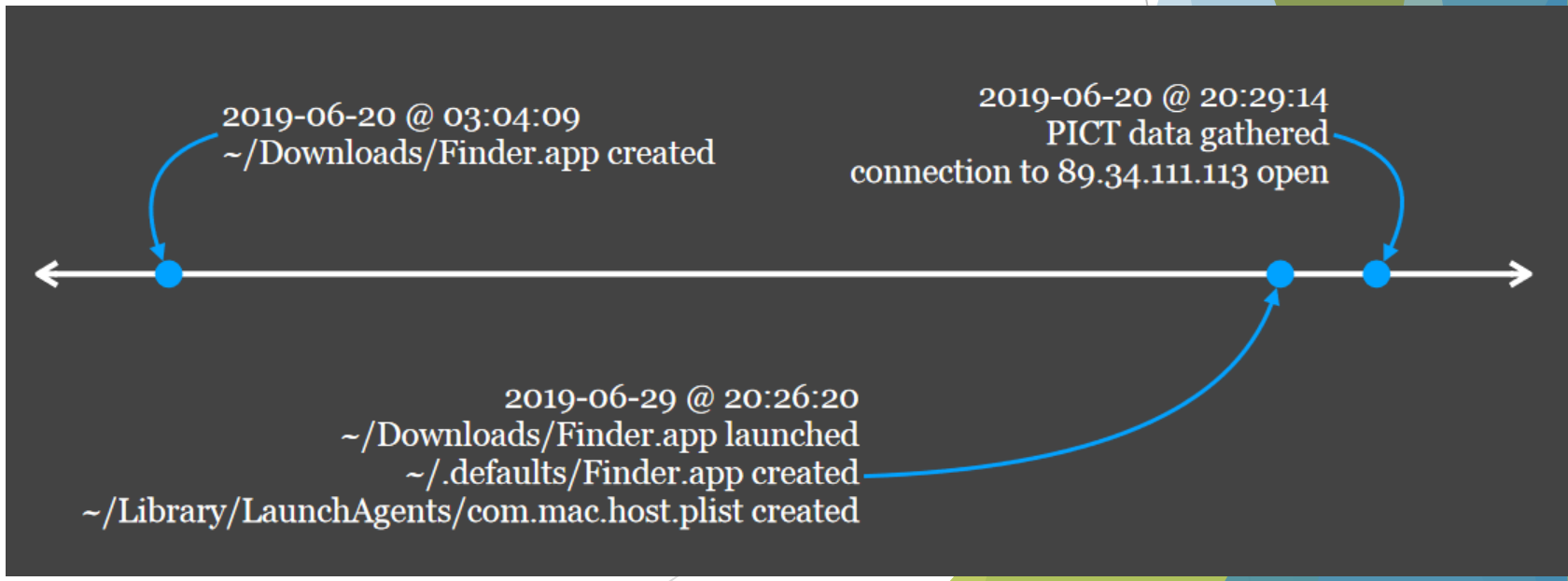
Zaman Çizelgesi Oluşturma

- fileinfo.txt
  - ~/Downloads/Finder.app created June 20, 2019 @ 03:04:09

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	40755	2019-06-20T 03:04:09	2019-06-20T 03:04:09	2019-06-29T 20:29:31	/Users/test/Downloads/Finder.app

2019-06-20 @ 03:04:09: Finder.app dosyası oluşturuldu.
2019-06-29 @ 20:26:20: Finder.app dosyası çalıştırıldı.
2019-06-29 @ 20:29:14: PICT verileri toplandı, 89.34.111.113 adresine bağlantı açık bırakıldı.

NOT:
'PICT verileri' macOS sistemlerinde kullanılan eski bir grafik dosya formatının içerdiği grafik öğeleridir.



Olayın Müdahalesi

- **Launch Agents Kaldırma:** com.mac.host.plist dosyasını ve ilgili dizindeki şüpheli dosyaları kaldırın.

- **Zararlı Yazılımın Kaldırılması:** Finder.app dosyasını ve ilgili tüm dosyaları sistemden temizleyin.

- **Ağ Bağlantılarını Kesme:** 89.34.111.113 IP adresine yapılan bağlantıları engelleyin.

- **Sistem Tarama:** Sistem üzerinde tam bir tarama yaparak başka zararlı yazılımların olup olmadığını kontrol edin.

Mokes

- Mokes Zararlı Yazılımı, bilgisayar sistemlerine bulaşarak kullanıcıların bilgilerini çalmayı amaçlayan gelişmiş bir kötü amaçlı yazılımdır.
- Genellikle phishing e-postaları veya kötü amaçlı web siteleri aracılığıyla yayılır.
- Mokes, kullanıcının klavye girdilerini izleyebilir, ekran görüntüsü alabilir, dosya çalabilir ve bilgisayara tam erişim sağlayabilir.

Mokes Walkthrough

1. Kalıcılık Mekanizması

Mokes, kalıcılığı sağlamak için launch agent kullanır. Bu amaçla ~/Library/LaunchAgents/ dizininde storeaccountd.plist adında bir plist dosyası oluşturur. Bu plist dosyası, sistem başlatıldığında storeaccountd adlı yürütülebilir dosyanın çalıştırılmasını sağlar. İşte plist dosyasının içeriği:

- artifacts/Users/test/Library/LaunchAgents/storeaccountd.plist
- launches ~/Library/App Store/storeaccountd

```
<dict>
   <key>Label</key>
   <string>storeaccountd</string>
   <key>ProgramArguments</key>
   <array>
      <string>/Users/test/Library/App
Store/storeaccountd</string>
   </array>
   <key>RunAtLoad</key><true/>
   <key>KeepAlive</key><true/>
</dict>
```

- persistence.txt
  - What is ~/Library/LaunchAgents/storeaccountd.plist? 🤔

```
User launch agents
----------------------------
/Users/test/Library/LaunchAgents
total 24
-rw-r--r--@  1 test  staff  -      808 Jun 20 08:42 com.google.keystone.agent.plist
-rw-r--r--@  1 test  staff  -      914 Jun 20 08:42 com.google.keystone.xpcservice.plist
-rw-r--r--   1 test  staff  -      400 Jun 29 17:34 storeaccountd.plist
```

Bu plist dosyası, sistem her başlatıldığında zararlı yazılımın otomatik olarak çalıştırılmasını sağlar.

2. Süreç Detayları

•**PID ve PPID Bilgisi**: storeaccountd süreci PID 495 ile başlatılır ve bu sürecin üst süreci launchd'dir (PPID=1).

•**(launchd**: macOS ve bazı Unix tabanlı sistemlerde kullanılan bir sistem ve servis yöneticisidir. Sistem başlatıldığında ilk olarak launchd başlatılır ve diğer tüm süreçler launchd tarafından yönetilir. Bu nedenle, launchd'nin PID numarası genellikle 1'dir.)

•**Başlatılma Zamanı**: Bu süreç yerel saatle 17:34'te başlatılmıştır.

NOT:

•**Yönetici İzinleri Gerektirmeden Çalışma:** storeaccountd işleminin, kullanıcı müdahalesi veya onayı olmadan başlatılması ve çalışması, zararlı yazılımların karakteristik özelliklerindendir.

3. Ağ Bağlantıları

•storeaccountd süreci, 185.49.69.210 IP adresine bağlanmaya çalışmıştır ancak bir yanıt alamamıştır:
•Bu bilgi, zararlı yazılımın dış dünyayla iletişim kurma çabasını gösterir ancak başarılı olamadığını belirtir .

- processes_network.txt
  - storeaccountd has attempted to connect with `185.49.69.210`, but has not received a response

```
COMMAND   PID   USER   FD   TYPE             DEVICE SIZE/OFF   NODE NAME
storeacco 495   test   25u  IPv4 0x9ddae8da804e137b      0t0    TCP
192.168.1.13:49224->185.49.69.210:http (SYN_SENT)
storeacco 495   test   28u  IPv4 0x9ddae8da7ac74ab3      0t0    UDP *:*
```

NOT:
•**Bağlantı Denemesi:** storeaccountd işleminin, 185.49.69.210 IP adresine bağlanmaya çalışması ve bu IP adresinin bilinmeyen veya şüpheli olması, zararlı yazılım olduğunun bir başka göstergesidir.

4. Dosya Bilgileri ve İşlemler

•storeaccountd ve storeaccountd.plist dosyaları 2019-06-29 tarihinde oluşturulmuştur.

- fileinfo.txt
  - storeaccountd, storeaccountd.plist created 2019-06-29 @ 21:34:01

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100555	2019-06-29T 21:34:01	2019-06-29T 21:34:01	2019-06-29T 21:34:01	/Users/test/Library/App Store/storeaccountd
0	501	20	100644	2019-06-29T 21:34:31	2019-06-29T 21:34:31	2019-06-29T 21:35:41	/Users/test/Library/ LaunchAgents/ storeaccountd.plist

NOT:

•**storeaccountd Program Dosyası:** Dosyanın kullanıcı kütüphanesi içerisinde (~/Library/App Store/) bulunması, meşru bir yazılımın olması gereken yerden farklı bir konumda olduğunu gösterir.

•**Dosya İzinleri ve Zaman Damgaları:** Dosyanın ve plist dosyasının aynı anda ve aynı kullanıcı tarafından oluşturulmuş olması şüphe uyandırır.

Zararlı yazılım tarafından kullanılan sıfır byte'lık bir dosya okunup/yazılmak üzere açılmıştır. Bu dosya, zararlı yazılımın hangi varyantının kurulu olduğunu belirlemek için kullanılır:

- processes_files.txt
  - storeaccountd has a zero-byte file open for read/write
  - (This is a marker file, used by the malware to identify which variant is installed)

```
COMMAND   PID  USER   FD      TYPE    DEVICE   SIZE/OFF   NODE NAME
storeacco 495  test   11u      REG       1,4          0 928151 /Users/test/
Library/Application Support/72769f032fd8c672bcb1a3e21a55726a
```

- fileinfo.txt
  - 72769f032fd8c672bcb1a3e21a55726a created 2019-06-29 @ 21:34:21

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100644	2019-06-29T 21:34:21	2019-06-29T 21:34:21	2019-06-29T 21:34:21	/Users/test/Library/ Application Support/ 72769f032fd8c672bcb1a3e 21a55726a

Burada dosyanın belirli bir zamanda oluşturulduğunu ve kimliğinin (72769f032fd8c672bcb1a3e21a55726a) benzersiz olduğunu belirtir.

- system_logs.logarchive
  - log show --start "2019-06-29 21:33:55+0000" --end "2019-06-29 21:34:05+0000" --timezone "00:00:00" --info --archive system_logs.logarchive

```
2019-06-29 21:33:55.600942+0000 0x249e     Info        0x0
492    0    mac: (LaunchServices) [com.apple.launchservices:cas]
{ "ApplicationType"="BackgroundOnly", "CFBundleExecutablePath"="/
Users/test/mac", "CFBundlePackageType"="????",
"CFBundleSignature"="????", "Flavor"=2, "LSArchitecture"="x86_64",
"LSCheckInTime*"=now-ish 2019/06/29 17:33:55, "LSDisplayName"="mac",
"LSExecutableFileName"="mac" }
```

Bu log kaydı, belirli bir zaman diliminde LaunchServices tarafından yönetilen bir arka plan uygulamasının ("mac" adlı uygulama) başlatıldığını ve bu uygulama hakkında çeşitli bilgileri içerir.

- **ApplicationType**: "BackgroundOnly", yani bu uygulama arka planda çalışan bir uygulama.
- **CFBundleExecutablePath**: Uygulamanın yürütülebilir dosyasının yolu ("/Users/test/mac").

5. Sistem Logları

•~/mac adlı dosya 2019-06-21 tarihinde oluşturulmuş ve 2019-06-29 tarihinde başlatılmıştır. Bu dosyanın oluşturulma ve başlatılma zamanları sistem loglarında belirtilmiştir.

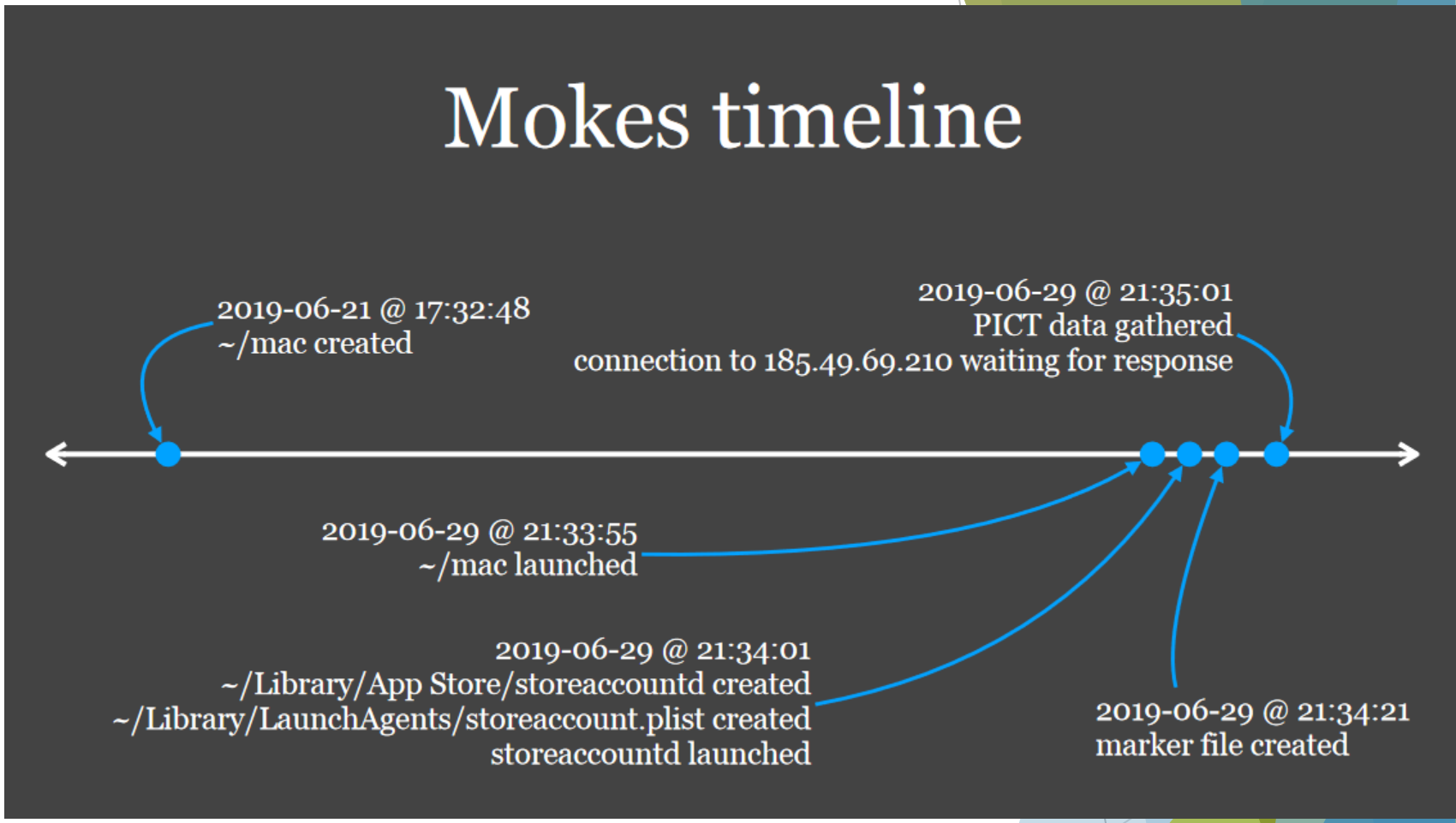
•Mokes zararlı yazılımı tarafından kullanılan diğer dosya ve süreçlerin log bilgileri de incelenmiş ve detaylı bir şekilde kaydedilmişti.

- fileinfo.txt
  - ~/mac created 2019-06-21 @ 17:32:48

Raw Flags	UID	GID	Mode (oct)	Created	Modified	Accessed	Path
0	501	20	100755	2019-06-21T 17:32:48	2019-06-21T 17:32:53	2019-06-29T 21:34:10	/Users/test/mac

NOT:

•Oluşturma ve Başlatma Zamanları: ~/Library/App Store/storeaccountd ve ~/Library/LaunchAgents/storeaccountd. plist dosyalarının aynı zaman diliminde oluşturulmuş ve başlatılmış olması, şüpheli etkinliğin yoğun bir dönemde gerçekleştiğini gösterir.



Sonuç

Mokes zararlı yazılımının macOS sistemlerinde nasıl çalıştığına dair yapılan bu inceleme, zararlı yazılımın kalıcılık mekanizması, süreç detayları, ağ bağlantıları ve dosya bilgileri gibi kritik noktaları kapsamaktadır. Bu bilgiler, zararlı yazılımın tespiti ve analiz edilmesi için önemli ipuçları sunmaktadır.

KAYNAKÇA

- https://www.youtube.com/watch?v=BdcGqy9VJ5M
- https://bpb-us-e1.wpmucdn.com/sites.psu.edu/dist/4/24696/files/2019/07/psumac2019-350-Learn-Incident-Response-for-Mac.pdf
- https://invictus-ir.medium.com/responding-to-macos-attacks-33f32332e0c