Malvertising campaign on PornHub and other top adult brands exposes users to tech support scams

blog.malwarebytes.com/cybercrime/2021/02/malvertising-campaign-on-top-adult-brands-exposes-users-to-tech-support-scams/

Threat Intelligence Team

February 12, 2021

Threat actors involved in tech support scams have been running a browser locker campaign from November 2020 until February 2021 on the world's largest adult platforms including PornHub.

The same group behind this campaign has been active for much longer and we believe is tied to previous schemes we've identified before, making it one of the most prolific tech support scam operations to date.

In late January, we heard several complaints of fake Microsoft alerts and started to investigate them. We discovered a number of decoy dating sites used by fraudulent advertisers on TrafficJunky, the advertising company for brands such as PornHub, RedTube and YouPorn owned by MindGeek.

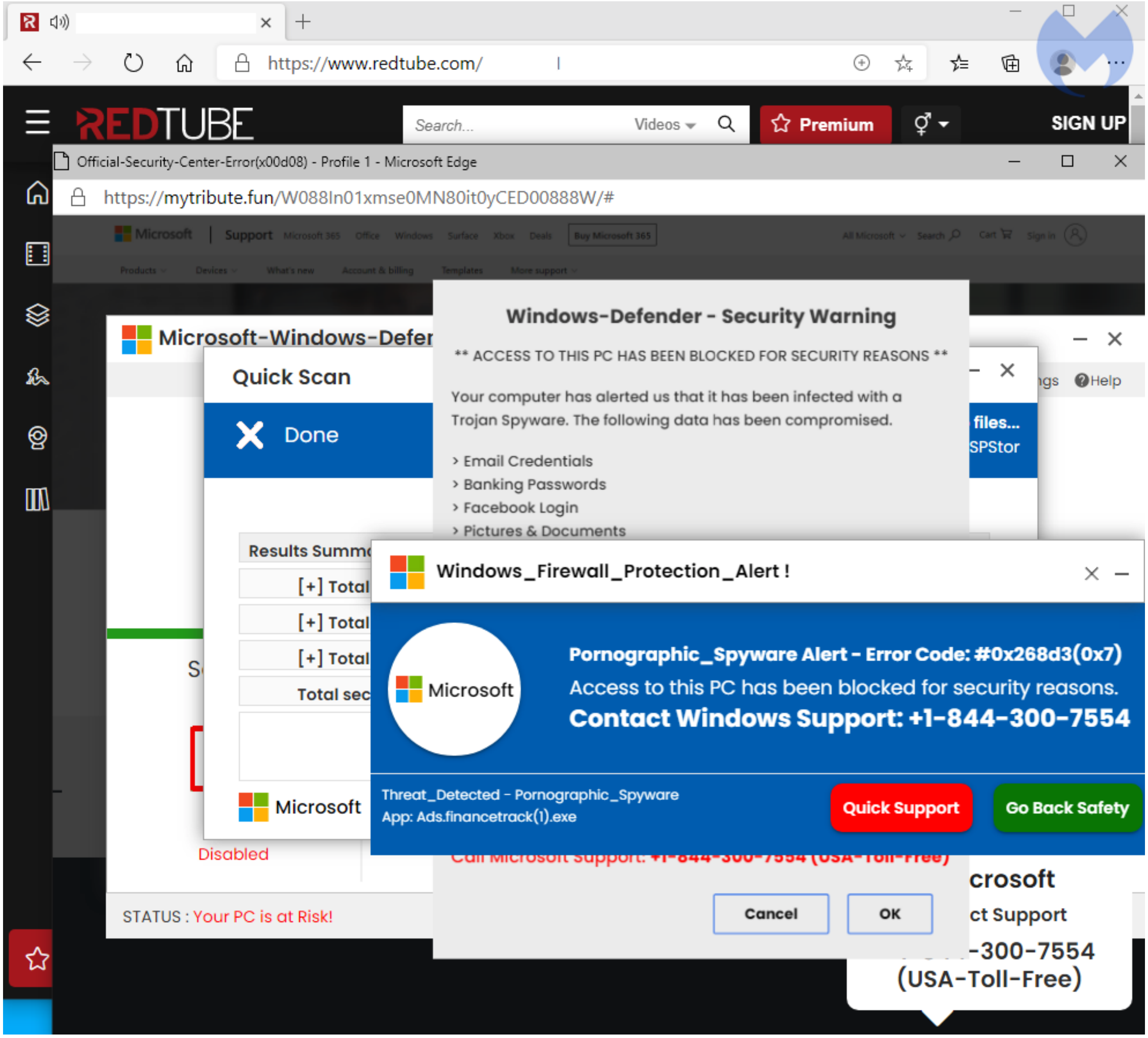
The scammers created those fake identities to redirect traffic away from the adult platforms onto pages showing bogus alerts claiming users were infected with pornographic spyware. This well-known scheme attempts to scare victims into calling so-called technicians for assistance but in fact defrauds them for hundreds of dollars.

We reported our findings to MindGeek and continue to track and share new incidents as they arise. We believe this threat actor will keep on tricking new victims until fully exposed and individuals apprehended by law enforcement.

Redirection chain

We were able to capture the malvertising redirection chain several times and the flow is almost identical. We know from our telemetry that the malicious advertiser is targeting victims from the U.S. and the U.K.

- User clicks to play a video
- A new browser window opens
- A request is sent to the TrafficJunky ad platform
- An ad is served and makes a request to a decoy dating site
- A redirect immediately loads the browser locker



https://www.redtube.com/

Official-Security-Center-Error(x00d08) - Profile 1 - Microsoft Edge

https://mytribute.fun/W088In01xmse0MN80it0yCED00888W/#

Windows-Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

› Email Credentials
› Banking Passwords
› Facebook Login
› Pictures & Documents

Windows_Firewall_Protection_Alert !

Pornographic_Spyware Alert - Error Code: #0x268d3(0x7)
Access to this PC has been blocked for security reasons.
Contact Windows Support: +1-844-300-7554

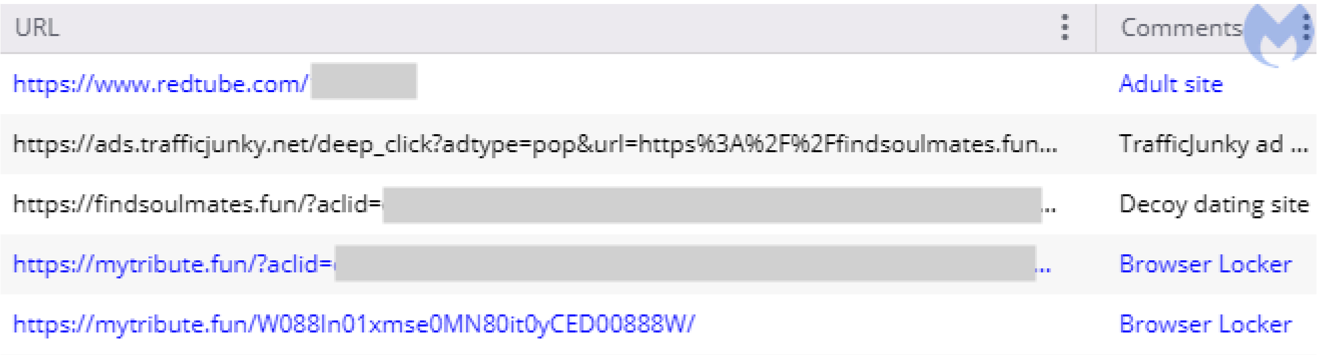
Threat_Detected - Pornographic_Spyware
App: Ads.financetrack(1).exe

Call Microsoft Support: +1-844-300-7554 (USA-Toll-Free)

STATUS : Your PC is at Risk!

crosoft
ct Support
-300-7554
(USA-Toll-Free)

This sequence of events can be summarized in the traffic capture below:



URL	Comments
https://www.redtube.com/[redacted]	Adult site
https://ads.trafficjunky.net/deep_click?adtype=pop&url=https%3A%2F%2Ffindsoulmates.fun...	TrafficJunky ad ...
https://findsoulmates.fun/?aclid=[redacted]...	Decoy dating site
https://mytribute.fun/?aclid=[redacted]...	Browser Locker
https://mytribute.fun/W088In01xmse0MN80it0yCED00888W/	Browser Locker

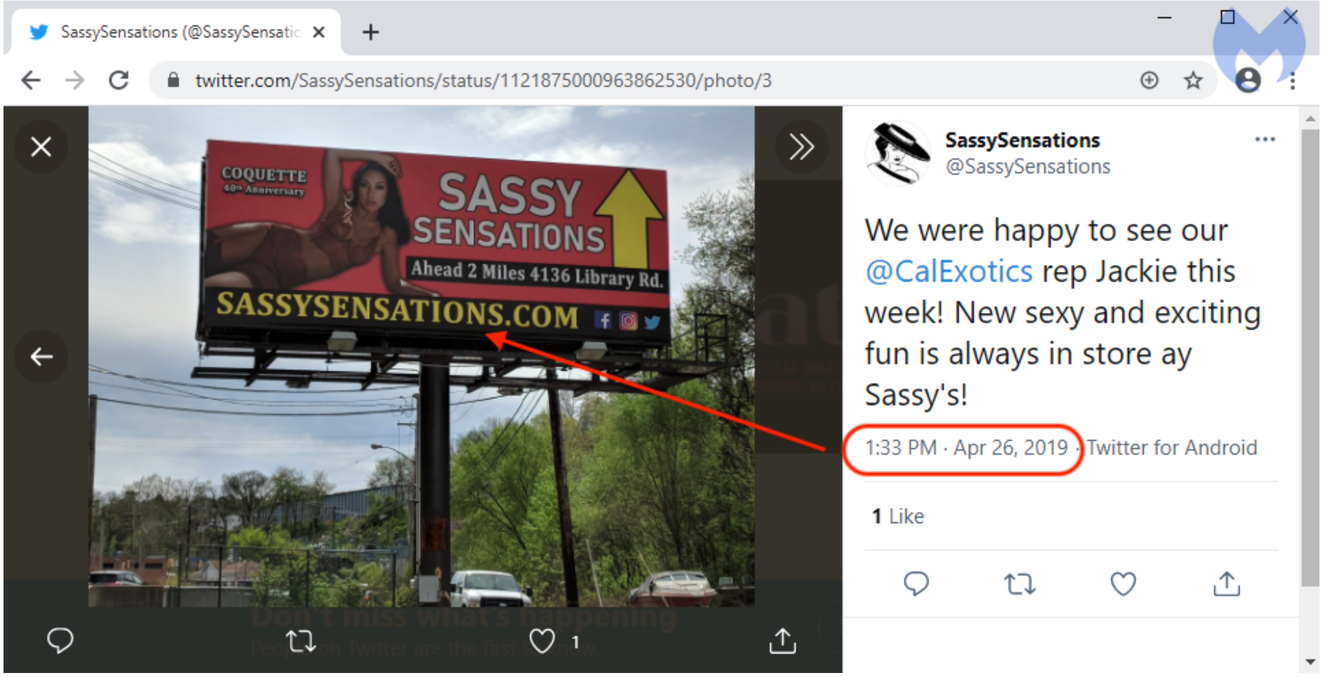
A key part of this malvertising chain is the use of many different fake dating portals that are hiding the redirection mechanism for the browser locker.

Beginnings

This browser locker campaign started well before showing up on PornHub[.]com and went undetected for a long time perhaps due to a clever typosquatting trick. In fact, we were fooled ourselves for a while before seeing what is obvious in hindsight.

On May 21 2020, the threat actor registered the domain name **sassysenssations[.]com** which contains a voluntary typo (two ‘s’) to mimic sassysensations[.]com which belongs to a legitimate business.

The real domain was registered in 2014 and we even found a billboard advertisement for it tweeted out on April 26 2019, long before the scammers had registered their copycat domain.


SassySensations (@SassySensatic
twitter.com/SassySensations/status/1121875000963862530/photo/3
COQUETTE
40th Anniversary
SASSY SENSATIONS
Ahead 2 Miles 4136 Library Rd.
SASSYSENSATIONS.COM
1

SassySensations
@SassySensations

We were happy to see our @CalExotics rep Jackie this week! New sexy and exciting fun is always in store ay Sassy's!

1:33 PM · Apr 26, 2019 · Twitter for Android

1 Like

What was clever is that the threat actor didn't seem to set up an actual site for that fake domain, but instead redirected all traffic to the real one if the visitor did not match the parameters from their malvertising campaign.

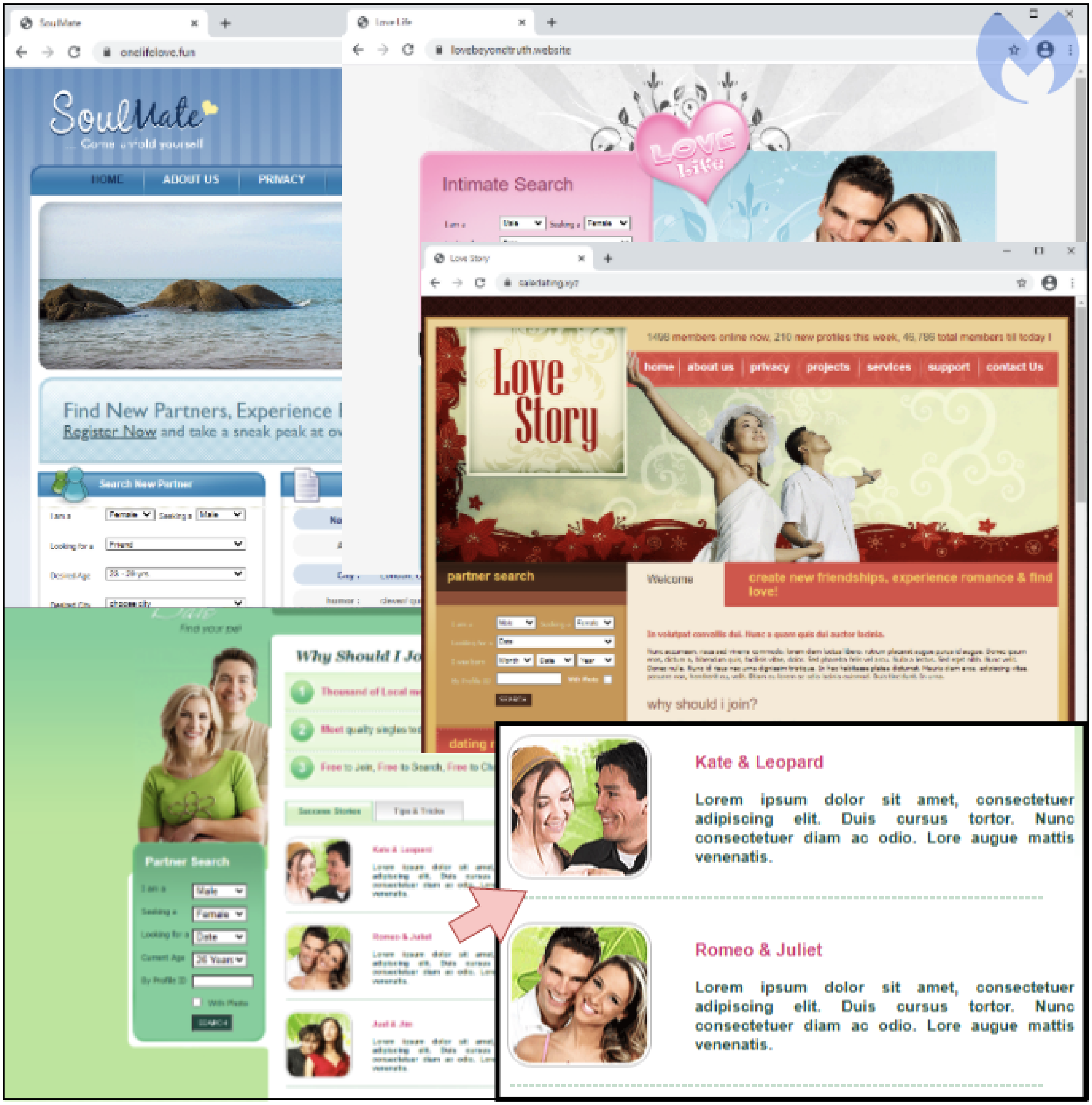
However, the malvertising chain shows that they leveraged that domain to perform conditional redirects, such as the one seen below:

```
(1) pornhub[.]com/_xa/ads?zone_id=[removed]
  (2) ads.trafficjunky[.]net/click?url=https%3A%2F%2Fsassysenssations[.]com%
    (3) sassysenssations[.]com/track.php?CampaignID=[removed]&Sitename=Pornhub
     (4) errorhelpline24x7msofficialsoftwareerrorcodex12[.]monster
```

Later on, it appears the threat actor started diversifying their scheme by creating a number of fake dating sites to use as redirects in addition to using the sassysenssations identity.

Fake dating sites

The malicious advertiser is using a model that has been tried before and consists of setting up fake identities in order to gain access to the ad platform. In this instance, we cataloged dating and romance sites. However, the majority of them did not look authentic or functional and even still had the 'Lorem ipsum' text filler.



Find New Partners, Experience

Register Now and take a sneak peak at o

Kate & Leopard

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis cursus tortor. Nunc consectetuer diam ac odio. Lore augue mattis venenatis.

Romeo & Juliet

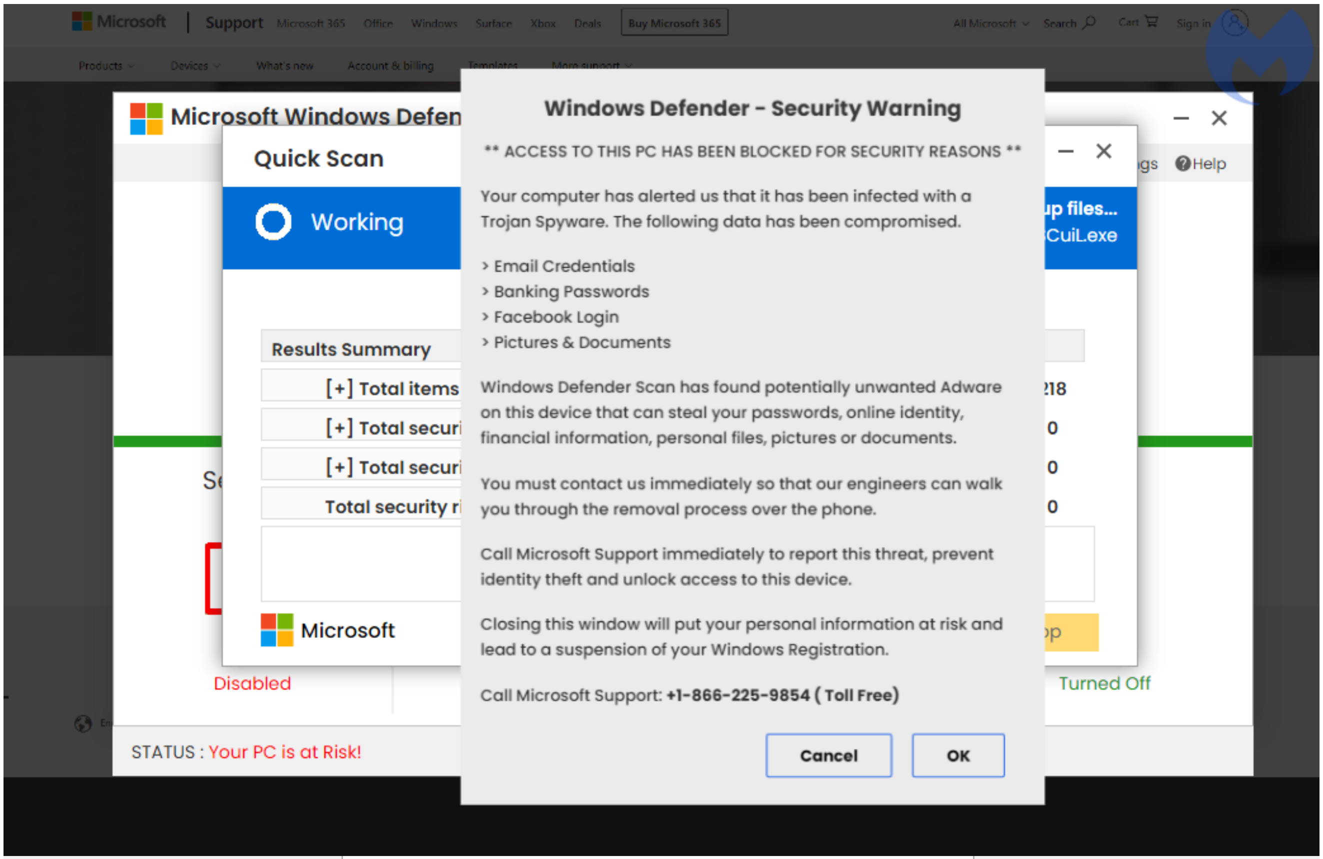
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis cursus tortor. Nunc consectetuer diam ac odio. Lore augue mattis venenatis.

If you were to visit one those sites directly, you may not see anything else of interest, at least nothing malicious in nature. However, the fraudulent advertiser can easily redirect traffic based on factors such as IP geolocation, referer and other artifacts.

In all, we detected close to 100 decoy domain names set up as “advertising landing pages” used to redirect victims to browser locker scams. Even though the templates are half finished, the threat actor is spending time creating a large inventory they can cycle through in their redirects towards browser lockers.

Browser locker

The browser locker is using a common theme of a fake Microsoft Windows Defender scanner. There is some browser profiling to serve the right template based on whether the user is on Windows or Mac.


Microsoft | Support Microsoft 365 Office Windows Surface Xbox Deals Buy Microsoft 365
All Microsoft Search Cart Sign in
Products Devices What's new Account & billing Templates More support
Microsoft Windows Defen
Quick Scan
Working
Results Summary
[+] Total items
[+] Total securi
[+] Total securi
Total security ri
Microsoft
Disabled
Turned Off
up files...
CuiLexe
218
0
0
0
gs
Help
STATUS : Your PC is at Risk!

Windows Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

> Email Credentials
> Banking Passwords
> Facebook Login
> Pictures & Documents

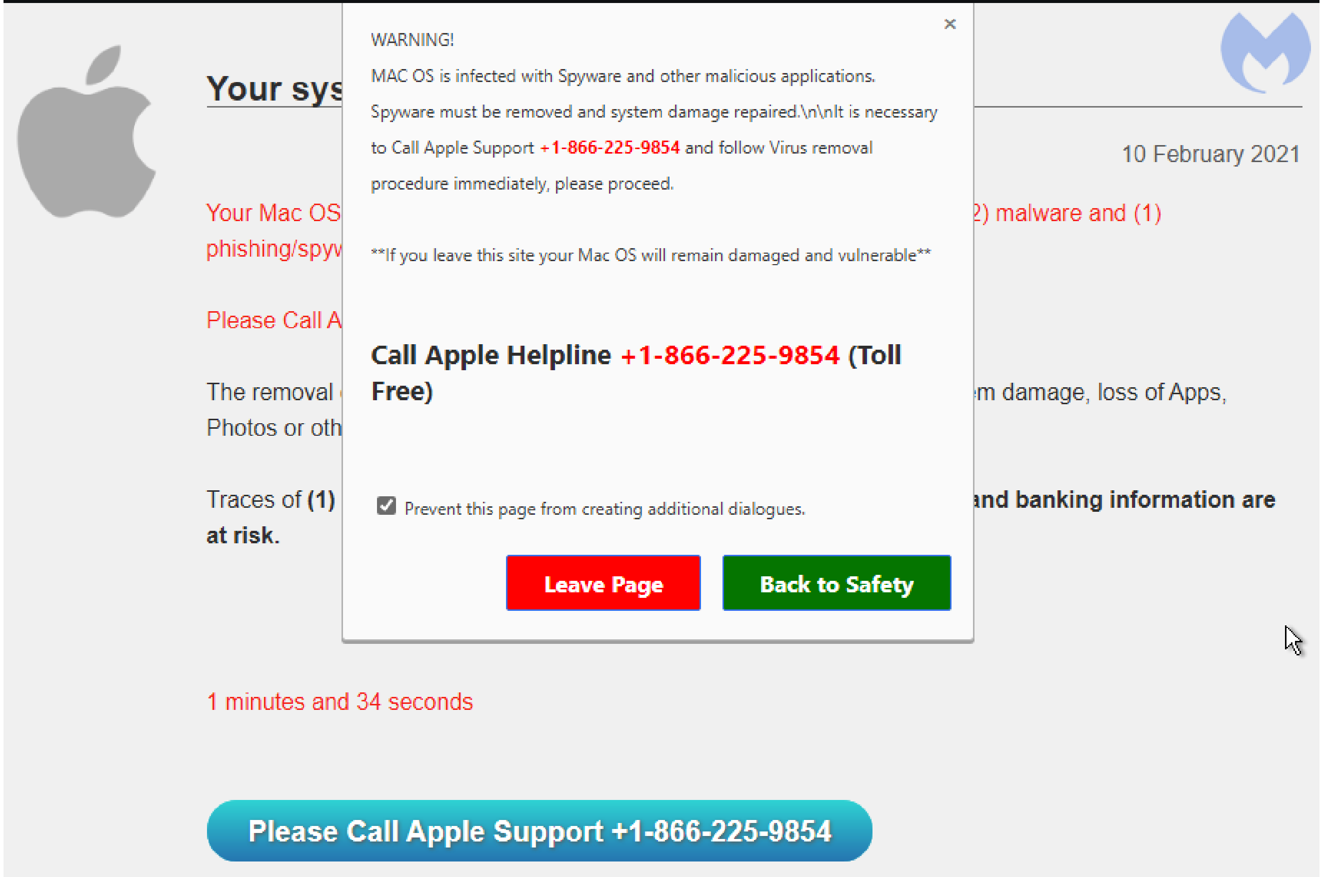
Windows Defender Scan has found potentially unwanted Adware on this device that can steal your passwords, online identity, financial information, personal files, pictures or documents.

You must contact us immediately so that our engineers can walk you through the removal process over the phone.

Call Microsoft Support immediately to report this threat, prevent identity theft and unlock access to this device.

Closing this window will put your personal information at risk and lead to a suspension of your Windows Registration.

Call Microsoft Support: **+1-866-225-9854 (Toll Free)**



WARNING!

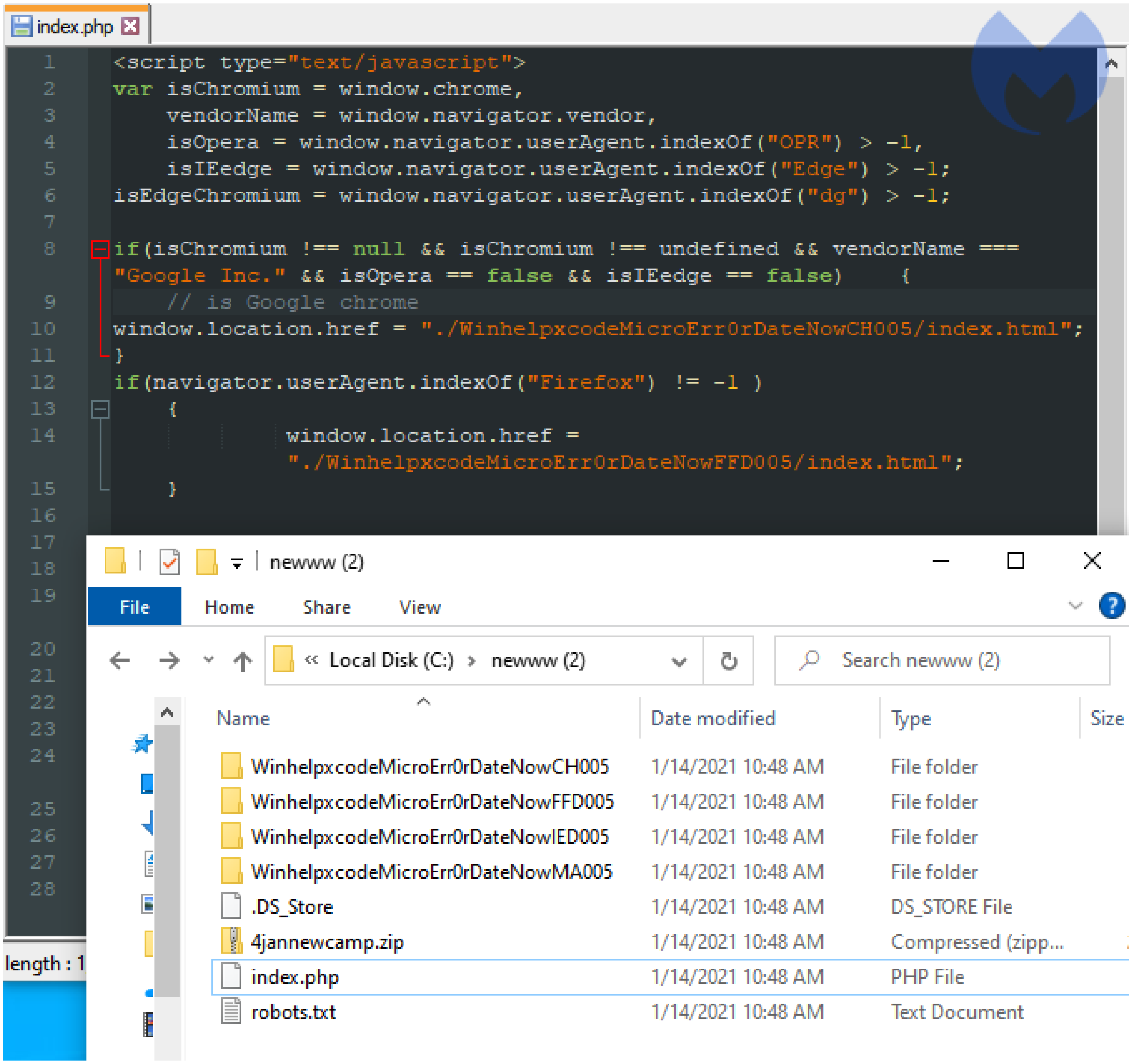
MAC OS is infected with Spyware and other malicious applications. Spyware must be removed and system damage repaired.\n\nIt is necessary to Call Apple Support +1-866-225-9854 and follow Virus removal procedure immediately, please proceed.

If you leave this site your Mac OS will remain damaged and vulnerable

Call Apple Helpline +1-866-225-9854 (Toll Free)

☑ Prevent this page from creating additional dialogues.

While browsing one of the many decoy sites, we found the HTML source code in an exposed directory showing a few additional variations of the browser locker:



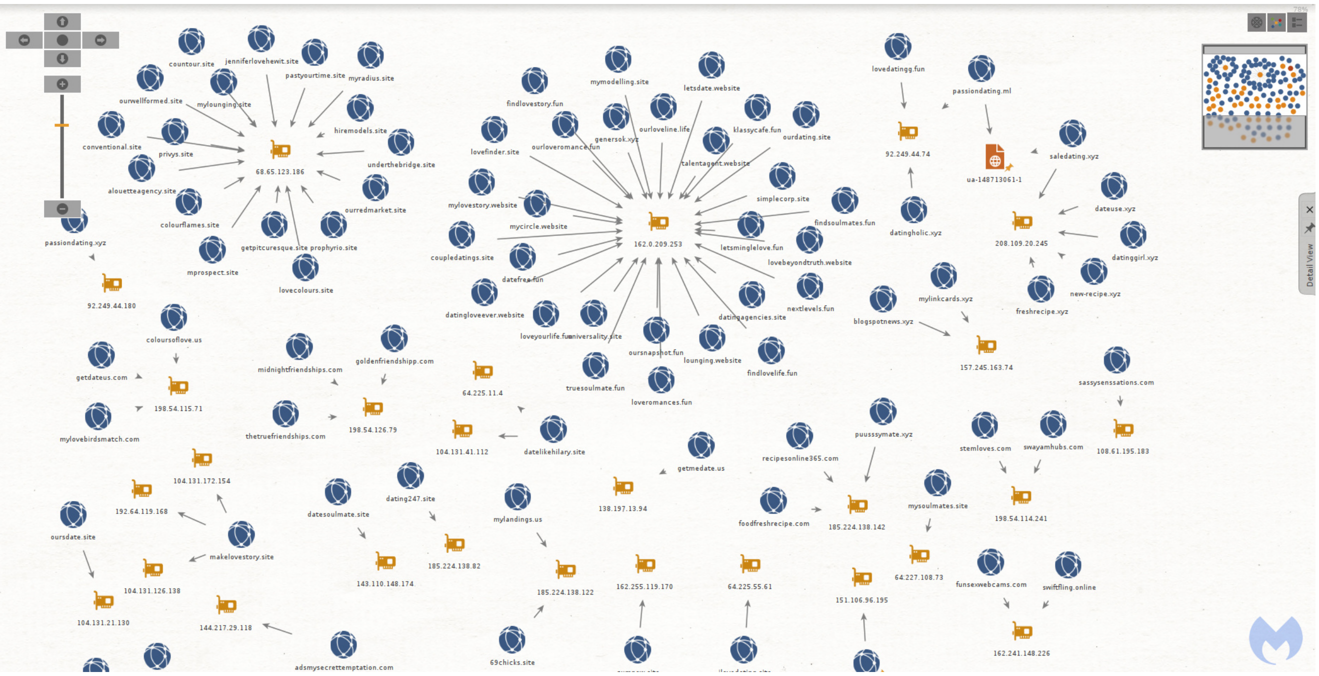
```
<script type="text/javascript">
var isChromium = window.chrome,
    vendorName = window.navigator.vendor,
    isOpera = window.navigator.userAgent.indexOf("OPR") > -1,
    isIEedge = window.navigator.userAgent.indexOf("Edge") > -1;
isEdgeChromium = window.navigator.userAgent.indexOf("dg") > -1;

if(isChromium !== null && isChromium !== undefined && vendorName === "Google Inc." && isOpera == false && isIEedge == false)    {
    // is Google chrome
window.location.href = "./WinhelpxcodeMicroErr0rDateNowCH005/index.html";
}
if(navigator.userAgent.indexOf("Firefox") != -1 )
    {
            window.location.href = "./WinhelpxcodeMicroErr0rDateNowFFD005/index.html";
    }
```

Name	Date modified	Type	Size
WinhelpxcodeMicroErr0rDateNowCH005	1/14/2021 10:48 AM	File folder	
WinhelpxcodeMicroErr0rDateNowFFD005	1/14/2021 10:48 AM	File folder	
WinhelpxcodeMicroErr0rDateNowIED005	1/14/2021 10:48 AM	File folder	
WinhelpxcodeMicroErr0rDateNowMA005	1/14/2021 10:48 AM	File folder	
.DS_Store	1/14/2021 10:48 AM	DS_STORE File	
4jannewcamp.zip	1/14/2021 10:48 AM	Compressed (zipp...	
index.php	1/14/2021 10:48 AM	PHP File	
robots.txt	1/14/2021 10:48 AM	Text Document	

Fake advertising infrastructure

Because this is a long running campaign, the infrastructure is fairly large but tends to reuse the same naming convention for domains. The graph below only shows the domains created to abuse the TrafficJunky ad platform. It does not include domains used for the browlock itself.



There was a domain (recipesonline365[.]com) whose naming convention differed from the other dating sites. In fact it is the only one with a non-adult theme.

```
(1) youporn[.]com/_xa/ads?zone_id=[removed]
  (2) ads.trafficjunky[.]net/deep_click?
adtype=pop&url=https%3A%2F%2Frecipesonline365[.]com
    (3) recipesonline365[.]com/?aclid=[removed]
      (4) oopi3.azurewebsites[.]net/Winhelpxcode161616winHelpSecurity0nlineCH007
```

Back in June 2019, we had identified an ad campaign targeting recipe keywords. The threat actor was using decoy recipe and food sites to lure victims via web searches. Those sites performed the same redirect mechanism as the decoy dating sites, and most of the time lead to a browlock hosted on Azure as well.

There are a number of other parallels between that campaign and the adult one such as the predominant use of NameCheap hosting and a large volume of decoy sites. For this reason we believe this is likely the same threat actor.

Protection

Browser lockers are not dangerous in and out of themselves. They are simply a fake warning which may be disrupting and annoying but one that does not indicate a computer problem.

In recent years they have become very common and affect all browsers, even mobile ones. In the past, we have seen browser lockers that were effectively giving the impression the machine was locked due to how they abused the user interface. As of know, most of them can be closed normally without requiring the use of special commands.

Malwarebytes users were already protected against this campaign. Our Browser Guard extension can detect and stop browser lockers using heuristic techniques that do not require to use a blacklist of known domain names or IP addresses.

Indicators of Compromise

The list of IOCs can be downloaded from our GitHub here.