# A DNS Deep Dive into Malware Crypting

## Table of Contents



## Executive Report

Each time organizations shore up their network defenses, cybercriminals devise new and innovative ways to up the cyber attack ante. That's actually the rationale behind malware crypting—the process of making malicious programs, apps, and files appear harmless to anti-malware and intrusion detection solutions. And given the huge threat malware crypting could pose to even the most secure networks, many in the cybersecurity community are strongly recommending a clampdown on the actors and sites that offer them.

In an effort to make the Internet safer, WhoisXML API recently took a DNS dive deep to find connections to malware crypting. First, we expanded a list of eight domains identified as malware crypting indicators of compromise (IoCs) related to the threat. Second, we conducted research specific to AceCryptor, which has been dubbed as one of the most prolific crypters out in the market today.

Read on to know more about our findings, including:

- 786 domains that contained the same strings as those with IP connections to Krebs's IoC list, two of which have been classified as malicious by a bulk malware check tool
- Four dedicated and possibly dedicated IP addresses to which some AceCryptor IoCs resolved, two of which have been categorized as malicious by a bulk malware check tool
- 279 domains hosted on the dedicated AceCryptor IP addresses, 17 of which have been dubbed malicious by a bulk malware check tool

### Part 1: Behind the Malware Crypting IoCs

We began our in-depth analysis with a bulk WHOIS lookup for the IoCs Krebs identified, which led to the following discoveries:

- Two domains were registered with PDR Ltd. while Dynadot, REGRU-RU, RU-CENTER-RU, and SALENAMES-RU each managed one domain.
- A majority of the domains were aged, created between 2006 and 2022.
- Three of the domain names were registered in the U.S.
- The domains resolved to eight unique IP addresses, one of which (138[.]201[.]203[.]122) turned out to be a dedicated host based on a reverse IP lookup.

A bulk IP geolocation lookup for the host IP addresses, meanwhile, revealed that:

- A majority of the IP addresses, five to be exact, pointed to the U.S. as their origin. One IP address each pointed to Germany, the Netherlands, and Russia.
- Four out of the five U.S.-geolocated IP addresses were managed by Cloudflare, Inc. while the remaining one fell under Trellian's administration. The German, Dutch, and Russian IP addresses, meanwhile, were managed by Hetzner Online GmbH; Serverel, Inc.; and REG.RU, Ltd., respectively.

To further our investigation, we looked for DNS traces connected to the malware crypting-related IoCs.

A reverse IP lookup for the dedicated IP address led to the discovery of two connected domains that remained live to this day.

Next, we noticed the presence of two strings that could potentially point to malware crypting sites in two of the domains identified as IoCs—**mobile-soft** and **cryptor**. Domains & Subdomains Discovery searches for these uncovered 786 domains created since 1 January 2023, two of which were classified as malicious by a bulk malware check tool.

## Part 2: AceCryptor Findings

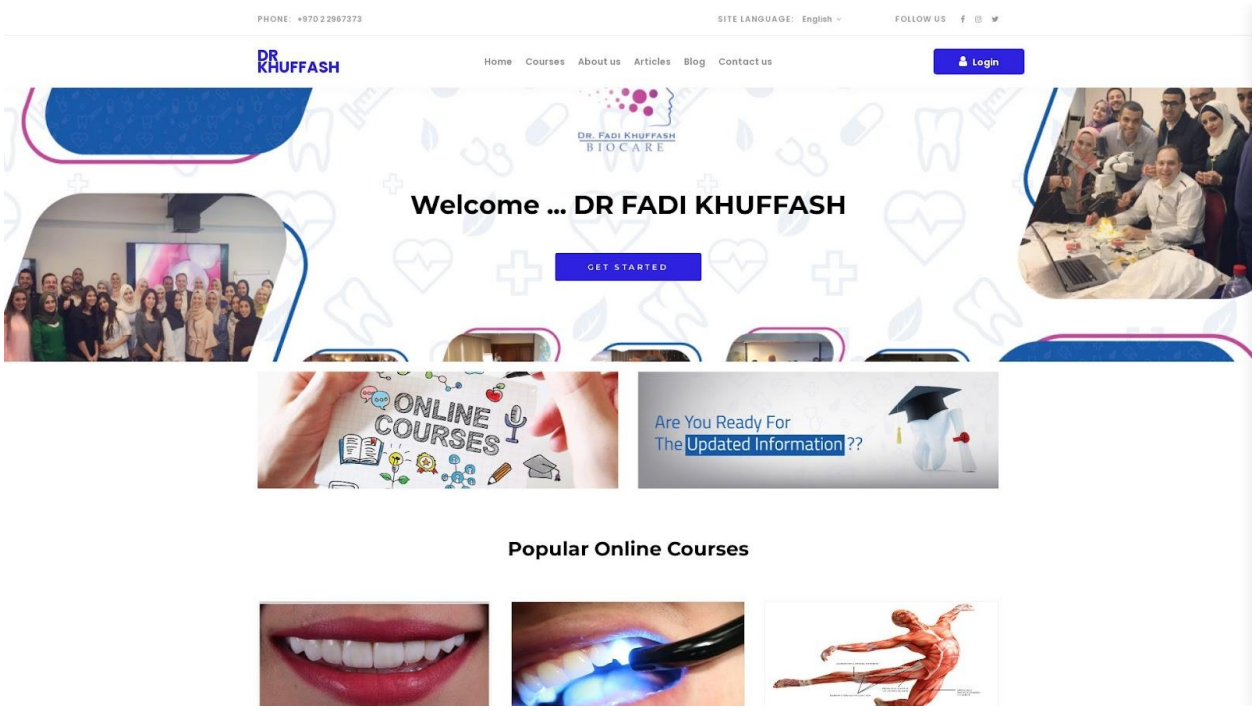
To gain more insights on what has been dubbed the top crypter today, we obtained a list of AceCryptor-related IoCs comprising seven domains and three IP addresses.

A bulk WHOIS lookup for the domains tagged as IoCs showed that only four had retrievable WHOIS records. Of these, two were registered with GoDaddy.com, LLC and one each with OnlineNIC, Inc. and Namecheap, Inc. All four were aged, having been created between 2005 and 2016 across four countries—two in the U.S. and one each in Afghanistan and Iceland.

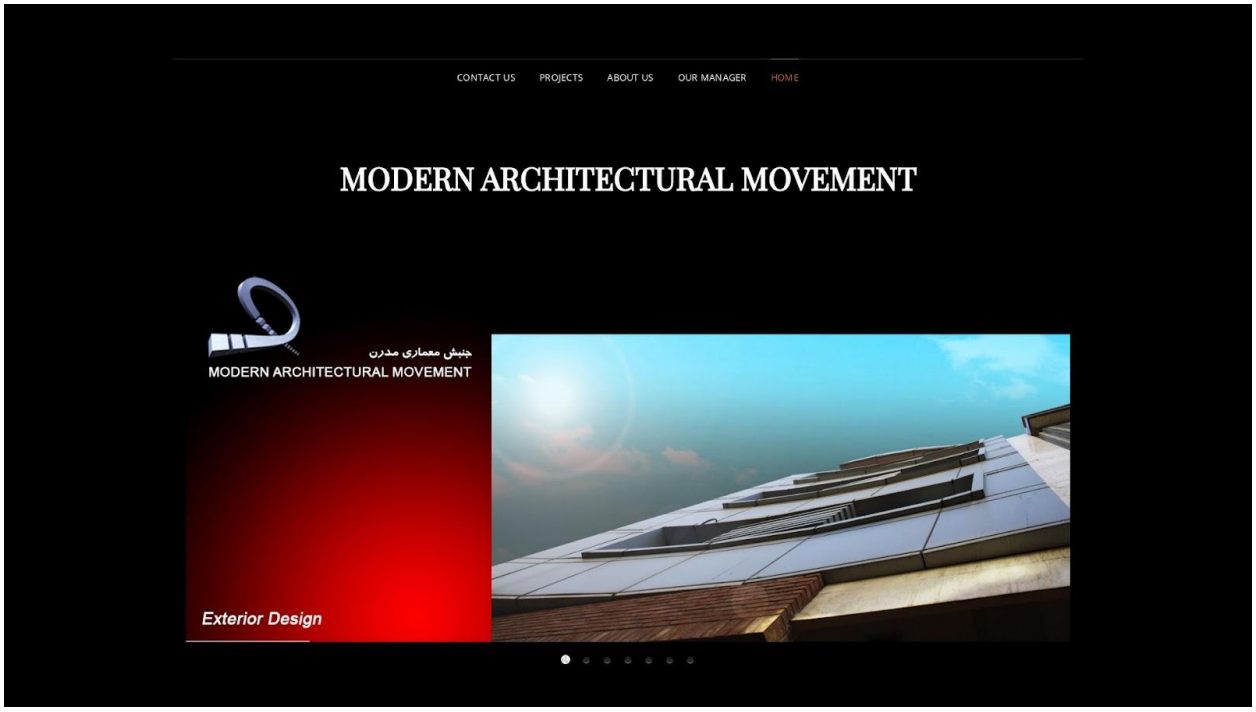
Next, we subjected the domains to DNS lookups that revealed they resolved to five unique IP addresses, none of which were included in the current list of AceCryptor IoCs. Reverse IP lookups for them showed that two of the IP addresses were dedicated and another two were

possibly dedicated. In addition, two of the IP hosts were categorized as malicious by a malware check tool.

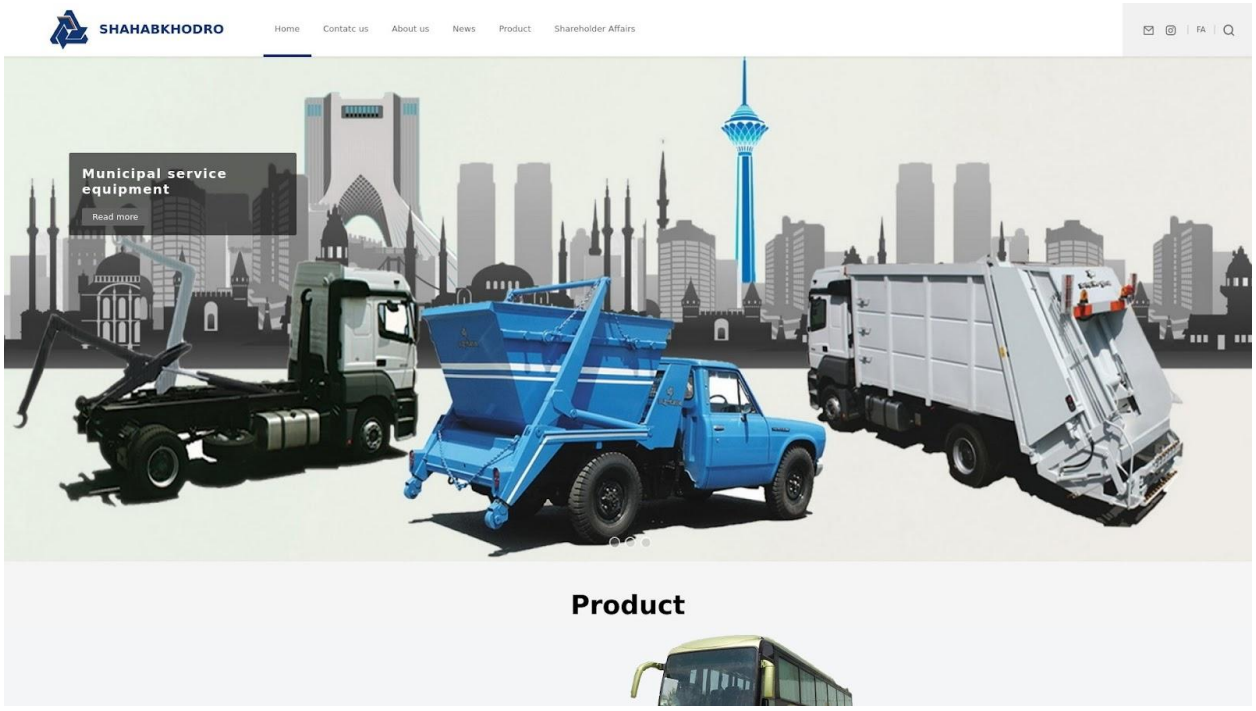
The reverse IP lookups also led to the discovery of 279 domains, 17 of which were deemed malicious by a malware check tool. In addition, 13 of them continued to host live content although none looked like malicious sites. Here are some examples.




*Screenshot of drkhuffash[.]com*




*Screenshot of jonbesh2m[.]com*




*Screenshot of shahabkhodro[.]co[.]ir*

—

We are bound to see more crypter-aided cyber attacks in the future, given the cloak of invisibility the solution provides to any malicious website.

Our latest DNS deep dive into general malware crypting services, for instance, uncovered 786 potentially connected artifacts while that for leading service AceCryptor led to the discovery of nearly 300 DNS-connected properties.

***If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.***

***Disclaimer:*** *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

# Appendix: Sample Artifacts and IoCs

## Malware Crypting IoCs

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

## Sample IoC IP Resolutions

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

## Sample Dedicated IP-Connected Domain

- modernlib[.]ru

## Sample String-Connected Domains

- 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

## Sample Malicious String-Connected Domain

- cryptoreach[.]space

## AceCryptor IoCs

- 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

## Sample AceCryptor IP Address Resolutions

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

## Sample Malicious AceCryptor IP Host

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

## Sample Domains That Shared the AceCryptor IP Hosts

- 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

## Sample Malicious AceCryptor IP-Connected Domains

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