AdGholas Malvertising Campaign Employs Astrum Exploit Kit

- Posted on:June 20, 2017 at 7:28 am
- Posted in:Bad Sites, Ransomware
- Author:
  Joseph C Chen (Fraud Researcher)

0

At the end of April this year, we found Astrum exploit kit employing Diffie-Hellman key exchange to prevent monitoring tools and researchers from replaying their traffic. As AdGholas started to push the exploit, we saw another evolution: Astrum using HTTPS to further obscure their malicious traffic.

We spotted a new AdGholas malvertising campaign using the Astrum exploit kit (also known as Stegano) across various countries. The attacks we've seen are capable of concealing their malicious traffic using the Hyper Text Transfer Protocol Secure (HTTPS) protocol, which can make detection of their activities more challenging. HTTPS—where the connection between the browser and application is encrypted with Transport Layer Security (TLS)—is employed to protect highly sensitive transactions such as online banking and shopping.

We were able to monitor 262,163 events triggered by AdGholas from May 14 to June 18, 2017. The most impacted countries from its recent activity include the US, Japan, Italy, Australia, and UK. We worked with ProofPoint's Kafeine to retrace AdGholas' activities.

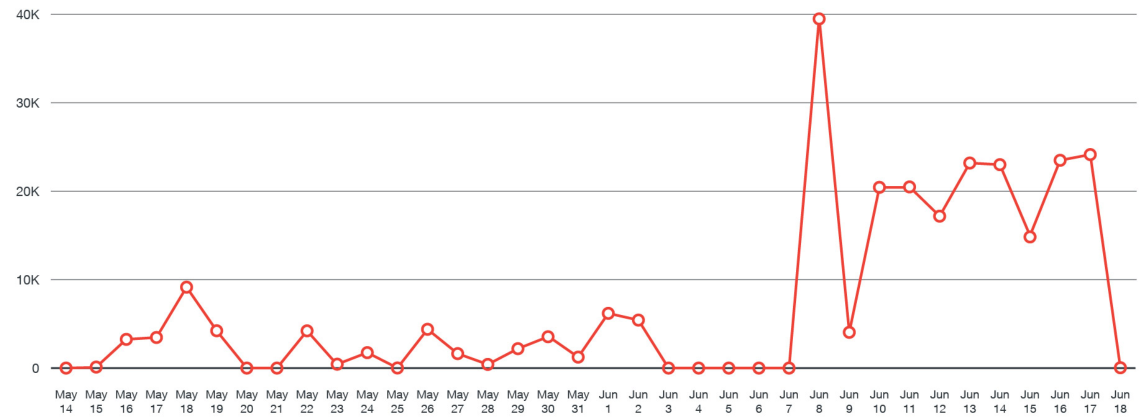


Figure 1: Timeline of AdGholas' activity from May 14 to June 18, 2017

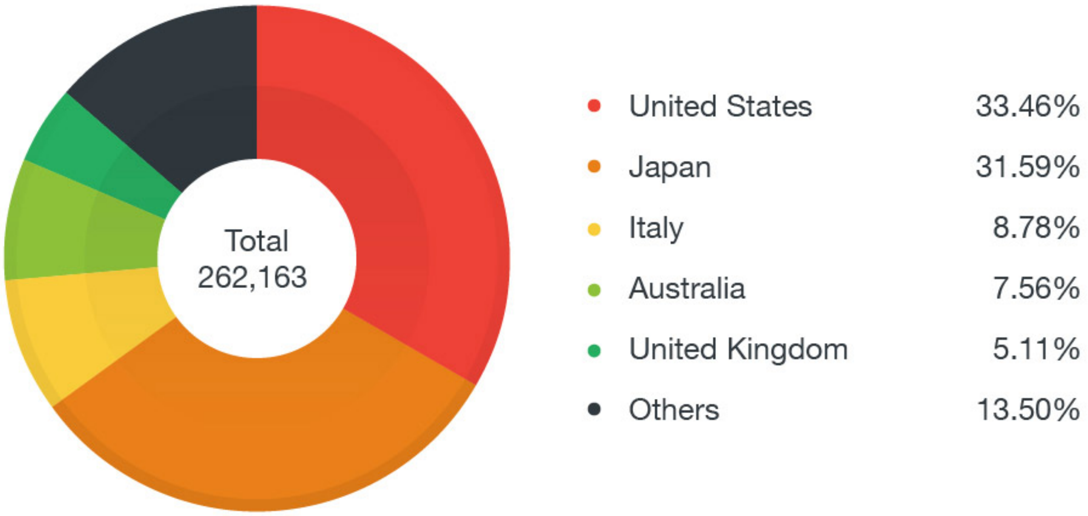


Figure 2: Distribution of AdGholas' activity per country

Given Astrum's capability to deter analysis and forensics, we were not able to capture the actual payloads the exploit kit delivered to different countries. Through our collaborative analysis with ProofPoint, however, we found a correlation with a recent string of ransomware attacks in the UK.

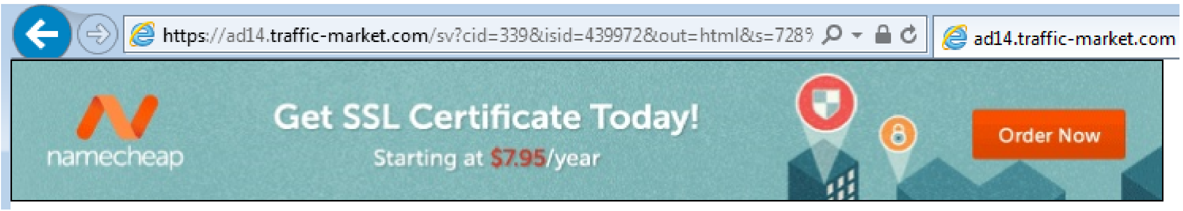

https://ad14.traffic-market.com/sv?cid=339&isid=439972&out=html&s=7289

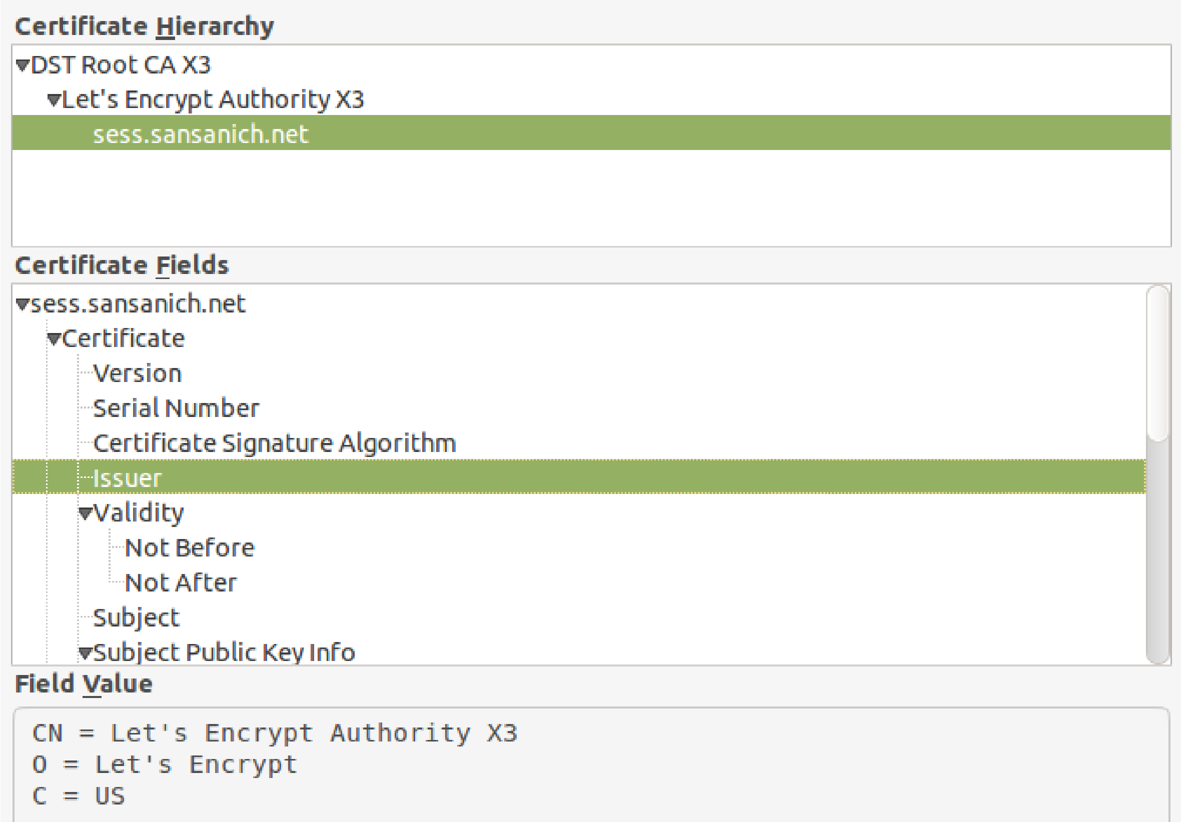
Figure 3: One of the malvertisements used by AdGholas

Astrum is known for being AdGholas' partner-in-crime. For instance, AdGholas is notorious for employing zero-day vulnerabilities in Internet Explorer, which other exploit kits would later incorporate. AdGholas was also notable for the scale of its campaigns and some of the techniques in its arsenal, like steganography.

When we saw the exploit kit back in May arming itself with anti-analysis capabilities as the exploit kit landscape continued to decline, we thought that it was only a matter of time before Astrum took advantage of the apparent lull by mounting actual malware campaigns.

The same can be construed during the height of WannaCry ransomware's outbreak and aftermath. On May 15, we saw Astrum's activities pick up again, and we've uncovered that they're delivered by the AdGholas malvertising operations. AdGholas is notorious for delivering multifarious threats, some of which include downloaders and banking Trojans Dreambot/Gozi/Ursnif and RAMNIT.

Between June 14 and 15, ProofPoint found that Astrum delivered ransomware, which is uncharacteristic (but unsurprising) of its usual payloads. The ones we saw are variants (detected by Trend Micro as RANSOM_CRYPAURA.SHLDJ and RANSOM_CRYPAURA.F117FF) of CryptAura family. Among them is CryptoMix: Mole, which first emerged in late April via abused Google Docs URLs.



Certificate Hierarchy

- DST Root CA X3
  - Let's Encrypt Authority X3
    - sess.sansanich.net

Certificate Fields

- sess.sansanich.net
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After
    - Subject
    - Subject Public Key Info

Field Value

```
CN = Let's Encrypt Authority X3
O = Let's Encrypt
C = US
```

Figure 4: The certificate to a shadow domain used by Astrum

Astrum has also started using HTTPS to encrypt and conceal its malicious traffic. They do this by applying a free HTTPS certificate to a shadow domain, a website that diverts users to the actual or primary URL. Shadowed domains can be traced to a black hat search engine optimization practice of creating websites expressly for search engine crawlers to generate rankings for the main domain. In Astrum's case, the shadow domain is mapped to the exploit kit's server and rotates the domain around every six hours. The cycle makes their activity (and attacks) more challenging to detect.

Mitigation

Exploit kits such as Astrum expose users to a plethora of threats—from personal information and financial theft to even encryption of important files—and can risk a company's bottom line and business continuity. Given the potent combination of Astrum and AdGholas, a defense-in-depth approach to security is recommended. Here are some best practices that can be adopted to mitigate them:

- ***Patch your systems and keep them updated.*** Exploit kits leverage vulnerabilities to infect machines, and Astrum in particular exploits at least three security flaws in Flash. Applying the latest patches and fixes helps mitigate threats that use vulnerabilities as doorways into the systems. Cybercriminals also take advantage of windows of exposure—the time between the disclosure and patching of a vulnerability—to infect systems. Enterprises should implement strong patch management policies, and consider employing virtual patching in the absence of patches.

- ***Secure your browsers from malicious websites.*** Exploit kits especially exploit web browsers, using malvertisements to lure victims. Keeping them updated is a must; automating their patches can also be considered. Blocking malware-hosting sites and implementing URL categorization helps avoid users from accessing malicious websites
- ***Proactively monitor your network and endpoints.*** Suspicious traffic from unknown locations (that sometimes masquerade as benign or legitimate) can indicate infection or exfiltration and incursion attempts. Firewalls, as well as intrusion detection and prevention systems, help provide red flags that IT/system administrators can watch out for. Whitelisting and monitoring applications and processes are just some of the measures that can help harden the endpoint.
- ***Apply the principle of least privilege.*** Disabling unnecessary or unused third-party components (i.e. web browser extensions or executables downloaded from dubious sources) and restricting unneeded administrator access to systems further reduce the system's attack surface. Network segmentation and data categorization help mitigates exposure and damage to data from threats like ransomware.
- ***Foster a culture of cybersecurity.*** Threats can arrive via a number of attack vectors, which is why end users and an organization's workplace must instill awareness to the significance of practicing cybersecurity hygiene. Securing points of entry such as email and being more prudent about socially engineered links/websites are just some of them.

Trend Micro Solutions

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)

Related Hashes (SHA256):

- 846416b8b5d3c83e0191e62b7a123e9188b7e04095a559c6a1b2c22812d0f25e — RANSOM_CRYPAURA.SHLDJ
- 7b3075b1a8cc0163d1e12000338adf3ed8a69977c4d4cacfc2e20e97049d727a — Ransom_CRYPAURA.F117FF

Domains and IP addresses related to the AdGholas malvertising campaign:

- ad14[.]traffic-market [.]com
  107[.]181[.]174[.]121
- avia-on[.]com
  195[.]123[.]218[.]25
- aviasales-online[.]com
  5[.]34[.]180[.]215
- ebooking-hotels[.].com
  185[.]82[.]217[.]43
- hotels-onlinebook[.]com
  107[.]181[.]174[.]140
- avia-discount[.]com
  195[.]123[.]212[.]72
- hotels-ebook[.]com
  185[.]82[.]217[.]127
- avia-bookings[.]com
  82[.]118[.]17[.]132
- avia-book[.]com
  195[.]123[.]209[.]229

Domains and IP addresses related to Astrum Exploit Kit:

- rsse[.]sansanich[.]net
  192[.]200[.]125[.]110
- arly[.]ipyjama[.]com
  188[.]138[.]125[.]39
- reta[.]carat-slim[.]com
  185[.]106[.]120[.]95
- requ[.]scorpyking-slim[.]com
  192[.]52[.]167[.]220
- unvai[.]albrightalliance[.]com
  185[.]45[.]193[.]123

Acknowledgement to ProofPoint's Kafeine whom we worked with in this research.

Related Posts:

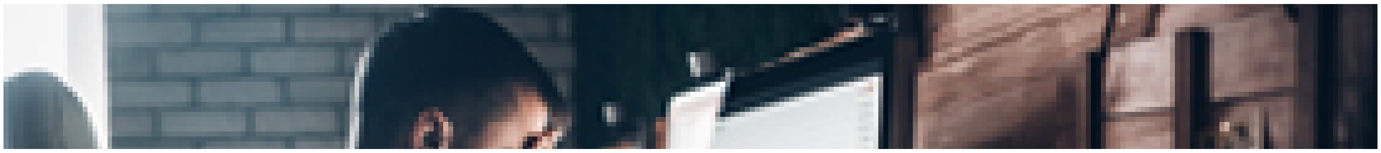
- **Microsoft Patches IE/Edge Zero-day Used in AdGholas Malvertising Campaign**
- **CVE-2016-3298: Microsoft Puts the Lid on Another IE Zero-day Used in AdGholas Campaign**
- **Will Astrum Fill the Vacuum in the Exploit Kit Landscape?**
- **CVE-2017-0022: Microsoft Patches a Vulnerability Exploited by AdGholas and Neutrino**

Tags: AdGholasAstrumexploit kitmalvertising

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

ADGHOLAS MALVERTISING CAMPAIGN EMPLOYS ASTRUM EXPLOIT KIT

Erebus Resurfaces as Linux Ransomware

Analyzing the Fileless, Code-injecting SOREBRECT Ransomware

Victims Lost US$1B to Ransomware

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

Recent Posts

- Following the Trail of BlackTech's Cyber Espionage Campaigns
- AdGholas Malvertising Campaign Employs Astrum Exploit Kit
- Erebus Resurfaces as Linux Ransomware
- Analyzing the Fileless, Code-injecting SOREBRECT Ransomware
- Microsoft Patches Windows XP Again As Part of June Patch Tuesday

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

Mouse Over, Macro: Spam Run in Europe Uses Hover Action to Deliver Banking Trojan
Erebus Resurfaces as Linux Ransomware
Analyzing the Fileless, Code-injecting SOREBRECT Ransomware
Analyzing Xavier: An Information-Stealing Ad Library on Android
MS17-010: EternalBlue's Large Non-Paged Pool Overflow in SRV Driver

Latest Tweets

- #Identitytheft hit an all-time high in 2016. Here's a more in-depth look at this growing cybercrime:… twitter.com/i/web/status/8…
  about 12 hours ago
- #SOREBRECT isn't the first #ransomware to misuse PsExec, but takes it up a notch with its code injection capability: bit.ly/2rxbG3P
  about 15 hours ago
- Our researchers found how cybercriminals take advantage of popular chat platforms: through their #APIs.… twitter.com/i/web/status/8…
  about 18 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