マルウェア・クリプターをDNSで徹底調査

目次

要旨

組織がネットワーク防衛を強化するたびに、サイバー犯罪者は攻撃の手口を巧妙化する斬新な方法を編み出します。マルウェア・クリプティング（悪意あるプログラム、アプリ、ファイルをマルウェア対策や侵入検知ソリューションに対して無害であるかのように見せかけるプロセス）の論理的根拠は、実はこれなのです。マルウェア・クリプティングは、最も安全なネットワークにさえも大きな脅威をもたらす可能性があります。そのため、サイバーセキュリティコミュニティでは、マルウェア・クリプティングを提供する脅威アクターやサイトの取り締まりを強く推奨しています。

インターネットの安全性を高める取り組みの一環として、WhoisXML APIは最近、マルウェア・クリプティングと関連するプロパティを探すため、DNSを徹底的に調査しました。調査ではまず、マルウェア・クリプティングのセキュリティ侵害インジケーター（IoC）としてKrebsが特定した8個のドメイン名のリストを拡張することから始めました。次に、現在最も多用されているクリプターの一つ「AceCryptor」に特化した調査を行いました。

その結果、以下が判明しました。

- KrebsのIoCと同じIPアドレスを使うドメイン名に見られた**mobile-soft**または**cryptor**という文字列を含む786個のドメイン名。そのうち2個は、マルウェア一括チェックツールによって悪意があると確認
- 一部の AceCryptorのIoCが名前解決した4個の専用または専用かもしれないIPアドレス。そのうちの2個については、悪意があることをマルウェア一括チェックツールで確認
- AceCryptorの専用IPアドレスでホストされている279個のドメイン名。そのうち17個は、マルウェア一括チェックツールによって悪意があることを確認

1. マルウェア・クリプティングのIoCの裏側

Krebsが特定したIoCをBulk WHOIS Lookupで分析したところ、以下のことがわかりました。

- PDR Ltd.というレジストラを介して登録されたドメイン名が2個。その他、Dynadot、REGRU-RU、RU-CENTER-RU、SALENAMES-RUがそれぞれ1個のドメイン名を管理
- ほとんどは2006年から2022年の間に登録されたドメイン名
- 3つは米国で登録されたドメイン名
- IoCが名前解決したIPアドレスは8個。それらをReverse IP Lookupで分析した結果、そのうち1個（138[.]201[.]203[.]122)）は専用ホストと判明

上記の8個のIPアドレスをBulk IP Geolocation Lookupで検索したところ、以下が明らかになりました。

- 米国に位置するアドレスが5個。その他、1個ずつがドイツ、オランダおよびロシアを指していた
- 米国にある5個のIPアドレスのうち4個はCloudflare, Inc.が、残りの1個はTrellianが管理。ドイツ、オランダ、ロシアのIPアドレスは、それぞれHetzner Online GmbH、Serverel, Inc.、REG.RU, Ltd.が管理していた

さらに調査を進めるため、私たちはマルウェア・クリプティング関連のIoCに繋がるDNSの痕跡を探しました。

そして、上記のIPアドレスをReverse IP Lookup で逆引きした結果、現在もアクティブな2つの関連ドメイン名に辿り着きました。

次に、IoCとして特定されたドメイン名のうち2つに、マルウェア・クリプティングのサイトを指す可能性のある2つの文字列（**mobile-soft**と**cryptor**）が含まれていることに気付きました。そこで、それらをDomains & Subdomains Discoveryにかけてみたところ、2023年1月1日以降に作成された786個のドメイン名が検出されました。マルウェア一括チェックツールで調べた結果、そのうちの2個は悪意あるドメインとして分類されました。

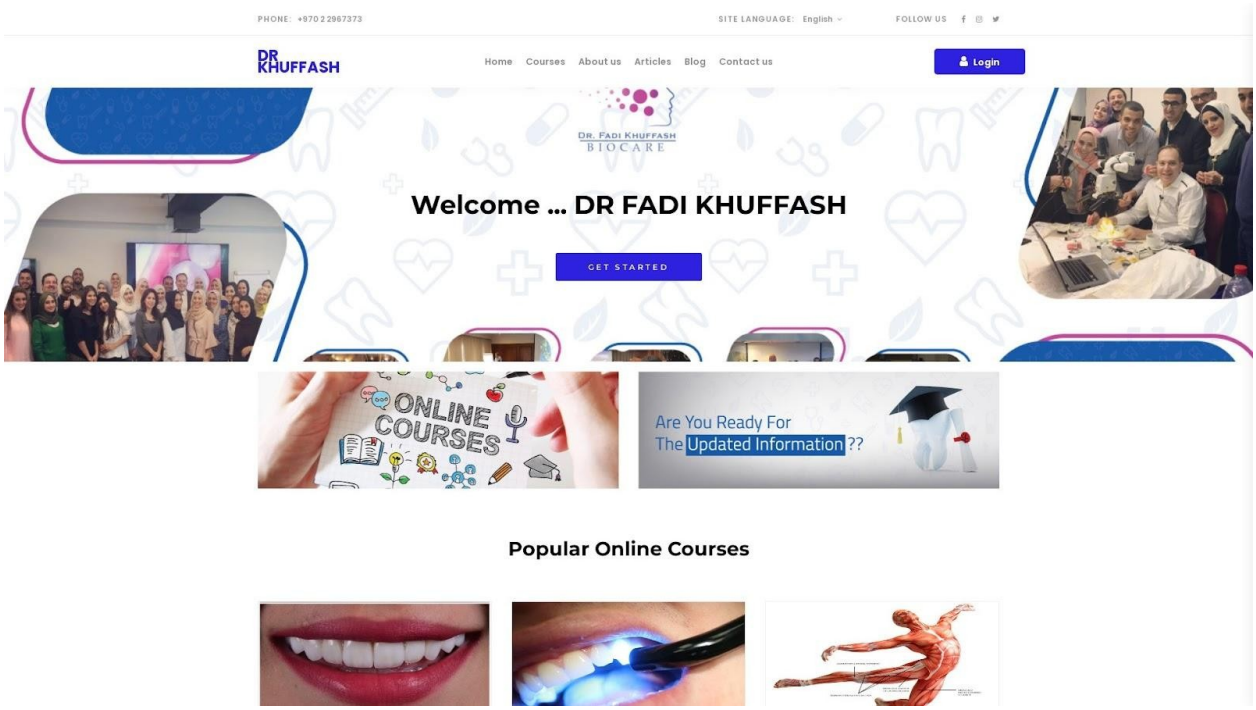
2. AceCryptorの調査結果

現在トップ・クリプターと呼ばれているAceCryptorに特化して詳しく調べるため、7個のドメイン名と3個のIPアドレスからなるAceCryptor関連のIoCリストを入手しました。

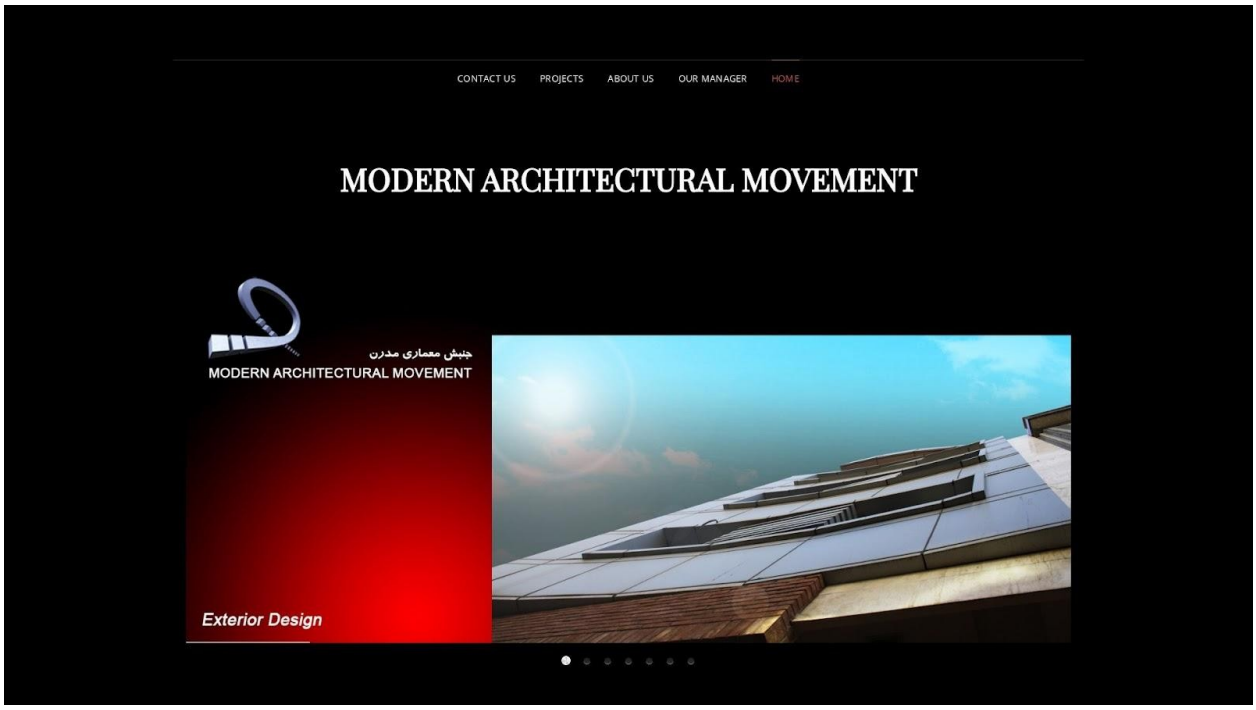
IoCと判定されたドメイン名を当社のBulk WHOIS Lookupで一括検索したところ、WHOISレコードを持っていたドメイン名は4個しかありませんでした。それらのドメイン名のうち2個はGoDaddy.com, LLCを、各1個はOnlineNIC, Inc.とNamecheap, Inc.を介して登録されたものでした。4つはいずれも2005年から2016年の間に登録された古いドメイン名で、うち2つは米国、1つはアフガニスタン、もう1つはアイスランドで登録されていました。また、それらのドメイン名をDNSで検索した結果、5つのユニークなIPアドレスに名前解決しました。さらにそれらのIPア

ドレスを当社のReverse IP Lookupにかけたところ、2つのIPアドレスは専用と確認され、もう2つは専用と思われました。また、マルウェアチェックツールで調べた結果、2つは悪意あるIPホストであることがわかりました。

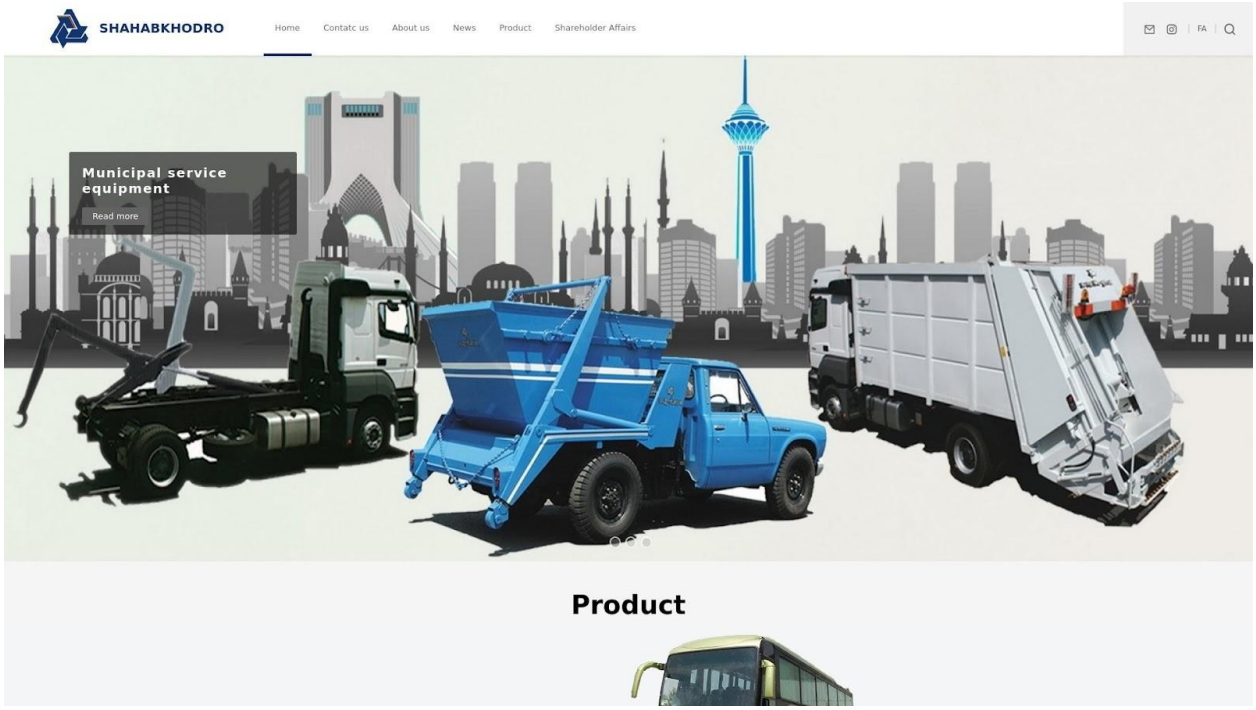
Reverse IP Lookup では、279個のドメイン名も検出できました。マルウェアチェックツールにより、そのうち17個は悪意あるドメイン名と判定されました。さらにそのうちの13個はアクティブなコンテンツをホストし続けていましたが、いずれも悪意あるサイトには見えませんでした。以下にいくつかの例を示します。



drkhuffash[.]comのスクリーンショット



jonbesh2m[.]comのスクリーンショット



shahabkhodro[.]co[.]irのスクリーンショット

—

悪意あるウェブサイトを無害に見せるソリューションであることから、クリプターを利用したサイバー攻撃は今後さらに増えると思われます。

今回、マルウェア・クリプティング全般を視野に最新のDNSデータを使って調査した結果、潜在的な関連アーティファクトが786個検出されました。他方、代表的なクリプターであるAceCryptorに特化した調査では、DNS情報から関連のプロパティを300個近く特定できました。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

マルウェア・クリプティング関連のIoC

- thelibrary[.]ru
- thelib[.]ru
- mobile-soft[.]su
- cryptor[.]biz
- crypt[.]guru
- bile[.]ru
- autodoska[.]biz
- antivirusxp09[.]com

マルウェア・クリプティング関連IoCが名前解決したIPアドレスの例

- 31[.]31[.]205[.]163
- 138[.]201[.]203[.]122
- 172[.]67[.]135[.]30
- 104[.]21[.]26[.]10

専用IPアドレスを共用していたドメイン名の例

- modernlib[.]ru

共通の文字列を含むドメイン名の例

- cryptor[.]cc
- cryptor[.]eu
- cryptor[.]ga
- cryptorc[.]io
- cryptore[.]cn
- cryptore[.]it
- cryptorm[.]vg
- cryptory[.]cc
- cryptort[.]cc
- cryptorr[.]cc

- cryptorw[.]cc
- cryptory[.]cn
- cryptoro[.]ru
- acryptor[.]cn
- cryptorq[.]cc
- cryptoro[.]de
- cryptors[.]ml
- cryptore[.]de
- cryptorus[.]vg
- decryptor[.]ph
- 0cryptor[.]com
- scryptory[.]co
- cryptorap[.]io
- recryptor[.]ru
- cryptorob[.]ml
- cryptornd[.]io
- excryptor[.]io
- cryptorim[.]io
- cryptoroi[.]de
- 0cryptor[.]xyz
- incryptor[.]de
- encryptor[.]ca
- cryptorho[.]tv
- cryptoreg[.]de
- cryptoron[.]de
- cryptorec[.]cc
- cryptorex[.]it
- cryptorey[.]es
- cryptoraj[.]in
- cryptori[.]xyz
- cryptorro[.]eu
- cryptoria[.]bg
- decryptor[.]nl
- cryptorom[.]ru
- cryptorom[.]nl
- cryptorho[.]io
- cryptoros[.]io
- cryptortb[.]tv
- encryptor[.]cn
- cryptorho[.]us
- cryptoron[.]eu
- scryptori[.]io
- cryptorip[.]co
- cryptorig[.]it
- cryptoroy[.]de
- cryptorxt[.]co
- cryptoria[.]ai
- cryptoroo[.]ru
- cryptorawa[.]vg
- cryptormt[.]com
- cryptorun[.]top
- cryptorcy[.]com
- cryptorigs[.]de
- cryptorate[.]it
- cryptorama[.]it
- cryptorim[.]bid
- cryptorich[.]tw
- cryptorace[.]nl
- cryptorado[.]cf
- cryptorekt[.]me
- cryptoriez[.]be
- cryptorium[.]tv
- cryptorain[.]io
- cryptoraid[.]eu
- cryptorobo[.]cn
- cryptoroma[.]it
- cryptorho[.]net
- cryptorom[.]pro
- cryptorace[.]de
- cryptorico[.]in
- cryptoroth[.]io
- endcryptor[.]fi
- cryptorobo[.]de
- cryptorata[.]it
- cryptoreca[.]me
- cryptorare[.]co
- cryptorica[.]cc
- cryptorise[.]uk
- cryptorise[.]vg
- cryptoroi[.]pro

- cryptorake[.]in
- cryptoreca[.]be
- cryptorho[.]xyz
- cryptorwa[.]xyz
- cryptorudi[.]vg
- cryptorho[.]org
- cryptorock[.]it
- cryptors[.]site
- cryptoroad[.]io
- cryptorack[.]ca

共通の文字列を含む悪意あるドメイン名の例

- cryptoreach[.]space

AceCryptorのIoC

- swiftlend[.]co
- paulbeebe[.]net
- musichild[.]com
- drkhuffash[.]com
- consultorescaracas[.]com
- arkan-intl[.]com
- ahmedadel[.]work
- 212[.]83[.]46[.]50
- 194[.]33[.]45[.]109
- 194[.]127[.]179[.]127

AceCryptorのIoCが名前解決したIPアドレスの例

- 50[.]62[.]6[.]196
- 107[.]180[.]57[.]28
- 173[.]212[.]207[.]172

悪意あるAceCryptorのIPホストの例

- 107[.]180[.]57[.]28

AceCryptorのIPホストを共用していたドメイン名の例

- 196[.]6[.]62[.]50[.]host[.]secureserver[.]net
- 237[.]165[.]148[.]132[.]host[.]secureserver[.]net
- 4points[.]ir
- abrance[.]com
- achilleasfereos[.]com
- adakalloys[.]com
- advancedgroup[.]co
- afghanistantransport[.]com
- afsco[.]ir
- ahangeparsian[.]com
- akniavaran[.]com
- aliparvaresh[.]com
- alleywaydxb[.]com
- andrijosefphotography[.]com
- angelosavgousti[.]live
- appletv[.]ir
- ariotek[.]ir
- arman-co[.]com
- armehgida[.]com
- armingolshahi[.]com
- aromatisch-pet[.]com
- artgallery[.]persianarc[.]com
- aryaroyanteb[.]com
- asaliftco[.]com

- ashkanchemistry[.]com
- atlascy[.]com
- atoz-co[.]com
- attintrade[.]com
- auctionsnicosia[.]com
- avatecgroup[.]com
- az-design[.]ir
- azarakhshavaco[.]com
- azdesignhome[.]com
- azdesignhome[.]ir
- azfreight[.]ir
- azpco[.]com
- bardiarezai[.]com
- bareqjam[.]com
- bitron[.]me
- bssco[.]ir
- c-moreestates[.]com
- cablehiran[.]ir
- cboline[.]com
- chabaharairlines[.]com
- chemicat[.]com
- chihtsai[.]info
- chnpos[.]xyz
- cmmm[.]ir
- cmstop[.]ir
- courier[.]ir

AceCryptorのIPホストを共用していた悪意あるドメイン名の例

- angelosavgousti[.]live
- atlascy[.]com
- drkhuffash[.]com
- granuleworld[.]net
- haminsepehr[.]com
- jonbesh2m[.]com
- moolianco[.]com