PikBotのインフラをDNSで分析

目次

要旨

最近では、悪意ある検索広告を使ってマルウェアを配布する脅威は珍しくなくなりました。ただ、そのような行為を実行するためには、おとりのインフラを設置してGoogleのセキュリティ対策を迂回する方法を知っている必要があります。

そのようなマルウェアの一つであるPikaBotは、2023年初頭にその名前を知られるようになりました。先般、Malwarebytes Labsの研究者がこの脅威の詳細な分析を行い、11個のセキュリティ侵害インジケーター（IoC）（2個のドメイン名と9個のIPアドレス）を公開しました。

インターネットをより安全で透明性の高いものにするというミッションのもと、WhoisXML APIがこのたび、上記のIoCリストをもとにDNSで調査を行い、関連している可能性のある数百にのぼるアーティファクトを新たに発見しました：

- ドメインIoCと同じメールアドレスを使用していたドメイン名112個
- 一部のドメインIoCが名前解決したIPアドレス3個。そのうち2個は悪意あるアドレス。
- 上記のIPアドレスまたはIPアドレスIoCと同じIPアドレスを共用していたドメイン名210個。そのうち3個は悪意あるドメイン名と確認。
- ドメインIoCと同じ文字列を含むドメイン名14個。

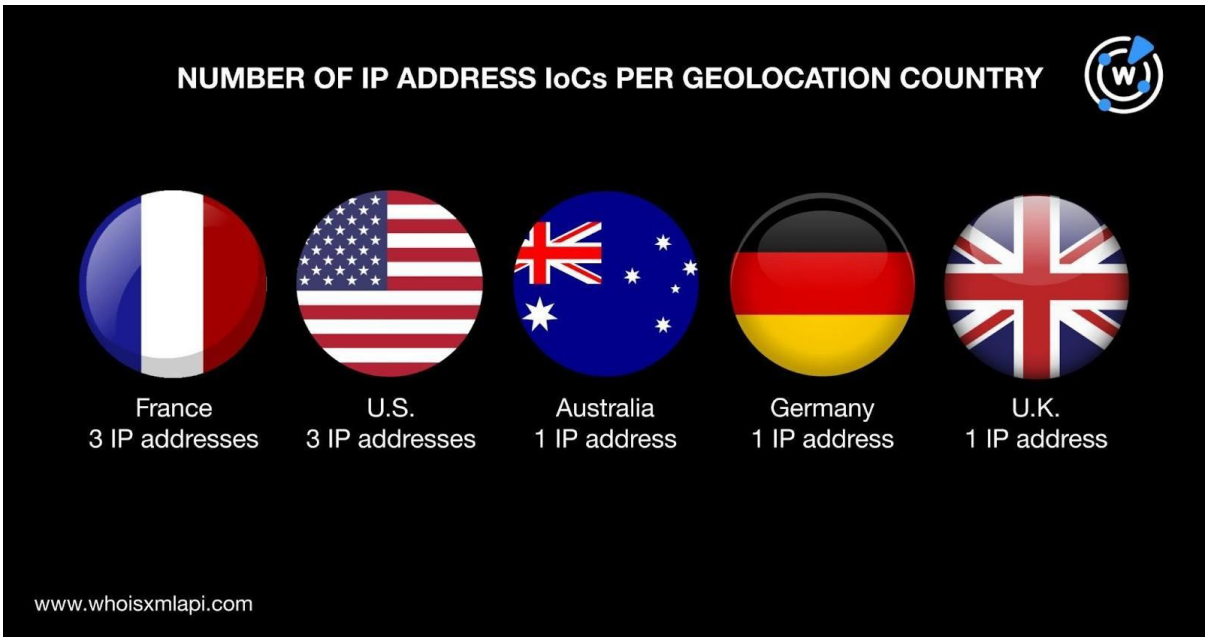
PikaBotのIoC

まず、IoCと特定された2個のドメイン名（以下「ドメインIoC」）をWHOIS Lookupを使って調べたところ、次のことがわかりました：

- cxtensones[.]topの管理レジストラはNiceNIC International Group Co. Ltd.、ovmv[.]netの管理レジストラはHosting Concepts B.V.。
- 両ドメインは2023年12月に作成され、攻撃に使用された時点では新規登録ドメイン名。
- cxtensones[.]topは米国、ovmv[.]netはオランダで登録。

次に、IoCと特定された9個のIPアドレス（以下「IPアドレスIoC」）をBulk IP Geolocation Lookupにかけたところ、以下が判明しました：

- ジオロケーションは米国とフランスに3個ずつ。オーストラリア、ドイツ、英国に1個ずつ位置。



- 6個の管理ISPはOVH、3個はAkamai Technologies, Inc.。

9個のIPアドレスIoCをキーにThreat Intelligence APIで検索したところ、下表の興味深い事実が明らかになりました：

IoC	関連する脅威の数	関連する 脅威の種類	初見日
139[.]99[.]222[.]29	1	Malware	2023年12月15日
172[.]232[.]162[.]198	4	Attack Botnet C2 Malware	2023年12月14日
172[.]232[.]164[.]77	4	Attack	2023年12月13日

		Botnet C2 Malware	
172[.]232[.]186[.]251	4	Attack Botnet C2 Malware	2023年12月14日
54[.]37[.]79[.]82	4	Attack Botnet C2 Malware	2023年12月15日
57[.]128[.]108[.]132	4	Attack Botnet C2 Malware	2023年12月14日
57[.]128[.]109[.]221	4	Attack Botnet C2 Malware	2023年12月15日
57[.]128[.]164[.]11	4	Attack Botnet C2 Malware	2023年12月14日
57[.]128[.]83[.]129	4	Attack Botnet C2 Malware	2023年12月14日

PikaBotキャンペーンの裏側

2個のドメインIoCに対してWHOIS History Lookupを実行した結果、そのうち1個（ovmv[.]net）の過去のWHOISレコードに4個のメールアドレスの存在が確認されました。また、そのうち3個は公開されていました。

3個の公開メールアドレスのうち2個を検索語としてReverse WHOIS APIで検索し、結果から重複とIoCを取り除いたところ、紐付けられているドメイン名112個が確認されました。112個のほぼ全ては中国語のような文字列またはランダムな数字の組み合わせで構成されたドメイン名です。以下に例を示します：

- 1869666[.]net
- 240690[.]com
- 242302[.]com
- 354374[.]com
- 375324[.]com
- dalianchu[.]com
- didichihuo[.]com
- duolianchu[.]com
- fulianchu[.]com
- hangtianyun[.]com

次に、2個のドメインIoCに対してDNS Lookupを実行したところ、元のIoCリストに含まれていない3個のIPアドレスに名前解決しました。

その3個のIPアドレスの位置をIP Geolocation Lookupで調べた結果、以下が判明しました：

- ブラジル、スイス、米国に1個ずつ位置。
- Threat Intelligence APIエンジンで分析したところ、2個（104[.]21[.]72[.]66と172[.]67[.]176[.]15）はさまざまな脅威と関連づけられました。また、2023年5月23日から今日までの間に、両方のアドレスに「Phishing」や「Generic」といった脅威のフラグが立てられていました。

これまでに特定された合計12個のIPアドレス（9個のIPアドレスIoCと上記のDNS Lookupで判明した3個のIPアドレス）をReverse IP Lookupで調べた結果、そのうち3個は専用ホストらしいことがわかりました。それらは元のIoCリストに含まれておらず、IoCと同じメールアドレスを使っているわけでもない210個にのぼる全く別のドメイン名をホストしていました。

それらをThreat Intelligence APIで検索したところ、3個のドメイン名（fakty-info[.]com、twinsources[.]shop、txid-coinbase[.]net）がさまざまな脅威と関連していることがわかりました。詳細は下表の通りです。

専用ホストらしいIPアドレスを使っていたドメイン名	関連する脅威の数	関連する脅威の種類
fakty-info[.]com	2	Phishing Generic
twinsources[.]shop	1	Malware
txid-coinbase[.]net	1	Phishing

次に、共通の単語を文字列として含んでいるドメイン名を探すことにしました。当社のDomains & Subdomains Discoveryツールで**Starts with** パラメータを使い、**ovmv**という文字列を含むドメイン名を検索しました。その結果、**ovmv**を含む14個のドメイン名が検出されました。それらはいずれも、トップレベルドメイン（TLD）部分を除けばovmv[.]netというドメインIoCと全く同じでした。

しかし、WHOISでドメインIoCのovmv[.]netと上記の検索で見つかった14個のドメイン名を比較したところ、共通点はなさそうでした。

—

今回、PikaBotのインフラをDNSで徹底調査した結果、関連が疑われるアーティファクトを339個（IoCと同じメールアドレスを使用していたドメイン名112個、追加で判明したIPアドレス3個、追加で判明したIPアドレスまたはIPアドレスIoCを共用していたドメイン名210個、IoCと同じ文字列を含むドメイン名14個）特定することができました。また、分析の結果、2個のIPアドレス（104[.]21[.]72[.]66、172[.]67[.]176[.]15）および3個のドメイン名（fakty-info[.]com、twinsources[.]shop、txid-coinbase[.]net）からなる合計5個の悪意あるウェブプロパティが明らかになりました。

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：アーティファクトとIoCの例

PikaBotのIoC

ドメインIoC	IPアドレスIoC
• cxtensones[.]top • ovmv[.]net	• 139[.]99[.]222[.]29 • 172[.]232[.]162[.]198 • 172[.]232[.]164[.]77 • 172[.]232[.]186[.]251 • 54[.]37[.]79[.]82 • 57[.]128[.]108[.]132 • 57[.]128[.]109[.]221 • 57[.]128[.]164[.]11 • 57[.]128[.]83[.]129

ドメインIoCと同じメールアドレスを使用していたドメイン名の例

- 1869666[.]net
- 240690[.]com

- 242302[.]com
- 354374[.]com
- 375324[.]com
- 375714[.]com
- 375974[.]com
- 376294[.]com
- 531773[.]wang
- 531775[.]wang
- 531776[.]wang
- 547276[.]com
- 547296[.]com
- 547376[.]com
- 547926[.]com
- 643185[.]com
- 643191[.]com
- 643193[.]com
- 643252[.]com
- 643257[.]com
- 645276[.]com
- 647916[.]com
- 714903[.]com
- 721504[.]com
- 725179[.]net
- 725181[.]net
- 725183[.]net
- 725186[.]net
- 725187[.]net
- 725381[.]net
- 725382[.]net
- 725385[.]net
- 725781[.]net
- 725783[.]net
- 725785[.]net
- 725787[.]net
- 725813[.]net
- 725815[.]net
- 725816[.]net
- 725817[.]net
- 725819[.]net
- 725821[.]net
- 725904[.]com
- 725935[.]net
- 725937[.]net
- 725939[.]net
- 725951[.]net
- 729054[.]com
- 729074[.]com
- 729104[.]com

追加で名前解決が判明したIPアドレスの例

- 104[.]21[.]72[.]66
- 172[.]67[.]176[.]15

追加で判明したIPアドレスまたはIPアドレスIoCを共用していたドメイン名の例

- 0212top[.]xyz
- 0ccctt[.]com
- 0zzccc[.]com
- 0zzmmm[.]com
- 0zzzjj[.]com
- 1009451[.]com
- 1cccss[.]com
- 1inchapp[.]com
- 2zzppp[.]com
- 2zzyyy[.]com
- 3aaann[.]com
- 3cccjj[.]com
- 3cccww[.]com
- 3ddduu[.]com
- 3zzzgg[.]com
- 3zzzll[.]com
- 4bbbqq[.]com
- 4dddoo[.]com
- 4dddrr[.]com
- 4zzkkk[.]com

- 4zzzee[.]com
- 6aaahh[.]com
- 6aaazz[.]com
- 7bbbvv[.]com
- 7dddxx[.]com
- 8aaaww[.]com
- 8h01[.]com
- 8qqqaa[.]com
- 8zzlll[.]com
- 9aaaxx[.]com
- 9bbbxx[.]com
- 9cccjj[.]com
- aaaww3[.]com
- abcash[.]co[.]uk
- argentina-changelife[.]com
- argentina-com[.]com
- argentina-job[.]com
- argentina-new[.]com
- arkhamprotocol[.]com
- avanzar-dream[.]com
- badkushmmo[.]com
- bankingston[.]com
- bbusjy[.]com
- binanselendas[.]com
- blessedtent[.]com
- boldcryptos[.]online
- bonusblackemdobro[.]com
- canadasignin[.]com
- cashbackcongrat[.]com
- chile-changelife[.]com

ドメインIoCと同じ文字列を含むドメイン名の例

- ovmv[.]be
- ovmv[.]cn
- ovmv[.]com
- ovmv[.]cz
- ovmv[.]dk
- ovmv[.]eu
- ovmv[.]link