Newscaster Team Leverages Updated Toolset to Target Petroleum, Financial and Tech Interests in Recent Campaign; BeEF Used in Watering Hole Attacks

Fusion (FS) | Cyber Espionage (CE)

March 01, 2016 10:10:00 AM, 16-00002388, Version: 3

Executive Summary

Newscaster Team has been implicated in a recent campaign affecting multiple industries through strategic website compromises and other social engineering vectors. Throughout the 2015 calendar year, Newscaster Team has shifted tactics multiple times and has expanded their operational scope. Strategically compromised websites used by Newscaster Team introduce the strong likelihood of far reaching impacts across multiple sensitive industries.

Key Points

- Newscaster Team has weaponized legitimate websites belonging to Lloyds Bank, Kronos Incorporated and an unofficial site associated with a Middle Eastern petroleum company using the Browser Exploitation Framework (BeEF).
- Since mid-2015, Newscaster Team has used an updated variant of their IRC bot malware. Additionally, these actors are believed to have targeted mobile platforms with malicious APKs.
- Linked infrastructure suggests that Newscaster Team has continued previously observed tactics involving the use of news-themed social engineering.

Threat Detail

Watering Hole Sites Attributed to Newscaster Team

iSIGHT Partners believes that multiple watering holes recently observed on websites associated with a Middle Eastern petroleum firm, UK-based Lloyds Bank and Kronos Incorporated, a workforce management provider, were carried out by Newscaster Team. Due to overlaps in infrastructure and tools introduced following exploitation and the continued use of news-oriented social engineering, we assess with moderate confidence this activity is attributed to the Iran-nexus cyber espionage operation.

- Compromised sites exposed visitors to exploitation by an open-source exploitation framework known as the Browser Exploitation Framework (BeEF) as early as late November 2015. A sensitive source indicates that during BeEF sessions operators leveraged payload delivery infrastructure (104[.]238[.]97[.]226) that overlaps with xvy.in, a domain previously used by Newscaster Team in social engineering attacks (for more information, see Intel-1034934, May 28, 2014).
- An additional domain, breaking-news.club, hosted payloads which beacon to command and control (C&C) at 64[.]150[.]189[.]90[.] IRC Bot malware of the same nature previously used by Newscaster Team also uses the C&C. Furthermore, news-oriented social engineering pretexts are a hallmark of Newscaster Team operations.
- Configurations found on C&C hosts resemble distinct configurations previously used by Newscaster Team.

Figure 1: Newscaster Team logo

Following a marked hiatus since the public disclosure of their operations in late 2014, Newscaster Team is suspected to have carried out limited targeted activity. We believe that Newscaster Team resumed operations in mid-2015 as demonstrated by the reuse and weaponization of domains intended for social engineering and continued development of implants.

- In April 2015 Newscaster Team registered news-themed infrastructure (breaking-news.club).
- Malware implants observed in May 2015 indicate that Newscaster Team expanded their operational capability by developing weaponized APKs used to target Android mobile devices that were distributed using xvy.in, a domain previously utilized by these actors. For more information, see the technical annex.
- Additionally, in September 2015 Newscaster Team distributed IRC bot implants leveraging another arbitrary URL shortening domain (shlnk.be) to unidentified targets (for more information, see Intel-1210331, Nov. 9, 2014).

We assess with low confidence that Newscaster Team expanded its operational scope to include the technology sector. Newscaster Team infrastructure overlaps with a domain which appears to have been created to target a digital security firm; however, we have no evidence of weaponization.

- In November 2015 iSIGHT Partners observed an IP overlap occurring between Newscaster domain xvy.in and a faux Gemalto job recruitment domain (jobsatgemalto.com) which had been registered in October 2015.
- Previous Newscaster Team domains have spoofed technology firms such as McAfee.

Open Source Tools BeEF and Meterpreter Used in Watering Hole Attacks

We observed multiple compromised websites in February 2015 that were weaponized with malicious code from BeEF, an open-source client-side attack framework.

- The compromised websites are characterized by a distinctive HTML script block which loads BeEF hook.js code within victim browsers.
- BeEF JavaScript resources were hosted on a number of attacker-controlled dynamic DNS domains and IP addresses.
- BeEF hook.js code repurposed by Newscaster Team were hosted on operator infrastructure and retained a consistent naming convention of either jquery3-1.js or jquery.js.

Figure 2: Injected website referencing externally hosted BeEF

Table 1: Sample Watering Hole Redirects

Compromised Host	Redirect URL	Resolved IP
international.lloydsbank.com	45[.]63[.]14[.]123 (embedded)	
www[.]kronos[.]com	45[.]79[.]157[.]129:3001/jquery[.]js	
forum.aramcoexpats.com	google-analytics.serveirc.com:3001/jquery3-1.js	85[.]90[.]246[.]94
aramcoexpats.com	w3schools.ddns.net/jquery.js	31[.]131[.]21[.]236

Based on historical observations of Newscaster Team infrastructure, we assess with moderate confidence that the primary payloads delivered to potential victims visiting compromised websites are Meterpreter variants coupled with legitimate applications such as Adobe Flash, Apache Benchmark and Putty. However, IRC Bot has been leveraged by the operators as well.

- In February 2016, iSIGHT Partners observed aramcoexpats.com redirecting visitors to google-analytics.servirc.com, which served BeEF. The domain has also served as C&C for a Meterpreter implant (MD5: 6b843c190600c0870d663d2af6af2dcc).
- We observed multiple Meterpreter samples that are linked by a combination of shared C&C infrastructure and spear-phishing domains.

IRC Bot Malware Updated and Used as First and Second-Stage Utility; Links to Newscaster Team Bolstered by Distinct IRC Configurations

IRC bot malware previously leveraged by Newscaster Team has seen continued distribution and incremental updates since its initial discovery. Given first-hand observations and sensitive source information, iSIGHT Partners believes IRC bot malware is distributed as a first- and second-stage payload. Furthermore, configurations observed within recent infrastructure shared between Meterpreter and IRC Bot samples reflect distinct configurations in infrastructure previously tied with Newscaster Team, further highlighting responsible operators.

- Meterpreter sessions in the September 2015 timeframe were used to distribute IRC Bot as a second-stage payload.
- In one instance, following initial profiling, visitors to weaponized websites were forced to download the IRC Bot payload Flashplayer_001.exe from 104[.]238[.]97[.]226 as a first-stage payload.
- A host (45[.]56[.]123[.]129) used for IRC bot malware C&C during the November 2015 timeframe was configured in a manner similar to historic Newscaster Team domain update.mcafeea.com as seen in Figure 2 (for more information, see Intel-1278296, Nov. 9, 2014).

```
USER AS_a # # :des
NICK Moreen
JOIN :#klik
:update.mcafeea.com NOTICE AUTH :*** Looki
:update.mcafeea.com NOTICE AUTH :*** Could
address instead
:update.mcafeea.com 001 Moreen :Welcome to
```

Figure 3: 45[.]56[.]123[.]129 IRC echo

Fake Resume Website Weaponized with BeEF; Likely Purposed for Social Engineering

We identified a domain sharing an IP address with an identified Meterpreter sample believed to be created by Newscaster Team to support elaborate social engineering pretexts. The domain is associated with content regarding a social network for musicians.

- The domain emilymarsden.serveblog.net historically resolved to 45[.]32[.]68[.]241 which shares a C&C IP with an identified Meterpreter sample (MD5: 99bce83e77383f50fcc3fa67266ca646).
- Analysis of the HTML markup of the website indicates that the website was actively weaponized with a BeEF inject located at w3schools.ddns.net:3003/jquery.js.
- Review of last modified times exposed by HTTP response headers indicates that the website was probably staged as early as Jan. 3, 2016.

Figure 4: Fake musician site established by Newscaster Team

Outlook and Implications

Despite utilization of common tools and techniques, Newscaster Team has carried out prolific campaigns through the use of complex social engineering schemes and aggressive behavior. Though there is no indication that they can leverage significant technical resources, Newscaster Team is a motivated operator who poses significant risk to global entities in the energy and financial sectors as well as entities associated with defense, diplomacy and policy. Furthermore, recent targeting of technology firms such as digital security purveyor Gemalto may demonstrate broadening interests and complex attempts to overcome sophisticated security countermeasures.

Technical Annex: Execution

Files Dropped

Malicious Android Application Package

Securitywarning.apk (MD5: 0796d76defb4f4ad1eaccd2b7f2fe343)

- Acquired from:
  - hxxp://breaking-news[.]club/download/securitywarning[.]apk

    - hxxp://xvy[.]in/q4fml
        - xvy.in is a link-shortener that has also been previously used by Newscaster Team.
- Meterpreter Payload
    - Reverse TCP shell
- C&C: 103[.]3[.]62[.]117:5555
- Permissions:
    - Manipulate SMS and GPS
    - Perform payments
    - Access Internet and private information

Malicious Droppers
The following malicious droppers follow the same installation steps in all four instances:

- Writes a legitimate Flash web installer in %TEMP%
- Writes a weaponized Putty SFTP client in %TEMP%
    - It is likely that the weaponized portion of the binary is a reverse Meterpreter shell
- Executes both

Sample #1:

- flashplayer19.7_install.exe (MD5: ab59ba909a34ec973045dcad6e867276)
    - Malicious dropper
    - Drops the following:
        - Flashplayer.exe (MD5: 96C436D7E2B49F213A983CB3E648B04D)
            - Legitimate Flash web installer
        - Serviceupda.exe (MD5: A6719AC8E069F3AA4ABE2A087A3DD317)
            - Weaponized Putty SFTP Client
            - C&C1: 94[.]237[.]25[.]45:443
            - C&C2: 45[.]79[.]4[.]164:443

Sample #2:

- 5eb673fee3b811910032788665886471
    - Malicious dropper
    - Drops the following:
        - Flashplayer.exe (MD5: 96C436D7E2B49F213A983CB3E648B04D)
            - Legitimate Flash web installer
        - serviceupdat.exe (MD5: d04bf56670f2a7ae9f7cc0fcc7fb8d37)
            - Weaponized Putty SFTP Client
            - C&C1: 94[.]237[.]25[.]45:443

Sample #3:

- flashplayer19_install.exe (MD5: db2c63eb90fe76111b1550f9409d9d16)
    - Retrieved from hxxp://86[.]105[.]54[.]144/download/flashplayer19_install[.]exe
    - Malicious dropper
    - Drops the following:
        - Flashplayer.exe (MD5: 96C436D7E2B49F213A983CB3E648B04D)
            - Legitimate Flash web installer
        - Serviceupdat.exe (MD5: D7EECD49E082D6314CBF33D15EE57AAD)
            - Weaponized Putty SFTP Client
            - C&C1: 94[.]237[.]25[.]45:443

Sample #4:

- Flashplayer20_ga_install.exe (MD5: 7243ab4937eb43d8b232e0a4cab6fb7d)
  - Malicious Dropper
  - Drops the following:
    - Flashplayer.exe (MD5: 96C436D7E2B49F213A983CB3E648B04D)
      - Legitimate Flash web installer
    - %TEMP%\taskmgor.exe (MD5: 282D5D0FF090299416F1EB5C9B1B7E9A)
      - Weaponized Putty SFTP Client
      - C&C1: 162[.]247[.]155[.]101:4545

Weaponized Putty Client, Dropper Not Obtainable
99bce83e77383f50fcc3fa67266ca646

- Weaponized Putty SFTP client
- C&C1: 45[.]32[.]68[.]241:443
- C&C2: 94[.]237[.]25[.]45:443

Reverse Meterpreter Powershell Script Droppers
Each of these two binaries follows the following execution path in respect to Powershell:

- Executes powershell
  - "powershell -nop -win hidden -noni –enc <BASE64 ENCODED DATA>"
    - The base64 encoded data decodes to a 32bit reverse Meterpreter shell, using Powershell, borrowed from the Teensy payload
    - Both payloads are configured to use the C&C: 64[.]150[.]189[.]90:5556
- The Powershell script writes three files that use the same randomly generated name and are stored temporarily in order to write supporting files:
  - %TEMP%\<RANDOM>.0.cs (MD5: 7319070C34DAA5F6F2ECE2DFC07119EE)
    - Compilation source for .NET library used to PInvoke Windows functions
  - %TEMP%\<RANDOM>.cmdline (MD5 varies)
    - Includes the output file and directory for the written DLL file and the compilation source file <RANDOM>.0.cs as parameters
  - %TEMP%\<RANDOM>.out (MD5 varies)
    - Compiler messages
- csc.exe is executed with the "@"%TEMP%\<RANDOM>.cmdline" in order to import more options and will write the following files:
  - <RANDOM>.dll (MD5 varies)
    - .NET library used to pinvoke VirtualAlloc, CreateThread, and memset

Sample #1:
interiordesigns.exe (MD5: 5cbf67bc5b4b8a8339d5bc5e09a0364d)

- Acquired from hxxp://breaking-news[.]club/download/interiordesigns[.]exe
- This sample also writes and executes the following files:
  - %TEMP%\flashplayer.bat (MD5: b14e2e6657e4591f9cd40f7cfdced616)
    - Malicious batch script that executes the initial Powershell command
  - %STARTUP%\winsys.lnk (MD5: d759530444791de5c890fe4dc485f066)
    - Persistence mechanism
  - %TEMPSlidershow1.exe (MD5: 8706cbfe45199f2bfd6e7a8fd93f0fae)
    - Benign lure video/slideshow

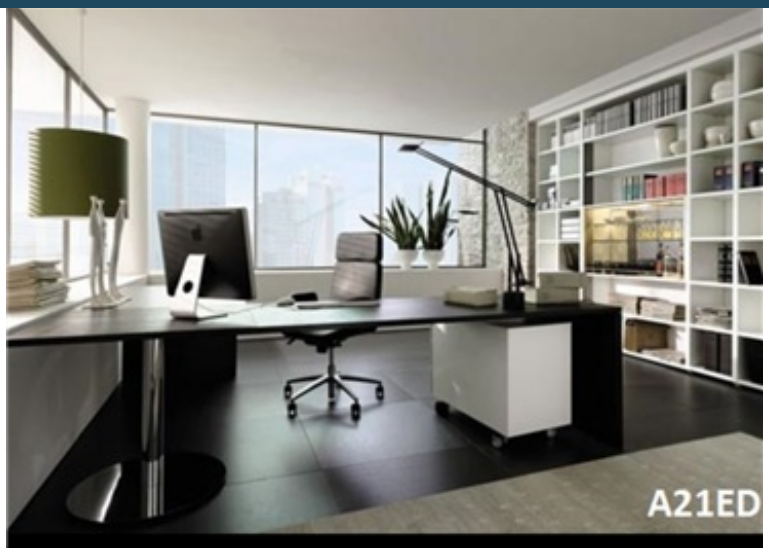

Figure 5: Sample picture from slideshow1.exe

Sample #2:
Flashplayer.exe (MD5: 7ddc67ef86ea12c2d368c33e52c0b47a)

- This sample presents the following dialog as a lure. When clicked the binary will execute a web browser that takes the user to Adobe's download page for Flash.

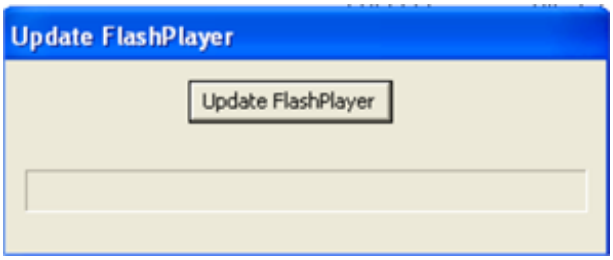

Figure 6: Lure dialog

IRC Bots
Sample #1:
microsoftupdate.exe (MD5: 49597b269fdf37faaa0962efc838aac7)

- Acquired from hxxp://45[.]58[.]37[.]142/microsoftupdate[.]exe
- Mutex: "MyOneCopyMutex"
- Appears to be an updated version of the following sample
  - This is due to similar functionality of the two with the addition of joining a channel, having a specific user, and using a random name pulled from an encoded list
- C&C/IRC server: 45[.]56[.]123[.]129
  - User: "AS_a # # :des"
  - Channel: #klik
  - Nick: (random name pulled from an encoded list found statically within binary)

Sample #2:
JoanSlideshow.exe (MD5: b144f64ecb51c4a9b940e882213b5f40)

- Acquired from:
  - hxxp://212[.]71[.]249[.]170/JoanSlideshow[.]exe
  - hxxp://shlnk[.]be/rpiwe
  - Self-extracting RAR archive

JoanSlideshow.exe drops the following files:

- %TEMP%\Slideshow.exe (MD5: ece5b62a4ed4e88dab4f1b5451f54794)
    - Also named My.exe
        - Also acquired from:
            - hxxp://212[.]71[.]249[.]170/my[.]exe
            - hxxp://64[.]150[.]189[.]90/my[.]exe
            - hxxp://64[.]150[.]189[.]90/tools/my[.]exe
- %TEMP%\Slideshow1.exe (MD5: a7adf752855a973abbfb04bf71bcba8a)
    - Benign lure video/slideshow

Figure 7: Pictures from benign lure video slideshow1.exe

When slideshow.exe/my.exe is executed, it drops and executes the following files:

- %TEMP%\dvvm.exetmp.vbs (MD5: 9fb92746bfe954a87b11a342f55ce224)
    - Copies one file to another
    - Accepts two parameters and copies parameter one to parameter two
- %TEMP%\dvvm.exetmp1.vbs (MD5: 39ac4187aaf38b986ff238c23daaf94e)
    - Sleeps 9000 and then executes "dvvm.exe [1]"

My.exe executes dvvm.exetmp.vbs with itself as the first parameter and the following as its second parameter, causing the file to be written to disk in this location:

- %TEMP%\dvvm.exe (MD5: ece5b62a4ed4e88dab4f1b5451f54794)
    - Mutex: mpk1
    - IRC bot
    - C&C/IRC Server: 45[.]58[.]37[.]142:6667
        - Nick and User are randomly generated

Dvvm.exe is then executed and connects to an IRC server, no channel, and then drops the following files:

- %TEMP%\nick435.tmp (MD5 varies)
    - Includes the randomly generated IRC nickname
- %TEMP%\save.tmp (MD5 varies)
    - Keylog file

Persistence Method

The IRC bot, MD5: ece5b62a4ed4e88dab4f1b5451f54794, maintains its persistence on the victim's system through the use of the following registry entry:

- **Key**: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\explorer

- **Value**: "%TEMP%\dvvm.exe" [1]

Technical Annex: Network Communications

Note: A large portion of the above activity leverages reverse Meterpreter shells to following servers and ports:

- 64.150.189.90:5556
- 94.237.25.45:443
- 45.79.4.164:443
- 45[.]32[.]68[.]241:443
- 162.247.155.101:4545

After successful installation / initialization of the IRC bot, dvvm.exe (MD5: ece5b62a4ed4e88dab4f1b5451f54794), it proceeds to make the following callback to the C&C server "45[.]58[.]37[.]142" via port TCP/6667:

VICTIM to C&C

NICK hcumeaskcx

USER hcumeaskcx hcumeaskcx hcumeaskcx hcumeaskcx

C&C to VICTIM

:mpk.Root NOTICE Auth :*** Looking up your hostname...

:mpk.Root NOTICE Auth :*** Could not resolve your hostname: Domain name not found; using your IP address (69[.]80[.]108[.]188) instead.

:mpk.Root NOTICE Auth :Welcome to .MpkNet.!

:mpk.Root 001 hcumeaskcx :Welcome to the MpkNet IRC Network hcumeaskcx!hcumeaskcx@69[.]80[.]108[.]188

:mpk[.]Root 002 hcumeaskcx :Your host is mpk.Root, running version 2.0

:mpk.Root 003 hcumeaskcx :This server was created 16:34:47 Aug 28 2013

:mpk.Root 004 hcumeaskcx mpk.Root 2.0 iosw biklmnopstv bklov

:mpk.Root 005 hcumeaskcx AWAYLEN=200 CASEMAPPING=rfc1459 CHANMODES=b,k,l,imnpst CHANNELLEN=64 CHANTYPES=# CHARSET=ascii ELIST=MU FNC KICKLEN=255 MAP MAXBANS=60 MAXCHANNELS=20 MAXPARA=32 :are supported by this server

:mpk.Root 005 hcumeaskcx MAXTARGETS=20 MODES=20 NETWORK=MpkNet NICKLEN=31 PREFIX=(ov)@+ STATUSMSG=@+ TOPICLEN=307 VBANLIST WALLCHOPS WALLVOICES :are supported by this server

:mpk.Root 042 hcumeaskcx 713AAAALV :your unique ID

:mpk.Root 375 hcumeaskcx :mpk.Root message of the day

:mpk.Root 372 hcumeaskcx :-

:mpk.Root 372 hcumeaskcx :- _____ _____ _____ _____ _

:mpk.Root 372 hcumeaskcx :- |_ _| |_ _| | __ \ / ____| | |

:mpk.Root 372 hcumeaskcx :- | | _ __ ___ _ __ | | | |__) || | __| |

:mpk.Root 372 hcumeaskcx :- | | | '_ \ / __| | '_ \ | | | _ / | | / _` |

:mpk.Root 372 hcumeaskcx :- _| |_ | | | | __ \ | |_) | _| |_ | | \ \ | |____ | (_| |

:mpk.Root 372 hcumeaskcx :- |_____| |_| |_| |___/ | .__/ |_____| |_| _\ _____| __,_|

:mpk.Root 372 hcumeaskcx :- _____| |_____

:mpk.Root 372 hcumeaskcx :- |_____|_|_____|

:mpk.Root 372 hcumeaskcx :-

:mpk.Root 372 hcumeaskcx :- Putting the ricer in IRCer since 2007

:mpk.Root 372 hcumeaskcx :-

:mpk.Root 372 hcumeaskcx :- //\

:mpk.Root 372 hcumeaskcx :- V \ WELCOME TO AN INSPIRCD NETWORK

```
:mpk.Root 372 hcumeaskcx :         \  \_    If you see this, I am probably new.
:mpk.Root 372 hcumeaskcx :          \,'.`-.   If I'm not new, my owner is lazy.
:mpk.Root 372 hcumeaskcx :           |\ `. `.
:mpk.Root 372 hcumeaskcx :           ( \  `. `-.                     _,.-:\
:mpk.Root 372 hcumeaskcx :            \ \   `.  `-._           __..--' ,-';/
:mpk.Root 372 hcumeaskcx :             \ `.   `-.   `-..___..---'   _.--' ,'/
:mpk.Root 372 hcumeaskcx :              `. `.    `-._        __..--'    ,' /
:mpk.Root 372 hcumeaskcx :                `. `-_     ``--..''       _.-' ,'
:mpk.Root 372 hcumeaskcx :                  `-_ `-.___        __,--'   ,'
:mpk.Root 372 hcumeaskcx :                     `-.__   `----"""    __.-'
:mpk.Root 372 hcumeaskcx :                          `--..____..--'
:mpk.Root 372 hcumeaskcx :
:mpk.Root 372 hcumeaskcx :        ---- To change, see motd.txt.example -----
:mpk.Root 372 hcumeaskcx :       /                                      \
:mpk.Root 372 hcumeaskcx :      /   * Web: hxxp://www[.]inspircd[.]org          \
:mpk.Root 372 hcumeaskcx :      |   * IRC: irc.inspircd.org #inspircd        |
:mpk.Root 372 hcumeaskcx :      |   * Docs: hxxp://wiki[.]inspircd[.]org       |
:mpk.Root 372 hcumeaskcx :      |   * Bugs: hxxp://inspircd[.]org/bugs         |
:mpk.Root 372 hcumeaskcx :      |                                        |
:mpk.Root 372 hcumeaskcx :      | We hope you like this software. Please do  |
:mpk.Root 372 hcumeaskcx :      | make  sure  you  put  some  effort  into   |
:mpk.Root 372 hcumeaskcx :      | your configuration, though, so you love it.|
:mpk.Root 372 hcumeaskcx :      | Enjoy.                                 |
:mpk.Root 372 hcumeaskcx :      |                                        |
:mpk.Root 372 hcumeaskcx :      \               -- The InspIRCd Team    /
:mpk.Root 372 hcumeaskcx :       ----------------------------------------
:mpk.Root 372 hcumeaskcx :
:mpk.Root 376 hcumeaskcx :End of message of the day.
:mpk.Root 251 hcumeaskcx :There are 3 users and 0 invisible on 1 servers
:mpk.Root 254 hcumeaskcx 0 :channels formed
:mpk.Root 255 hcumeaskcx :I have 3 clients and 0 servers
:mpk.Root 265 hcumeaskcx :Current Local Users: 3  Max: 6
:mpk.Root 266 hcumeaskcx :Current Global Users: 3  Max: 6
```

VICTIM to C&C

```
PRIVMSG mpk :!MpkPing <<mpk>>62402<<mpk>> <<mpk>>0<<mpk>>
```

C&C to VICTIM

```
:mpk!mpk@127[.]0[.]0[.]1 PRIVMSG hcumeaskcx :!Hello <<mpk>>11964<<mpk>>
<<mpk>>0<<mpk>>
```

VICTIM to C&C

```
PRIVMSG mpk :!Hello <<mpk>>57361<<mpk>>Administrator<<mpk>>0<<mpk>>
PRIVMSG mpk :!Hello <<mpk>>57361<<mpk>>Admin<<mpk>>1<<mpk>>
PRIVMSG mpk :!Hello <<mpk>>57361<<mpk>>WilsonNelly<<mpk>>2<<mpk>>
PRIVMSG mpk :!Hello <<mpk>>57361<<mpk>>2B344D56-9566-A012-89E7-
185F703A62F6<<mpk>>3<<mpk>>
PRIVMSG mpk :!Hello <<mpk>>57361<<mpk>>Windows XP<<mpk>>4<<mpk>>
PRIVMSG mpk :!MpkPing <<mpk>>38169<<mpk>> <<mpk>>0<<mpk>>
```

After successful installation / initialization of the IRCBot, dvvm.exe (MD5: ece5b62a4ed4e88dab4f1b5451f54794), it proceeds to make the following callback to the C&C server "45[.]56[.]123[.]129" via port TCP/80:

VICTIM to C&C
USER AS_a # # :des
NICK Moreen
JOIN :#klik
C&C to VICTIM
:update.mcafeea.com NOTICE AUTH :*** Looking up your hostname...
:update.mcafeea.com NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
:update.mcafeea.com 001 Moreen :Welcome to the update.mcafeea.com-Netherlands IRC Network Moreen!AS_a@66[.]187[.]149[.]88
:update.mcafeea.com 002 Moreen :Your host is update.mcafeea.com, running version Unreal3[.]2[.]8[.]1
:update.mcafeea.com 003 Moreen :This server was created Sun Feb 15 2015 at 18:33:12 UTC
:update.mcafeea.com 004 Moreen update.mcafeea.com Unreal3[.]2[.]8[.]1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCuzNTGj
:update.mcafeea.com 005 Moreen UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 MAXTARGETS=20 :are supported by this server
:update.mcafeea.com 005 Moreen WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTG NETWORK=update.mcafeea.com-Netherlands CASEMAPPING=ascii EXTBAN=~,cqnr ELIST=MNUCT STATUSMSG=~&@%+ :are supported by this server
:update.mcafeea.com 005 Moreen EXCEPTS INVEX CMDS=KNOCK,MAP,DCCALLOW,USERIP :are supported by this server
:update.mcafeea.com 251 Moreen :There are 1 users and 2 invisible on 1 servers
:update.mcafeea.com 254 Moreen 1 :channels formed
:update.mcafeea.com 255 Moreen :I have 3 clients and 0 servers
:update.mcafeea.com 265 Moreen :Current Local Users: 3 Max: 24
:update.mcafeea.com 266 Moreen :Current Global Users: 3 Max: 9
:update.mcafeea.com 422 Moreen :MOTD File is missing
:Moreen MODE Moreen :+iwx
:Moreen!AS_a@3448818D.CC98A37E.E11C9AB3.IP JOIN :#klik
:update.mcafeea.com 353 Moreen = #klik :Moreen Foster Michelle
:update.mcafeea.com 366 Moreen #klik :End of /NAMES list.

Technical Annex: Network Intelligence

Passive DNS

Passive DNS was queried for the IP address (45[.]56[.]123[.]129) but no relevant results were returned.
Passive DNS was queried for the IP address (64[.]150[.]189[.]90) but no relevant results were returned.
Passive DNS was queried for the IP address (212[.]71[.]249[.]170) but no relevant results were returned.
Passive DNS was queried for the IP address (86[.]105[.]54[.]144) but no results were returned.
Passive DNS was queried for the IP address (94[.]237[.]25[.]45) but no results were returned.

Table 2: Passive DNS for IP Address 45[.]79[.]4[.]164

Resolve	First	Last
elegomall.com	2015-11-12 09:12:48	2015-12-31 10:53:17
www[.]elegomall[.]com	2015-10-14 13:50:05	2015-12-31 10:52:43
elegomall.com	2015-11-12 01:12:48	2015-12-31 02:53:17

www[.]elegomall[.]com	2015-10-14 06:50:05	2015-12-31 02:52:43
old.elegomall.com	2015-12-26 13:53:25	2015-12-29 11:12:14
elegomall.com	2015-11-21 17:48:00	2015-11-26 00:00:00
www[.]elegomall[.]com	2015-11-02 00:00:00	2015-11-02 21:45:27

Table 3: Passive DNS for IP Address 45[.]32[.]68[.]241

Resolve	First	Last
emilymarsden.serveblog.net	2016-02-01 10:46:44	2016-02-02 12:37:43
download-google.ddns.net	2016-01-05 01:32:28	2016-01-10 08:38:06

Table 4: Passive DNS for IP Address 162[.]247[.]155[.]101

Resolve	First	Last
vuus0003566.online-vm.com	2016-02-18 00:00:00	2016-02-18 00:00:00
download-google.ddns.net	2016-01-20 20:44:42	2016-02-16 17:44:46
update-system.ddns.net	2016-02-09 21:46:05	2016-02-16 07:07:10
download-google.ddns.net	2016-02-09 21:44:35	2016-02-16 06:51:12
update-system.ddns.net	2016-02-16 02:31:29	2016-02-16 02:31:29
download-google.ddns.net	2016-01-21 04:44:42	2016-02-16 02:31:11
update-system.ddns.net	2016-02-09 21:46:05	2016-02-15 07:12:34
download-google.ddns.net	2016-02-09 21:44:35	2016-02-15 06:55:28
update-system.ddns.net	2016-02-12 21:52:36	2016-02-13 09:06:08
download-google.ddns.net	2016-02-11 13:52:14	2016-02-12 21:35:49
update-system.ddns.net	2016-02-11 22:57:31	2016-02-11 22:57:31
download-google.ddns.net	2016-02-11 22:44:29	2016-02-11 22:44:29
update-system.ddns.net	2016-02-11 21:29:32	2016-02-11 21:29:32
download-google.ddns.net	2016-02-11 15:13:05	2016-02-11 21:28:56
update-system.ddns.net	2016-02-11 15:06:49	2016-02-11 15:06:49

download-google.ddns.net	2016-02-11 13:52:14	2016-02-11 13:52:14
update-system.ddns.net	2016-02-09 21:46:05	2016-02-11 06:39:59
download-google.ddns.net	2016-02-09 21:44:35	2016-02-11 06:27:37
update-system.ddns.net	2016-02-09 21:46:05	2016-02-10 06:31:36
download-google.ddns.net	2016-02-09 21:44:35	2016-02-10 06:19:09
update-system.ddns.net	2016-02-09 21:46:05	2016-02-09 21:46:05
download-google.ddns.net	2016-02-09 21:44:35	2016-02-09 21:44:35
update-system.ddns.net	2016-02-09 19:48:51	2016-02-09 19:48:51
download-google.ddns.net	2016-01-21 04:44:42	2016-02-09 19:47:22

Table 5: Passive DNS for IP Address 103[.]3[.]62[.]117

Resolve	First	Last
android.top7apps.com	2015-11-09 07:01:46	2015-12-06 23:57:51

IP Information
IP Location: United States Overland Park Codero
ASN: AS10316
Resolve Host: 64-150-189-90.dedicated.codero.net
IP Address: 64[.]150[.]189[.]90
NetRange: 64[.]150[.]176[.]0 - 64[.]150[.]191[.]255
OrgName: Codero
IP Location: Germany Frankfurt Am Main Upcloud Ltd
ASN: AS202053
Resolve Host: db.hosting.evecy.net
IP Address: 94[.]237[.]25[.]45
NetRange:94[.]237[.]24[.]0 - 94[.]237[.]31[.]255
OrgName: UpCloud Ltd
IP Location: United States Atlanta Linode
ASN: AS36351
Resolve Host: li1103-164.members.linode.com
IP Address: 45[.]79[.]4[.]164
NetRange:45[.]79[.]0[.]0 - 45[.]79[.]255[.]255
OrgName: Linode
IP Location: United States Los Angeles Vultr Holdings Llc
ASN: AS20473
Resolve Host: 45[.]32[.]68[.]241.vultr.com
IP Address: 45[.]32[.]68[.]241
NetRange:45[.]32[.]0[.]0 - 45[.]32[.]255[.]255
OrgName: Choopa, LLC

IP Location: United States Nashua Twinservers Hosting Solutions Inc.
ASN: AS30235
IP Address: 162[.]247[.]155[.]101
NetRange:162[.]247[.]152[.]0 - 162[.]247[.]155[.]255
OrgName: Twinservers Hosting Solutions Inc.
IP Location: United States Atlanta Linode
ASN: AS36351
Resolve Host: li941-129.members.linode.com
IP Address: 45[.]56[.]123[.]129
NetRange:45[.]56[.]64[.]0 - 45[.]56[.]127[.]255
OrgName: Linode
IP Location: Canada Toronto Atlantic.net - Toronto Llc.
ASN: AS13768
IP Address: 45[.]58[.]37[.]142
NetRange:45[.]58[.]32[.]0 - 45[.]58[.]47[.]255
OrgName: Atlantic.net, Inc.
IP Location: United Kingdom Leeds Linode Llc
ASN: AS15830
Resolve Host: li622-170.members.linode.com
IP Address: 212[.]71[.]249[.]170
NetRange:212[.]71[.]248[.]0 - 212[.]71[.]251[.]255
OrgName: Linode
IP Location: Germany Sachsenhausen Cloud Services Dc
ASN: AS200185
Resolve Host: host144-54-105-86.static.arubacloud.de
IP Address: 86[.]105[.]54[.]144
NetRange:86[.]105[.]54[.]0 - 86[.]105[.]54[.]255
OrgName: ARUBA NOC
IP Location: Australia Sydney Linode Ap
ASN: AS63949
Resolve Host: li818-117.members.linode.com
IP Address: 103[.]3[.]62[.]117
NetRange:103[.]3[.]60[.]0 - 103[.]3[.]63[.]255
OrgName:Linode
Information Cut-Off Date: Feb. 25, 2016

Please rate this product by taking a short four question survey

First Version Publish Date

February 25, 2016 09:11:00 AM

Threat Intelligence Tags

Actor

- APT35

Target Geography

- United States

- Saudi Arabia
- United Kingdom
- Netherlands
- Germany

Affected Industry

- High Tech/Software/Hardware/Services
- Energy & Utilities → Energy Producers (Oil/Gas)
- Energy & Utilities → Utilities (Gas/Water)
- Financial Services → Retail Banks/ATMs/Credit Cards
- Electricity
- Technology
- Financial Services

Malware Family

- Kronos

Source Geography

- Iran

Technical Indicators & Warnings

IP:	45[.]32[.]68[.]241
Identifier:	Attacker
Network Type:	network
URL:	hxxp://64[.]150[.]189[.]90/my[.]exe
Network Type:	url
Identifier:	Attacker
URL:	aramcoexpats.com
Network Type:	wateringHole
URL:	hxxp://212[.]71[.]249[.]170/my[.]exe
Network Type:	url
Identifier:	Attacker
URL:	hxxp://86[.]105[.]54[.]144/download/flashplayer19_install[.]exe
Network Type:	url
Identifier:	Attacker
IP:	103[.]3[.]62[.]117
Domain:	android.top7apps.com
Identifier:	Related
Network Type:	network

IP:	45[.]79[.]4[.]164
Domain:	elegomall.com
Identifier:	Related
Network Type:	network
URL:	hxxp://w3schools[.]ddns[.]net/jquery[.]js
Network Type:	url
Identifier:	Related
URL:	hxxp://w3schools[.]ddns[.]net/jquery[.]js
Network Type:	url
Identifier:	Related
IP:	64[.]150[.]189[.]90
Identifier:	Attacker
Network Type:	network
URL:	international.lloydsbank.com
Network Type:	wateringHole
URL:	hxxp://breaking-news[.]club/download/interiordesigns[.]exe
Network Type:	url
Identifier:	Attacker
IP:	45[.]79[.]4[.]164
Domain:	www[.]elegomall[.]com
Identifier:	Related
Network Type:	network
IP:	45[.]79[.]4[.]164
Identifier:	Attacker
Network Type:	network
Domain:	xvy.in
IP:	104[.]238[.]97[.]226
Registrant Name:	md riyaz
Registrant Email:	riyaz.me@gmail.com
Network Type:	network
Identifier:	Attacker
URL:	hxxp://google-analytics[.]serveirc[.]com:3001/jquery3-1[.]js
Network Type:	url
Identifier:	Related
Network Type:	network
Domain:	www[.]kronos[.]com
Identifier:	Compromised

Network Type:	network
Domain:	aramcoexpats.com
Identifier:	Compromised
Network Type:	network
Domain:	xvy.in
Identifier:	Attacker
Registrant Name:	md riyaz
Registrant Email:	riyaz.me@gmail.com
URL:	hxxp://45[.]58[.]37[.]142/microsoftupdate[.]exe
Network Type:	url
Identifier:	Attacker
Network Type:	network
Domain:	international.lloydsbank.com
Identifier:	Compromised
URL:	hxxp://forum[.]aramcoexpats[.]com
Network Type:	url
Identifier:	Compromised
IP:	94[.]237[.]25[.]45
Identifier:	Attacker
Network Type:	network
URL:	hxxp://45[.]79[.]157[.]129:3001/jquery[.]js
Network Type:	url
Identifier:	Attacker
Network Type:	network
Domain:	forum.aramcoexpats.com
Identifier:	Compromised
IP:	31[.]131[.]21[.]236
Domain:	w3schools.ddns.net
Identifier:	Attacker
Network Type:	network
IP:	45[.]32[.]68[.]241
Domain:	emilymarsden.serveblog.net
Identifier:	Attacker
Network Type:	network
IP:	162[.]247[.]155[.]101
Domain:	download-google.ddns.net
Identifier:	Attacker
Network Type:	network

IP:	45[.]56[.]123[.]129
Identifier:	Attacker
Network Type:	network
URL:	hxxp://86[.]105[.]54[.]144/download/flashplayer19_install[.]exe
Network Type:	url
Identifier:	Attacker
URL:	hxxp://aramcoexpats[.]com
Network Type:	url
Identifier:	Compromised
IP:	94[.]237[.]25[.]45
Identifier:	Attacker
Network Type:	network
URL:	hxxp://download-google[.]ddns[.]net/download/flashplayerinstall[.]exe
Network Type:	url
Identifier:	Attacker
Network Type:	network
Domain:	breaking-news.club
Identifier:	Attacker
IP:	162[.]247[.]155[.]101
Domain:	update-system.ddns.net
Identifier:	Attacker
Network Type:	network
IP:	45[.]58[.]37[.]142
Identifier:	Attacker
Network Type:	network
URL:	hxxp://212[.]71[.]249[.]170/JoanSlideshow[.]exe
Network Type:	url
Identifier:	Attacker
IP:	85[.]90[.]246[.]94
Domain:	resumeworld.serveblog.net
Identifier:	Attacker
Network Type:	network
URL:	resumeworld.serveblog.net
Network Type:	wateringHole
IP:	45[.]63[.]14[.]123
Identifier:	Attacker

Network Type:	network
URL:	hxxp://64[.]150[.]189[.]90/tools/my[.]exe
Network Type:	url
Identifier:	Attacker
IP:	162[.]247[.]155[.]101
Domain:	update-system.ddns.net
Identifier:	Attacker
Network Type:	network
URL:	hxxp://w3schools[.]ddns[.]net/jquery[.]js
Network Type:	url
Identifier:	Related
URL:	hxxp://45[.]79[.]157[.]129:3001/jquery3-1[.]js
Network Type:	url
Identifier:	Attacker
URL:	hxxp://breaking-news[.]club/download/securitywarning[.]apk
Network Type:	url
Identifier:	Attacker
URL:	hxxp://w3schools[.]ddns[.]net/jquery[.]js
Network Type:	url
Identifier:	Attacker
URL:	hxxp://google-analytics[.]serveirc[.]com:3001/jquery3-1[.]js
Network Type:	url
Identifier:	Attacker
Domain:	jobsatgemalto.com
IP:	104[.]238[.]97[.]226
Registrant Name:	Domain Privacy Service FBO Registrant.
Registrant Email:	jobsatgemalto.com@domainprivacygroup.com
Network Type:	network
Identifier:	Attacker
IP:	45[.]79[.]157[.]129
Identifier:	Attacker
Network Type:	network
IP:	45[.]32[.]68[.]241
Domain:	download-google.ddns.net
Identifier:	Attacker
Network Type:	network
URL:	hxxp://45[.]63[.]14[.]123
Network Type:	url

Identifier:	Related
IP:	103[.]3[.]62[.]117
Identifier:	Attacker
Network Type:	network
URL:	www[.]kronos[.]com
Network Type:	wateringHole
URL:	hxxp://shlnk[.]be/rpiwe
Network Type:	url
Identifier:	Attacker
URL:	emilymarsden.serveblog.net
Network Type:	wateringHole
IP:	85[.]90[.]246[.]94
Domain:	multiplayer.servegame.com
Identifier:	Attacker
Network Type:	network
URL:	hxxp://w3schools[.]ddns[.]net/jquery[.]js
Network Type:	url
Identifier:	Related
URL:	forum.aramcoexpats.com
Network Type:	wateringHole
IP:	162[.]247[.]155[.]101
Identifier:	Attacker
Network Type:	network
URL:	hxxp://xvy[.]in/q4fml
Network Type:	url
Identifier:	Attacker
IP:	86[.]105[.]54[.]144
Identifier:	Attacker
Network Type:	network
IP:	45[.]79[.]4[.]164
Identifier:	Attacker
Network Type:	network
Network Type:	network
Domain:	update.mcafeea.com
Identifier:	Attacker
IP:	45[.]32[.]68[.]241

Domain:	download-google.ddns.net
Identifier:	Attacker
Network Type:	network
IP:	104[.]238[.]97[.]226
Identifier:	Attacker
Network Type:	network
IP:	45[.]32[.]68[.]241
Domain:	emilymarsden.serveblog.net
Identifier:	Attacker
Network Type:	network
IP:	184[.]168[.]221[.]46
Domain:	shlnk.be
Identifier:	Attacker
Network Type:	network
URL:	forum.aramcoexpats.com
Network Type:	wateringHole
IP:	162[.]247[.]155[.]101
Domain:	vuus0003566.online-vm.com
Identifier:	Related
Network Type:	network
URL:	hxxp://45[.]79[.]157[.]129:3001/jquery[.]js
Network Type:	url
Identifier:	Related
SHA1:	cffd1a8252f418d6d5c8ea3fc36295ca1dd4edcb
Fuzzy Hash:	6144:IdP9v0fGSLexD8Bvn0aRLrk6eJFfbPouAXasItUPMi54rni6kYrw0+AP/JPwCZkY:IdP9MfGp81n096EJMewMi54ribFyJZ3h
Packer:	Microsoft Visual C++ v7.0
File Name:	serviceupda.exe
SHA256:	ec187fa1b5e8322ee8f0638c5bc8def4d231b2525d5ec47bf6ba5112b31e8866
File Size:	368640
Identifier:	Attacker
Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit
MD5:	a6719ac8e069f3aa4abe2a087a3dd317
SHA1:	dd538f5e0847a245a6b3256983aa3cf2677b137e
Fuzzy Hash:	24576:hfAqOavfPNman8jarwLeXfB0yfM8GUS/heII8oyn6yKXbs1x3/rcpBpnuq9zq4Mq:hua82rNJKU0n8Xg1V/yrBXP
Packer:	Microsoft Visual C++ v6.0
File Name:	flashplayer19.7_install.exe
SHA256:	ee1e2823184ac4e3549f8774db700170ea763a2fde7ddcb4379837ed2487463a
File Size:	2183168

Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	ab59ba909a34ec973045dcad6e867276
SHA1:	8b8048415a61546cb1f898129f8447e16fcffd0a
Fuzzy Hash:	6144:FdP9v0fGSLexD8Bvn0aRLrk6eJFfbPoCasItUPMi54rni6kYrw0+AP/JPwCZk2/5:FdP9MfGp81n096EZewMi54ribFyJZ3h
Packer:	Microsoft Visual C++ v7.0
File Name:	serviceupdat.exe
SHA256:	a093e19b6f278e93cdede9ae371616471fc881e9d93ec577f5239f3a49212a98
File Size:	364032
Identifier:	Attacker
Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit
MD5:	d7eecd49e082d6314cbf33d15ee57aad
SHA1:	1ea0748503ded1ac4be5789557e7c2782805178a
Fuzzy Hash:	49152:i4jkMPQtvp+1rzcowEzEvX0hXKB7e47nO8Kfi3HGbAjOJcKic2d7pngXyAy:i4j/PQtlK/gLfi3OuOJcVc2XnYyt
Packer:	Borland Delphi 3.0 (???)
File Name:	Slideshow1.exe
SHA256:	af54f670d356a62d9971132f1196d4980be1a65e899e4fb7d4351d3c384b76e9
File Size:	3474188
Identifier:	Related
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	8706cbfe45199f2bfd6e7a8fd93f0fae
SHA1:	1df2864a3414fe6186beffc6fe0b83c3d3b6a26d
Fuzzy Hash:	24576:LxWGwA22CFFmwLeXfB0yfM8GUS/heII8oyn6yKXbs1x3/rcpBpnuq9zq4Mk/BXdf:QLsNJKU0n8Xg1V/yrBXP
Packer:	Microsoft Visual C++ v6.0
File Name:	flashplayer20_ga_install.exe
SHA256:	f591a3c16ddf18df056441e2614af2b2d7d48738992b4d97e3d95ab5fdb80652
File Size:	2211840
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	7243ab4937eb43d8b232e0a4cab6fb7d
SHA1:	87c708d40c60cb2058823131c33f1ce7db6ad5a8
Fuzzy Hash:	49152:ATipttnjny4buFSR+10NG+NtLvgbzc3aRH:AGtnjywuQc0NNfL6XH
Packer:	Microsoft Visual C++ 8
File Name:	JoanSlideshow.exe
SHA256:	e60fca4a46aefc3940a0d7a902f4bb57931beb87f9bea3211829e68b1f4f58ed
File Size:	1753278
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	b144f64ecb51c4a9b940e882213b5f40

SHA1:	22f3f57850ede3019b4825aa6c8808cc711223b9
Fuzzy Hash:	768:5yVYOts/vZk9AMtHwn7XXCEkMfoBRbgmVPwgMRrI7YK4:Sdts3eqNn7icoQdR7
Packer:	Borland Delphi 3.0 (???)
File Name:	my.exe
SHA256:	d08d737fa59edbea4568100cf83cff7bf930087aaa640f1b4edf48eea4e07b19
File Size:	39936
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	ece5b62a4ed4e88dab4f1b5451f54794

SHA1:	f2cd6c8107f6ab35212f4ef6a24027183e5fe255
Fuzzy Hash:	6144:ddP9v0f9SLexD8Bvn0aRLrk6eJFfbPoCasItUPMi54rni6kYrw0+AP/JPwCZk2/5:ddP9Mf9p81n096EZewMi54ribFyJZ3h
Packer:	Microsoft Visual C++ v7.0
File Name:	serviceupdat.exe
SHA256:	9bcba009c85d664d1b60ea9be2eff2d325ac73b37891555c5adef13c658d50a6
File Size:	367104
Identifier:	Attacker
Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit
MD5:	d04bf56670f2a7ae9f7cc0fcc7fb8d37

SHA1:	22f3f57850ede3019b4825aa6c8808cc711223b9
Fuzzy Hash:	768:5yVYOts/vZk9AMtHwn7XXCEkMfoBRbgmVPwgMRrI7YK4:Sdts3eqNn7icoQdR7
Packer:	Borland Delphi 3.0 (???)
File Name:	Slideshow.exe
SHA256:	d08d737fa59edbea4568100cf83cff7bf930087aaa640f1b4edf48eea4e07b19
File Size:	39936
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	ece5b62a4ed4e88dab4f1b5451f54794

SHA1:	39941f87a6aa2a3a12a5a11c4ce39a93f064890b
Fuzzy Hash:	6:pAu+H2Lv5jrJDdq++bDdqB0dEARm59z/2AY5bjzqmGsSAE2CdEARm59z/2AY5bjb:p37Lv5jumjPQlqnPAE2CmjPQlP
Identifier:	Attacker
File Name:	ywtdzsv7.cmdline
File Size:	361
SHA256:	bef4a501cf4ff91492268e46973af9c94663193fe52c7ffdb938d3c0455cace2
Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
MD5:	02bbb9fe8eb976ca763833332cc68e46

SHA1:	43099cd7c7646b3d77d08d0703d46632f1c471b3
Fuzzy Hash:	3:5Zn:j
Identifier:	Attacker
File Name:	nick435.tmp

File Size:	10
SHA256:	5486ecc66de4b9db35743ca43ded119494eaeb634c80a9b5068d919b60f569be
Type:	ASCII text, with no line terminators
MD5:	8bba3481fdd6f5c8d0806325254c8080
SHA1:	fa5859848e73e76c7036fb672a41b0d567951bc8
Fuzzy Hash:	1536:PMEFXcWn9wkAo7cK1pH++qjwuzjHw/xig3YpbzUhQQQlA:Pfcy9Ao7cKfH++MwuHwZsXKQQQlA
Packer:	Microsoft Visual C++ 8
File Name:	UNKNOWN
SHA256:	0f143594b5fda4929a938b82d63489a85d247f9450520c8d26dbb44c23def1a4
File Size:	105472
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	6b843c190600c0870d663d2af6af2dcc
SHA1:	37883adf8bb4ad8ea5d641d5397128f16fde0b93
Fuzzy Hash:	6:zz/BamfXllNS/6Xe5411mllxrS/77715KZYXxGQTae0KpYXxXe5aQioGggksl/cI:zz/H1W/6XNfSXS/pwiaqqXaiRD
Identifier:	Attacker
File Name:	zgqrp0zq.pdb
File Size:	7680
SHA256:	a625382b2b111f77251853597d578c34458cd1023ba1966a207dbf3fbfa590b6
Type:	MSVC program database ver \002
MD5:	7ee895e1c256a1e1896b4024190b52df
SHA1:	44caca508a1fce06c538ff782d5fc0e56107d2ea
Fuzzy Hash:	6:zz/BamfXllNS/mVEd1mllxrS/77715KZYXxGQTae0KpYXZVEsMoGggksl/cEDf:zz/H1W/MEXSXS/pwiaq8EtRD
Identifier:	Attacker
File Name:	ywtdzsv7.pdb
File Size:	7680
SHA256:	df04914791d1d36c7fbae217c67b0f957ca51b6ab8fda51bf21b613368dd6478
Type:	MSVC program database ver \002
MD5:	520f5ad9c6ff5afd82b8439589124b59
SHA1:	e00f6a5df85b256084dc277163d6c916d2133e64
Fuzzy Hash:	6144:i3dP9v0fGSLexD8Bvn0aRLrk6eJFfbPoCasItUPMi54rni6kYrw0+AP/JPwCZk2U:i3dP9MfGp81n096EZewMi54ribFyJZ3a
Packer:	Microsoft Visual C++ v7.0
File Name:	secure.exe
SHA256:	9769f422e2a84b5747e0b045062d622024c2f302be8ee30b5bbf9f4f64ac88f4
File Size:	369152
Identifier:	Attacker
Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit
MD5:	99bce83e77383f50fcc3fa67266ca646
SHA1:	a0c1447bd5752d90767b8024aa9c93da1e347940

Fuzzy Hash:	6:SUUUUUUUUUyqWn+SmqlrgHoNUUUUUUUUUyek8jzUUUUUUUUUyqWn+SmlUwnJ4sct:SUUUUUUUUURNqpPNUUUUUUUUU4uzUUUR
Identifier:	Attacker
File Name:	Save.tmp
File Size:	274
SHA256:	b5cd7397ba667cb80538bc82cc422ca1d11969c0cd1356e8fdae748052ea90b7
Type:	data
MD5:	14ec45a1dc86913d2d832b593d6fe7a2
SHA1:	1ad2f6a4b122d57ecb23bf5876a8ded6470ed4d6
Fuzzy Hash:	3:cc7kvc/VHH/n0eFHlTndAFrK:3kEVn/lFHljCFm
Identifier:	Attacker
File Name:	dvvm.exetmp1.vbs
File Size:	69
SHA256:	dbf099ee10341f471b47e8651a92c5c6b6a9505255f75d0edcd7ea539b2574a3
Type:	ASCII text, with CRLF line terminators
MD5:	39ac4187aaf38b986ff238c23daaf94e
SHA1:	3052a72c11d49758c6e2972c542ac385669f6ee9
Fuzzy Hash:	12:tjPQjSOnzR37Lv5jumjPQlqnPAE2CmjPQl2Kai3WEKIMBj6I5BFR5y:V8SOnzd35jV6qnIE2Cu62Kai3rKIMl6v
Identifier:	Attacker
File Name:	ywtdzsv7.out
File Size:	682
SHA256:	332777103b8d67d10a02c1d1900fa5e0131eb59f0c1478dcdd8a78c3c37275bd
Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
MD5:	d6f61635d08fedbc697528fdfdf0243d
SHA1:	a3825b85a9270be298f02966ef7e90b878bc7451
Fuzzy Hash:	6:pAu+H2Lv5jrJDdq++bDdqB0dEARm59z/2AY5btVfPmGsSAE2CdEARm59z/2AY5b4:p37Lv5jumjPQXVXnPAE2CmjPQXV4
Identifier:	Attacker
File Name:	zgqrp0zq.cmdline
File Size:	361
SHA256:	2b632a1d9eaceda5611a9f90aa94443358fa56cddd66def53d82d768fcf3c558
Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
MD5:	7aa8e99e3a6dc4eea60b24a1b42c88e8
SHA1:	a6c485631c1407d72dfb9daa01dd951fcccf5165
Fuzzy Hash:	24:H1h9wumJZUJ3TUnhKLI+ycuZhNXakSJPNnqjld:au8nhKL1ulXa3rqjP
Identifier:	Attacker
File Name:	RESDD.tmp
File Size:	1220
SHA256:	573975752bb7b9065db63dd611781e0a77977b1799665700046d08ebd66ecfe0
Type:	80386 COFF executable not stripped - version 25189

MD5:	e8a316e527c902f5d6dafc41a543ac82
SHA1:	74e32a7d8151e60553e15c32d2460ce1cda44149
Fuzzy Hash:	49152:Y5KTjnMyT1OodNCDe8dUi0A0YHc8r+z4yzJHKZ9fnAei26FuoK8:ZTjnxTtdee8dh0A0YHc8ruDJHK/nAeil
Packer:	Microsoft Visual C++ 8
File Name:	flashplayer.exe
SHA256:	8b7f1015c82d526599497f3026ba367b0683b3ef4d78ded749010c0c7439952c
File Size:	2065408
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	7ddc67ef86ea12c2d368c33e52c0b47a
SHA1:	b58a8047074fea0a61322263be99598125ced570
Fuzzy Hash:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryWUJak7Ynqq7U+PN5Dlq5J:+RI+ycuZhNXakSJPNnqX
Identifier:	Attacker
File Name:	CSCDC.tmp
File Size:	652
SHA256:	49806817bfda29e37a094062311856284edc94bf4ee679f6e25ebfc339057d68
Type:	MSVC .res
MD5:	a496b06b37b34ddc263b3164d1231c26
SHA1:	84ad2263701b370caa15ec6142fa81b2db3342c2
Fuzzy Hash:	24576:pLIjnopwsfAHYd0pce51YTrhs75+7jDBtx9pNPAlv5yB/GNOHtvC1B:Q0yCe53qH9mEJG4HE
Packer:	PECompact 2.x -> Jeremy Collake
File Name:	flashplayer.exe
SHA256:	22225caeedc7e46ccc98af1c6622c626f4d75a93b6a9976a2eed11b429e59188
File Size:	1190616
Identifier:	Related
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	96c436d7e2b49f213a983cb3e648b04d
SHA1:	22f3f57850ede3019b4825aa6c8808cc711223b9
Fuzzy Hash:	768:5yVYOts/vZk9AMtHwn7XXCEkMfoBRbgmVPwgMRrI7YK4:Sdts3eqNn7icoQdR7
Packer:	Borland Delphi 3.0 (???)
File Name:	dvvm.exe
SHA256:	d08d737fa59edbea4568100cf83cff7bf930087aaa640f1b4edf48eea4e07b19
File Size:	39936
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	ece5b62a4ed4e88dab4f1b5451f54794
SHA1:	40ae1b13a340b6ff3ee8da6f75d3bf9cb67f3b6f
Fuzzy Hash:	6144:JS4uLZafn14KtsNpEKCxZh2wuovEcq6qBbLL2uegxfkgD9mx1VphUz2L3arwI+AY:I4uLZCn14KKubxD3uov3bOJenFgz2zj8

Packer:	Microsoft Visual C++ v7.0
File Name:	taskmgor.exe
SHA256:	86db81f6d9c7e538ebbf60e6eb6204c3a432a277823b148695dbc16849416163
File Size:	392704
Identifier:	Attacker
Type:	PE32 executable for MS Windows (console) Intel 80386 32-bit
MD5:	282d5d0ff090299416f1eb5c9b1b7e9a
SHA1:	f26a4a48518a5608e93c8b77368f588b0433973c
Fuzzy Hash:	12:V/DTLDfuUv+mQMTHtc9JFqmmsmPzJJ+djqA3Iy:JjmA+mZTH29LqtsmPzudYy
Identifier:	Attacker
File Name:	zgqrp0zq.0.cs
File Size:	557
SHA256:	b240a9bb4f72d886522e19fa40b9c688fa94c1bd6dc7b7185f94e4466273a5dc
Type:	UTF-8 Unicode (with BOM) C++ program text, with very long lines
MD5:	7319070c34daa5f6f2ece2dfc07119ee
SHA1:	acc74489ef0db80478a07168b73d51b7497818cf
Fuzzy Hash:	6:sQ7M+7y3+yw6+dtXeM1jGkOAu7sQnKmr1Q3m3BMURpBHB2h:sQ7dGktOM1GkOArQ/Um3BMUbBH8h
Identifier:	Attacker
File Name:	dvvm.exetmp.vbs
File Size:	366
SHA256:	648bb6e87c3ca886192774f33f5f4971e9cfdbe53db3fd508099d494dab68051
Type:	ASCII text, with CRLF line terminators
MD5:	9fb92746bfe954a87b11a342f55ce224
SHA1:	46d46462c0ffd15eab951e6e697780dbf6efe091
Fuzzy Hash:	3072:6owqmZx9fb916mEBxzcL/rafWUONrDpGHWz4OGc2Ttdy9k+IVorjb/:eHlb916FBxwmfANrDp/DeyeJy
Packer:	Microsoft Visual C++ v6.0
File Name:	microsoftupdate.exe
SHA256:	ba3560d3c789984ca29d80f0a2ea38a224e776087e0f28104569630f870adaf4
File Size:	196608
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	49597b269fdf37faaa0962efc838aac7
SHA1:	baea37b170c65b6393a24f6bdacac0d04200626f
Fuzzy Hash:	12:tjPQjSOnzR37Lv5jumjPQXVXnPAE2CmjPQXVtKai3WEKIMBj6I5BFR5y:V8SOnzd35jVsnIE2Cu4Kai3rKIMl6I5G
Identifier:	Attacker
File Name:	zgqrp0zq.out
File Size:	682
SHA256:	4d860dcd6b4dd131911cb3e82d8351aa8740f1b364f2fd104311d423b9355156

Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
MD5:	dbc534efc7c2dd2d529f59291d1ed0fc
SHA1:	8eb58fc6a1416adc65c3c237d59b6bd7d76a69d6
Fuzzy Hash:	24576:HG8154OavfMNman8jaMwLeXfB0yfM8GUS/heII8oyn6yKXbs1x3/rcpBpnuq9zq4:J1ka82MNJKU0n8Xg1V/yrBXP
Packer:	Microsoft Visual C++ v6.0
File Name:	flashplayer19_install.exe
SHA256:	ae2890d330da00fa8b1103718e90eb0bd389f65d3831590971bfcf6b87a8f7f0
File Size:	2179072
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	db2c63eb90fe76111b1550f9409d9d16

Description: Persistence for an IRCBot

Registry:

	Hive	Key	Value
1.	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\explore	explorer	"%TEMP%\dvvm.exe" [1]

SHA1:	6b34cd7f2d9193744ae3ed4f7df17bbcde0b38db
Fuzzy Hash:	24:etGSgoMkT11e/0euTglCA3/qa8NX/XWbdPtkZfo7MXIJKN5SVHmh61FmI+ycuZhx:6gMu/XHZeXuuJqANqHA1ulqJa3Liq
Packer:	Microsoft Visual C# / Basic .NET
File Name:	ywtdzsv7.dll
SHA256:	806d8a705d1b58409e11bcc881fd283310071dc1bcd964f05280505d87f46338
File Size:	3584
Identifier:	Attacker
Type:	PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit Mono/.Net assembly
MD5:	d7fbb66bbbb8256ecc645a59c7a25db7

SHA1:	e1615d3385014b149fa0de0688d5ea7ead9b1a04
Fuzzy Hash:	12:8mT9IX7hWmn+XmK/7mBtJMaMUMEtJedxig2nl/9t6UVdngGSjAfjPQ0BxiEGUB/U:8miOXVeYNEidxGlVtvuAb7BxaI/X49
Identifier:	Attacker
File Name:	winsys.lnk
File Size:	883
SHA256:	425f2c172ee968e33fe6297347c96bb65cdc7e9542f03a7f825429a7e0bef558
Type:	MS Windows shortcut
MD5:	d759530444791de5c890fe4dc485f066

SHA1: d5b0aae208ba44accb5746eeda05243cf04892a8

Fuzzy Hash:	49152:AxHIdj6h6bTYwYS8v1IeSBIb3yvPkVV9K/Wijg5qmt801FuOMwkbZbP418n3a:AGdj6h6np8qJrb3yvPkVzK/WBEmt80JT
Packer:	Microsoft Visual C++ 8
File Name:	interiordesigns.exe
SHA256:	2d6037959a8a462690bb98758cdce1aa436b17521abce862d6e5a575b55ed1a1
File Size:	2810488
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	5cbf67bc5b4b8a8339d5bc5e09a0364d
SHA1:	c7b9927e5667672382bb1330d626afc78bc57ee4
Fuzzy Hash:	192:NxG6fqZMpfEw/FQACRbsgFmnrzLSyFYSRj:6mqyMwWACNLQSy+SRj
Identifier:	Attacker
File Name:	securitywarning.apk
File Size:	7513
SHA256:	d9df90b7126c2df33bbe2a4f3d89e8550ec334fd41c9d3d357041a26973e8d91
Type:	Zip archive data, at least v2.0 to extract
MD5:	0796d76defb4f4ad1eaccd2b7f2fe343
SHA1:	3d94d71a23f73f84335170371bbc15acc5b5f15b
Fuzzy Hash:	24:etGSDMkT11e/0euTglCA3/qa8NX94WbdPtkZfAmMXIJKNzHHHocpRmI+ycuZhNXb:6ru/XHZeX9luJPANVHLm1ulXa3rq
Packer:	Microsoft Visual C# / Basic .NET
File Name:	zgqrp0zq.dll
SHA256:	d0fa109dd306eb745f990e004fe455039b872083a25c3b94846c91569fd3ac2f
File Size:	3584
Identifier:	Attacker
Type:	PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit Mono/.Net assembly
MD5:	c254dcb02e7526aa7c04d4d48e05c029
SHA1:	f26a4a48518a5608e93c8b77368f588b0433973c
Fuzzy Hash:	12:V/DTLDfuUv+mQMTHtc9JFqmmsmPzJJ+djqA3Iy:JjmA+mZTH29LqtsmPzudYy
Identifier:	Attacker
File Name:	ywtdzsv7.0.cs
File Size:	557
SHA256:	b240a9bb4f72d886522e19fa40b9c688fa94c1bd6dc7b7185f94e4466273a5dc
Type:	UTF-8 Unicode (with BOM) C++ program text, with very long lines
MD5:	7319070c34daa5f6f2ece2dfc07119ee
SHA1:	7d94539bbc038a7f4fb1c7b5eb8b10f5252da8ad
Fuzzy Hash:	49152:i4jkMPQtvp+1rM9U/oWoe8dlNBqhDONeefdXvQX:i4j/PQtT9U/oee4tOUe6X
Packer:	Borland Delphi 3.0 (???)
File Name:	Slideshow1.exe
SHA256:	c2b065e1a63a30192e2e99eb4bcd44c23ca022f495bd17aa65d3505e35826960

File Size:	2378237
Identifier:	Related
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	a7adf752855a973abbfb04bf71bcba8a
SHA1:	ff90e09acbd38e5cb35b1727165f327844be6538
Fuzzy Hash:	96:+b6bcZh3JZcZh+dS8hXUnV6lIvmKUPaMKau1Ke/m1L9mytWkfudtDW:gh5Ch4S8yn85amBMytWkfstDW
Identifier:	Attacker
File Name:	flashplayer.bat
File Size:	6775
SHA256:	f4ca8b6a142d3f45b326d313d7a9a51b8b2356b2055807bf6b2f16e0f43a945d
Type:	ASCII text, with very long lines, with no line terminators
MD5:	b14e2e6657e4591f9cd40f7cfdced616
SHA1:	2e5be571a02334359f9dcb562cebf36b7dc522c5
Fuzzy Hash:	24576:8hGOavfMNman8jajwLeXfB0yfM8GUS/heII8oyn6yKXbs1x3/rcpBpnuq9zq4Mkr:8+a82jNJKU0n8Xg1V/yrBXP
Packer:	Microsoft Visual C++ v6.0
File Name:	UNAVAILABLE
SHA256:	43e84fb00f356e01f7d9c451c8b43bb3c193a4406f001cf589d380e99225d628
File Size:	2183168
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	5eb673fee3b811910032788665886471

Version Information

Version:1.0, February 25, 2016 09:11:00 AM
Newscaster Team Leverages Updated Toolset to Target Petroleum, Financial and Tech Interests in Recent Campaign; BeEF Used in Watering Hole Attacks

Version:2.0, February 29, 2016 04:01:00 PM
Newscaster Team Leverages Updated Toolset to Target Petroleum, Financial and Tech Interests in Recent Campaign; BeEF Used in Watering Hole Attacks

Version:3.0, March 01, 2016 10:10:00 AM
Newscaster Team Leverages Updated Toolset to Target Petroleum, Financial and Tech Interests in Recent Campaign; BeEF Used in Watering Hole Attacks

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/16-00002388