AdGholas Malvertising Campaign Using Astrum EK to Deliver Mole Ransomware

proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware

June 20, 2017

Blog

Threat Insight

AdGholas Malvertising Campaign Using Astrum EK to Deliver Mole Ransomware

June 20, 2017 Kafeine

Overview

The AdGholas group has been implicated in some of the largest malvertising campaigns we have ever observed. While this group has remained active, it appears that a number of universities in the United Kingdom were recently infected with ransomware via an AdGholas infection chain, a marked departure from the banking Trojans this group usually distributes. Although the universities made headlines as a result of the infection, it appears that the attack was far more widespread, with malvertising appearing on a number of high-profile websites.

Analysis

On June 15, 2017, several universities in the United Kingdom reported that they were victims of a ransomware attack [2] [3]. We decided to investigate this and ensure we were protecting and alerting our customers appropriately.

Because little information was available, we first followed public indicators [1] that actually pointed to an unrelated spam campaign: we had already internally documented this campaign spreading Dridex botnet ID 2302. We were unable to detect email activity explaining the reported infections and turned to assessing the drive-by landscape for associated activity. The Magnitude infection chain continued to avoid the UK while still spreading Cerber in Taiwan and the Republic of Korea. We also ensured that the EITest [5] infection chain in the UK was not redirecting to an exploit kit (EK). We were aware of an instance of RIG EK chain dropping GlobeImposter ransomware, but the scale did not match that of the outbreaks reported by the UK universities.

At this point, we began to consider whether AdGholas [11] into Astrum EK (also known as Stegano EK [12] [9]) might be the infection vector, despite the fact that the ransomware payload was inconsistent with the activity of their usual customers who normally spread banking malware.

We then learned that the command and control (C&C) IP address for the reported ransomware (137.74.163[.]43) was a Mole Ransomware C&C based on ET Intelligence portal data. This also matched other forensic information from the events.

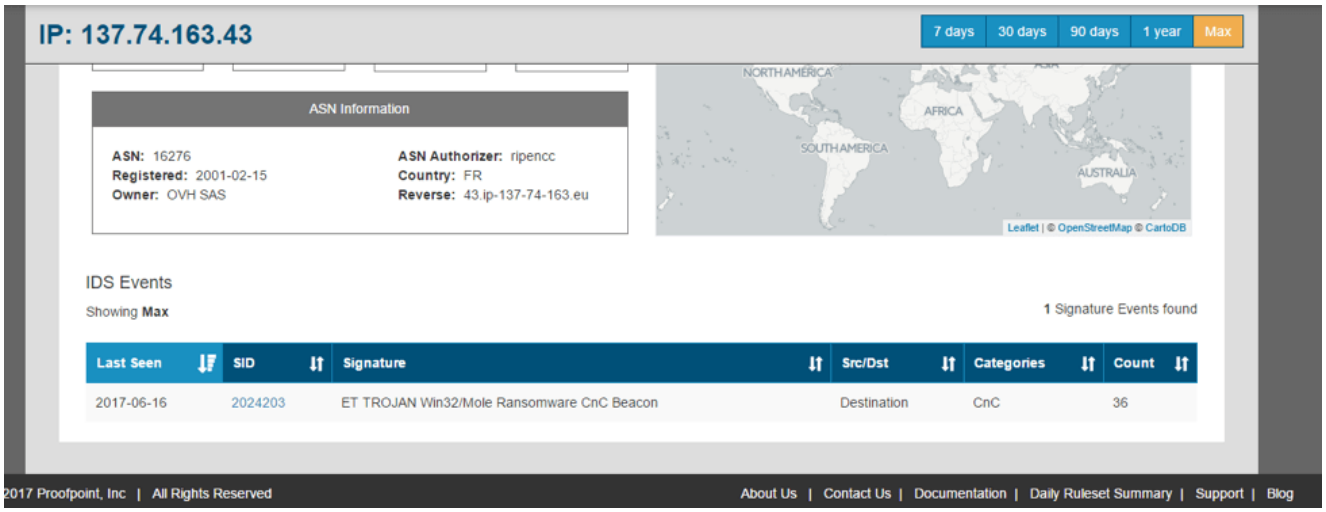

Figure 1: ET Pro data for 137.74.163[.]43

We searched for malware samples contacting this IP and found two, both of which had submission filenames to VirusTotal (mopslb.tmp and ldmso.tmp) that were consistent with an Astrum payload name on disk.

At that stage, we were almost convinced the events were tied to AdGholas / Astrum EK ([11] [12]) activity. We confirmed this, however, via an HTTPS connection common to the compromised host avia-book[.]com. We had been tracking its activity for several days with colleagues at Trend Micro and contacts in the Advertising industry.

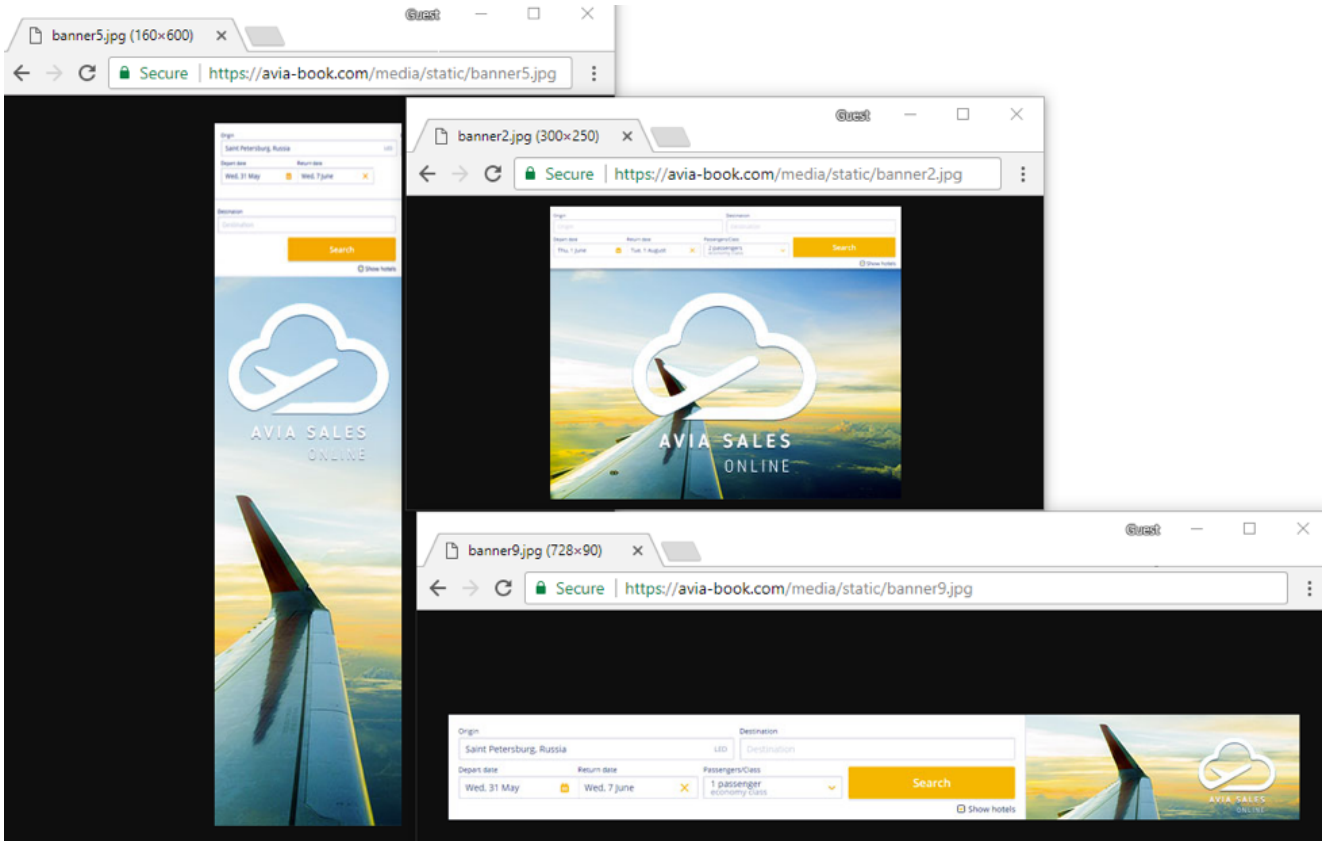

Figure 2: Three AdGholas banners in use, captured June 9, 2017

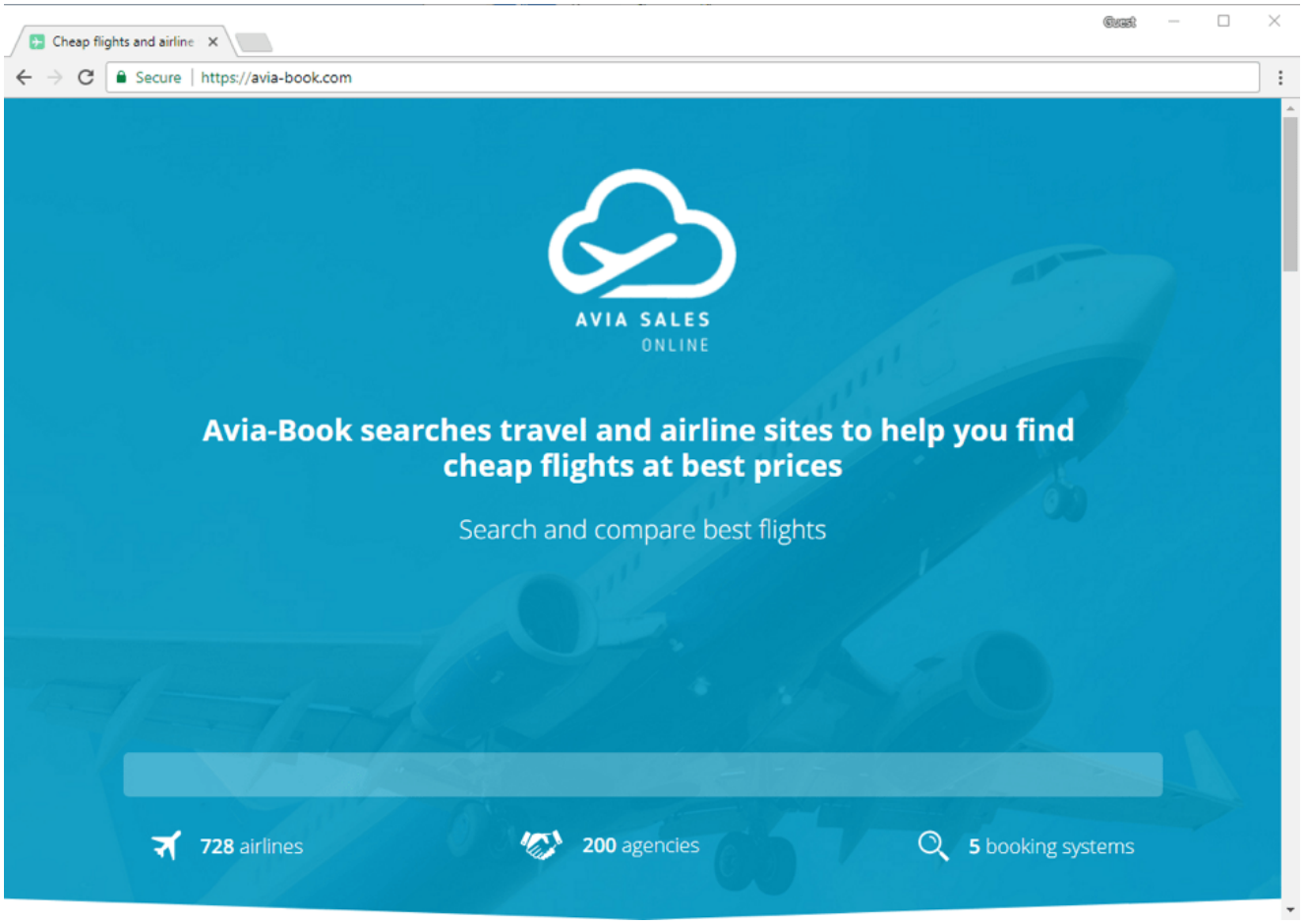

Figure 3: Air booking template in use by Avia-Book; this is not seen by users but aimed at ad agencies, captured June 9, 2017

This host was used in malvertising campaign targeting a number of countries: Great Britain, Australia, Canada, Italy, Monaco, Liechtenstein, Luxembourg, and Switzerland. Later, the host was also used in Japan, Taiwan, and the United States. We received confirmation that all of the compromised hosts also contacted the current Astrum IP, 185.45.193[.]123.

We attempted to replicate the infection chain and successfully witnessed AdGholas activity but were not able to trigger the EK redirection.

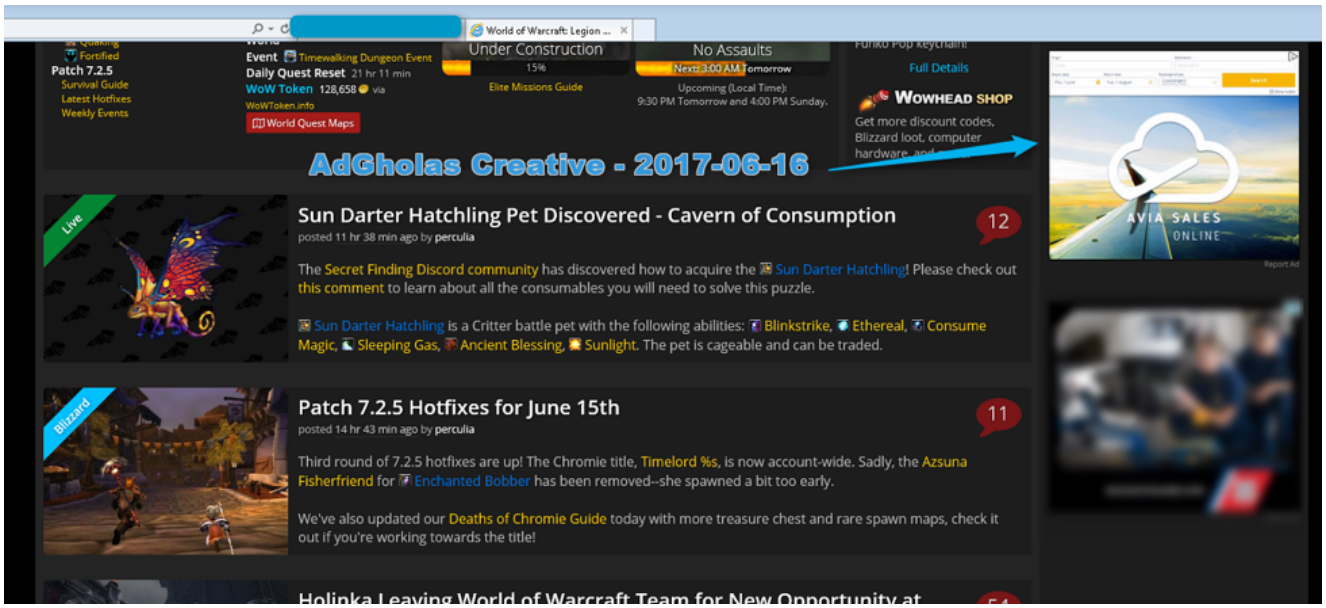

Figure 4: AdGholas activity captured live on June 16, 2017

Figure 5: AdGholas Malvertising Chain with involved nodes highlighted, captured June 16, 2017

However, while we did not capture the redirection in our lab systems, we know this conditionally leads to Astrum hosted with full HTTPS support on the host 185.45.193[.]123. [13]

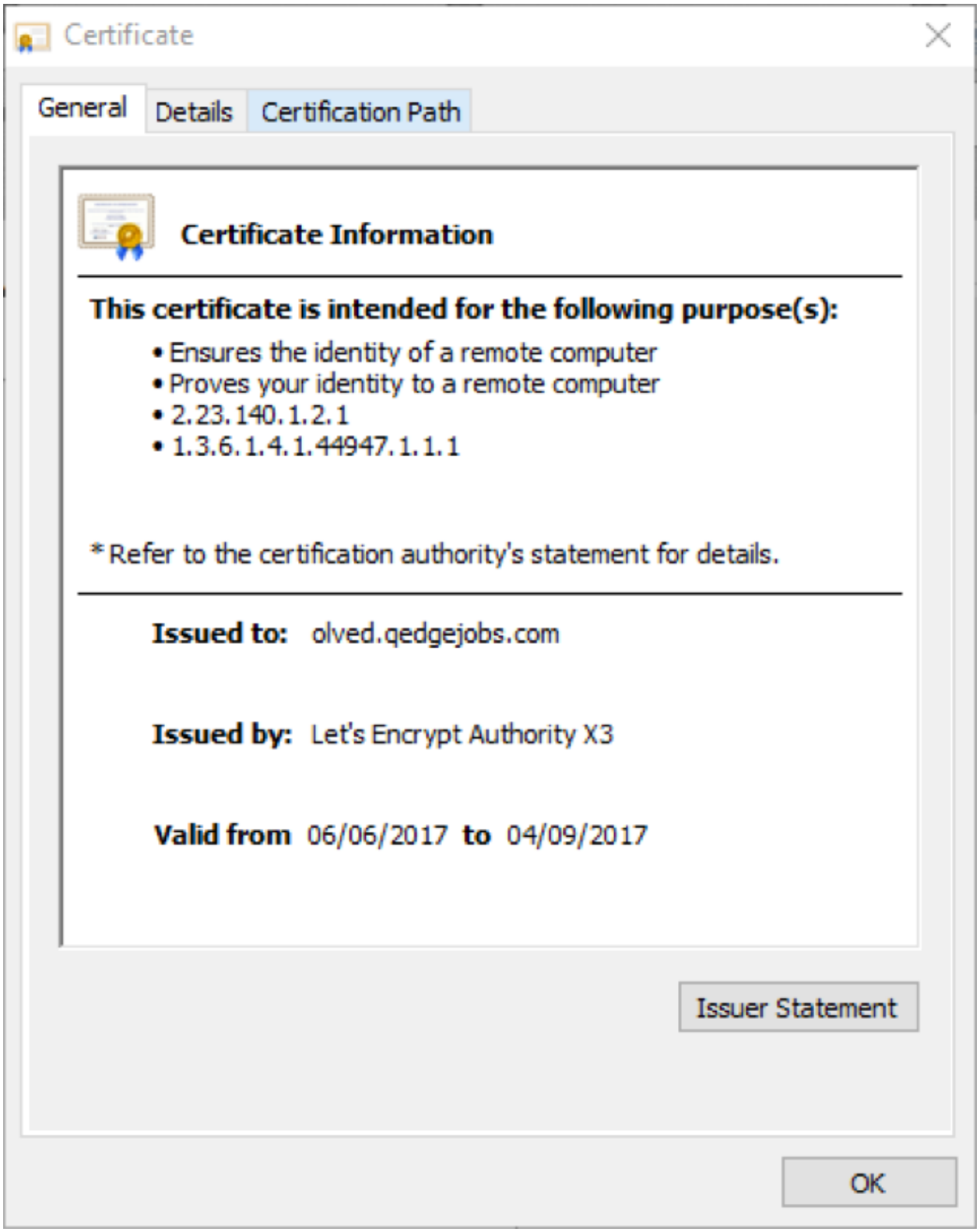

Figure 6: A Let's Encrypt Certificate used by Astrum - June 15, 2017

Astrum tried HTTPS between March 30 and April 4, 2017, before adopting it permanently at the end of May. Known CVEs used by Astrum include CVE-2016-0189 [7], CVE-2016-1019 [6], and CVE-2016-4117 [8]. The introduction of Diffie-Hellman [9] suggests that there might

be a new exploit the actors are trying to hide in this chain. Obtaining the patch state of the compromised hosts would help rule out this possibility.

It appears that between June 14 and 15, Astrum was dropping Mole ransomware in the United Kingdom and likely in the US [4]. Mole is a member of the CryptFile2/CryptoMix ransomware family. We do not know the payloads in other countries, but, based on past activity, we are confident they were banking Trojans. Unlike ransomware, bankers are generally less noisy and often remain unnoticed by victims.

Tags	Date
exploit-kit Astrum AdGholas Malvertising SmartAdServer GBR Mole Ransomware	2017-06-14
exploit-kit Astrum Seamless Malvertising CAN UndefinedDrop	2017-04-26
exploit-kit Astrum AdGholas Malvertising CAN Dreambot OvZz8XVH91INT7ek 2005	2017-03-24
exploit-kit Astrum AdGholas Malvertising AppNexus GBR BEL LUX Dridex 7200	2017-03-21
exploit-kit Astrum AdGholas Malvertising CAN Dreambot OvZz8XVH91INT7ek 2004 Comodo	2017-03-18
exploit-kit Astrum Undefined Keitaro CAN Dreambot OvZz8XVH91INT7ek 2004	2017-03-21

Figure 7: Sample of documented Astrum activity

```
!!!IMPORTANT INFORMATION!!!

All of your files are encrypted with RSA 2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

Follow these steps:
1. Download and install Tor Browser: http://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: http://supportiv2xvvdmx.onion/
4. Follow the instructions on the site.
!!! Your DECRYPT-ID: 6[redacted]1-2b04-4f72-8[redacted]5-12[redacted]6e0 !!!
```

Figure 8: _HELP_INSTRUCTION.TXT dropped by Mole ransomware on victim machines

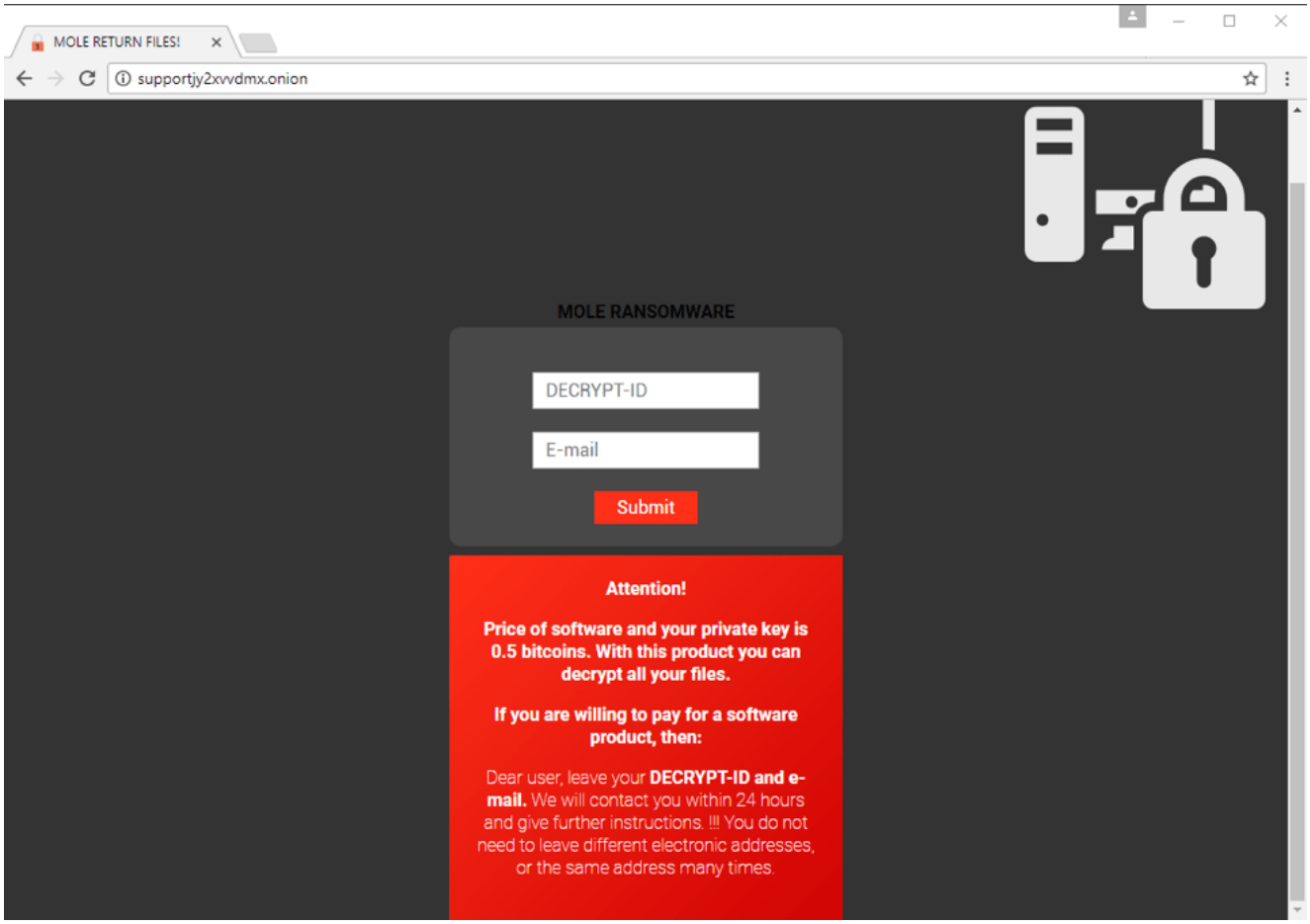

Figure 9: Mole Ransomware Payment Server - June 15, 2017

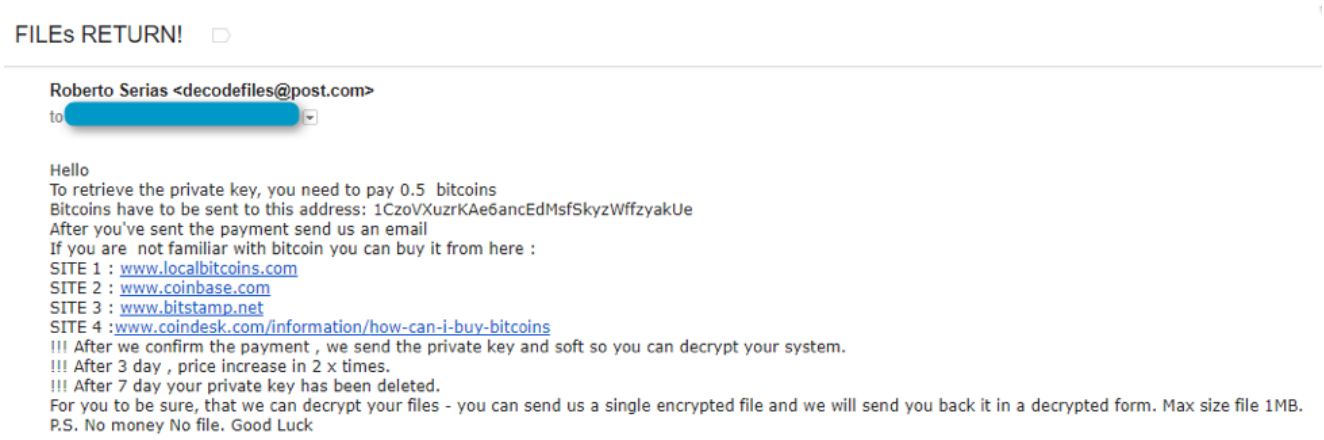

Figure 10: Mole FILEs RETURN! Email - June 15, 2017

Conclusion

AdGholas malvertising redirecting to the Astrum Exploit Kit is the most evolved blind mass infection chain known today. Full HTTPS, heavy smart filtering, domain shadowing, Diffie-Hellman, and perfect knowledge of how the Advertising industry operates allow these threat actors to lure large agencies to bring them high volumes of traffic from high-value website and targets.

Moreover, it is worth remembering that a common misperception about drive-by malvertising attacks remains prevalent: there is no need to click on the advertisement to be infected. *It is enough simply to display the ad:* if the machine is vulnerable and targeted, then the infection occurs without any user interaction.

Acknowledgements

We would like to thank first our colleagues Joseph C. Chen at Trend Micro and Frank Ruiz at Fox-IT InTELL for their tremendous help in this study. We would also like to thank people in the Advertising industry and on the victim side who helped us directly.

References

[1] https://twitter.com/TheRegister/status/875110325275643904

[2] https://www.ulster.ac.uk/isd/incident-response

[3] https://www.ucl.ac.uk/isd/news/isd-news/jun2017/ucl-wide-ransomware-attack-14062017

[4] http://www.radioiowa.com/2017/06/16/waverly-hospitals-computers-hacked-by-ransomware/

[5] https://www.proofpoint.com/us/threat-insight/post/EITest-Nabbing-Chrome-Users-Chrome-Font-Social-Engineering-Scheme

[6] https://www.proofpoint.com/us/threat-insight/post/killing-zero-day-in-the-egg

[7] http://malware.dontneedcoffee.com/2016/07/cve-2016-0189-internet-explorer-and.html

[8] http://malware.dontneedcoffee.com/2016/05/cve-2016-4117-flash-up-to-2100213-and.html

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/astrum-exploit-kit-abuses-diffie-hellman-key-exchange/

[10] https://www.bleepingcomputer.com/forums/t/649297/mole02-virus/

[11] https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight

[12] https://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/

[13] http://blog.trendmicro.com/trendlabs-security-intelligence/adgholas-malvertising-campaign-employs-astrum-exploit-kit/

Indicators of Compromise

Domain | IP	Comment
sess.sansanich[.]net|192.200.125[.]110	Astrum - 2017-05-15
indi.kmlaustenesq[.]com|192.200.125[.]110	Astrum - 2017-05-25
ific.finethreadsbespoketailors[.]com|188.138.125[.]39	Astrum - 2017-05-30
requ.scorpyking-slim[.]com|192.52.167[.]220	Astrum - 2017-06-06
unvai.albrightalliance[.]com|185.45.193[.]123	Astrum - 2017-06-12
olved.qedgejobs[.]com|185.45.193[.]123	Astrum - 2017-06-14
tioze.rigimediadity[.]cricket|104.200.67[.]126	Astrum - 2017-03-30
lity.albrightalliance.com|185.45.193[.]123	Astrum - 2017-06-14
compr.darthom[.]com|188.165.62[.]20	Astrum - 2017-03-30
mous.straightorwadly[.]top|185.61.149[.]52	Astrum - 2017-04-03
avia-on[.]com|195.123.218[.]25	AdGholas - 2017-06-02
ad14.traffic-market[.]com|107.181.174[.]121	AdGholas - 2017-05-15 > 21
www.aviasales-online[.]com|5.34.180[.]215	AdGholas - 2017-05-25/26
hotels-onlinebook[.]com|107.181.174[.]140	AdGholas - 2017-05-28/29
avia-discount[.]com|195.123.212[.]72	AdGholas - 2017-05-30
avia-book[.]com|195.123.209[.]229	AdGholas - 2017-06-08 > 14
ebooking-hotels[.]com|185.82.217[.]43	AdGholas - 2017-05-27

hotels-ebook[.]com|185.82.217[.]127	AdGholas - 2017-05-30
avia-bookings[.]com|82.118.17[.]132	AdGholas - 2017-06-01
137.74.163[.]43	Mole C2
supportjy2xvvdmx[.]onion	Mole Payment Server
decodefiles@post[.]com	Files Return email sender
1CzoVXuzrKAe6ancEdMsfSkyzWffzyakUe	Bitcoin address mentioned in “Files Return” Email

sha256	**Comment**
7b3075b1a8cc0163d1e12000338adf3ed8a69977c4d4cacfc2e20e97049d727a	Mole Ransomware - 2017-06-14
846416b8b5d3c83e0191e62b7a123e9188b7e04095a559c6a1b2c22812d0f25e	Mole Ransomware - 2017-06-14

Select ET Signatures that would fire on such traffic:

2024203 || ET TROJAN Win32/Mole Ransomware CnC Beacon

Subscribe to the Proofpoint Blog