NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Malware Initial Findings Report (MIFR) - 10135300

2017-10-13

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

A single PDF file was submitted for analysis.

Files

Processed	1 e29d1f5d79cd906f75c88177c7f6168e (document.pdf)

Domains

Identified	3 bit.ly tinyurl.com imageliners.com

IPs

Identified	3 67.199.248.10 104.20.219.42 192.81.76.117

Files

document.pdf

Details

Name	document.pdf
Size	237179
Type	PDF document, version 1.5
MD5	e29d1f5d79cd906f75c88177c7f6168e
SHA1	be0a15d1aa85c9d39c4757efda861da014156d31
ssdeep	6144:P3xUxs8qpZ5gB8zo35Gm0bLsSWpa9IP8F9/xZbbSxk:P+xs8Xio3ZOWpaSmpxZYk
Entropy	7.97898152566

Antivirus

No matches found.

PDF Metadata

Title	
Subject	
Author	Dan Richards
Creator	Microsoft Word
Producer	
Creation Date	2017-03-02T18:35:50+00:00
Mod Date	2017-03-02T18:35:50+00:00

Relationships

(F) document.pdf (e29d1)	Characterized_By	(S) Screenshot of PDF
(F) document.pdf (e29d1)	Connected_To	(D) bit.ly

Description

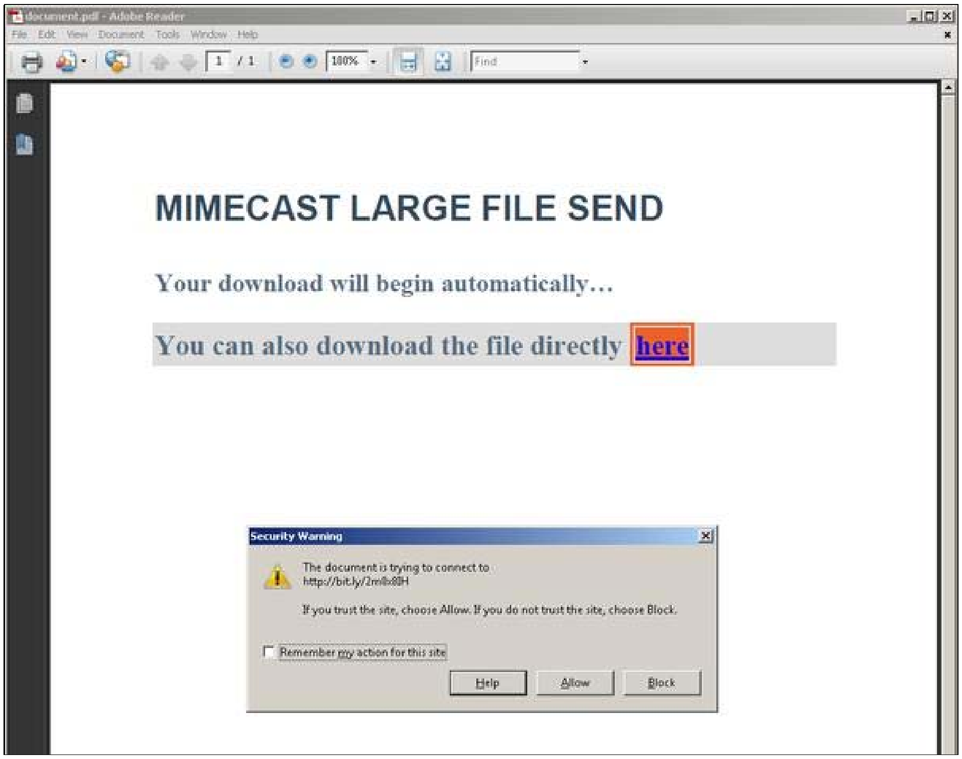
This PDF contains a malicious link. The PDF prompts the victim to click on the link to download a file (see screenshot).

The link connects to a "bit.ly" domain, which in turn connects to a "tinyrul.com" address. The "tinyurl.com" address resolves to "www[.]imageliners.com/nitel" website that returns a HTTP 404 error. The file at imageliners.com was not available for download at the time of analysis.

--Begin URIs--
bit.ly/2m0x8IH
tinyurl.com/h3sdqck
www[.]imageliners.com/nitel
--End URIs--

Screenshots

- **Screenshot of PDF**



document.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 1
100%
Find

MIMECAST LARGE FILE SEND

Your download will begin automatically…

You can also download the file directly here

Security Warning

The document is trying to connect to
http://bit.ly/2m0x8IH

If you trust the site, choose Allow. If you do not trust the site, choose Block.

□ Remember my action for this site

Domains

bit.ly

URI

- tinyurl.com

Ports

- 80

HTTP Sessions

-
```
GET /2m0x8IH HTTP/1.1
Host: bit.ly
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Thu, 03 Aug 2017 18:51:10 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 113
Connection: keep-alive
Cache-Control: private, max-age=90
Location: http[:]//tinyurl.com/h3sdqck
Set-Cookie: _bit=h73iPa-4621b905c62ea92ae9-00j; Domain=bit.ly; Expires=Tue, 30 Jan 2018 18:51:10 GMT



moved here
```

Whois

```
Address lookup
canonical name      bit.ly.
aliases
addresses      67.199.248.11
67.199.248.10
Domain Whois record

Queried whois.nic.ly with "bit.ly"...

Domain Name: bit.ly
- Domain Status: Strings shorter than four symbols long are to be registered directly under .ly ONLY through Libya Telecom and Technology
co. (LTT) in the upcoming period to guarantee that registrants have Local presence.
--
Whois information provided by:
LY Registry
whois.nic.ly
-For Whois usage policy please check:
 http[:]//whois.nic.ly/policy.php

Network Whois record

Queried whois.arin.net with "n 67.199.248.11"...

NetRange:      67.199.248.0 - 67.199.248.255
CIDR:          67.199.248.0/24
NetName:       BITLY
NetHandle:     NET-67-199-248-0-1
Parent:        NET67 (NET-67-0-0-0-0)
NetType:       Direct Assignment
OriginAS:      AS395224, AS36351, AS32787
Organization:  Bitly Inc (BITLY)
RegDate:       2016-05-31
Updated:       2016-07-06
Ref:           https[:]//whois.arin.net/rest/net/NET-67-199-248-0-1


OrgName:       Bitly Inc
OrgId:         BITLY
Address:       139 5th Ave
Address:       5th Floor
City:          New York
StateProv:     NY
PostalCode:    10010
Country:       US
RegDate:       2011-11-18
Updated:       2016-04-28
Ref:           https[:]//whois.arin.net/rest/org/BITLY


OrgAbuseHandle: ABUSE3257-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  abuse[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3257-ARIN

OrgAbuseHandle: OPERA345-ARIN
OrgAbuseName:   Operations, Bitly
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  hostmaster[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

OrgTechHandle: OPERA345-ARIN
OrgTechName:   Operations, Bitly
OrgTechPhone:  +1-646-678-5610
OrgTechEmail:  hostmaster[@]bitly.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

DNS records
DNS query for 11.248.199.67.in-addr.arpa returned an error from the server: NameError
name      class     type data time to live
bit.ly IN   SOA
server:     ns1.p26.dynect.net
email:      hostmaster[@]bit.ly
serial:     1212581715
refresh:    3600
retry:      600
expire:     604800
minimum ttl:    3600
    3600s       (01:00:00)
bit.ly IN   NS   ns1.p35.dynect.net 86400s   (1.00:00:00)
bit.ly IN   NS   ns4.p35.dynect.net 86400s   (1.00:00:00)
bit.ly IN   NS   ns2.p35.dynect.net 86400s   (1.00:00:00)
bit.ly IN   NS   ns3.p35.dynect.net 86400s   (1.00:00:00)
bit.ly IN   A    67.199.248.10 3600s     (01:00:00)
bit.ly IN   A    67.199.248.11 3600s     (01:00:00)
bit.ly IN   MX
preference:      10
exchange:        aspmx.l.google.com
    86400s       (1.00:00:00)
bit.ly IN   MX
preference:      30
exchange:        aspmx3.googlemail.com
    86400s       (1.00:00:00)
bit.ly IN   MX
preference:      20
exchange:        alt1.aspmx.l.google.com
    86400s       (1.00:00:00)
bit.ly IN   MX
preference:      30
exchange:        aspmx2.googlemail.com
    86400s       (1.00:00:00)
bit.ly IN   MX
preference:      20
exchange:        alt2.aspmx.l.google.com
    86400s       (1.00:00:00)
bit.ly IN   TXT  yandex-verification: 41b3ec866726729d3600s     (01:00:00)
bit.ly IN   TXT  google-site-verification: zhEwFAQvtUWYInQtt81loDiZmomsEmkAbuRsSSxk1YI 3600s     (01:00:00)
bit.ly IN   TXT  2205ECE8B9  3600s     (01:00:00)
bit.ly IN   TXT  v=spf1 include:mktomail.com include:_spf.google.com include:_spf.salesforce.com include:mailgun.org -all     3600s
(01:00:00)

-- end --
```

Relationships

(D) bit.ly	Related_To	(H) GET /2m0x8IH HTTP/1.
(D) bit.ly	Related_To	(P) 80
(D) bit.ly	Connected_From	(F) document.pdf (e29d1)
(D) bit.ly	Connected_To	(D) tinyurl.com
(D) bit.ly	Resolved_To	(I) 67.199.248.10
(D) bit.ly	Characterized_By	(W) Address lookup

Description

Connects to "tinyurl.com/h3sdqck"

tinyurl.com

URI

- bit.ly
- imageliners.com
- tinyurl.com/h3sdqck

Ports

- 80

HTTP Sessions

-
  ```
  GET /h3sdqck HTTP/1.1
  Host: tinyurl.com
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate
  Connection: keep-alive
  Upgrade-Insecure-Requests: 1

  HTTP/1.1 301 Moved Permanently
  Date: Thu, 03 Aug 2017 18:51:11 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  Set-Cookie: __cfduid=dbaf95a174187c31f6498cf418b035f381501786270; expires=Fri, 03-Aug-18 18:51:10 GMT; path=/;
  domain=.tinyurl.com; HttpOnly
  Set-Cookie: tinyUUID=98370a0a5311a4846aa20000; expires=Fri, 03-Aug-2018 18:51:07 GMT; Max-Age=31536000; path=/;
  domain=.tinyurl.com
  Location: https[:]//www[.]imageliners.com/nitel
  X-tiny: cache 0.010951995849609
  Server: cloudflare-nginx
  CF-RAY: 388b7781471d6944-CDG
  ```

Whois

```
Address lookup
canonical name       tinyurl.com.
aliases
addresses       2400:cb00:2048:1::6814:da2a
2400:cb00:2048:1::6814:db2a
104.20.218.42
104.20.219.42
Domain Whois record

Queried whois.internic.net with "dom tinyurl.com"...

   Domain Name: TINYURL.COM
   Registry Domain ID: 83069101_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.tucows.com
   Registrar URL: http[:]//www[.]tucowsdomains.com
   Updated Date: 2017-04-03T14:20:36Z
   Creation Date: 2002-01-27T06:17:41Z
   Registry Expiry Date: 2026-01-27T06:17:41Z
   Registrar: Tucows Domains Inc.
   Registrar IANA ID: 69
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
   Name Server: CONSTITUTION.NS.TINYURL.COM
   Name Server: FREEDOM.NS.TINYURL.COM
   Name Server: LIBERTY.NS.TINYURL.COM
   Name Server: REVOLUTION.NS.TINYURL.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https[:]//www[.]icann.org/wicf/
>>> Last update of whois database: 2017-08-03T20:31:43Z <<<

Queried whois.tucows.com with "tinyurl.com"...

Domain Name: TINYURL.COM
Domain ID: 83069101_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http[:]//tucowsdomains.com
Updated Date: 2016-09-06T15:29:05Z
```

```
Creation Date: 2002-01-27T06:17:41Z
Registrar Registration Expiration Date: 2026-01-27T06:17:41Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse[@]tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: Kevin Gilbertson
Registrant Organization: TinyURL, LLC
Registrant Street: 3916 N Potsdam Ave #4535
Registrant City: Sioux Falls
Registrant State/Province: SD
Registrant Postal Code: 57104
Registrant Country: US
Registrant Phone: +1.7633900044
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domains[@]tinyurl.com
Registry Admin ID:
Admin Name: Kevin Gilbertson
Admin Organization: TinyURL, LLC
Admin Street: 3916 N Potsdam Ave #4535
Admin City: Sioux Falls
Admin State/Province: SD
Admin Postal Code: 57104
Admin Country: US
Admin Phone: +1.7633900044
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domains[@]tinyurl.com
Registry Tech ID:
Tech Name: Kevin Gilbertson
Tech Organization: TinyURL, LLC
Tech Street: 3916 N Potsdam Ave #4535
Tech City: Sioux Falls
Tech State/Province: SD
Tech Postal Code: 57104
Tech Country: US
Tech Phone: +1.7633900044
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domains[@]tinyurl.com
Name Server: REVOLUTION.NS.TINYURL.COM
Name Server: CONSTITUTION.NS.TINYURL.COM
Name Server: LIBERTY.NS.TINYURL.COM
Name Server: FREEDOM.NS.TINYURL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2016-09-06T15:29:05Z <<<

Network Whois record

Queried whois.arin.net with "n 104.20.218.42"...

NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
```

```
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/net/NET-104-16-0-0-1



OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/org/CLOUD14


OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  admin[@]cloudflare.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

OrgNOCHandle: NOC11962-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc[@]cloudflare.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse[@]cloudflare.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse[@]cloudflare.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  admin[@]cloudflare.com
RTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc[@]cloudflare.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

DNS records
name       class       type data time to live
tinyurl.com      IN    A      104.20.218.42 146s(00:02:26)
tinyurl.com      IN    A      104.20.219.42 146s(00:02:26)
tinyurl.com      IN    AAAA      2400:cb00:2048:1::6814:da2a63s  (00:01:03)
tinyurl.com      IN    AAAA      2400:cb00:2048:1::6814:db2a63s  (00:01:03)
tinyurl.com      IN    NS   freedom.ns.tinyurl.com    86400s    (1.00:00:00)
tinyurl.com      IN    NS   liberty.ns.tinyurl.com       86400s    (1.00:00:00)
tinyurl.com      IN    NS   constitution.ns.tinyurl.com      86400s    (1.00:00:00)
tinyurl.com      IN    NS   revolution.ns.tinyurl.com 86400s    (1.00:00:00)
42.218.20.104.in-addr.arpa     IN     HINFO
CPU:       Please stop asking for ANY
OS:  See draft-ietf-dnsop-refuse-any
       3789s      (01:03:09)
a.2.a.d.4.1.8.6.0.0.0.0.0.0.0.0.1.0.0.0.8.4.0.2.0.0.b.c.0.0.4.2.ip6.arpa   IN    HINFO
```

```
CPU:       ANY obsoleted
OS:  See draft-ietf-dnsop-refuse-any
        3789s      (01:03:09)
0.0.b.c.0.0.4.2.ip6.arpa   IN    NS   chloe.ns.cloudflare.com  57873s    (16:04:33)
0.0.b.c.0.0.4.2.ip6.arpa   IN    NS   scott.ns.cloudflare.com  57873s    (16:04:33)

-- end --
```

Relationships

(D) tinyurl.com	Related_To	(P) 80
(D) tinyurl.com	Related_To	(H) GET /h3sdqck HTTP/1.
(D) tinyurl.com	Connected_From	(D) bit.ly
(D) tinyurl.com	Resolved_To	(I) 104.20.219.42
(D) tinyurl.com	Connected_To	(D) imageliners.com
(D) tinyurl.com	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(U) tinyurl.com/h3sdqck

Description

Connects to "www[.]imageliners.com/nitel"

imageliners.com

URI

- tinyurl.com
- www[.]imageliners.com/nitel

Whois

```
Address lookup
canonical name       imageliners.com.
aliases     www[.]imageliners.com
addresses       192.81.76.117
Domain Whois record

Queried whois.internic.net with "dom imageliners.com"...

   Domain Name: IMAGELINERS.COM
   Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gofrancedomains.com
   Registrar URL: http[:]//www[.]gofrancedomains.com
   Updated Date: 2017-02-16T15:48:21Z
   Creation Date: 2015-01-31T19:08:25Z
   Registry Expiry Date: 2018-01-31T19:08:25Z
   Registrar: Go France Domains, LLC
   Registrar IANA ID: 1153
   Registrar Abuse Contact Email: abuse[@]godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https[:]//icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https[:]//icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https[:]//icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https[:]//icann.org/epp#clientUpdateProhibited
   Name Server: NS1.MINDLASH.COM
   Name Server: NS2.MINDLASH.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https[:]//www[.]icann.org/wicf/
>>> Last update of whois database: 2017-08-03T19:50:01Z <<<

Queried whois.gofrancedomains.com with "imageliners.com"...

Domain Name: IMAGELINERS.COM
Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http[:]//www[.]gofrancedomains.com
Update Date: 2017-02-16T15:48:20Z
Creation Date: 2015-01-31T19:08:25Z
Registrar Registration Expiration Date: 2018-01-31T19:08:25Z
```

```
Registrar: Go France Domains, LLC
Registrar IANA ID: 1153
Registrar Abuse Contact Email: abuse[@]godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http[:]//www[.]icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http[:]//www[.]icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http[:]//www[.]icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http[:]//www[.]icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Matt Hudson
Registrant Organization: Mindlash, Inc.
Registrant Street: 1233 Washington Street
Registrant Street: Suite 600
Registrant City: Columbia
Registrant State/Province: South Carolina
Registrant Postal Code: 29201
Registrant Country: US
Registrant Phone: +1.8035530053
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: dnsadmin[@]mindlash.com
Registry Admin ID: Not Available From Registry
Admin Name: Matt Hudson
Admin Organization: Mindlash, Inc.
Admin Street: 1233 Washington Street
Admin Street: Suite 600
Admin City: Columbia
Admin State/Province: South Carolina
Admin Postal Code: 29201
Admin Country: US
Admin Phone: +1.8035530053
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: dnsadmin[@]mindlash.com
Registry Tech ID: Not Available From Registry
Tech Name: Matt Hudson
Tech Organization: Mindlash, Inc.
Tech Street: 1233 Washington Street
Tech Street: Suite 600
Tech City: Columbia
Tech State/Province: South Carolina
Tech Postal Code: 29201
Tech Country: US
Tech Phone: +1.8035530053
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: dnsadmin[@]mindlash.com
Name Server: NS1.MINDLASH.COM
Name Server: NS2.MINDLASH.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http[:]//wdprs.internic.net/
>>> Last update of WHOIS database: 2017-08-03T19:00:00Z <<<

Network Whois record

Queried whois.arin.net with "n ! NET-192-81-76-112-1"...

NetRange:       192.81.76.112 - 192.81.76.127
CIDR:           192.81.76.112/28
NetName:        PEER9NET
NetHandle:      NET-192-81-76-112-1
Parent:         PEER9NET (NET-192-81-76-0-1)
NetType:        Reassigned
OriginAS:       AS54750
Customer:       Mindlash Inc (C03402230)
RegDate:        2013-05-16
```

```
Updated:       2013-05-16
Ref:           https[:]//whois.arin.net/rest/net/NET-192-81-76-112-1


CustName:       Mindlash Inc
Address:        5000 T-Rex Ave
Address:        Suite 325
City:           Boca Raton
StateProv:      FL
PostalCode:     33431
Country:        US
RegDate:        2013-05-16
Updated:        2013-05-16
Ref:            https[:]//whois.arin.net/rest/customer/C03402230

OrgTechHandle: NETWO6039-ARIN
OrgTechName:   Network Administrator
OrgTechPhone:  +1-561-549-9500
OrgTechEmail:  network[@]peer9.net
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

OrgAbuseHandle: ABUSE3773-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-561-549-9500
OrgAbuseEmail:  abuse[@]peer9.net
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3773-ARIN

OrgNOCHandle: NETWO6039-ARIN
OrgNOCName:   Network Administrator
OrgNOCPhone:  +1-561-549-9500
OrgNOCEmail:  network[@]peer9.net
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

DNS records

DNS query for 117.76.81.192.in-addr.arpa returned an error from the server: NameError
name       class       type data time to live
www[.]imageliners.com   IN    CNAME   imageliners.com      14400s    (04:00:00)
imageliners.com     IN    TXT v=spf1 +a +mx +ip4:162.212.212.44 +ip4:192.81.76.116 +ip4:208.115.33.52 ~all14400s    (04:00:00)
imageliners.com     IN    MX
preference:     0
exchange:       imageliners.com
       14400s    (04:00:00)
imageliners.com     IN    SOA
server:    ns1.mindlash.com
email:     mindlash[@]gmail.com
serial:    2017020701
refresh:   86400
retry:     7200
expire:    3600000
minimum ttl:    86400
       86400s    (1.00:00:00)
imageliners.com     IN    NS   ns1.mindlash.com   86400s    (1.00:00:00)
imageliners.com     IN    NS   ns2.mindlash.com   86400s    (1.00:00:00)
imageliners.com     IN    A     192.81.76.117 14400s    (04:00:00)

-- end --
```

Relationships

(D) imageliners.com	Connected_From	(D) tinyurl.com
(D) imageliners.com	Resolved_To	(I) 192.81.76.117
(D) imageliners.com	Characterized_By	(W) Address lookup
(D) imageliners.com	Characterized_By	(S) 10135300_Screenshot-2.png
(D) imageliners.com	Related_To	(U) www[.]imageliners.com/nitel

IPs

67.199.248.10

URI

- bit.ly

Whois

```
Address lookup
lookup failed    67.199.248.10
        Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n 67.199.248.10"...

NetRange:       67.199.248.0 - 67.199.248.255
CIDR:           67.199.248.0/24
NetName:        BITLY
NetHandle:      NET-67-199-248-0-1
Parent:         NET67 (NET-67-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS395224, AS36351, AS32787
Organization:   Bitly Inc (BITLY)
RegDate:        2016-05-31
Updated:        2016-07-06
Ref:            https[:]//whois.arin.net/rest/net/NET-67-199-248-0-1


OrgName:        Bitly Inc
OrgId:          BITLY
Address:        139 5th Ave
Address:        5th Floor
City:           New York
StateProv:      NY
PostalCode:     10010
Country:        US
RegDate:        2011-11-18
Updated:        2016-04-28
Ref:            https[:]//whois.arin.net/rest/org/BITLY


OrgAbuseHandle: ABUSE3257-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  abuse[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3257-ARIN

OrgAbuseHandle: OPERA345-ARIN
OrgAbuseName:   Operations, Bitly
OrgAbusePhone:  +1-646-678-5610
OrgAbuseEmail:  hostmaster[@]bitly.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

OrgTechHandle: OPERA345-ARIN
OrgTechName:   Operations, Bitly
OrgTechPhone:  +1-646-678-5610
OrgTechEmail:  hostmaster[@]bitly.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/OPERA345-ARIN

DNS records

DNS query for 10.248.199.67.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --
```

Relationships

(I) 67.199.248.10	Resolved_To	(D) bit.ly
(I) 67.199.248.10	Characterized_By	(W) Address lookup

104.20.219.42

URI

- tinyurl.com

Whois

```
Address lookup
lookup failed    104.20.219.42
        Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n 104.20.219.42"...

NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/net/NET-104-16-0-0-1


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2017-02-17
Comment:        All Cloudflare abuse reporting can be done via https[:]//www[.]cloudflare.com/abuse
Ref:            https[:]//whois.arin.net/rest/org/CLOUD14


OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  admin[@]cloudflare.com
OrgTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse[@]cloudflare.com
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

OrgNOCHandle: NOC11962-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc[@]cloudflare.com
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
```

```
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc[@]cloudflare.com
RNOCRef:    https[:]//whois.arin.net/rest/poc/NOC11962-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  admin[@]cloudflare.com
RTechRef:    https[:]//whois.arin.net/rest/poc/ADMIN2521-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse[@]cloudflare.com
RAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE2916-ARIN

DNS records
name       class       type data time to live
42.219.20.104.in-addr.arpa     IN    HINFO
CPU:       Please stop asking for ANY
OS:  See draft-ietf-dnsop-refuse-any
       3789s      (01:03:09)

-- end --
```

Relationships

(I) 104.20.219.42	Resolved_To	(D) tinyurl.com
(I) 104.20.219.42	Characterized_By	(W) Address lookup

192.81.76.117

URI

- imageliners.com

Ports

- 443

Whois

```
Address lookup
lookup failed    192.81.76.117
       Could not find a domain name corresponding to this IP address.
Domain Whois record

Don't have a domain name for which to get a record
Network Whois record

Queried whois.arin.net with "n ! NET-192-81-76-112-1"...

NetRange:       192.81.76.112 - 192.81.76.127
CIDR:           192.81.76.112/28
NetName:        PEER9NET
NetHandle:      NET-192-81-76-112-1
Parent:         PEER9NET (NET-192-81-76-0-1)
NetType:        Reassigned
OriginAS:       AS54750
Customer:       Mindlash Inc (C03402230)
RegDate:        2013-05-16
Updated:        2013-05-16
Ref:            https[:]//whois.arin.net/rest/net/NET-192-81-76-112-1


CustName:       Mindlash Inc
Address:        5000 T-Rex Ave
Address:        Suite 325
City:           Boca Raton
StateProv:      FL
PostalCode:     33431
```

```
Country:       US
RegDate:       2013-05-16
Updated:       2013-05-16
Ref:           https[:]//whois.arin.net/rest/customer/C03402230

OrgTechHandle: NETWO6039-ARIN
OrgTechName:   Network Administrator
OrgTechPhone:  +1-561-549-9500
OrgTechEmail:  network[@]peer9.net
OrgTechRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

OrgAbuseHandle: ABUSE3773-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-561-549-9500
OrgAbuseEmail:  abuse[@]peer9.net
OrgAbuseRef:    https[:]//whois.arin.net/rest/poc/ABUSE3773-ARIN

OrgNOCHandle: NETWO6039-ARIN
OrgNOCName:   Network Administrator
OrgNOCPhone:  +1-561-549-9500
OrgNOCEmail:  network[@]peer9.net
OrgNOCRef:    https[:]//whois.arin.net/rest/poc/NETWO6039-ARIN

DNS records

DNS query for 117.76.81.192.in-addr.arpa returned an error from the server: NameError

No records to display

-- end --
```

Relationships

(I) 192.81.76.117	Related_To	(P) 443
(I) 192.81.76.117	Resolved_To	(D) imageliners.com
(I) 192.81.76.117	Characterized_By	(W) Address lookup

Relationship Summary

(F) document.pdf (e29d1)	Characterized_By	(S) Screenshot of PDF
(F) document.pdf (e29d1)	Connected_To	(D) bit.ly
(S) Screenshot of PDF	Characterizes	(F) document.pdf (e29d1)
(D) bit.ly	Related_To	(H) GET /2m0x8IH HTTP/1.
(D) bit.ly	Related_To	(P) 80
(D) bit.ly	Connected_From	(F) document.pdf (e29d1)
(D) bit.ly	Connected_To	(D) tinyurl.com
(D) bit.ly	Resolved_To	(I) 67.199.248.10
(D) bit.ly	Characterized_By	(W) Address lookup
(I) 67.199.248.10	Resolved_To	(D) bit.ly
(I) 67.199.248.10	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(P) 80
(D) tinyurl.com	Related_To	(H) GET /h3sdqck HTTP/1.
(D) tinyurl.com	Connected_From	(D) bit.ly
(D) tinyurl.com	Resolved_To	(I) 104.20.219.42
(D) tinyurl.com	Connected_To	(D) imageliners.com
(D) tinyurl.com	Characterized_By	(W) Address lookup
(D) tinyurl.com	Related_To	(U) tinyurl.com/h3sdqck
(I) 104.20.219.42	Resolved_To	(D) tinyurl.com
(I) 104.20.219.42	Characterized_By	(W) Address lookup
(D) imageliners.com	Connected_From	(D) tinyurl.com

(D) imageliners.com	Resolved_To	(I) 192.81.76.117
(D) imageliners.com	Characterized_By	(W) Address lookup
(D) imageliners.com	Characterized_By	(S) 10135300_Screenshot-2.png
(D) imageliners.com	Related_To	(U) www[.]imageliners.com/nitel
(I) 192.81.76.117	Related_To	(P) 443
(I) 192.81.76.117	Resolved_To	(D) imageliners.com
(I) 192.81.76.117	Characterized_By	(W) Address lookup
(S) 10135300_Screenshot-2.png	Characterizes	(D) imageliners.com
(H) GET /2m0x8IH HTTP/1.	Related_To	(D) bit.ly
(P) 80	Related_To	(D) bit.ly
(P) 80	Related_To	(D) tinyurl.com
(H) GET /h3sdqck HTTP/1.	Related_To	(D) tinyurl.com
(P) 443	Related_To	(I) 192.81.76.117
(W) Address lookup	Characterizes	(D) tinyurl.com
(W) Address lookup	Characterizes	(I) 104.20.219.42
(W) Address lookup	Characterizes	(D) bit.ly
(W) Address lookup	Characterizes	(I) 67.199.248.10
(W) Address lookup	Characterizes	(D) imageliners.com
(W) Address lookup	Characterizes	(I) 192.81.76.117
(U) tinyurl.com/h3sdqck	Related_To	(D) tinyurl.com
(U) www[.]imageliners.com/nitel	Related_To	(D) imageliners.com

Mitigation Recommendations

US-CERT recommends monitoring activity to the following domain(s) and/or IP(s) as a potential indicator of infection:

- imageliners.com

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.

Contact Information

- 1-888-282-0870
- soc@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact

US-CERT and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Can I submit malware to US-CERT? Malware samples can be submitted via three methods. Contact us with any questions.

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at www.us-cert.gov.