ResumeLootersのさらなる兆候をDNSでチェック

目次

要旨

Group-IBは最近、求職者の個人情報を盗むことを専門とする脅威アクターグループ「ResumeLooters」を発見し、2024年2月にその詳細な脅威分析とともに15個のセキュリティ侵害インジケーター（7個のドメインIoC、3個のサブドメインIoCおよび5個のIPアドレスIoC）を公開しました。

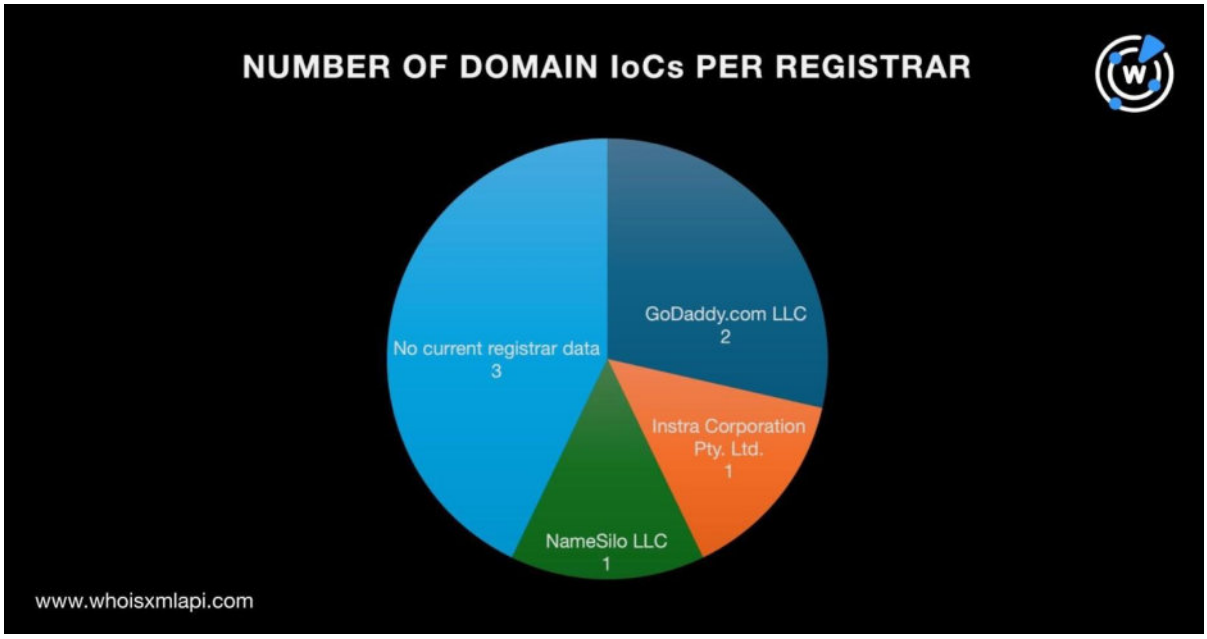
これを受け、WhoisXML APIの研究チームがこのほど、その15個のIoCを足がかりにDNSを詳細に調べ、ResumeLootersに関連する以下の潜在的攻撃ベクトルを新たに発見しました：

- ドメインIoCと同じ登録者によって登録されていたドメイン名302個
- ドメインIoCと同じメールアドレスを使用して登録されていたドメイン名69個
- 新たに検出されたIPアドレス6個。その全てが悪意あるIPアドレス
- IPアドレスIoCがホストしていたドメイン名3個
- ドメインIoCと同じ文字列を含むドメイン名573個。そのうち2個は悪意あるドメイン名

ResumeLootersのIoC

調査の第一歩として、WhoisXML APIはまず7個のドメインIoCを詳細に調べることにしました。7個のドメインIoCをキーにBulk WHOIS Lookup で検索したところ、以下が明らかになりました：

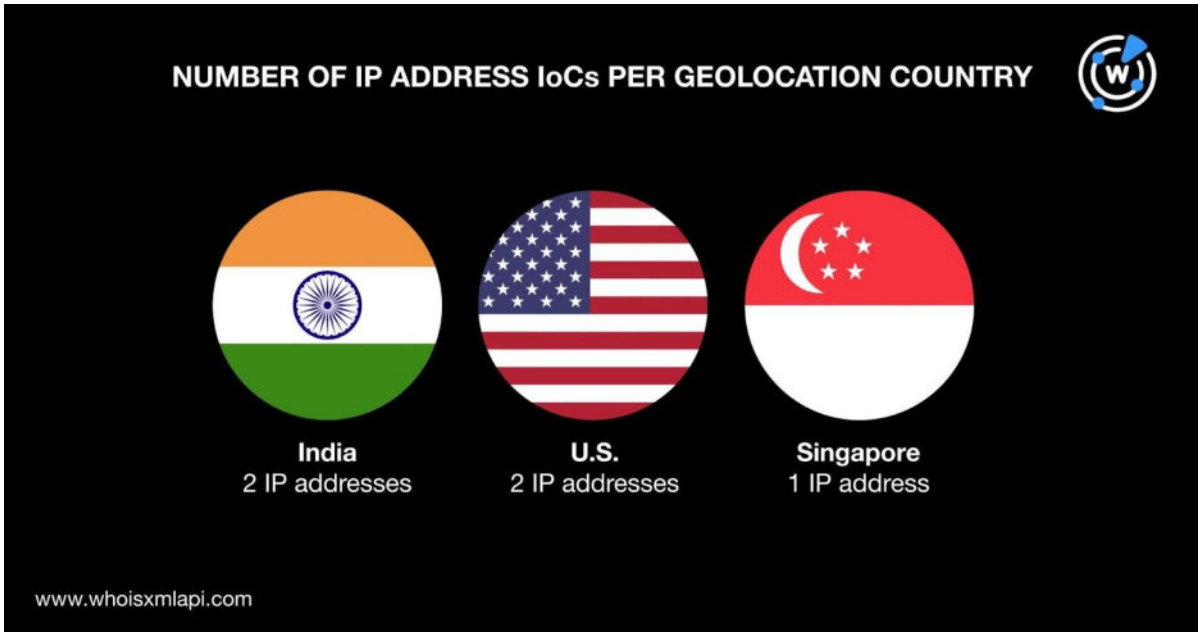
- 7個のドメインIoCを管理するレジストラは3社ありました。GoDaddy.com LLCが2個、Instra Corporation Pty. Ltd.とNameSilo LLCが1個ずつを管理していました。残り3個については、現在のWHOISレコードにレジストラのデータがありませんでした。



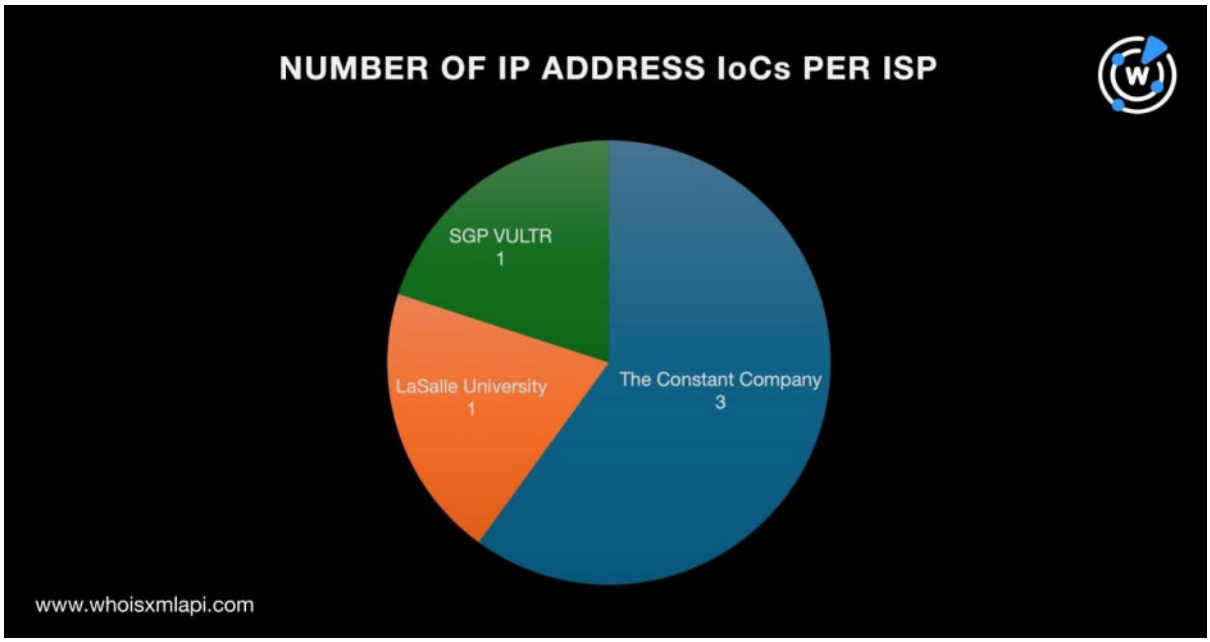
- 現在のWHOISレコードに登録年月日が記録されている3個のドメインIoCは、2023年に新規登録されたものでした。残り4個のドメイン名には、現在のWHOISレコードに登録年月日の情報がありませんでした。
- 現在のWHOISレコードに登録者の国のデータがある唯一のドメインIoCは、米国で登録されたものでした。
- 8t[.]aeというドメインIoCについては、登録者名と登録組織の情報が公開されていました。

5個のIPアドレスIoCに対してBulk IP Geolocation Lookupを実行したところ、次のことが判明しました：

- インドと米国を指すIPアドレスIoCが2個ずつありました。そして、残りの1個はシンガポールに位置していました。



- 5個のIPアドレスIoCを管理するISPは3社ありました。The Constant Companyが3個、LaSalle UniversityとSGP VULTRがそれぞれ1個を管理していました。



ResumeLootersのIoCリスト拡張分析

このセクションでは、ResumeLootersの潜在的な関連アーティファクトをどのように探し出したかを説明します。

前述のBulk WHOIS Lookupで、8t[.]aeというドメインIoCの登録者名と組織名が判明しました。そこで、その登録者名をキーワードにしてReverse WHOIS Searchを実行したところ、その登録者と関連性を持つドメイン名が302個見つかりました（重複と既存のIoCを除く）。また、Screenshot APIで調べた結果から、そのうち77個は本稿執筆時点でアクセス可能なままになっていたことがわかりました。

また、WHOIS History APIにより、7個のドメインIoCの過去のWHOISレコードから4個のメールアドレスを収集できました（重複を除く）。そのうち2個は公開されていたため、それらをReverse WHOIS APIにかけてみました。その結果、2つのメールアドレスのいずれかを使用していたドメイン名が69個特定されました（重複、IoCおよび登録者が同じドメイン名を除く）。69個のうち27個のドメイン名は、現在も有効なページをホストし続けています。

次に、7個のドメインIoCに対してDNS Lookupを実行したところ、新たに6個のIPアドレスに名前解決しました（重複と既存IoCを除く）。IPアドレスIoCのうち2個と同様に6個は全て米国に位置し、管理ISPはCloudflare, Inc.でした。また、6個は全て何らかの脅威と関連していました。具体的には以下の通りです：

- 6個全てがフィッシングに関連。
- 4個は「generic」な脅威に関連。
- 2個はマルウェア攻撃に関連。
- 2個は「suspicious」な活動に関連。

さらに、合計11個のIPアドレス（5個のIPアドレスIoCと新たに名前解決が判明した6個のIPアドレス）を使ってReverse IP Lookupを実行したところ、3個は専用アドレスらしいことがわかりました。そして、それらの専用アドレスがホストしているドメイン名が3個見つかりました（重複、IoC、登録者およびメールアドレスがドメインIoCと共通しているドメイン名を除く）。

この分析の締めくくりとして、Domains & Subdomains Discoveryを使い、7個のドメインIoCに含まれている文字列で始まるドメイン名を探しました。この検索により、573個のドメイン名が判明しました。そのうち8t[.]pmと8t[.]wfは、Threat Intelligence APIによるとマルウェア攻撃と関連していました。

DNSに他の就活サイト偽装の兆候はあるか

Group-IBは報告書の中で、ResumeLootersのサブドメインIoCも3個特定しました。そのうちの2個、すなわちrecruit[.]iimjobs[.]asiaとrecruiter[.]foundit[.]asiaは、合法的な就職活動サイトになりすましているようでした。

この2つのサイトをGoogleで検索したところ、正規の就活サイトのドメイン名はiimjobs[.]comとfoundit[.]inであることが判明しました。また、WHOIS Lookupの検索結果から、両者とも現在のWHOISで登録者組織のデータが公開されていることがわかりました。他方、iimjobs[.]asiaとfoundit[.]asiaを同じように検索しても、登録者組織の情報は出てきませんでした。iimjobs[.]asiaとfoundit[.]asiaをScreenshot Lookupにかけてみましたが、本稿執筆時点でどちらもアクセス不能でした。

ResumeLootersが自分達のキャンペーン用にiimjobs[.]asiaとfoundit[.]asiaを新規登録したとしたら、彼らや他のサイバー犯罪者は同じように他のドメイン名も登録しているのでしょうか？私たちはそれを突き止めるために、Domains & Subdomains Discoveryを使って調べました。

この調査の結果、**iimjobs.**を含むドメイン名8個、 **foundit.**を含むドメイン名が166個検出されました。

iimjobs.を含むドメイン名8個はいずれも脅威と無関係でしたが、WHOISで正規サイトのiimjobs[.]comの登録者組織に帰属していることが確認できたものは3個にとどまりました。

iimjobs.を含むドメイン名と同様、**foundit.**を含むドメイン名の中にも、悪意あるドメイン名と断定できるものはありませんでした。しかし、WHOIS情報を比較したところ、正規のfoundit[.]inの登録者組織に帰属していることが確認できたドメイン名は1個しかありませんでした。

—

今回行ったResumeLootersの分析により、953個の潜在的な関連ウェブプロパティ（ドメインIoCと同じ登録者によって登録されていたドメイン名302個、ドメインIoCと同じメールアドレスを使用して登録されていたドメイン名69個、新たに検出されたIPアドレス6個、IPアドレスIoCがホストしていたドメイン名3個、ドメインIoCと同じ文字列を含むドメイン名573個）が発見されました。また、そのうち8個は、フィッシング、マルウェア攻撃、genericな脅威、suspiciousな活動などに関連していました。

ResumeLootersが使用した2個のサブドメインを分析したところ、iimjobs[.]comとfoundit[.]inになりすました偽の就職活動サイトである可能性があることがわかりました。

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：アーティファクトの例

ドメインIoCと同じ登録者によって登録されていたドメイン名の例

- 36084[.]wang
- 3sumz[.]com
- 51bisai[.]com
- 51xifu[.]net
- aacgroup[.]com[.]au
- aboveevent[.]com
- abovevent[.]com
- acmoney[.]com[.]au
- adjusted-book-value[.]com
- adjusted-earnings[.]com
- adorningembellishments[.]com
- afmg[.]com[.]au
- aipa20[.]com
- airhotsale[.]com
- airtelchampionsleague[.]com
- algrealestate[.]com[.]au
- allofhalf[.]com
- alorabeautystudio[.]com[.]au
- americas-goods[.]com
- amsterdambyfood[.]com
- amsterdamchinatown[.]com
- annuo-leather[.]com
- antaiengineering[.]com
- aoborealty[.]com[.]au
- asianaac[.]com
- asianaac[.]org
- asiancuisinenorman[.]com
- asset-approach[.]com
- asset-sale[.]com
- aussie-home[.]com[.]au
- australianunityparty[.]com[.]au
- bambusplatten[.]com
- base-year[.]com
- beautybridaldress[.]com
- bjdmty[.]com
- bodyorbust[.]com
- boyalife[.]com
- bsfgtj[.]net
- burstratecreative[.]com
- buying-american-real-estate[.]com
- c60changshou[.]com
- caiche-printing[.]com
- camedia[.]com[.]au
- canadian2for1pizza[.]com
- cannatonicstrain[.]com
- cannyowldesigns[.]com
- charterlicensing[.]com
- chaunisthebomb[.]com
- cheapbestbags[.]com
- cheapbestbags[.]net

ドメインIoCと同じメールアドレスを使って登録されていたドメイン名の例

- 1533[.]one
- 1663[.]online

- 18girl[.]sex
- 3155[.]one
- 3338[.]com[.]cn
- 3522[.]online
- 6122[.]online
- 68008[.]net
- 7258[.]online
- 7268[.]online
- 9077[.]com[.]cn
- agelocgamma[.]org
- cunhua[.]cn
- cunshe[.]cn
- dblw[.]com[.]cn
- diaogui[.]cn
- dqd[.]one
- fjf[.]one
- fkf[.]one
- fwf[.]one

新たに検出されたIPアドレスの例

- 104[.]21[.]71[.]172
- 104[.]21[.]75[.]250
- 104[.]21[.]9[.]29

IPアドレスIoCによってホストされていたドメイン名の例

- cloudnetsofe[.]com
- futurexah[.]life

ドメインIoCと同じ文字列を含むドメイン名の例

- 3x1[.]ai
- 3x1[.]app
- 3x1[.]aquila[.]it
- 3x1[.]at
- 3x1[.]biz
- 3x1[.]ca
- 3x1[.]cc
- 3x1[.]ch
- 3x1[.]cl
- 3x1[.]club
- 3x1[.]cn
- 3x1[.]co
- 3x1[.]co[.]uk
- 3x1[.]com
- 3x1[.]com[.]br
- 3x1[.]com[.]cn
- 3x1[.]de
- 3x1[.]es
- 3x1[.]eu
- 3x1[.]gratis
- 3x1[.]hu
- 3x1[.]immobilien
- 3x1[.]in
- 3x1[.]info
- 3x1[.]io
- 3x1[.]ir
- 3x1[.]it
- 3x1[.]lat
- 3x1[.]link
- 3x1[.]mil[.]ph
- 3x1[.]net
- 3x1[.]net[.]ph
- 3x1[.]ngo[.]ph
- 3x1[.]nl
- 3x1[.]nyc
- 3x1[.]one
- 3x1[.]online
- 3x1[.]org
- 3x1[.]org[.]ph
- 3x1[.]pizza

- 3x1[.]pl
- 3x1[.]ro
- 3x1[.]ru
- 3x1[.]site
- 3x1[.]tk
- 3x1[.]top
- 3x1[.]uk
- 3x1[.]us
- 3x1[.]uz
- 3x1[.]wang
- 3x1[.]xin
- 3x1[.]xn--kprw13d
- 3x1[.]xn--node
- 3x1[.]xyz
- 3x1[.]zone
- 7o[.]africa
- 7o[.]ai
- 7o[.]am
- 7o[.]at
- 7o[.]au
- 7o[.]audio
- 7o[.]be
- 7o[.]beauty
- 7o[.]beer
- 7o[.]blackfriday
- 7o[.]boats
- 7o[.]ca
- 7o[.]casa
- 7o[.]casino
- 7o[.]cc
- 7o[.]charity
- 7o[.]christmas
- 7o[.]ci
- 7o[.]click
- 7o[.]club
- 7o[.]cm
- 7o[.]cn
- 7o[.]co
- 7o[.]co[.]uk
- 7o[.]co[.]za
- 7o[.]com
- 7o[.]com[.]au
- 7o[.]com[.]br
- 7o[.]com[.]cn
- 7o[.]com[.]tw
- 7o[.]com[.]ws
- 7o[.]country
- 7o[.]cx
- 7o[.]cz
- 7o[.]de
- 7o[.]diet
- 7o[.]dk
- 7o[.]edu[.]ws
- 7o[.]ee
- 7o[.]eu
- 7o[.]feedback
- 7o[.]fi
- 7o[.]fit
- 7o[.]flowers
- 7o[.]football

iimjobs.を含むドメイン名の例

- iimjobs[.]jobs
- iimjobs[.]xyz
- iimjobs[.]org
- iimjobs[.]net

foundit.を含むドメイン名の例

- foundit[.]fun
- foundit[.]loans
- foundit[.]com[.]hk
- foundit[.]homes
- foundit[.]top
- foundit[.]tech

- foundit[.]digital
- foundit[.]ai
- foundit[.]ga
- foundit[.]market
- foundit[.]ir
- foundit[.]dk
- foundit[.]marketing
- foundit[.]com[.]ph
- foundit[.]pro
- foundit[.]info
- foundit[.]fit
- foundit[.]company
- foundit[.]page
- foundit[.]co[.]zm
- foundit[.]co[.]za
- foundit[.]com[.]my
- foundit[.]education
- foundit[.]com[.]tw
- foundit[.]jobs
- foundit[.]io
- foundit[.]space
- foundit[.]london
- foundit[.]technology
- foundit[.]name
- foundit[.]insure
- foundit[.]cool
- foundit[.]repair
- foundit[.]click
- foundit[.]uk
- foundit[.]online
- foundit[.]construction
- foundit[.]vlaanderen
- foundit[.]com[.]au
- foundit[.]nu
- foundit[.]ventures
- foundit[.]kiwi
- foundit[.]net
- foundit[.]app
- foundit[.]systems
- foundit[.]forsale
- foundit[.]nyc
- foundit[.]eco
- foundit[.]me