

IN THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
IN AND FOR PINELLAS COUNTY, FLORIDA
CIVIL DIVISION

CLAY G. COLSON,

CASE NO.: 21-005793-CI

Plaintiff,

v.

THE CITY OF TARPON SPRINGS, FLORIDA,

Defendant.

**PLAINTIFF'S VERIFIED AMENDED MOTION FOR REHEARING
OF THE ORDER DISMISSING THIS ACTION WITH PREJUDICE**

COMES NOW, the Plaintiff, CLAY G. COLSON, and files his Verified Amended Motion for Rehearing of the Order Denying Plaintiff's Motion to Enlarge Time to File an Amended Complaint filed on June 28, 2022 which dismissed this action with prejudice showing:

1. On January 25, 2022, counsel for the Defendant, CITY OF TARPON SPRINGS, filed the Defendant's Motion to Dismiss for Failure to Join Indispensable Parties. Such motion did not seek dismissal with prejudice, but instead, it sought dismissal without prejudice and cited *Fulmer v. Northern Central Bank*, 386 So.2d 856 (Fla. 2d DCA 1980) which holds that it is improper to dismiss an action for failure to join indispensable parties with prejudice. Most importantly, such motion did not cite a single case concerning indispensable parties to an action to challenge the consistency of a development order with a comprehensive plan pursuant to Florida Statutes §163.3215.
2. On May 2, 2022, a hearing was held on such motion.
3. After counsel for the Defendant, CITY, presented its motion, I pointed out that the Second District Court of Appeal's decision in *City of St. Petersburg, v. Marelli*, 728

So.2d 1197 (Fla. 2d DCA 1999) held that a property owner and developer for whom a variance was granted is not an indispensable party, and thus, that such precedent requires denial of the CITY's motion to dismiss. See the transcript of the hearing on such motion held on May 2, 2022 which is attached as Exhibit A.

4. In *City of St. Petersburg, v. Marelli*, 728 So.2d 1197 (Fla. 2d DCA 1999), the court cited *Brigham v. Dade County*, 305 So.2d 756 (Fla.1974) in which the Florida Supreme Court held that a party challenging a zoning regulation change does not have to join the affected property owner who was the applicant for the zoning change because such property owner is not an indispensable party and reversed the lower courts which had dismissed the action for failure to join such property owner.
5. Also, "The Florida Supreme Court has held that in proceedings to review completed administrative action where it is claimed that the essential requirements of law have not been followed, it is not absolutely necessary that interested third parties be joined as respondents." *Tampa Bay Cab Company, Inc. v. Yellow Cab Company of Tampa, Inc.*, 446 So.2d 246, 247 (Fla. 2d DCA 1984) citing *Brigham v. Dade County*, 305 So.2d 756 (Fla. 1975) and *Great American Insurance Co. of New York v. Peters*, 105 Fla. 380, 141 So. 322 (1932).
6. "The real respondent is the tribunal whose judgment is sought to be quashed...." *Brigham* at 757; see also, *Tampa Bay Cab Company, Inc.*, at 247.
7. In spite of my citation to *City of St. Petersburg, v. Marelli* at the hearing on May 2, 2022, Judge Muscarella directed counsel for the CITY to prepare a proposed order granting the motion to dismiss for failing to include an indispensable party with 30 days leave to amend and to send a copy of the proposed order to me. See Exhibit A.

8. However, before I had a chance to receive, review and object to the proposed order prepared by counsel for the CITY, Judge Muscarella signed the proposed order on May 9, 2022, and the Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties was filed on May 10, 2022.
9. Such Order provides that the CITY's Motion to Dismiss for Failure to Join Indispensable Parties is granted without prejudice, but then, it provides that failure to file an amended complaint within 30 days shall result in dismissal with prejudice. However, no request to grant the relief of dismissal with prejudice was made in the CITY's motion or at the hearing. See Exhibit A.
10. Such Order also does not explain who the Court considers indispensable parties, but instead, such Order just grants the Defendant CITY's Motion to Dismiss for Failure to Join Indispensable Parties. However, while such Motion mentions both Kamil Salame and Morgan Development Group, LLC, it does not clarify whether one or both are indispensable parties. Moreover, at the hearing on May 2, 2022, counsel for the CITY mentioned both Kamil Salame and Morgan Development Group, LLC, but then asks the Court to require me to add Morgan Development to my amended complaint. See Exhibit A.
11. Furthermore, such Order states that the amended complaint is due within 30 days of the date of the hearing when Judge Muscarella stated that the order should provide 30 days to amend, and as a result, I believed that I would have 30 days from the date that the Order was filed to file an amended complaint. As such Order was filed on May 10, 2022, I believed that pursuant to Judge Muscarella's ruling at the hearing on May 2, 2022, I had

30 days after the Order was filed which was until June 9, 2022 in order to file an amended complaint.

12. As the proposed order prepared by counsel for the CITY does not clearly specify who the Court believes should be added as an indispensable party, is contradictory, did not accurately reflect Judge Muscarella's ruling at the hearing on May 2, 2022, was entered before I received a copy to review and object to, and provides for dismissal with prejudice contrary to the precedent submitted by counsel for the CITY in its motion, on June 8, 2022, I filed my Motion for Reconsideration of Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties requesting the Court to either clarify or vacate such Order, and at the same time, I filed my Motion to Enlarge Time to File an Amended Complaint requesting an additional 20 days from the date of entry of the Court's order on my Motion for Reconsideration of Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties in which to file an amended complaint if necessary.
13. On June 17, 2022, counsel for the CITY filed a Notice which pursuant to Admin. Order No. 2020-012 PA/PI-CIR requested that the Court determine my outstanding motions without a hearing and stating that I had until July 5, 2022 to file my argument and legal memorandum in opposition to the relief requested by counsel for the CITY.
14. As a result of such Notice, I began working on my argument; however, before being able to file my argument and legal memorandum in opposition to the relief requested by counsel for the CITY, I learned that the Court entered Orders on June 27, 2022 which denied my Motion for Reconsideration and my Motion to Enlarge Time to File an Amended Complaint.

15. As such Orders were also confusing, I asked some friends to take a look at them, but I was informed that although the Clerk's office had noted the entry of such Orders on June 28, 2022, such Orders were not posted on the docket by the Clerk's office until July 5, 2022. See a copy of the docket as of the end of the business day on July 1, 2022 showing that such Orders still had not been uploaded to the docket which is attached as Exhibit B.
16. In addition, the Order Denying my Motion for Reconsideration contained spyware which reported the downloading and opening of such Order to some unknown entities. Apparently, the spyware that was embedded in such Order was the reason that the Clerk's office took over a week to post such Orders on the docket for download by the public. See the report obtained from Virus Total analyzing the Order Denying my Motion for Reconsideration which showed during such analysis that the spyware embedded in such Order attempted to contact 4 different domains and 8 different IP addresses, attempted to embed additional files on any computer opening such Order, and was able to avoid detection by all major anti-virus software which is attached as Exhibit C.
17. Obviously, sophisticated spyware embedded in the Order Denying my Motion for Reconsideration explains why it took the Clerk of Court over a week after such Order was signed by Judge Muscarella to post such Order on the docket, and likewise, such spyware that was embedded in such Order was an illegal effort to attempt to identify and spy upon anyone who downloaded or opened such Order which included multiple people who were asked to look at such Order including a reporter for the Tampa Bay Times.
18. As the Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties is contrary to the Second District Court of Appeal's holding in *City of St. Petersburg, v. Marelli*, 728 So.2d 1197 (Fla. 2d DCA 1999) and the

Florida Supreme Court's holding in *Brigham v. Dade County*, 305 So.2d 756 (Fla.1974) that a property owner and developer for whom a variance was granted is not an indispensable party to an action to challenge a decision by local government to grant a variance to allow a development, the Court should vacate such Order.

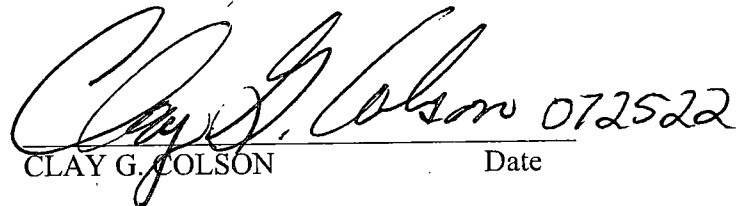
19. As the Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties is not clear, is contradictory, did not accurately reflect Judge Muscarella's ruling at the hearing on May 2, 2022, was entered before I received a copy to review and object to, and provides for dismissal with prejudice contrary to the precedent submitted by counsel for the CITY in its motion; as I raised such cause in my Motion for Reconsideration of such Order and my Motion to Enlarge Time to file an Amended Complaint; and as counsel for the CITY filed a Notice which pursuant to Admin. Order No. 2020-012 PA/PI-CIR requested that the Court determine my outstanding motions without a hearing and stating that I had until July 5, 2022 to file my argument and legal memorandum in opposition to the relief requested by counsel for the CITY, Judge Muscarella should have at least granted my Motions requesting clarification of such Order and enlarging the time in which I could file an Amended Complaint.
20. Finally, in spite of my citation to *City of St. Petersburg, v. Marelli* at the hearing on May 2, 2022, Judge Muscarella granted the city's motion so quickly that she could not have looked up the case that I cited and did not even appear to consider it. See Exhibit A.
21. A party has the due process right to a full and fair hearing before an impartial judge. See e.g., *Robbins v. Robbins*, 429 So.2d 424 (Fla. 3rd DCA 1983).

22. "Due process requirements must be met." *Id.* at 429 citing, *Shillitani v. United States*, 384 U.S. 364, 86 S.Ct. 1531, 16 L.Ed.2d 622 (1966). "A fundamental due process requirement is a hearing, one that may be neither sham nor pretense." *Id.* citing, *Palko v. Connecticut*, 302 U.S. 319, 58 S.Ct. 149, 82 L.Ed. 288 (1937).
23. As the hearing on May 2, 2022, appeared to be no more than a sham hearing in which the outcome was predetermined, my right to due process was violated, and therefore, both the Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties and the Order Denying Plaintiff's Motion to Enlarge Time to File an Amended Complaint which dismissed this action with prejudice should be vacated.

WHEREFORE, for the foregoing reasons, I respectfully request that the Court grant my Motion for Rehearing, vacate or clarify the Order Granting Defendant CITY OF TARPON SPRINGS' Motion to Dismiss for Failure to Join Indispensable Parties, vacate the Order Denying Plaintiff's Motion to Enlarge Time to File an Amended Complaint, and grant me at least an additional 20 days from the date of entry of the Court's order on this Motion in which to file an amended complaint if necessary.

VERIFICATION

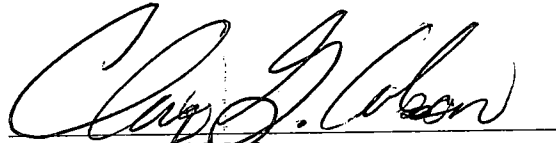
Under penalties of perjury, I declare that I have read the foregoing motion and the facts stated in it are true.


CLAY G. COLSON 072522
Date

CERTIFICATE OF SERVICE

I hereby certify that a copy of this motion has been served by U.S. Mail to Jay

Daigneault, Esq. of Trask Daigneault, LLP at 1001 S. Fort Harrison Ave., Suite 201 in
Clearwater, FL 33756 on this 25th day of July 2022.

A handwritten signature in black ink, appearing to read "Clay G. Colson", written over a horizontal line.

CLAY G. COLSON
4318 Joy Drive
Land O'Lakes, FL 34638
813-601-3391

Exhibit A

1 IN THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT
2 IN AND FOR PINELLAS COUNTY, STATE OF FLORIDA
3 CIVIL DIVISION
4

5 CLAY G. COLSON,
6 Plaintiff,

Case No. 21-005793-CI

7 vs.

8 THE CITY OF TARPON SPRINGS, FLORIDA,
9 Defendant.

10
11 PROCEEDINGS HELD TELEPHONICALLY

12
13 PROCEEDINGS: DEFENDANT'S MOTION TO DISMISS FOR
14 FAILURE TO JOIN INDISPENSABLE PARTIES
15 BEFORE: The Honorable Patricia Muscarella
16 Circuit Court Judge
17 DATE: May 2, 2022
18 11:09 a.m. - 11:24 a.m.
19 REPORTED BY: Annemarie Christodoulou
20 PLACE: Pinellas County Courthouse
21 315 Court Street, 4th Floor
22 Clearwater, Florida 33756

23
24
25

MAXA ENTERPRISES, INC.
1275 Cleveland Street
Clearwater, Florida 33755
(727) 441-2404 Fax: (727) 448-0028

1 **APPEARANCES:**

2 JAY DAIGNEAULT, ESQUIRE
3 Trask Daigneault, LLP
4 1001 S. Fort Harrison Avenue, Suite 201
5 Clearwater, Florida 33756
6 Email: jay@cityattorneys.legal
7 Phone: 727-733-0494
8 Counsel for Defendant

9 SHANE T. COSTELLO, ESQUIRE
10 Hill Ward Henderson
11 101 E Kennedy Blvd., Suite 3700
12 Tampa, Florida 33602-5195
13 Email: shane.costello@hwlaw.com
14 Phone: 813-221-3900
15 Counsel for the Intervener

16 **ALSO PRESENT:**

17 Clay Colson, pro se
18
19
20
21
22
23
24
25

1 **THE COURT:** This is Clay Colson vs. City of Tarpon
2 Springs. This is defendant's motion to dismiss for
3 failure to join indispensable parties. Who is here on
4 behalf of the plaintiff?

5 **MR. COLSON:** Yes, Your Honor. I'm here.

6 **THE COURT:** Mr. Colson is that you or are you
7 represented?

8 **MR. COLSON:** No, it's me. I represent myself pro
9 se, Your Honor.

10 **THE COURT:** Okay. Great. Thank you. And for the
11 defense?

12 **ATTORNEY DAIGNEAULT:** Good morning, Your Honor.
13 Jay Daigneault on behalf of the City of Tarpon Springs.

14 **THE COURT:** Okay. Thank you. So it's your
15 motion --

16 **THE COURT REPORTER:** And I'm sorry, Your Honor, a
17 court reporter is on the line also.

18 **THE COURT:** Oh, sorry. Who else is on the line?
19 Is there a court reporter?

20 **THE COURT REPORTER:** Yes, Your Honor.

21 (An unknown speaker speaks.)

22 **THE COURT:** I think we have two court reporter's
23 is that right?

24 **UNKNOWN SPEAKER:** Yes.

25 **THE COURT REPORTER:** I am here for Colson vs. City

1 of Tarpon Springs, and I was hired by Mr. Daigneault's
2 office. This is Annemarie with Maxa Enterprises.

3 **THE COURT:** Mr. Colson, did you hire a court
4 reporter?

5 **MR. COSTELLO:** Your Honor, there is an additional
6 appearance. Your Honor, my name is Shane Costello. I
7 represent the intervener. We filed a notice to
8 intervene that is set for hearing, and my office also,
9 I guess, secured a court reporter.

10 **MR. COLSON:** The response to your question, Your
11 Honor. I'm just recording this. I don't have a court
12 reporter.

13 **THE COURT:** It's against all the rules to record
14 anything, Mr. Colson.

15 **MR. COLSON:** Oh, it is?

16 **THE COURT:** Yes. You have to stop and erase what
17 you have now.

18 **MR. COLSON:** I will stop it now.

19 **THE COURT:** And erase whatever you have.

20 **UNKNOWN SPEAKER:** And, Your Honor, this is the
21 court reporter Mr. Costello hired.

22 **THE COURT:** Who is Mr. Costello?

23 **ATTORNEY COSTELLO:** Your Honor, Shane Costello, I
24 just announced my appearance. I'm on behalf of the
25 intervener, Morgan Group Development, we filed a motion

1 to intervene that is connected with the City's motion
2 to dismiss for failure to join an indispensable party.
3 We are that indispensable party. So those are the two
4 matters set for hearing today.

5 **UNKNOWN SPEAKER:** Your Honor, I'm okay with
6 signing off and letting the other court reporter stay
7 on who originally set the motion to dismiss.

8 **ATTORNEY DAIGNEAULT:** That's correct.

9 **THE COURT:** I think that's the proper thing. I
10 never say your name right, Mr. Daigneault. You have to
11 tell me one more time how to say your name.

12 **ATTORNEY DAIGNEAULT:** It's Daigneault, Your Honor.

13 **THE COURT:** Spell it for me phonetically, so I
14 never forget this again.

15 **ATTORNEY DAIGNEAULT:** It's a Great Dane dog and a
16 yo-yo.

17 **THE COURT:** Daigneault. All right. So if you are
18 in agreement for keeping your court reporter and
19 releasing everyone else that would be fine with me.

20 **ATTORNEY DAIGNEAULT:** I think that's fine.
21 Thanks, Your Honor.

22 **THE COURT:** Okay. So the other court reporter is
23 released and will not be recording this at all.

24 **UNKNOWN SPEAKER:** Thank you.

25 **THE COURT:** Okay. Mr. Daigneault, this is your

1 motion. The other motion to intervene was added time
2 permitting. I have an 11:30, and so would you like to
3 proceed.

4 **ATTORNEY DAIGNEAULT:** Yes, Your Honor. Thank you.
5 And I will be brief respecting the Court's time with a
6 second motion that we'd like to have -- be heard in
7 resolving. So in short, Your Honor -- challenge --

8 **THE COURT:** Mr. Daigneault, you are breaking up.
9 I apologize. But I cannot hear you very well.

10 **ATTORNEY DAIGNEAULT:** Is that better?

11 **THE COURT:** That is better. Thank you.

12 **ATTORNEY DAIGNEAULT:** All right. So we're here on
13 two development orders issued by the City regarding the
14 Anclote Harbor residential planned development. The
15 first order is Ordinance Number 2021-15. The second is
16 a Resolution Number 2021-60.

17 These development orders are in service of and
18 paved a way, if you will, for development called
19 Anclote Harbor that is proposed undertaken by Kamil
20 Salame and the Morgan Group Development, LLC, which is
21 the contract purchaser and proposed developer of the
22 development project up in Tarpon Springs.

23 Because they are the contract purchaser, they are
24 very much of a real party of interest in this case as
25 set forth in the City's motion, particularly the Two

1 Island Development case, cannot proceed without them.
2 Their presence is necessary for the Court to make a
3 complete determination of the parties' rights, duties
4 and obligations in the case.

5 So pursuant to Rule 1.210(1), as well as the case
6 law cited within the motion, which includes *Santiago*
7 *vs. Sunset Cove Investments*, and *Two Island Development*
8 *Corporation vs. Clarke*, which I know also that the
9 proposed intervener relies upon in its motion.

10 The intervener and Morgan Development needs to be
11 a party to this case because it's really their rights
12 that are at issue here. Whether these development
13 orders comply with the City's Comprehensive Plan,
14 certainly the City is required to be a party, but due
15 to the contract purchase status and the development
16 proposed by intervener they need to be a party. We had
17 a similar fact pattern in the *Two Islands* case and this
18 case, according to the City, and we argue should be
19 decided similarly.

20 And so for that reason I think we probably should
21 discuss what is the appropriate remedy in the case.
22 The City here has moved for dismissal for failure to
23 join an indispensable party, and I think that dismissal
24 is really the appropriate remedy, wherein the plaintiff
25 would be permitted to amend his complaint to determine

1 whether he wishes to add Morgan Development as the
2 developer, and if he chooses not to the case should not
3 proceed forward.

4 And with that I'm happy to answer any questions
5 that the Court has.

6 **THE COURT:** Thank you, Mr. Daigneault. I'd like
7 to hear -- Mr. Colson, would you like to respond to
8 that?

9 **MR. COLSON:** I would, Your Honor. My complaint is
10 with the City for its failure to do it's due diligence
11 in following its Comprehensive Plan, Land Development
12 Ordinances, and Land Development Codes in granting
13 this, which has nothing to do High Woods -- with the
14 Morgan Group.

15 In the High Wood's case was an appellate review of
16 the City's decision. However, this action is a de novo
17 review of the development under Florida Statutes
18 Section 163.3215(3); and, therefore, as recognized by
19 the court in High Woods the Florida Rules of Appellate
20 Procedure do not apply because this is an action
21 provided by general law and is not an appellate review
22 of Tarpon's decision.

23 Therefore, the Second DCA holding in the *City of*
24 *St. Pete vs. Marelli* and the Florida Supreme Court
25 holding in *Brigham vs. Dade City* -- or Dade County that

1 the property owner is not an indispensable party
2 prohibits Morgan Group's intervention as well requires
3 a denial of Tarpon's motion to dismiss.

4 **THE COURT:** Okay. Thank you. Now I'd like to
5 hear from the intervener.

6 **ATTORNEY COSTELLO:** Yes, Your Honor. We're in
7 agreement with the motion to dismiss for failure to
8 join an indispensable party. As we've laid out in the
9 motion to intervene, Morgan is the contract purchaser,
10 is the equitable titleholder to the property. It is
11 the real party of interest that stands to gain or lose
12 from the outcome of this proceeding.

13 If the Court rules in the plaintiff's favor in
14 this proceeding, Morgan will not be able to complete
15 the development of its property as has been approved by
16 the City. So Morgan certainly meets the test for
17 intervention, which is whether you stand to gain or
18 lose by the outcome of the proceeding.

19 And as Mr. Daigneault argued, Morgan is, in fact,
20 a necessary, or indeed, an indispensable party in this
21 proceeding. The test of an indispensable party is
22 whether it is impossible to completely adjudicate the
23 matter without affecting the interests of that party,
24 the *Two Island* case that Mr. Daigneault cited.

25 Plaintiff in this action, their request for relief

1 would include an injunction preventing the development
2 of my client's property. That most certainly affects
3 my client's interest. Likewise, the test for a
4 necessary party is whether the person is materially
5 interested in the subject matter and would be directly
6 affected by an adjudication, and we certainly would.

7 These clients cannot be adjudicated without
8 affecting Morgan's private property rights and
9 entitlements on the property. And so we would request
10 that Morgan be included in this case as a party
11 defendant.

12 **THE COURT:** Okay. Mr. Colson?

13 **MR. COLSON:** As pointed out earlier, Your Honor,
14 the Morgan Group had nothing to do with the decision
15 rendered by the City of Tarpon Springs, other than
16 applying for it, and the City of Tarpon Springs failed
17 to follow its own rules and regulations in the
18 Comprehensive Plan in issuing that development order.
19 So it's moot whether or not Morgan is going to be
20 affected or not as being the intervener in this.

21 The complaint is strictly about whether or not the
22 City Commission of Tarpon Springs followed its rules
23 and regulations in granting them that order. IF they
24 did not do that, then they have no standing.

25 **THE COURT:** Okay. So I am going to grant the

1 motion to dismiss without prejudice.

2 Mr. Colson, you may -- how many days would you
3 like to amend your pleading?

4 **MR. COLSON:** Well, motion to dismiss, I'd like to
5 ask for 30 days to file an amended complaint since I am
6 pro se plaintiff and needs extra time.

7 **THE COURT:** Okay. That's fine with me.

8 Provide an order -- I guess, Mr. Daigneault, would
9 you provide the order? It's your motion. And run it
10 around for everyone.

11 I don't know, Mr. Colson, are you associated in
12 JAWS in some way or would you like hard copies of
13 everything?

14 **MR. COLSON:** Hard copies. I don't have internet
15 access and want everything by U.S. mail, please.

16 **THE COURT:** Okay. So, Mr. Daigneault, would you
17 provide that, run it by Mr. Colson if you can.

18 Do you have email, Mr. Colson?

19 **MR. COLSON:** I do not.

20 **THE COURT:** Okay. So I guess you just send me
21 hard copies with your proposed order, and we will
22 proceed.

23 **MR. COLSON:** Thank you so much, Your Honor.

24 **ATTORNEY DAIGNEAULT:** Your Honor, do you want me
25 to run the order by Mr. Colson for form approval or

1 would you rather that I simply copy him on it and copy
2 to Your Honor as well?

3 **THE COURT:** I don't think it's complicated for a
4 motion to dismiss for failing to include an
5 indispensable party is -- the motion to dismiss is
6 granted, 30 days leave to amend. So I think it's
7 pretty simple. I think a copy to Mr. Colson is fine.

8 **ATTORNEY DAIGNEAULT:** Agreed. Thank you, Your
9 Honor.

10 **THE COURT:** Okay. Anything else for today?

11 **MR. COSTELLO:** No, Your Honor.

12 **ATTORNEY DAIGNEAULT:** No, Your Honor. Thank you
13 for your time.

14 **THE COURT:** Okay. If you need to address the
15 intervener motion that was -- just leave it for now?

16 **MR. COSTELLO:** I don't think it -- Your Honor,
17 this is Shane Costello. I don't think it needs to be
18 addressed given the ruling on the motion to dismiss.
19 Mr. Colson will either need to include Morgan Group as
20 a party defendant in his amended complaint or the
21 action would be dismissed.

22 **THE COURT:** Okay. Thank you, everyone.

23 (The hearing was concluded at
24 11:24 a.m.)

25

CERTIFICATE OF REPORTER

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

STATE OF FLORIDA)
COUNTY OF PINELLAS)

I, Annemarie Christodoulou, Court Reporter,
certify that I was authorized to and did stenographically
report the foregoing proceedings in CLAY G. COLSON vs. THE
CITY OF TARPON SPRINGS, Case Number 21-005793-CI, held on
May 2, 2022 before the Honorable Patricia Muscarella held
telephonically; and that the transcript, pages numbered 1
through 13, inclusive, is a true and complete record of my
stenographic notes.

I further certify that I am not a relative,
employee, attorney, or counsel of any of the parties, nor am
I a relative or employee of any of the parties' attorney or
counsel connected with the action, nor am I financially
interested in the action.

Annemarie Christodoulou
ANNEMARIE CHRISTODOULOU
Court Reporter

Exhibit B

[Skip to Main Content](#) [Logout](#) [My Account](#) [Search Menu](#) [New Civil Search](#) [Refine Search](#) [Back](#)

Location : Pinellas County [Help](#)

REGISTER OF ACTIONS CASE No. 21-005793-CI



Order Documents! *Click Here!*
Request Now! Including Certified!

CLAY G COLSON Vs. CITY OF TARPON SPRINGS FLORIDA

§
§
§
§
§
§
§

Case Type: **DECLARATORY - CIRCUIT**
Date Filed: **12/09/2021**
Location: **Section 7**
Judicial Officer: **MUSCARELLA, PATRICIA ANN**
UNIFORM CASE NUMBER: **522021CA005793XXCICI**

PARTY INFORMATION

DEFENDANT CITY OF TARPON SPRINGS FLORIDA

324 PINE ST
TARPON SPRINGS, FL 34689

Attorneys
JAY DAIGNEAULT, ESQ

TRASK DAIGNEAULT, LLP
1001 SOUTH FORT
HARRISON AVE
SUITE 201
CLEARWATER, FL 33756

727-733-0494(W)

PLAINTIFF COLSON, CLAY G
4318 JOY DRRIVE
LAND O LAKES, FL 34637

EVENTS & ORDERS OF THE COURT

OTHER EVENTS AND HEARINGS

- 06/28/2022 **ORDER DENYING** Doc # 41
PLAINTIFFS MOTION TO ENLARGE TIME TO FILE AN AMENDED COMPLAINT
- 06/28/2022 **ORDER DENYING** Doc # 42
PLAINTIFFS MOTION FOR RECONSIDERATION
- 06/28/2022 **CORRESPONDENCE TO COURT RE** Doc # 43
PROPOSED ORDER
- 06/21/2022 **DCA ORDER** Doc # 40
DENYING THE PETITION TO REVIEW ORDER EXCLUDING PRESS COVERAGE OF PROCEEDINGS IN THE CIRCUIT COURT OF THE SIXTH JUDICIAL CIRCUIT, IN AND FOR PINELLAS COUNTY, FLORIDA, WITHOUT PREJUDICE TO PETITIONER'S SEEKING PERMISSION TO RECORD FUTURE PROCEEDINGS IN ACCORDANCE WITH SIXTH JUDICIAL CIRCUIT ADMINISTRATIVE ORDER NO. 2008-076 PAV/PI-CIR. / 2D22-1756
- 06/20/2022 **CORRESPONDENCE TO CLERK RE** Doc # 39
SUPPLEMENT TO APPENDIX - RCVD BY COURT 06162022
- 06/17/2022 **NOTICE** Doc # 38
OF REQUEST
- 06/15/2022 **RESPONSE** Doc # 36
TO PLAINTIFF'S MOTION TO ENLARGE TIME TO FILE AN AMENDED COMPLAINT
- 06/15/2022 **EXHIBIT** Doc # 37
A-LETTER/APPLICATION/CASE RECORDS
- 06/08/2022 **PLTF-PET'S MOTION FOR RECONSIDERATION** Doc # 34
OF ORDER GRANTING DEFENDANT CITY OF TARPON SPRINGS' MOTION TO DISMISS FOR FAILURE TO JOIN INDISPENSABLE PARTIES
- 06/08/2022 **MOTION** Doc # 35
TO ENLARGE TIME TO FILE AN AMENDED COMPLAINT
Filed by: COLSON, CLAY G
- 06/03/2022 **COPY** Doc # 33
OF CORRESPONDENCE TO SECOND DCA RE: THE PETITION TO REVIEW ORDER EXCLUDING PRESS COVERAGE RECEIVED BY COURT 06/02/2022 2D22-1756
- 06/02/2022 **DCA ORDER** Doc # 32
BY 06/12/2022 PETITIONER SHALL SUPPLEMENT THE APPENDIX WITH EITHER WRITTEN ORDER OR TRANSCRIPT OF THE TRIAL JUDGE'S ORAL PRONOUNCEMENT. RESPONDENT SHALL SERVE A RESPONSE TO THE PETITION WITHIN 10 DAYS. 2D22-1756
- 06/01/2022 **LETTER FROM 2ND DCA RE ASSIGN APPEAL NO.** Doc # 30
2D22-1756
- 06/01/2022 **DCA ORDER** Doc # 31
APPROVING AFFIDAVIT OF INSOLVENCY/INDIGENT AND ACCOMPANYING MOTN FILED ; FILING FEE NOT REQUIRED. 2D22-1756

- 05/31/2022 **RESPONSE** Doc # 28
(PLTF'S) TO DEFT'S FIRST REQUEST TO PRODUCE
- 05/31/2022 **NOTICE OF SERVICE OF INTERROGATORIES** Doc # 29
(PLTF'S)
- 05/25/2022 **ORDER DENYING** Doc # 27
MOTION TO DISQUALIFY JUDGE
- 05/20/2022 **MOTION** Doc # 25
TO DISQUALIFY JUDGE PATRICIA ANN MUSCARELLA
Filed by: COLSON, CLAY G
- 05/20/2022 **APPLICATION FOR INDIGENT STATUS APPROVED** Doc # 26
Party: COLSON, CLAY G
- 05/17/2022 **MOTION TO COMPEL DISCOVERY** Doc # 20
Party: CITY OF TARPON SPRINGS FLORIDA
- 05/17/2022 **EXHIBIT** Doc # 21
FIRST REQUEST TO PRODUCE
Party: CITY OF TARPON SPRINGS FLORIDA
- 05/17/2022 **EXHIBIT** Doc # 22
NOTICE OF SERVING FIRST SET OF INTERROGATORIES
- 05/17/2022 **EXHIBIT** Doc # 23
LETTER DATED 04182022
- 05/17/2022 **NOTICE** Doc # 24
OF REQUEST FOR COURT TO CONSIDER MOTION TO COMPEL DISCOVERY WITHOUT HEARING
- 05/10/2022 **ORDER GRANTING** Doc # 18
DEFT'S MOTION TO DISMISS
- 05/10/2022 **CORRESPONDENCE TO COURT RE** Doc # 19
PROPOSED ORDER - RCVD BY COURT 05062022
- 03/16/2022 **NOTICE OF HEARING** Doc # 17
(CROSS TELEPHONIC) 05022022 11:00
- 03/09/2022 **REQUEST FOR PRODUCTION** Doc # 15
- 03/09/2022 **NOTICE OF SERVICE OF INTERROGATORIES** Doc # 16
- 03/07/2022 **NOTICE OF HEARING** Doc # 12
05022022 11:00 TELEPHONIC
- 03/07/2022 **MOTION TO INTERVENE** Doc # 13
FILED BY MORGAN GROUP DEVELOPMENT LLC
- 03/07/2022 **EXHIBIT** Doc # 14
COMPOSITE A- COPIES ORDERS
- 01/31/2022 **NOTICE OF CANCELLATION** Doc # 11
OF TELEPHONIC HEARING 03312022
- 01/26/2022 **SUMMONS - SERVED** Doc # 10
01252022
Party: CITY OF TARPON SPRINGS FLORIDA
- 01/25/2022 **SUMMONS - ISSUED** Doc # 7
AMMENDED
Party: COLSON, CLAY G
- 01/25/2022 **DEF-RESP'S MOTION TO DISMISS** Doc # 8
FOR FAILURE TO JOIN INDISPENSABLE PARTIES
- 01/25/2022 **NOTICE OF HEARING** Doc # 9
03312022 10:15 TELEPHONIC
- 01/19/2022 **NOTICE OF APPEARANCE** Doc # 6
Party: CITY OF TARPON SPRINGS FLORIDA
- 12/17/2021 **DEF-RESP'S MOTION** Doc # 5
TO QUASH PROCESS AND SERVICE OF PROCESS
- 12/14/2021 **SUMMONS - SERVED** Doc # 4
12/10/2021
Party: CITY OF TARPON SPRINGS FLORIDA
- 12/10/2021 **SUMMONS - ISSUED** Doc # 3
NCB - GIVEN TO PLAINTIFF FOR PROCESS SERVER
Party: CITY OF TARPON SPRINGS FLORIDA
- 12/09/2021 **COMPLAINT** Doc # 1
- 12/09/2021 **ATTACHMENT** Doc # 2
ORDINANCE

FINANCIAL INFORMATION

PLAINTIFF COLSON, CLAY G

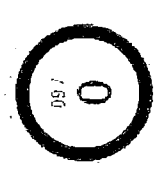


Court Ordered [Click Here!](#)

Pay Now! Fines, Fees, Costs?

	Total Financial Assessment		420.00
	Total Payments and Credits		420.00
	Balance Due as of 07/01/2022		0.00
12/09/2021	Transaction Assessment		400.00
12/09/2021	Counter Payment	Receipt # CV-2021-29455	(400.00)
12/10/2021	Transaction Assessment		10.00
12/10/2021	Counter Payment	Receipt # NC-2021-10328	(10.00)
01/25/2022	Transaction Assessment		10.00
01/25/2022	Counter Payment	Receipt # NC-2022-00657	(10.00)

Exhibit C



No security vendors and no sandboxes flagged this file as malicious

71326b8e0634570ba4e99a38f2901e5888b0dde1c9725614ea9d04695a52a5
 Order Denying Mot for Recon 22 6 28.pdf

18.31 KB 2022-07-20 15:32:05 UTC
 Size 1 hour ago



Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Contacted Domains ⓘ Considered Domains from this file being analyzed.

Domain	Detections	Created	Registrar
acropm2.adobe.com	0 / 94	1986-11-17	NOM-IQ Ltd dba Com Laude
armmf.adobe.com	0 / 94	1986-11-17	NOM-IQ Ltd dba Com Laude
geo2.adobe.com	1 / 94	1986-11-17	NOM-IQ Ltd dba Com Laude
p13n.adobe.io	0 / 94	2012-03-12	Nom-iq Ltd. dba COM LAUDE

Contacted IP Addresses ⓘ

IP	Detections	Autonomous System	Country
104.96.196.134	0 / 94	20940	GB

geo2.adobe.com 1 / 94 1986-11-17 NOWHQ Ltd dba Com Laude
 p13n.adobe.io 0 / 94 2012-03-12 Norm-ig Ltd. dba COM LAUDE

Contacted IP Addresses Contingent IP Addresses from the file being studied.

IP	Detections	Autonomous System	Country
104.96.196.134	0 / 94	20940	GB
18.213.11.84	0 / 94	14618	US
184.31.224.145	0 / 94	16625	GB
34.237.241.83	0 / 94	14618	US
50.16.47.176	0 / 94	14618	US
54.224.241.105	0 / 94	14618	US
92.123.140.146	0 / 93	20940	GB
92.123.143.219	0 / 93	20940	GB

Dropped Files

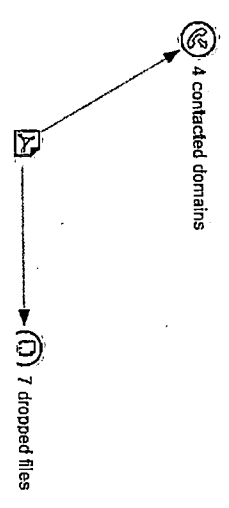
Scanned	Detections	File type	Name
2022-07-20	0 / 57	BMP	icon-220720235001Z-169.bmp
2022-07-20	0 / 58	Text	DC_Reader_RHP_Banner
2022-07-20	0 / 57	Text	SOPHIA.json
2022-07-20	0 / 58	Text	Edit_InApp_Aug2020
?	?	file	16a9eb8b067c6b8269f6e52bd5b49ece855d7f1b5b10ea7528b3dcb3b8774d
?	?	file	A3a4f70c-0b8c-1c4c-19b8-0ff07c2c130b8b14a-0f5c7c20-0f0c0f-99c-91c37f14

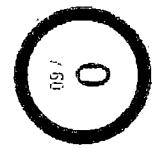
92.123.140.146	0 / 93	20940	GB
92.123.143.219	0 / 93	20940	GB

Dropped Files Files dropped by this file

Scanned	Detections	File type	Name
2022-07-20	0 / 57	BMP	icon-220720235001Z-169.bmp
2022-07-20	0 / 58	Text	DC_Reader_RHP_Banner
2022-07-20	0 / 57	Text	SOPHIA.json
2022-07-20	0 / 58	Text	Edit_InApp_Aug2020
?	?	file	16a9eb8b067c16b8269fce52bd5b19ece855d7f1b5b10ea7528b3db3b8774d
?	?	file	43bdf70ba9b0e1a618bee4f1026513089418a46b5269ce0dface88c21537f1d
?	?	file	55c338568a83ed7ef07ccbcb0583cd4e0870940d4417e89144ee6943893243

Graph summary





Community Score

No security vendors and no sandboxes flagged this file as malicious

71326b8e0634570fba4e99a38f2901e5888b8dde1c9725614ea9d04695a52a5
Order Denying Mot for Recon 22 6 28.pdf

18.31 KB
Size
2022-07-20 15:32:05 UTC
1 hour ago



DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

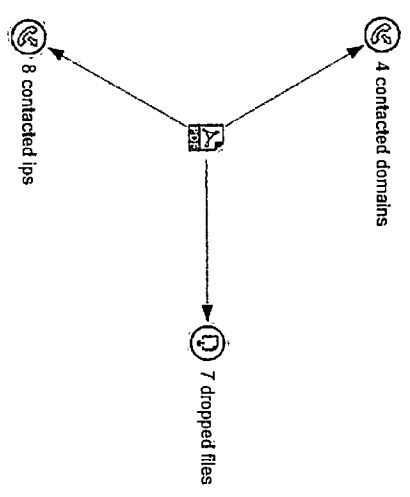
Basic Properties

Md5	d82ab65eb0e9699be342a7d8fe5d131c
SHA-1	309e86638972c30dccc7ed7b15a4e787077724
SHA-256	71326b8e0634570fba4e99a38f2901e5888b8dde1c9725614ea9d04695a52a5
Vhash	9bae2a95213f641381e3d80e1c4c1b69
SSDEEP	384:DdCQb3lphd7rH5Wz+4ldc5kwiw5r9bcj0qz6txGlcqfza:Des63hp37cyuR4a68zkw4uioxZs
TLSH	T1C982CF49AB93348BDCE2447DF30C73935A95B4D6ADCF4152824BC9B030C8EB72B44D62
File type	PDF
Magic	PDF document, version 1.4
TiID	Adobe Portable Document Format (100%)
File size	18.31 KB (18752 bytes)



Graph summary

Summarized file graph - click on the illustration to explore in VirusTotal
 Graph and dig into relationships



SHA-256 71f326b78e0634570bba4e99a362901a5688bde1c9725614ea9d04695a52a5

Vhash 9bae2a95213f641381e3d80e1c4c1b69

SSDEEP 384:DdCQ63h7d7cHSWz+M46c5KwW5r9bgOqlz6XGlcqfzaDc63np37cyUR4a68zlw4uioxZs

TLSH T1C882CF49A933488DCE2447DF30C73935A95B4D6AD0FA152624BC9B030C8EB72B44D62

File type PDF

Magic PDF document, version 1.4

TiD Adobe Portable Document Format (100%)

File size 18.31 KB (18752 bytes)

History

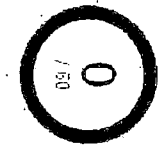
Creation Time	2022-06-28 15:29:34 UTC
First Submission	2022-07-08 03:03:33 UTC
Last Submission	2022-07-20 15:31:54 UTC
Last Analysis	2022-07-20 15:32:05 UTC

Names

Order: Denying Mot for Recon 22_6_28.pdf

71f326b78e0634570bba4e99a362901a5688bde1c9725614ea9d04695a52a5.sample






No security vendors and no sandboxes flagged this file as malicious

71f326b8e0634570bda4e99a38f2901e5888b8dde1c9725614ea9d04695a62a5 18.31 KB 2022-07-20 15:32:05 UTC

Order Denying Mot for Recon 22.6.28.pdf Size 1 hour ago


Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

 VirusTotal Juijibox 3

Behavior Tags  Summary of key behavioral patterns worth highlighting.

checks-network-adapters checks-user-input detect-debug-environment direct-cpu-clock-access long-sleeps runtime-modules

File System Actions 

Files Opened

- C:\Windows\system32\kernel32.dll
- c:\program files (x86)\adobe\reader 9.0\reader\AcroRd32.dll
- C:\Windows\system32\VERSION.dll
- c:\program files (x86)\adobe\reader 9.0\reader\AAGM.dll

[Full report](#) 



Behavior Tags

checks-network-adapters checks-user-input detect-debug-environment direct-cpu-clock-access long-sleeps runtime-modules

File System Actions When executing the file being analyzed, it performed the following actions on the filesystem of the sandbox environment

Files Opened

- C:\Windows\system32\kernel32.dll
- c:\program files (x86)\adobe\reader\9.0\reader\AcroRd32.dll
- C:\Windows\system32\VERSION.dll
- c:\program files (x86)\adobe\reader\9.0\reader\AAGM.dll
- C:\Windows\WinSxS\x86_microsoft_vc80_crt_1fc8b389a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
- c:\program files (x86)\adobe\reader\9.0\reader\CoatType.dll
- C:\Windows\WinSxS\x86_microsoft_windows_common_controls_6595b64144cfd1f_6.0.7601.18837_none_41e855142bd5705d
- C:\Windows\WinSxS\x86_microsoft_windows_common_controls_6595b64144cfd1f_6.0.7601.18837_none_41e855142bd5705d\COMCTL32.dll
- c:\program files (x86)\adobe\reader\9.0\reader\BIB.dll
- c:\program files (x86)\adobe\reader\9.0\reader\ACE.dll

Files Written

- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\AdobeCMAppFnt09.lst
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\User\Cache bin
- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\9.0\AcroFnt09.lst





71f326bf8e06345701ba4e99a3882901e5388bdde1c9725f_14ea9d04695a52a5

Files Written

- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\9.0\Cache\AcroFrt09.lst
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\AdobeCMapFrt09.lst
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\UserCache.bin
- C:\Users\<USER>\AppData\Local\Adobe\Updater\9\AdobeUpdaterPrefs.dat

Files Deleted

- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\SharedDataEvents-Journal

Registry Actions

When executing the file being studied, it performed the following actions on the registry of the sandbox environment:

Registry Keys Opened

- HKLM\Software\Adobe\Acrobat Reader\9.0\ORO
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher
- HKLM\System
- HKLM\System\Acrobat\viewer\cpu304
- HKLM\Software\Adobe
- HKCU\Software\Adobe\Acrobat Reader\9.0\Installer\Migrated
- HKCU\Software\Microsoft\Internet Explorer\Main
- HKCU\Software\Microsoft\Internet Explorer\Main\FramedWindow
- HKCU\Software\Microsoft\Internet Explorer\Main\FramedMerging

HKCU\Software\Microsoft\Internet Explorer\Main\FrameTabWindow

HKCU\Software\Microsoft\Internet Explorer\Main\FrameMerging

Registry Keys Set

- + Software\Adobe\Acrobat Reader\9.0\AV\General\blastExitNormal
- + Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- + Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Content\ContentCachePrefix
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Content\ContentCachePrefix
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Content\History\ContentCachePrefix
- + {2900B012-EB42-4B90-BF06-41027268EC68}\Wpad\DecisionReason
- + {2900B012-EB42-4B90-BF06-41027268EC68}\Wpad\DecisionTime
- + {2900B012-EB42-4B90-BF06-41027268EC68}\Wpad\Decision
- + {2900B012-EB42-4B90-BF06-41027268EC68}\Wpad\NetworkName

Registry Keys Deleted

HKLM\System\Acrobat\viewer\cpp304

71f326bf8e0634570ba4e99a38f2901e5688b0dde1c9725614ea9d04695a52a5

+ {2900E012-EB42-4B90-BF06-41027268EC68}\WpadDecision

+ {2900E012-EB42-4B90-BF06-41027268EC68}\WpadNetworkName

^

Registry Keys Deleted

HKLM\System\Acrobat\viewer\cpp304

Process And Service Actions

When executing the file being analyzed, it performed the following actions with respect to the processes and services in the sandbox environment.

Processes Created

C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe -doActionAppID=reader9dr-es_ES

Processes Terminated

C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe -doActionAppID=reader9dr-es_ES

Synchronization Mechanisms & Signals

Mutexes Created

ZAC1A572DB6944B0A65C38C4140AF2F446473B6310C

Acrobat Instance Mutex

lkvTlIkBkH4L+RZH5lg==

5cc/mBQhsQNlWE+6NHDXg==



Processes Terminated

C:\Program Files (x86)\Common Files\Adobe\Updater6\Adobe_Updater.exe -doAction=AppID=reader9dr-res_ES

Synchronization Mechanisms & Signals

When executing the file being studied, I performed the following actions related to synchronization and signals.

Mutexes Created

- 2AC1A572DB6944B0A65C38C4140AF2F446473B6310C
- Acrobat Instance Mutex
- {kwTlhkBl4nLa+RZHh5ig==}
- 5ccfbqhsqNME+6NHDXg==
- 2AC1A572DB6944B0A65C38C4140AF2F4464c0DD033B0
- dbaKjcozqEY5BO9qnlW0g==
- 2AC1A572DB6944B0A65C38C4140AF2F4464c0DD033B8
- Cx7Rk2E5nRNj416G9Z73w==

Modules Loaded

- Runtime Modules
- comctl32.dll
- c:\program files (x86)\adobe\reader 9.0\reader\rdlang32.asp
- ADVAPI32.dll
- ole32.dll
- ACTI ENG INF...144 n.dll



71f326bf8e0634570bba4e99a3882901e5888bdcde1c9725614ea9d04695a52a5
2AG1A572DB8944B0A65CC38C4140AF2F4b1c00D033B8
C*7RK2IEN5RNj416G9273w==

Modules Loaded ⓘ
When executing the file being studied, it loaded the following modules and made use of the following dynamic functionality:

Runtime Modules

- comctl32.dll
- c:\program files (x86)\adobe\reader\9.0\reader\rdlang32.esp
- ADVAPI32.dll
- ole32.dll
- API-MS-Win-Core-LocalRegistry-L-1-1-0.dll
- propsys.dll
- SHELL32.dll
- API-MS-Win-Security-LSALookup-L-1-1-0.dll
- CRYPTBASE.dll
- UXTheme.dll

Highlighted Actions ⓘ

- Calls Highlighted**
- GetTickCount



VirusTotal - File - 71f326bf8e0634570bba4e99a382901e5888bde1c9725614ea9d04695a52a5 X

VirusTotal Windows Sandbox X +



https://www.virustotal.com/gui/file/71f326bf8e0634570bba4e99a382901e5888bde1c9725614ea9d04695a52a5



Search



71f326bf8e0634570bba4e99a382901e5888bde1c9725614ea9d04695a52a5

CRYPTBASE.dll

LxTheme.dll

Highlighted Actions

When executing the file being studied, it performed the following actions that are worth highlighting because they involve suspicious calls, use of cryptography or encoding, displaying dialog, etc.

Calls Highlighted

GetTickCount

IsDebuggerPresent

SetWindowsHookExW

Sleep

GetAdaptersAddresses

Highlighted Text

71f326bf8e0634570bba4e99a382901e5888bde1c9725614ea9d04695a52a5.pdf - Adobe Reader

Adobe Acrobat

C:\Windows\System32\cmd.exe

BitDefenderThata	<input checked="" type="checkbox"/> Undetected	Bkav Pro	<input checked="" type="checkbox"/> Undetected
CiaramAV	<input checked="" type="checkbox"/> Undetected	Comodo	<input checked="" type="checkbox"/> Undetected
Cyance	<input checked="" type="checkbox"/> Undetected	Gynet	<input checked="" type="checkbox"/> Undetected
Cyren	<input checked="" type="checkbox"/> Undetected	DWWeb	<input checked="" type="checkbox"/> Undetected
Emnisoft	<input checked="" type="checkbox"/> Undetected	eScan	<input checked="" type="checkbox"/> Undetected
ESET-NOD32	<input checked="" type="checkbox"/> Undetected	F-Secure	<input checked="" type="checkbox"/> Undetected
Fortinet	<input checked="" type="checkbox"/> Undetected	GData	<input checked="" type="checkbox"/> Undetected
Gridinsoft	<input checked="" type="checkbox"/> Undetected	Ikarus	<input checked="" type="checkbox"/> Undetected
Jiangmin	<input checked="" type="checkbox"/> Undetected	KTAntiVirus	<input checked="" type="checkbox"/> Undetected
KTGW	<input checked="" type="checkbox"/> Undetected	Kaspersky	<input checked="" type="checkbox"/> Undetected
Kingsoft	<input checked="" type="checkbox"/> Undetected	Lionic	<input checked="" type="checkbox"/> Undetected
Malwarebytes	<input checked="" type="checkbox"/> Undetected	MAX	<input checked="" type="checkbox"/> Undetected
MaxSecure	<input checked="" type="checkbox"/> Undetected	Mcafee	<input checked="" type="checkbox"/> Undetected
Mcafee-GW-Edition	<input checked="" type="checkbox"/> Undetected	Microsoft	<input checked="" type="checkbox"/> Undetected

VirusTotal - File - 71f326b8e0634570bba4e99a38f2901e5888bddd1c9725614e89d04695a52a5

VirusTotal Windows Sandbox

← → 🔍 <https://www.virustotal.com/gui/file/71f326b8e0634570bba4e99a38f2901e5888bddd1c9725614e89d04695a52a5> Search

71f326b8e0634570bba4e99a38f2901e5888bddd1c9725614e89d04695a52a5

McAfee-GW-Editon	<input checked="" type="checkbox"/>	Undetected	Microsoft	<input checked="" type="checkbox"/>	Undetected
NANO-Antivirus	<input checked="" type="checkbox"/>	Undetected	Panda	<input checked="" type="checkbox"/>	Undetected
QuickHeal	<input checked="" type="checkbox"/>	Undetected	Rising	<input checked="" type="checkbox"/>	Undetected
Sangfor Engine Zero	<input checked="" type="checkbox"/>	Undetected	SentinelOne (Static ML)	<input checked="" type="checkbox"/>	Undetected
Sophis	<input checked="" type="checkbox"/>	Undetected	SUPERAntiSpyware	<input checked="" type="checkbox"/>	Undetected
Symantec	<input checked="" type="checkbox"/>	Undetected	TACHYON	<input checked="" type="checkbox"/>	Undetected
Tencent	<input checked="" type="checkbox"/>	Undetected	Trellix (FireEye)	<input checked="" type="checkbox"/>	Undetected
TrendMicro	<input checked="" type="checkbox"/>	Undetected	TrendMicro-HouseCall	<input checked="" type="checkbox"/>	Undetected
VBA32	<input checked="" type="checkbox"/>	Undetected	VIPRE	<input checked="" type="checkbox"/>	Undetected
VirIT	<input checked="" type="checkbox"/>	Undetected	V/Robot	<input checked="" type="checkbox"/>	Undetected
Yandex	<input checked="" type="checkbox"/>	Undetected	Zillya	<input checked="" type="checkbox"/>	Undetected
ZoneAlarm by Check Point	<input checked="" type="checkbox"/>	Undetected	Zoner	<input checked="" type="checkbox"/>	Undetected
Allibaba	<input checked="" type="checkbox"/>	Undetected	Avast-Mobile	<input checked="" type="checkbox"/>	Undetected
BitDefenderFalx	<input checked="" type="checkbox"/>	Undetected	CrowdStrike Falcon	<input checked="" type="checkbox"/>	Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

Undetected

VirusTotal
Contact Us

Community
Join Community

Tools
API Scripts

Premium Services
Intelligence

Documentation
Searching



Dropped File Info from Relations Report

VirusTotal - File - 71f326b8e0634570bba4e99a38f2901e5888bdae1c9725614ea9d046956a52a5

<https://www.virustotal.com/gui/file/71f326b8e0634570bba4e99a38f2901e5888bdae1c9725614ea9d046956a52a5>

Dropped Files

Scanned	Detections	File type	Name
2022-07-20	0 / 57	BMP	icon-220720235001Z-169.bmp
SHA-256	0b1e770c988ee741dfc2b6b8122604cf2d65bbabade3510e23bec69b9b5b949		
File Size	69.52 KB		
2022-07-20	0 / 58	Text	DC_Reader_RHP_Banner
SHA-256	3cafd9c3471c027fa8d9e0de1e7e3f160516699446a70b386c30a171f5d422b4		
File Size	1.36 KB		
2022-07-20	0 / 57	Text	SOPHIA.json
SHA-256	6e0b6e5e1807e7193bd2598180c82dd08da4259b4d38c39879cb8b0e5bc56f		
File Size	767 B		
2022-07-20	0 / 58	Text	Edit_InApp_Aug2020
SHA-256	d3f7e2887fc779d61c492e84b1f6156f6a713c974491360bab6a0be71f6f64		
File Size	782 B		
?	?	file	16a9eb8b067c6b8269fce52bd5b49ece855d7f1b5b10ea7528b3dc3b8774d
SHA-256	16a9eb8b067c6b8269fce52bd5b49ece855d7f1b5b10ea7528b3dc3b8774d		
File Size	?	file	43bd70a9bde1a618bee4f1026513088418a46b5269ce0d1aefc88c21537f1d
SHA-256	43bd70a9bde1a618bee4f1026513088418a46b5269ce0d1aefc88c21537f1d		
File Size	?	file	55c338568883e07ef07c9cbcf6583c4e0870840dd4417eb8144eeb843a93243
SHA-256	55c338568883e07ef07c9cbcf6583c4e0870840dd4417eb8144eeb843a93243		

Graph Summary



Full File System Actions Info from Behavior Report

VirusTotal - File - 71f326bf8e0634570fb4e99a38f2901e5888bddd1c97256 X + X

← → <https://www.virustotal.com/gui/file/71f326bf8e0634570fb4e99a38f2901e5888bddd1c97256> Search

71f326bf8e0634570fb4e99a38f2901e5888bddd1c9725614ea9d04695a52a5

Behavior Tags

checks-network-adapters checks-user-input detect-debug-environment direct-cpu-clock-access long-sleeps runtime-modules

File System Actions

When executing the file being analyzed, it performed the following actions on the file system of the sandbox environment.

Files Opened

- C:\Windows\system32\kernel32.dll
- c:\program files (x86)\adobe\reader 9.0\reader\AcroRd32.dll
- C:\Windows\system32\VERSION.dll
- c:\program files (x86)\adobe\reader 9.0\reader\AGM.dll
- C:\Windows\WinSxS\x86_microsoft_wc80_crt_1fc8b3ba1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
- c:\program files (x86)\adobe\reader 9.0\reader\CoolType.dll
- C:\Windows\WinSxS\x86_microsoft_windows_common_controls_6595b64144cctfd_6.0.7601.18837_none_41e855142bd5705d
- C:\Windows\WinSxS\x86_microsoft_windows_common_controls_6595b64144cctfd_6.0.7601.18837_none_41e855142bd5705d\COMCTL32.dll
- c:\program files (x86)\adobe\reader 9.0\reader\BJB.dll
- c:\program files (x86)\adobe\reader 9.0\reader\ACE.dll
- C:\Windows\WindowsShell.Manifest
- C:\Windows\system32\iiframe.dll
- C:\Windows\system32\api-ms-win-downlevel-shell32-l1-1-0.dll
- c:\program files (x86)\adobe\reader 9.0\reader\rdlang32.esp
- c:\program files (x86)\adobe\reader 9.0\reader\rdlang32.lpk.esp
- C:\Users\KUSER>AppData\Roaming



C:\Users\<USER>\AppData\Roaming

C:\Windows\system32\ipropys.dll

MountPointManager

C:\Windows\system32\ipropys.dll

C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches

C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches\cversions_1.db

C:\Windows\system32\ntmarta.dll

C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches\AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9\1ver0x00000000000012.db

C:\Users\desktop.ini

C:\Users

C:\Users\admin

C:\Users\<USER>\AppData

C:\Users\<USER>\Desktop\desktop.ini

C:\Users\<USER>\AppData\Roaming\

C:\Users\<USER>\AppData\Roaming\Adobe\

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat19.0\UserCache.bin

C:\Users\<USER>\AppData\Local

STORAGE#Volume#46f0a3e-0848-11ed-a714-806e6f6e6953#000000000000100000#f53f56304-b6bf-11d0-94f2-00a0c91efb8b

STORAGE#Volume#46f0a3e-0848-11ed-a714-806e6f6e6953#0000000000000650000#f53f56304-b6bf-11d0-94f2-00a0c91efb8b

C:\Windows\system32\CRRYPTSP.dll

C:\Windows\system32\rsaaenh.dll

C:\Windows\system32\RpcRtRemote.dll





71326b8e0634570ba4e99a38f2901e5888bddd1c9725614ea9d04695a52a5

C:\Windows\system32\RpcRTRemote.dll

c:\program files (x86)\adobe\reader 9.0\reader\

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\sl

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\Compare.api

C:\Windows\system32\lzres.dll

C:\Windows\system32\UXTheme.dll

C:\Windows\Fonts\staticcache.dat

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\Annots.api

C:\Users\<USER>\Downloads

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\Annots.ESP

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\Annots.lpk.ESP

C:\Users\<USER>\AppData\LocalLow

C:\Users\<USER>\Downloads\

C:\Users\<USER>\Downloads\71326b8e0634570ba4e99a38f2901e5888bddd1c9725614ea9d04695a52a5.pdf

C:\Users\

C:\Users\<USER>\

C:\Users\<USER>\Desktop\

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\EScript.api

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\EScript.ESP

c:\program files (x86)\adobe\reader 9.0\reader\plug_in\EScript.lpk.ESP

C:\Windows\system32\ole32.dll

C:\Windows\system32\ole32.dll.mui





C:\Windows\system32\win-US\USER32.dll.mui

c:\program files (x86)\adobe\reader 9.0\reader\BIB\Unite.dll

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\

C:\Users\<USER>\AppData\

c:\program files (x86)\adobe\reader 9.0\reader\sqtile.dll

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\SharedData\Events

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\SharedData\Events-journal

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\JavaScripts\

c:\program files (x86)\adobe\reader 9.0\reader\JavaScripts\

c:\program files (x86)\adobe\reader 9.0\Resource\ClMap

c:\program files (x86)\adobe\reader 9.0\Resource\CIMap\

c:\program files (x86)\adobe\reader 9.0\Resource\CIDFont\

c:\program files (x86)\adobe\reader 9.0\Resource\

c:\program files (x86)\adobe\reader 9.0\Resource\CIDFont\

c:\program files (x86)\adobe\reader 9.0\Resource\Font

c:\program files (x86)\adobe\reader 9.0\Resource\Font\

c:\program files (x86)\adobe\reader 9.0\Resource\Font\PFM\

C:\Program Files (x86)\Common Files

C:\Program Files (x86)\desktop.ini

C:\Program Files (x86)

C:\Program Files (x86)\Common Files\

C:\Users\<USER>\AppData\Local\

C:\Program Files (x86)\Common Files\Adobe\Fonts

C:\Program Files (x86)\Common Files\Adobe\Fonts

C:\Program Files (x86)\Common Files\Adobe\Fonts

C:\Program Files (x86)\Common Files\Adobe

C:\Program Files (x86)\Common Files\Adobe\Fonts

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\AdobeCom\Fnt09.lst

C:\Program Files (x86)\Common Files\Adobe\Fonts\Reqd\CMaps1

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\AdobeCom\Fnt09.lst

C:\program files (x86)\adobe\reader 9.0\Resource\CMap\Reqd\CMaps1

C:\program files (x86)\adobe\reader 9.0\Resource\CMap\Identity-H

C:\program files (x86)\adobe\reader 9.0\Resource\CMap\Identity-V

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\9.0\AdobeSys\Fnt09.lst

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\9.0\Cache\AcroFnt09.lst

C:\program files (x86)\adobe\reader 9.0\Resource\Font\Adobe\F1Std.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\CourierStd-Bold.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\CourierStd-BoldOblique.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\CourierStd-Oblique.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\CourierStd.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\MinionPro-Bold.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\MinionPro-BoldIt.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\MinionPro-It.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\MinionPro-Regular.otf

C:\program files (x86)\adobe\reader 9.0\Resource\Font\MyriadPro-Bold.otf



Full Registry Actions from Behavior Report

VirusTotal - File - 71f326br8e0634570fb4e99a38f2901e5888b8bde1c972561

VirusTotal Windows Sandbox X +

https://www.virustotal.com/gui/file/71f326br8e0634570fb4e99a38f2901e5888b8bde1c972561

71f326br8e0634570fb4e99a38f2901e5888b8bde1c9725614ea9d04695a52a5

Registry Actions

When executing the file being studied, it performed the following actions on the registry of the sandbox environment.

Registry Keys Opened

- HKLM\Software\Adobe\Acrobat Reader\9.0\ORO
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher
- HKLM\System
- HKLM\System\Acrobat\viewer\cpp304
- HKLM\Software\Adobe
- HKCU\Software\Adobe\Acrobat Reader\9.0\Installer\Migrated
- HKCU\Software\Microsoft\Internet Explorer\Main
- HKCU\Software\Microsoft\Internet Explorer\Main\FrameTab\Window
- HKCU\Software\Microsoft\Internet Explorer\Main\Frame\Merging
- HKCU\Software\Microsoft\Internet Explorer\Main\Session\Merging
- HKCU\Software\Microsoft\Internet Explorer\Main\AdminTab\Procs
- HKCU\Software\Policies\Microsoft\Internet Explorer\Main
- HKCU\Software\Microsoft\Internet Explorer\Main\Tab\Proc\Growth
- HKCU\Software\Adobe\Acrobat Reader\9.0\Language\path
- HKCU\Software\Adobe\Acrobat Reader\9.0\Language\select
- HKCU\Software\Adobe\Acrobat Reader\9.0\Language\next
- HKCU\Software\Adobe\Acrobat Reader\9.0\Language\useMLU
- HKCU\Software\Adobe\Acrobat Reader\9.0\Language\current
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer

- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\MaxDoc
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\MaxApp
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogX0
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogY0
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogW0
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogH0
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogX1
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogY1
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogW1
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogH1
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogX2
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogY2
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogW2
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogH2
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogX3
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogY3
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogW3
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogH3
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogX4
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogY4
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogW4
- HKCU\Software\Adobe\Acrobat Reader\9.0\Adobe\Viewer\DialogH4



VirusTotal - File - 71326bf8e06345701ba4e99a38f2901e5888b8dde1c9725614ea9d04695a52a5

VirusTotal\Windows Sandbox

https://www.virustotal.com/gui/file/71326bf8e06345701ba4e99a38f2901e5888b8dde1c9725614ea9d04695a52a5



71326bf8e06345701ba4e99a38f2901e5888b8dde1c9725614ea9d04695a52a5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogV4

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogH4

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogX5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogY5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogW5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DialogH5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\PrintToFile

HKCU\Software\Adobe\Acrobat\Reader\9.0\Adobe\Viewer\DomMarkPostScriptJob

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\DocumentsInTaskbar

HKCU\Software\Adobe\Acrobat\Reader\9.0\SDI

HKCU\Software\Adobe\Acrobat\Reader\9.0\SDI\NullDocMaximized

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\Private

HKCU\Software\Adobe\Acrobat\Reader\9.0\Private

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\Dockables

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles1

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles2

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles3

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles4

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles5

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles6

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles7

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles8

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles9

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles10

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles11

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles12

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles13

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles14

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles15

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles16

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles17

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles18

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles19

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles20

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles21

HKCU\Software\Adobe\Acrobat\Reader\9.0\AV\General\RecentFiles22

- HKCU\Software\Adobe\Acrobat Reader\UI\Selection\JPanel>Select
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\ExecMenuItem
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\ExecMenuItem\Whitel
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\Attachment\Perms
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\Attachment\Perms\Builtin\Permlist
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\URL\Perms
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\URL\Perms\FlashContent\Scheme\Whitel
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\URL\Perms\SponsoredContent\Scheme\Whitel
- HKLM\SOFTWARE\Policies\Adobe\Acrobat Reader\19.0\FeatureL\ockdown\CDDefault\Launch\URL\Perms\Scheme\Whitel
- HKCU\Software\Adobe\Acrobat Reader\19.0\Originals
- HKCU\Software\Adobe\Acrobat Reader\19.0\AV\Display
- HKCU\Software\Adobe\Acrobat Reader\19.0\Workflows
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FrontLink\SystemLink
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFile\Path
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\Surrogate\Fallback
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\Surrogate\Fallback\Sequo UI
- HKCU\Software\Adobe\Acrobat Reader\19.0\Annot
- HKCU\Software\Adobe\Acrobat Reader\19.0\Annot\cAnnot
- HKCU\Software\Adobe\Acrobat Reader\19.0\Annot\cAnnot
- HKCU\Software\Adobe\Acrobat Reader\19.0\Annot\cAnnot\author



VirusTotal - File - 71f326cf8e0634570bba4e99a38f2901e58688bdde1c9725614ea9d04695a52a5

VirusTotal Windows Sandbox

X +

← → <https://www.virustotal.com/gui/file/71f326cf8e0634570bba4e99a38f2901e58688bdde1c9725614ea9d04695a52a5> Search



71f326cf8e0634570bba4e99a38f2901e58688bdde1c9725614ea9d04695a52a5

HKCU\Software\Adobe\Acrobat\Reader\9.0\Annotations\AnnotationsAuthor

HKCU\Software\Adobe\Acrobat\Reader\9.0\AVAlert

HKCU\Software\Adobe\Adobe Acrobat

HKCU\Software\Adobe\Adobe Acrobat\9.0

HKCU\Software\Adobe\Adobe Acrobat\9.0\DiskCache

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\Server

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter\DisMethod

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter\UI

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter\URL

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter\Settings

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\DocumentCenter\Settings\Setting

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution\DisMethod

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution\UI

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution\URL

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution\Settings

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\EmailDistribution\Settings\Setting

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\Initiation\WizardFirstLaunch

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\Server\Settings

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\Server\Settings\CONFIG

HKCU\Software\Adobe\Acrobat\Reader\9.0\Collab\Server\Settings\WDVAWDF



VirusTotal - File - 71326bf8e0634570b9a4e99a38f2901e5888bde1c9725614ea904695a52a5

VirusTotal Windows Sandbox

X +

← → <https://www.virustotal.com/gui/file/71326bf8e0634570b9a4e99a38f2901e5888bde1c9725614ea904695a52a5> Search



71326bf8e0634570b9a4e99a38f2901e5888bde1c9725614ea904695a52a5

HKCU\Software\Adobe\Acrobat Reader\9.0\Collab\ServerSettings\IDAV\DF

HKCU\Software\Adobe\Acrobat Reader\9.0\Collab\ServerSettings\FSD\F

HKCU\Software\Adobe\Acrobat Reader\9.0\Collab\ServerSettings\NONE

HKCU\Software\Adobe\Acrobat Reader\9.0\AVTracker

HKCU\Software\Adobe\Acrobat Reader\9.0\TaskButtons

HKCU\Software\Adobe\Acrobat Reader\9.0\AcrobatDocs

HKLM\Software\Adobe\Acrobat Reader\9.0\AdobeViewer\EULA

HKCU\Software\Adobe\Acrobat Reader\9.0

HKCU\Software\Adobe\Acrobat Reader\9.0\hasUnread

HKCU\Software\Adobe\Acrobat Reader\9.0\AVPrivate

HKCU\Software\Adobe\Acrobat Reader\9.0\Preview

HKCU\Software\Adobe\Acrobat Reader\9.0\Access

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocHistory

HKCU\Software\Adobe\Acrobat Reader\9.0\LayoutAndZoom

HKCU\Software\Adobe\Acrobat Reader\9.0\FullScreen

HKCU\Software\Adobe\Acrobat Reader\9.0\Debug

HKCU\Software\Adobe\Acrobat Reader\9.0\AdobeViewer\Launched

HKCU\Software\Adobe\Acrobat Reader\9.0\Measurements

HKCU\Software\Adobe\Acrobat Reader\9.0\RememberedViews

HKCU\Software\Adobe\Acrobat Reader\9.0\RememberedViews\NoCategoryFiles

HKCU\Software\Adobe\Acrobat Reader\9.0\RememberedViews\NoCategoryFiles\1

HKCU\Software\Adobe\Acrobat Reader\9.0\RememberedViews\NoCategoryFiles\1\ViewDef

HKCU\Software\Adobe\Acrobat Reader\9.0\RememberedViews\NoCategoryFiles\1\ViewDef



71f326bf8e0634570bba4e93a382901e5688b8dd1e9725614ea9d04695a52a5

- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_LOW_NULL_IN_RESPONSE_HEADERS
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DIGEST_NO_EXTRAS_IN_URI
- HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
- HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
- HKLM\Software\Policies
- HKCU\Software
- HKLM\Software\Policies\Microsoft\Internet Explorer
- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1_1
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1_1
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
- HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache



71326bf8e0634570bba4e99a382901e5888bddd1c9725614ea9d04695a52a5

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache

HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266

HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_COMPACT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543

HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SCH_SEND_AUX_RECORD_KB_2618444

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WpadOverride

HKLM\Software\Policies\Microsoft\PeerDist\Service

HKLM\Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

HKLM\System\Setup

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

HKLM\Software\Microsoft\OLEAut

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC683

HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915

HKCU\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

HKCU\Software\Microsoft\Internet Explorer\Security

- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
- HKCU\Software\Internet Explorer\Security
- HKCU\Software\Internet Explorer\SecurID\DisablesSecurity\Settings\Check
- HKLM\System\Setup\SystemSetup\Progress
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones0
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones1
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones2
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones3
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones4
- HKCU\Software\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN
- HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUrlCacheSize
- HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CreateUrlCacheSize
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnablePunycode
- HKCU\Software\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPpad\52-54-00-b2-3b-fe
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPpad\2900B012-EB42-4B90-BF06-41027268EC689\52-54-00-b2-3b-fe
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPpad\2900B012-EB42-4B90-BF06-41027268EC689\WPpad\Decision
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPpad\2900B012-EB42-4B90-BF06-41027268EC689\WPpad\DecisionTime



Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDecision

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDecisionTime

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\ExpirationDays

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDecisionReason

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDhcp

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDns

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\2900B012-EB42-4B90-BF06-41027268EC689\WpadDetectedUri

52-54-00-b2-3b-fe\WpadDecision

52-54-00-b2-3b-fe\WpadDecisionTime

52-54-00-b2-3b-fe\WpadDecisionReason

52-54-00-b2-3b-fe\WpadDhcp

52-54-00-b2-3b-fe\WpadDns

52-54-00-b2-3b-fe\WpadDetectedUri

HKLM\System\CurrentControlSet\Services\LanmanServer\DefaultSecurity

HKLM\System\CurrentControlSet\Services\LanmanServer\DefaultSecurity\SystemService\DefaultShareInfo

HKLM\System\CurrentControlSet\Services\Explorer\Sharing

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma

Registry Keys Set

- + Software\Adobe\Acrobat Reader\9.0\AV\General\LastExitNormal
- + Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

Full Registry Key Set Info from Behavior Report

VirusTotal - File - 71f326bf8e0634570fba4e99a382901e5888b8dde1e9725614ea9dd04695a552a5

VirusTotal Windows Sandbox

https://www.virustotal.com/gui/file/71f326bf8e0634570fba4e99a382901e5888b8dde1e9725614ea9dd04695a552a5

71f326bf8e0634570fba4e99a382901e5888b8dde1e9725614ea9dd04695a552a5

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePacks\SurrogateFallback\Tahoma

Registry Keys Set

- Software\Adobe\Acrobat Reader\9.0\AV\General\blaste\ExitNormal
- 0
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Enable
- 0
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- F
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
- Cookie:
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
- Visited:
- {29005012-EB42-4B90-BF06-41027268EC68}\Wpad\DecisionReason
- 1



VirusTotal - File - 71f326bf8e0634570bba4e99a38f2901a5888bdc1c9725614ea9d04695ae2a5

VirusTotal Windows Sandbox X +

← → <https://www.virustotal.com/gui/file/71f326bf8e0634570bba4e99a38f2901a5888bdc1c9725614ea9d04695ae2a5> Search Sign in Sign up

71f326bf8e0634570bba4e99a38f2901a5888bdc1c9725614ea9d04695ae2a5

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix

Visited:

- {2900B012-EB42-4B90-BF06-41027268EC68}\WpaddDecisionReason

1

- {2900B012-EB42-4B90-BF06-41027268EC68}\WpaddDecisionTime

折叠器\D

- {2900B012-EB42-4B90-BF06-41027268EC68}\WpaddDecision

0

- {2900B012-EB42-4B90-BF06-41027268EC68}\WpaddNetworkName

Network 3

- 52-54-00-b2-3b-f6\WpaddDetectedUrl

Registry Keys Deleted

HKLM\System\Acrobat\Viewer\pp304

Process And Service Actions

DropProc Creation



Full Modules Loaded Info from Behavior Report

VirusTotal - File - 71f326bf8e0634570ba4e99a38f2901e5888b0dde1c9725614ea9d04695a52a5 X
VirusTotal - Windows Sandbox X +
https://www.virustotal.com/gui/file/71f326bf8e0634570ba4e99a38f2901e5888b0dde1c9725614ea9d04695a52a5
71f326bf8e0634570ba4e99a38f2901e5888b0dde1c9725614ea9d04695a52a5
Search
Sign in Sign up

Modules Loaded When executing the file being studied, it loaded the following modules and made use of the following dynamic functionality:

Runtime Modules

- comctl32.dll
- c:\program files (x86)\adobe\reader 9.0\reader\rlang32.esp
- ADVAPI32.dll
- ole32.dll
- API-MS-Win-Core-LocalRegistry-L1-1-0.dll
- propsys.dll
- SHELL32.dll
- API-MS-Win-Security-LSALookup-L1-1-0.dll
- GRYPTEASE.dll
- UxTheme.dll
- IMM32.dll
- Annots.api
- c:\program files (x86)\adobe\reader 9.0\reader\plug_inst\Annots.ESP
- c:\program files (x86)\adobe\reader 9.0\reader\acord32.exe
- EScript.api
- c:\program files (x86)\adobe\reader 9.0\reader\plug_inst\EScript.ESP
- Updater.api
- c:\program files (x86)\adobe\reader 9.0\reader\plug_inst\Updater.ESP
- OLEAUT32.dll

Updater.apl

- c:\program files (x86)\adobe\reader_9.0\reader\plug_ins\Updater.ESP
- OLEAUT32.dll
- SHLWAPI.dll
- Secur32.dll
- api-ms-win-downlevel-advapi32-l1-1-0.dll
- api-ms-win-downlevel-ole32-l1-1-0.dll
- WS2_32.dll
- winhttp.dll
- IPHLPAPI.DLL
- api-ms-win-downlevel-shlwapi-l2-1-0.dll
- DNSAPI.dll
- dhcpcsvc.DLL
- urlmon.dll
- C:\Windows\system32\shell32.dll
- C:\Windows\system32\ntshrui.dll
- srvc1.dll
- sic.dll
- API-MS-Win-Security-SDCL-1-1-0.dll
- netutils.dll

^



IP Address Info

All of the IP address go to either Akamai International which is a major hosting platform or Amazon-AES which is Amazon Email Service. See below

Browser tabs: VirusTotal - File - 71326f88d055 X, VirusTotal - Ip address - 92.123. X, VirusTotal - Ip address - 34.237. X, what is Amazon-AES at DuckD... X, +

Address bar: <https://www.virustotal.com/gui/ip-address/92.123.140.146>

Navigation: Home, Back, Forward, Refresh, Stop, Print, Sign in, Sign up



1 detected file communicating with this IP address

92.123.140.146 (92.123.140.0/22)
AS 20940 (Akamai International B.V.)

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security Vendors' Analysis

Vendor	Status	Vendor	Status
0xSI_833d	Clean	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICG (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Arnis	Clean	AutoShun	Clean
Avira	Clean	BADWARE.INFO	Clean



