TREND MICRO

TrendLabs SECURITY INTELLIGENCE Blog

SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Will Astrum Fill the Vacuum in the Exploit Kit Landscape?

- Posted on:May 18, 2017 at 7:40 am
- Posted in:Exploits, Vulnerabilities
- Author:
  Joseph C Chen (Fraud Researcher)

0

The decline of exploit kit activity—particularly from well-known exploit kits like Magnitude, Nuclear, Neutrino, and Rig during the latter half of 2016—doesn't mean exploit kits are throwing in the towel just yet. This is the case with Astrum (also known as Stegano), an old and seemingly reticent exploit kit we observed to have been updated multiple times as of late.

Astrum was known to be have been exclusively used by the AdGholas malvertising campaign that delivered a plethora of threats including banking Trojans Dreambot/Gozi (also known as Ursnif, and detected by Trend Micro as BKDR_URSNIF) and RAMNIT (TROJ_RAMNIT, PE_RAMNIT). We're also seeing Astrum redirected by the Seamless malvertising campaign, which is known for using the Rig exploit kit.

Astrum's recent activities feature several upgrades and show how it's starting to move away from the more established malware mentioned above. It appears these changes were done to lay the groundwork for future campaigns, and possibly to broaden its use. With a modus operandi that deters analysis and forensics by abusing the Diffie-Hellman key exchange, it appears Astrum is throwing down the gauntlet.

Astrum's Attack Flow

On March 23rd, our colleague *Kafeine* found Astrum starting to exploit CVE-2017-0022, an information disclosure vulnerability in Windows systems (patched last March 14, 2017 via MS17-022). The exploit was used to determine if certain antivirus (AV) products were installed in the affected computer in order to evade their detection and analysis.

By the end of April, we saw Astrum updated yet again—this time to prevent security researchers from replaying their malicious network traffic. We found that this anti-replay feature was designed to abuse the Diffie-Hellman key exchange—a widely used algorithm for encrypting and securing network protocols. Angler was first observed doing this back in 2015.

Implementing the Diffie-Hellman key exchange prevents malware analysts and security researchers from getting a hold of the secret key Astrum uses to encrypt and decrypt their payloads. Consequently, obtaining the original payload by solely capturing its network traffic can be very difficult.

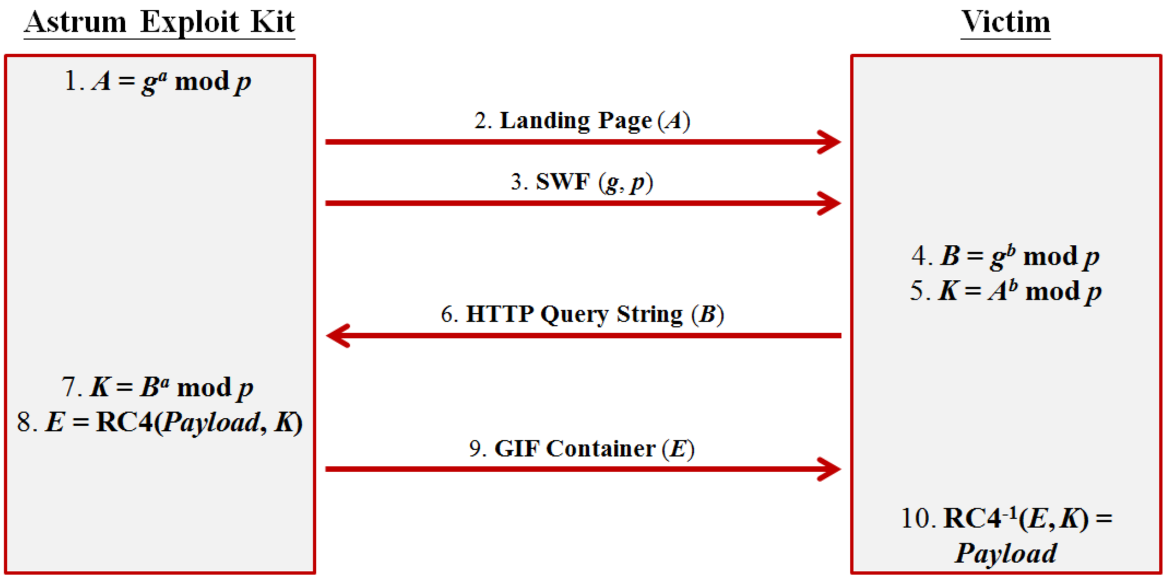
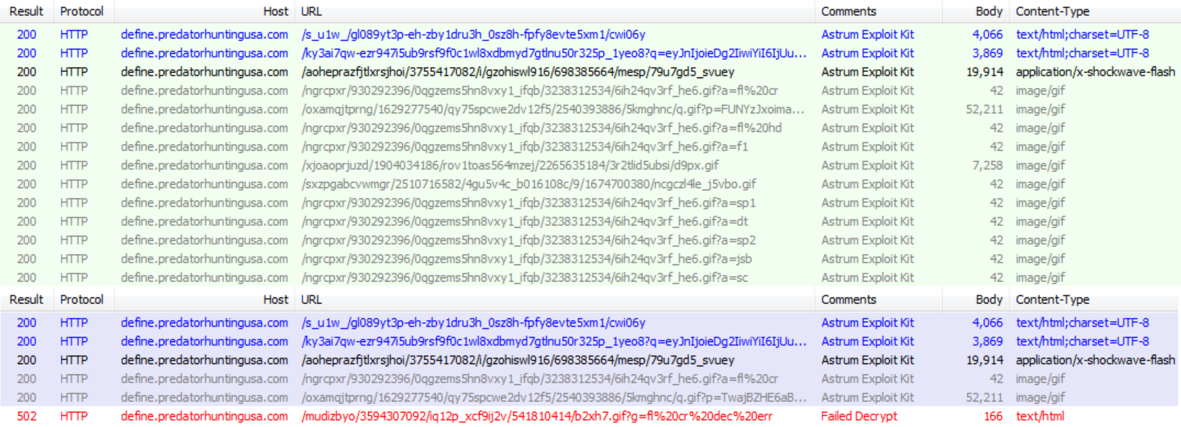


Figure 1: Diffie-Hellman key exchange flow implemented by Astrum exploit kit

How does Astrum implement the Diffie-Hellman key exchange? As detailed by the figure above, a precomputed value, ***A***, is first embedded on the exploit kit's landing page, which it then passes as a parameter into the first loaded Flash (SWF) file. The script inside the SWF file will generate a random value ***b***, which is saved only in the victim side's memory.

A secret key ***K*** could be calculated at the victim side with value ***A***, shared value ***p***, and the generated random value ***b***. Then, a value ***B*** will also be calculated by shared value ***g***, ***p***, and random value ***b***. The value will be sent to the exploit kit server in the query string of the next HTTP request. Astrum can then calculate based on value ***B*** to have the same secret key ***K*** based on the Diffie-Hellman theory. This secret key can then be used to encrypt the real exploit payload by RC4 encryption.

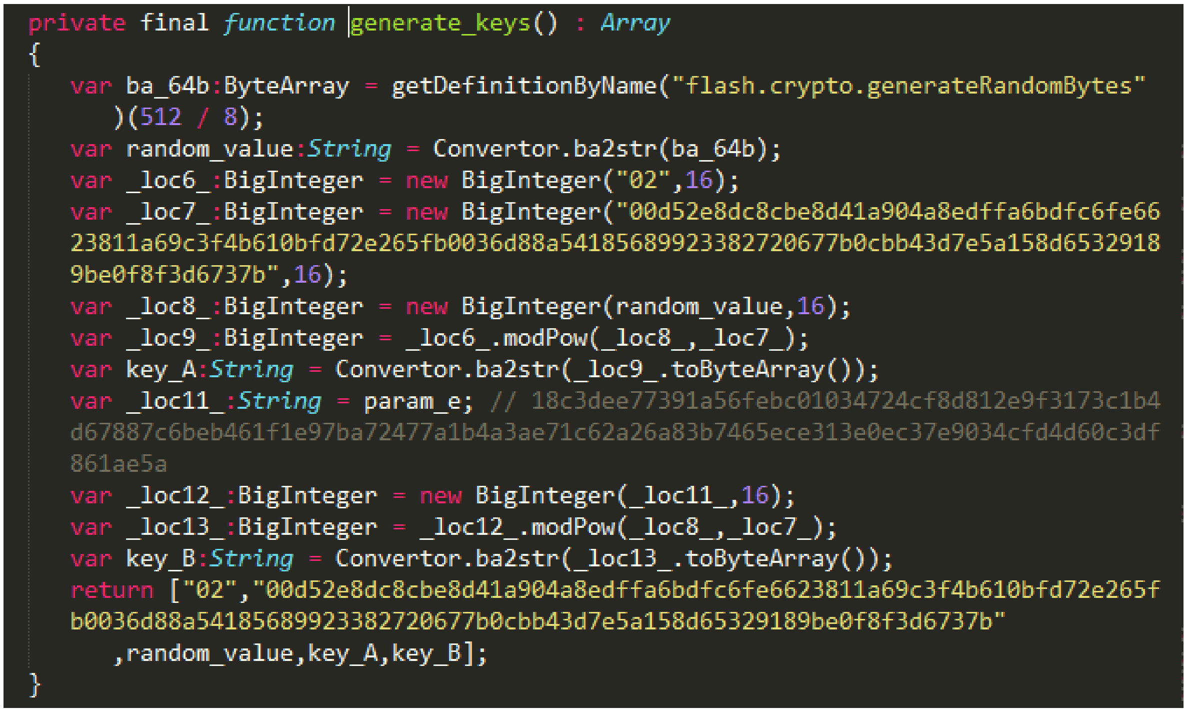
Consequently, each time we replay Astrum's attacks, the value ***b*** is randomly generated and would be different each time. The calculated secret key ***K*** will also differ from the original key the exploit kit used to encrypt the payload, causing the replayed attack to fail decrypting the encrypted payload. If the secret key cannot correctly decrypt the payload, Astrum sends an error call to the server.



Result	Protocol	Host	URL	Comments	Body	Content-Type
200	HTTP	define.predatorhuntingusa.com	/s_u1w_/gl089yt3p-eh-zby1dru3h_0sz8h-fpfy8evte5xm1/cwi06y	Astrum Exploit Kit	4,066	text/html;charset=UTF-8
200	HTTP	define.predatorhuntingusa.com	/ky3ai7qw-ezr947i5ub9rsf9f0c1wl8xdbmyd7gtlnu50r325p_1yeo8?q=eyJnIjoieDg2IiwiYiI6IjUu...	Astrum Exploit Kit	3,869	text/html;charset=UTF-8
200	HTTP	define.predatorhuntingusa.com	/aoheprazfjtlxrsjhoi/3755417082/i/gzohiswl916/698385664/mesp/79u7gd5_svuey	Astrum Exploit Kit	19,914	application/x-shockwave-flash
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=fl%20cr	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/oxamqjtprng/1629277540/qy75spcwe2dv12f5/2540393886/5kmghnc/q.gif?p=FUNYzJxoima...	Astrum Exploit Kit	52,211	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=fl%20hd	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=f1	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/xjoaoprjuzd/1904034186/rov1toas564mzej/2265635184/3r2tlid5ubsi/d9px.gif	Astrum Exploit Kit	7,258	image/gif
200	HTTP	define.predatorhuntingusa.com	/sxzpgabcvwmgr/2510716582/4gu5v4c_b016108c/9/1674700380/ncgczl4le_j5vbo.gif	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=sp1	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=dt	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=sp2	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=jsb	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=sc	Astrum Exploit Kit	42	image/gif

Result	Protocol	Host	URL	Comments	Body	Content-Type
200	HTTP	define.predatorhuntingusa.com	/s_u1w_/gl089yt3p-eh-zby1dru3h_0sz8h-fpfy8evte5xm1/cwi06y	Astrum Exploit Kit	4,066	text/html;charset=UTF-8
200	HTTP	define.predatorhuntingusa.com	/ky3ai7qw-ezr947i5ub9rsf9f0c1wl8xdbmyd7gtlnu50r325p_1yeo8?q=eyJnIjoieDg2IiwiYiI6IjUu...	Astrum Exploit Kit	3,869	text/html;charset=UTF-8
200	HTTP	define.predatorhuntingusa.com	/aoheprazfjtlxrsjhoi/3755417082/i/gzohiswl916/698385664/mesp/79u7gd5_svuey	Astrum Exploit Kit	19,914	application/x-shockwave-flash
200	HTTP	define.predatorhuntingusa.com	/ngrcpxr/930292396/0qgzems5hn8vxy1_ifqb/3238312534/6ih24qv3rf_he6.gif?a=fl%20cr	Astrum Exploit Kit	42	image/gif
200	HTTP	define.predatorhuntingusa.com	/oxamqjtprng/1629277540/qy75spcwe2dv12f5/2540393886/5kmghnc/q.gif?p=TwajBZHE6aB...	Astrum Exploit Kit	52,211	image/gif
502	HTTP	define.predatorhuntingusa.com	/mudizbyo/3594307092/iq12p_xcf9ij2v/541810414/b2xh7.gif?g=fl%20cr%20dec%20err	Failed Decrypt	166	text/html

Figure 2: The normal Astrum exploit kit traffic pattern (above) and failed replay (below)



```
private final function generate_keys() : Array
{
    var ba_64b:ByteArray = getDefinitionByName("flash.crypto.generateRandomBytes"
      )(512 / 8);
    var random_value:String = Convertor.ba2str(ba_64b);
    var _loc6_:BigInteger = new BigInteger("02",16);
    var _loc7_:BigInteger = new BigInteger("00d52e8dc8cbe8d41a904a8edffa6bdfc6fe66
    23811a69c3f4b610bfd72e265fb0036d88a5418568992338272067 7b0cbb43d7e5a158d6532918
    9be0f8f3d6737b",16);
    var _loc8_:BigInteger = new BigInteger(random_value,16);
    var _loc9_:BigInteger = _loc6_.modPow(_loc8_,_loc7_);
    var key_A:String = Convertor.ba2str(_loc9_.toByteArray());
    var _loc11_:String = param_e; // 18c3dee77391a56febc01034724cf8d812e9f3173c1b4
    d67887c6beb461f1e97ba72477a1b4a3ae71c62a26a83b7465ece313e0ec37e9034cfd4d60c3df
    861ae5a
    var _loc12_:BigInteger = new BigInteger(_loc11_,16);
    var _loc13_:BigInteger = _loc12_.modPow(_loc8_,_loc7_);
    var key_B:String = Convertor.ba2str(_loc13_.toByteArray());
    return ["02","00d52e8dc8cbe8d41a904a8edffa6bdfc6fe6623811a69c3f4b610bfd72e265f
    b0036d88a54185689923382720677b0cbb43d7e5a158d65329189be0f8f3d6737b"
      ,random_value,key_A,key_B];
}
```

Figure 3: The code in Astrum exploit kit that generates random value and calculates the secret key

Apart from leveraging CVE-2017-0022, we found Astrum using exploits for vulnerabilities in Adobe Flash:

- CVE-2015-8651, a code execution vulnerability patched December 28, 2015
- CVE-2016-1019, a remote code execution flaw patched April 7, 2016
- CVE-2016-4117, an out-of-bound read bug in Flash patched May 10, 2016

Testing the Waters

Our analysis indicates the payloads currently delivered by Astrum are not established malware. Likewise, Astrum itself is maintaining very low traffic. These activities can be construed as dry runs for their future attacks.

So what else can we expect from Astrum? It wouldn't be a surprise if its operators turn it into an exclusive tool of the trade—like Magnitude and Neutrino did—or go beyond leveraging security flaws in Adobe Flash. Emulating capabilities from its predecessors such as fileless infections that can fingerprint its targets and deliver encrypted payloads shouldn't be far off.

Mitigation

Indeed, exploit kits expose end users to theft of personal information and even unauthorized encryption of personal files. For organizations, exploit kits can entail crippled operations, damaged business reputation, and bigger downtime expenses. Unpatched vulnerabilities are the bread and butter of any exploit kit, so regularly patching and keeping the system updated play critical roles in thwarting it and even the malicious payloads that come with it.

Information security and IT/system administrators can further secure their enterprise's networks and endpoints by deploying firewalls and employing intrusion detection and prevention systems to better scan and validate traffic traveling the network. Virtual patching and a stronger patch management policy for the workplace also help mitigate attacks that leverage vulnerabilities.

Trend Micro Solutions

Exploit kits such as Astrum rely on system and software vulnerabilities, and thwarting them is like a race against time. A proactive, multilayered approach to security is key— from the gateway, endpoints, networks, and servers.

Trend Micro™ OfficeScan™ with XGen™ endpoint security has Vulnerability Protection that shields endpoints from identified and unknown vulnerability exploits even before patches are even deployed. Trend Micro's endpoint solutions such as Trend Micro™ Smart Protection Suites, and Worry-Free™ Business Security protect end users and businesses from these threats by detecting and blocking malicious files and all related malicious URLs.

Indicators of Compromise (IoCs):

IP Address and domain related to Astrum exploit kit:

- 141[.]255[.]161[.]68
- hxxp://define[.]predatorhuntingusa[.]com

Hashes of dropped payloads (SHA256):

- 39b1e99034338d7f5b0cbff9fb9bd93d9e4dd8f4c77b543da435bb2d2259b0b5
- ccf89a7c8005948b9548cdde12cbd060f618234fd00dfd434c52ea5027353be8

IP Addresses related to Seamless Malvertising Campaign:

- 193[.]124[.]200[.]194
- 193[.]124[.]200[.]212
- 194[.]58 [.]40 [.]46

With additional insights/analysis from Michael Du

Related Posts:

- **After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity**
- **Updated Sundown Exploit Kit Uses Steganography**
- **Tracking the Decline of Top Exploit Kits**
- **New Bizarro Sundown Exploit Kit Spreads Locky**

TREND MICRO

Say **NO** to ransomware.

Trend Micro has **blocked over 100 million** threats and counting

Learn how to protect Enterprises, Small Businesses, and Home Users from ransomware:

ENTERPRISE » SMALL BUSINESS » HOME »

Tags: Astrumdiffie-hellmanexploit kit

Featured Stories

- IIS 6.0 Vulnerability Leads to Code Execution
- Winnti Abuses GitHub for C&C Communications
- MajikPOS Combines PoS Malware and RATs to Pull Off its Malicious Tricks
- New Linux Malware Exploits CGI Vulnerability
- CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Business Email Compromise

- How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
  See the numbers behind BEC

Latest Ransomware Posts

Victims Lost US$1B to Ransomware

After WannaCry, UIWIX Ransomware and Monero-Mining Malware Follow Suit

Massive WannaCry/Wcry Ransomware Attack Hits Various Countries

Cerber Version 6 Shows How Far the Ransomware Has Come (and How Far it’ll Go)

Cerber Starts Evading Machine Learning

Recent Posts

- A Rising Trend: How Attackers are Using LNK Files to Download Malware
- Victims Lost US$1B to Ransomware
- Android Security Bulletin Tackles Additional Critical Mediaserver Issues
- Will Astrum Fill the Vacuum in the Exploit Kit Landscape?
- After WannaCry, UIWIX Ransomware and Monero-Mining Malware Follow Suit

Ransomware 101

-

  This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
  Check the infographic

Popular Posts

Massive WannaCry/Wcry Ransomware Attack Hits Various Countries
After WannaCry, UIWIX Ransomware and Monero-Mining Malware Follow Suit
Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras
Pawn Storm Abuses Open Authentication in Advanced Social Engineering Attacks
Cerber Version 6 Shows How Far the Ransomware Has Come (and How Far it’ll Go)

Latest Tweets

- New post: A Rising Trend: How Attackers are Using LNK Files to Download Malware bit.ly/2qmGWx3 @TrendMicro
  about 3 hours ago
- The @TrendMicro Zero Day Initiative Team investigates #SCADA #HMI #vulnerabilities in new report.… twitter.com/i/web/status/8…
  about 3 hours ago
- Have we found #Mirai's successor? A look at #IoT botnet, #Persirai: bit.ly/2pi9U5u

  about 9 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies

- Copyright © 2017 Trend Micro Incorporated. All rights reserved.