MALICIOUS

Classifications: Phishing

Threat Names: Phishkit.Xbalti

Verdict Reason: -

Sample Type	URL
File Name	**https://amazom.ideainternational.cn/pc/**
ID	#2756555
MD5	d8a678e362b0cac9c250d99603d112fb
SHA1	13140df43cc13a6721b7003e38f901301e9cfe7a
SHA256	344cd73a1b4ede344ce232144f273756f0e681adff0ae8335850b10127d1eafa
File Size	39 bytes
Report Created	2021-09-22 15:56 (UTC+2)
Target Environment	win10_64_th2_en_web | web_root

OVERVIEW

VMRay Threat Identifiers (5 rules, 10 matches)

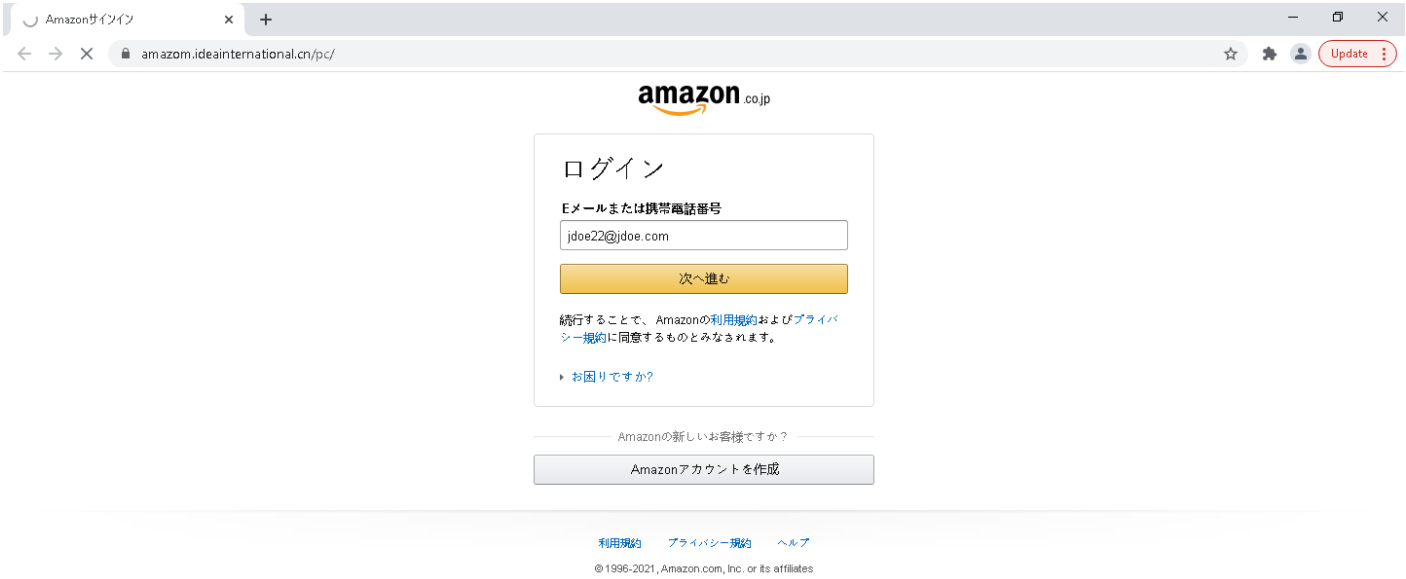
Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	4	Phishing
	• Rule "Phishkit_Xbalti" from ruleset "Xbalti" has matched on response data of URL "https://amazom.ideainternational.cn/pc/". • Rule "Phishkit_Xbalti" from ruleset "Xbalti" has matched on response data of URL "https://amazom.ideainternational.cn/pc/js/sire.form.js". • Rule "Phishkit_Xbalti" from ruleset "Xbalti" has matched on response data of URL "https://amazom.ideainternational.cn/pc/homepage/?update_billing". • Rule "Phishkit_Xbalti" from ruleset "Xbalti" has matched on response data of URL "https://amazom.ideainternational.cn/pc/homepage/Card.php?Update_Your_Card".		
5/5	Heuristics	Page is determined to be phishing attempt	1	Phishing
	• Pretends to belong to Amazon.			
2/5	Heuristics	Page secured via a Domain Validated SSL certificate	1	-
	• Host amazom.ideainternational.cn uses DV certificate issued by R3 to amazon.hhrdkj.cn.			
1/5	Heuristics	Page presents itself as a logon page	3	-
	• URL of https://amazom.ideainternational.cn/pc/signin.php?login indicates it is a logon page. • Page https://amazom.ideainternational.cn/pc/ contains a logon form. • Page https://amazom.ideainternational.cn/pc/signin.php?login contains a logon form.			
1/5	Masquerade	Page uses exact favicon of a popular online service	1	-
	• Uses the exact favicon of Amazon.			

Sample Information

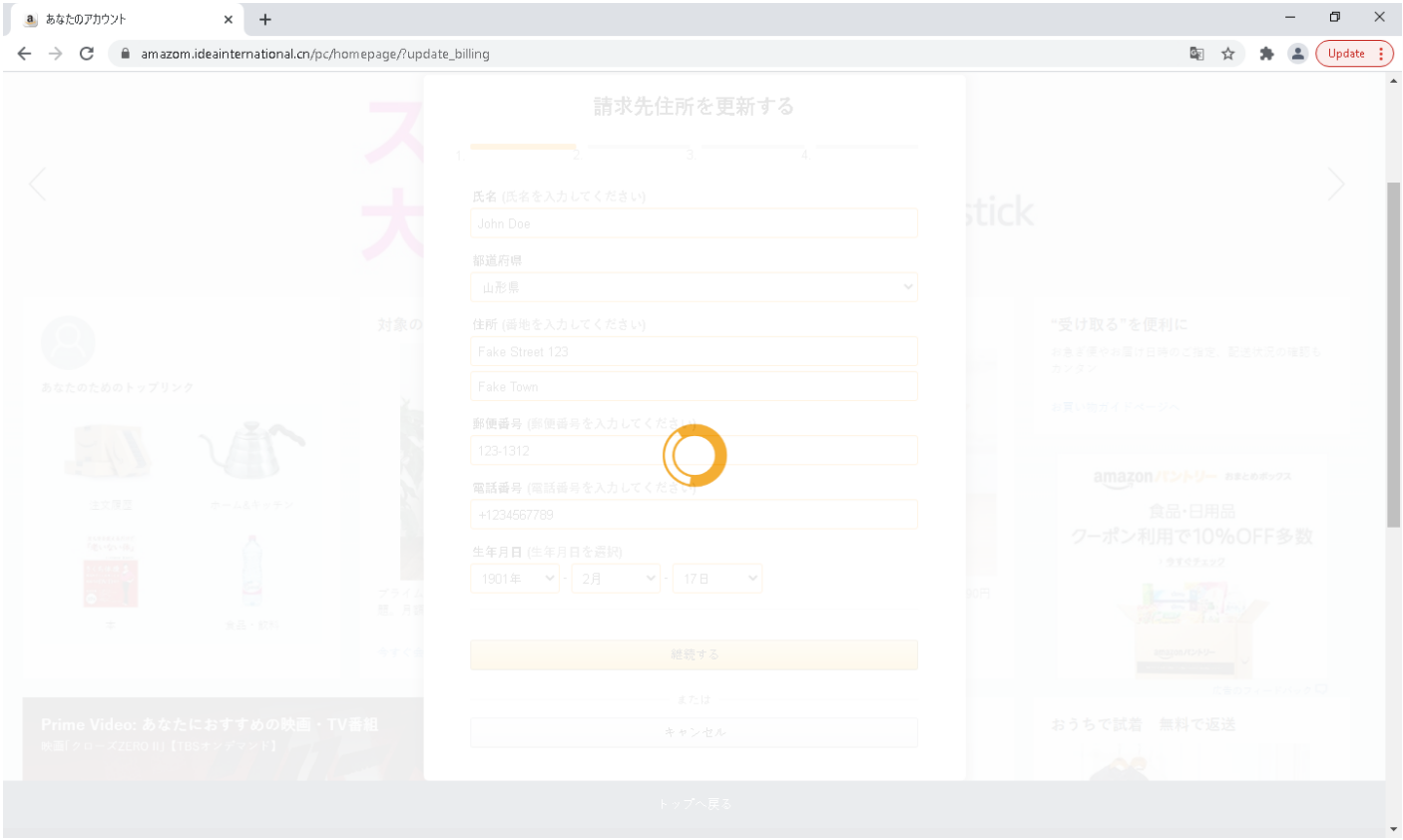
ID	#2756555
MD5	d8a678e362b0cac9c250d99603d112fb
SHA1	13140df43cc13a6721b7003e38f901301e9cfe7a
SHA256	344cd73a1b4ede344ce232144f273756f0e681adff0ae8335850b10127d1eafa
SSDeep	3:N89BAllAVKacKr:29uAgack
File Name	https://amazom.ideainternational.cn/pc/
File Size	39 bytes
Sample Type	URL
Has Macros	✓

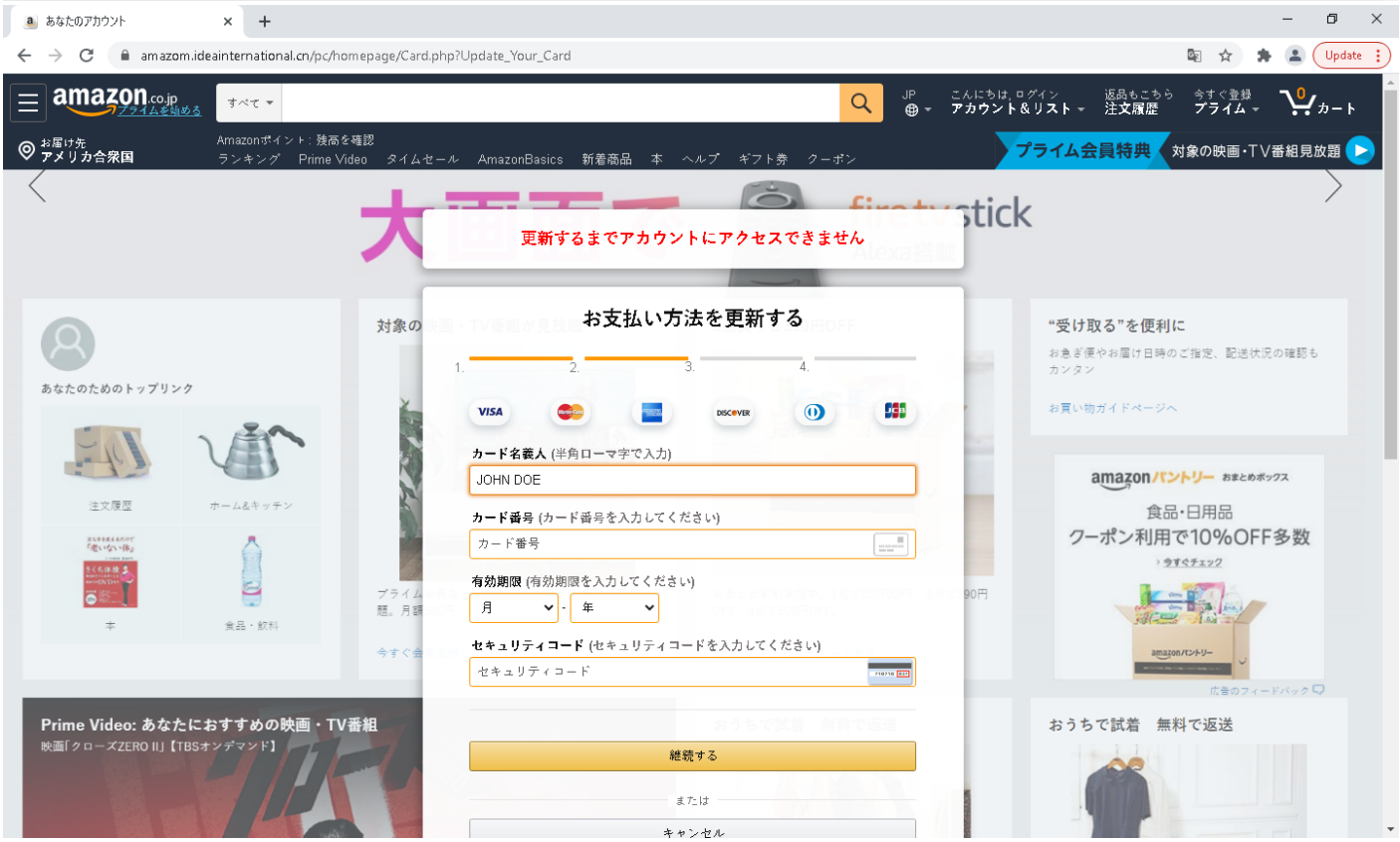
Analysis Information

Creation Time	2021-09-22 15:56 (UTC+2)
Analysis Duration	00:04:59
Termination Reason	Timeout
Number of Monitored Processes	0
Execution Successful	False
Reputation Enabled	✗
WHOIS Enabled	✗
Built-in AV Enabled	✓
Built-in AV Applied On	PCAP File, Downloaded Files, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	PCAP File, Downloaded Files, Embedded Files
Number of YARA Matches	4


Amazonサインイン
amazom.ideainternational.cn/pc/
Update
amazon.co.jp
ログイン
Eメールまたは携帯電話番号
jdoe22@jdoe.com
次へ進む
続行することで、Amazonの利用規約およびプライバシー規約に同意するものとみなされます。
お困りですか?
Amazonの新しいお客様ですか？
Amazonアカウントを作成
利用規約
プライバシー規約
ヘルプ
© 1996-2021, Amazon.com, Inc. or its affiliates


Waiting for amazom.ideainternational.cn...
Amazonサインイン
amazom.ideainternational.cn/pc/signin.php?login
Update
amazon.co.jp
ログイン
jdoe22@jdoe.com 変更
パスワード
パスワードを忘れた場合
ログイン
ログインしたままにする 詳細
利用規約
プライバシー規約
ヘルプ
© 1996-2021, Amazon.com, Inc. or its affiliates


あなたのアカウント
amazom.ideainternational.cn/pc/homepage/?update_billing
Update
請求先住所を更新する
氏名 (氏名を入力してください)
John Doe
都道府県
山形県
住所 (番地を入力してください)
Fake Street 123
Fake Town
郵便番号 (郵便番号を入力してください)
123-1312
電話番号 (電話番号を入力してください)
+1234567789
生年月日 (生年月日を選択)
1901年 - 2月 - 17日
継続する
または
キャンセル
トップへ戻る


あなたのアカウント
amazom.ideainternational.cn/pc/homepage/Card.php?Update_Your_Card
Update
更新するまでアカウントにアクセスできません
お支払い方法を更新する
1. 2. 3. 4.
カード名義人 (半角ローマ字で入力)
JOHN DOE
カード番号 (カード番号を入力してください)
カード番号
有効期限 (有効期限を入力してください)
月 - 年
セキュリティコード (セキュリティコードを入力してください)
セキュリティコード
継続する
または
キャンセル

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 443

2 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

39 URLs contacted, 2 servers

2 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://amazom.ideainternational.cn/pc/	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/style3.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/style2.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/style1.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/jquery.min.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/sire.form.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/jquery.validate.min.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/AmazonUIBaseCSS-sprite_1x-28bd59af93d9b1c745bb0aca4de58763b54df7cf._V2_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/AmazonUIBaseCSS-sprite_jp_1x-f8582354fc42b464ef5eb709dd98f9371d3eafea._V2_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/icon.png	-	-		0 bytes	NA
POST	https://amazom.ideainternational.cn/pc/XBALTI/get_pass.php	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/signin.php?login	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/styel/style1.css	-	-		0 bytes	NA
POST	https://amazom.ideainternational.cn/pc/XBALTI/send_login.php	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/?update_billing	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/hanan.css	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://amazom.ideainternational.cn/pc/style/css/style3.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/css/style2.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/css/style1.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/41VXYQh+WJL.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/style4.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/css.css	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/nav-sprite-global_bluebeacon-1x_optimized_layout1._CB468502046_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/corgi._CB485918084_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/swm_400x39_180701_WOCTA._CB485945278_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/a1/Prime_Logo_PIN._CB485924482_.png	-	-		0 bytes	NA
GET	https://images-fe.ssl-images-amazon.com/images/G/09/gno/sprites/nav-sprite-global_bluebeacon-1x_optimized_layout1._CB468502046_.png	-	-		0 bytes	NA
GET	https://m.media-amazon.com/images/G/01/AUIClients/InternationalCustomerPreferencesNavAssets-icp_sprite-0b528ccc99b2eed18447291de6df851bc2c6fe68._V2_.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/loading.gif	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/jquery.mask.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/back.png	-	-		0 bytes	NA
POST	https://amazom.ideainternational.cn/pc/XBALTI/send_billing.php	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/homepage/Card.php?Update_Your_Card	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/jquery.card.min.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/js/add.class.js	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/cc.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/card_sprite.png	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/ccv.gif	-	-		0 bytes	NA
GET	https://amazom.ideainternational.cn/pc/style/img/eror.png	-	-		0 bytes	NA

ARTIFACTS

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://amazom.ideainternational.cn/pc/	-	198.98.58.236	-	GET	MALICIOUS
https://amazom.ideainternational.cn/pc/js/sire.form.js	-	198.98.58.236	-	GET	MALICIOUS
https://amazom.ideainternational.cn/pc/homepage/?update_billing	-	198.98.58.236	-	GET	MALICIOUS
https://amazom.ideainternational.cn/pc/homepage/Card.php?Update_Your_Card	-	198.98.58.236	-	GET	MALICIOUS
https://amazom.ideainternational.cn/pc/style/style3.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/style2.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/style1.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/js/jquery.min.js	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/js/jquery.validate.min.js	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/AmazonUIBaseCSS-sprite_1x-28bd59af93d9b1c745bb0aca4de58763b54df7cf._V2_.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/AmazonUIBaseCSS-sprite_jp_1x-f8582354fc42b464ef5eb709dd98f9371d3eafea._V2_.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/icon.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/XBALTI/get_pass.php	-	198.98.58.236	-	POST	SUSPICIOUS
https://amazom.ideainternational.cn/pc/signin.php?login	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/styel/style1.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/XBALTI/send_login.php	-	198.98.58.236	-	POST	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/hanan.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/css/style3.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/css/style2.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/css/style1.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/homepage/a1/41VXYQh+WJL.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/style4.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/homepage/a1/css.css	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/homepage/a1/nav-sprite-global_bluebeacon-1x_optimized_layout1._CB468502046_.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/homepage/a1/corgi._CB485918084_.png	-	198.98.58.236	-	GET	SUSPICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://amazom.ideainternational.cn/pc/homepage/a1/swm_400x39_180701_WOCTA._CB485945278_.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/homepage/a1/Prime_Logo_PIN._CB485924482_.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/loading.gif	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/js/jquery.mask.js	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/back.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/XBALTI/send_billing.php	-	198.98.58.236	-	POST	SUSPICIOUS
https://amazom.ideainternational.cn/pc/js/jquery.card.min.js	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/js/add.class.js	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/cc.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/card_sprite.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/ccv.gif	-	198.98.58.236	-	GET	SUSPICIOUS
https://amazom.ideainternational.cn/pc/style/img/eror.png	-	198.98.58.236	-	GET	SUSPICIOUS
https://images-fe.ssl-images-amazon.com/images/G/09/gno/sprites/nav-sprite-global_bluebeacon-1x_optimized_layout1._CB468502046_.png	-	199.232.137.16	-	GET	CLEAN
https://m.media-amazon.com/images/G/01/AUIClients/InternationalCustomerPreferencesNavAssets-icp_sprite-0b528ccc99b2eed18447291de6df851bc2c6fe68._V2_.png	-	199.232.137.16	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
amazom.ideainternational.cn	198.98.58.236	-	HTTPS	SUSPICIOUS
images-fe.ssl-images-amazon.com	199.232.137.16	-	HTTPS	CLEAN
m.media-amazon.com	199.232.137.16	-	HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
198.98.58.236	amazom.ideainternational.cn	United States	TCP, DNS, TLS	CLEAN
199.232.137.16	media.amazon.map.fastly.net, images-fe.ssl-images-amazon.com, m.media-amazon.com	Germany	TCP, DNS, TLS	CLEAN

YARA / AV

YARA (4)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Xbalti	Phishkit_Xbalti	Phishing page from Phishkit.Xbalti	Web Request	-	Phishing	5/5
Xbalti	Phishkit_Xbalti	Phishing page from Phishkit.Xbalti	Web Request	-	Phishing	5/5
Xbalti	Phishkit_Xbalti	Phishing page from Phishkit.Xbalti	Web Request	-	Phishing	5/5
Xbalti	Phishkit_Xbalti	Phishing page from Phishkit.Xbalti	Web Request	-	Phishing	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_web
Description	win10_64_th2_en_web
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Web Engine Version	1.5.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.0.4 / 2021-09-16 11:30:34
Web Engine Auto UI Rules Version	4.3.0.0 / 2021-09-20 03:00:12
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-22 11:17:13+00:00
Built-in AV Database Records	10404586

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	90.0.4430.85
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows