Atomic Stealerのインフラの裏側に迫る

目次

要旨

「AMOS」とも呼ばれるAtomic Stealerが初めて人々の知るところとなったのは2023年9月で、その時は人気のアプリケーションを装ってMac上で拡散しました。今回は、「ClearFake」と呼ばれる偽ブラウザアップデートで、さらに大混乱を引き起こしています。Atomic Stealerの運用者は、被害者の裾野を広げるために複数のウェブサイトを侵害し、不正な利益を得てきました。

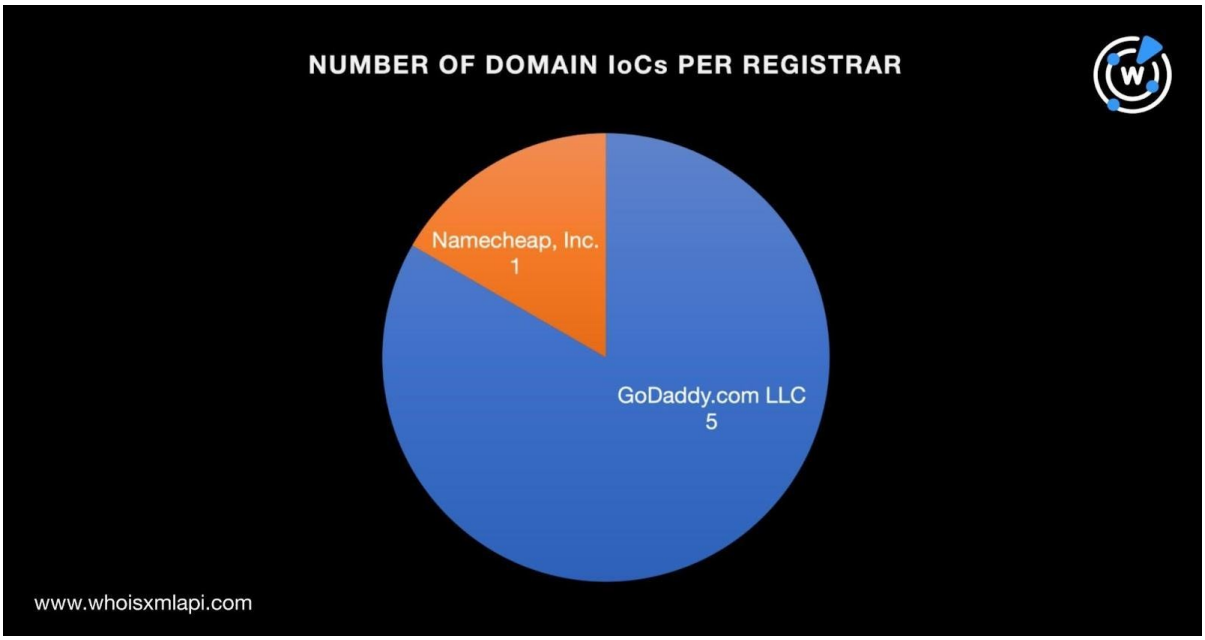
Malwarebytes Labsは今年11月初め、Atomic Stealerのセキュリティ侵害インジケーター（IoC）のリスト（ドメイン名6個とIPアドレス1個）と詳細なマルウェア分析を公開しました。WhoisXML APIでは、Atomic Stealerについてより多くの情報を収集して未公開の潜在的脅威ベクトルを特定するため、Malwarebytes LabsのIoCリストを出発点としてDNSを詳細に調査しました。その結果、以下が検出されました：

- IoCとして特定されたドメイン名の過去のWHOISレコードで見つかったメールアドレスを共用していたドメイン名31個
- IoCと特定されたドメイン名が名前解決したIPアドレス7個
- IoCと特定されたドメイン名と共通の文字列を含むドメイン名12個
- IoCと特定されたドメイン名と共通の文字列を含むサブドメイン14個

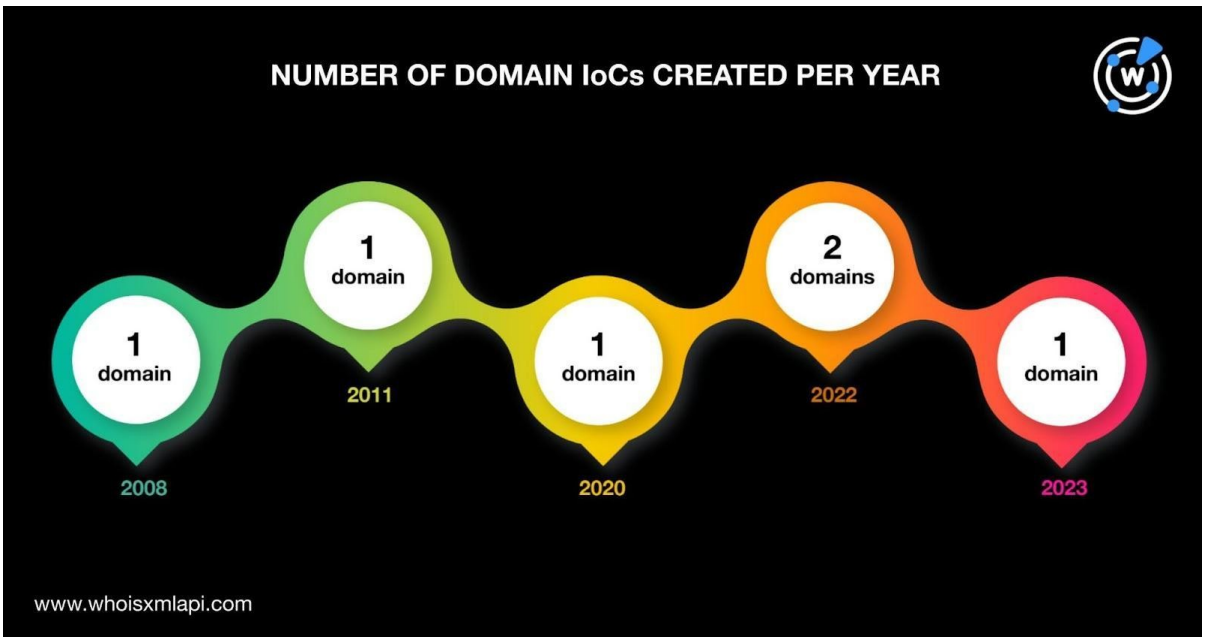
Atomic Stealer IoCのDNSにおける実態

まず、IoCとして特定されたドメイン名（以下「ドメインIoC」）6個をBulk WHOIS Lookupで検索したところ、以下が判明しました：

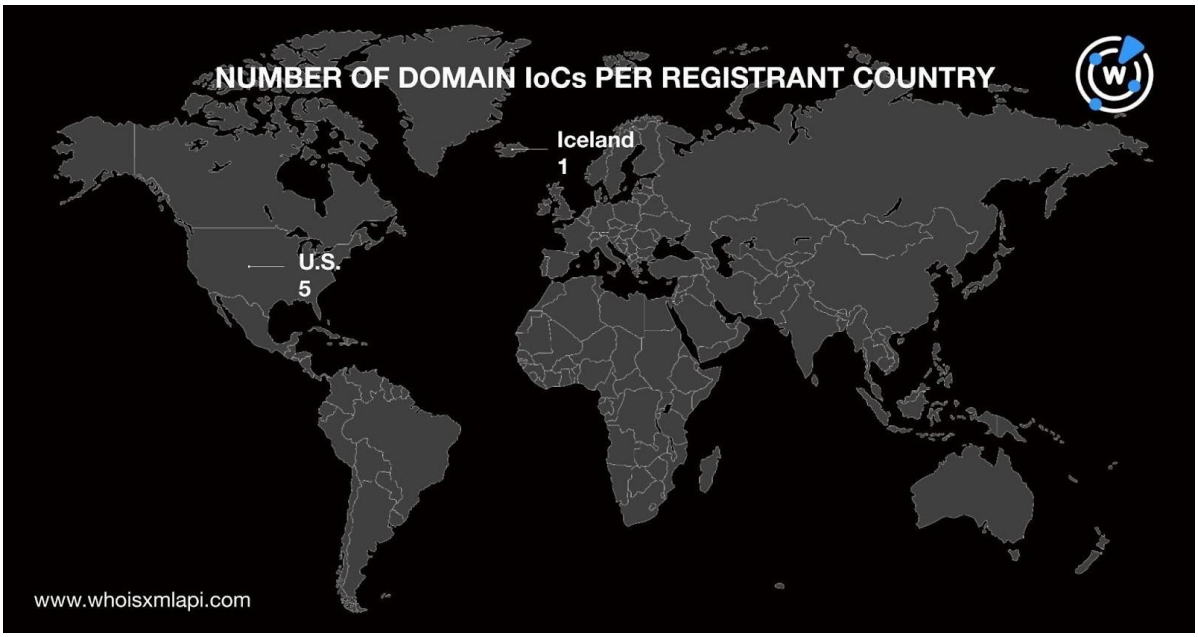
- 5個のレジストラはGoDaddy.com LLC、残り1個のレジストラはNamecheap, Inc.でした。



- 6個のドメインIoCは2008年から2023年までの間に新規登録されていました。内訳は次の通りです： 2022年（2個）、2008年（1個）、2011年（1個）、2020年（1個）、2023年（1個）。



- 5個の登録者が所在している国は米国で、残り1個はアイスランドでした。



次に、IoCとして特定されたIPアドレス（以下「IPアドレスIoC」）1個についてIP Geolocation Lookupを実行したところ、以下のことがわかりました：

- ジオロケーションはベルギー。管理ISPはMatrix Telecom Ltd。
- Threat Intelligence Lookupで調べた結果、203件の脅威と関連している、などの追加情報が得られました。

DNS徹底調査の結果

Atomic StealerのIoCリストを拡張するため、まず6個のドメインIoCをWHOIS History Searchで検索しました。その結果、それらのドメイン名の過去のWHOISレコードに表示されていた15個のメールアドレスが見つかりました。

そのうち7個の公開メールアドレスをキーワードとしてReverse WHOIS Searchを実行し、結果から重複とIoCを取り除いたところ、4個のメールアドレスが、ドメイン名31個の現在のWHOISレコードに表示されました。

その31個のドメイン名を詳しく調べた結果、下表に示す通り、9個のドメイン名がカナダの3つの組織（Costco Wholesale Canada、Royal Bank of Canada、Scotiabank Canada）を模倣している可能性があることがわかりました。

共通のメールアドレスを使用していたドメイン名	模倣されている可能性がある組織
canada-costco-redeem2percent[.]com	Costco Wholesale Canada
rbctrustroyalcanada[.]com trustclientrbc[.]com	Royal Bank of Canada
canadascotia-sign-intrust[.]com scotiabank-sign-in[.]com scotiacatrust[.]com scotiaonline-client[.]com scotiatrustweb[.]com sign-intrust-scotiaonline[.]com	Scotiabank Canada

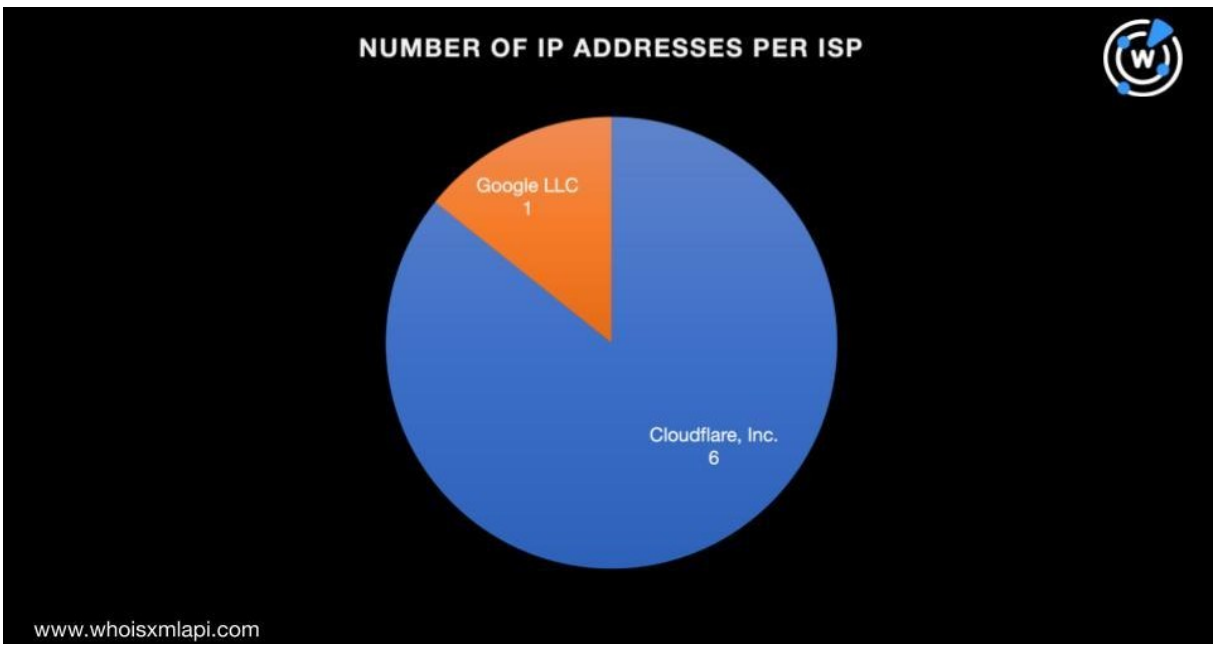
3つの組織のWHOISレコードには、身元を照合できる情報が含まれていました。Costco WholesaleとRoyal Bank of Canadaの公式ドメイン名（それぞれcostco[.]caとrbcroyalbank[.]com）のWHOIS Lookupにより、登録者のメールアドレスがわかりました。また、Scotiabank Canadaの公式ドメイン名（scotiabank[.]com）のWHOIS Lookupから、登録者組織名を確認できました。

その一方で、共通のメールアドレスを使用していた9個のドメイン名のWHOISレコードにはそのような情報が含まれておらず、いずれもレコードが非公開化されていました。これらは正規の企業に帰属するドメイン名であることが確認できないため、タイポスクワッティングドメイン名かもしれません。

次に、6個のドメインIoCをDNS Lookupにかけたところ、7個のユニークなIPアドレスに名前解決しました。それらのIPアドレスをBulk IP Geolocation Lookupで調べた結果、以下が判明しました：

- 全てのIPアドレスは米国を指しているようでした。

- 6個のIPアドレスの管理ISPはCloudflare, Inc.で、1個はGoogle LLCによって管理されていました。



- WhoisXML APIのThreat Intelligence Lookupを使った検索により、6個は様々な脅威と関連していることが判明しました。以下の表の通りです。

IPアドレス	THREAT INTELLIGENCE LOOKUP の結果
104[.]21[.]43[.]174	8,149の脅威に関連
104[.]21[.]49[.]159	8,171の脅威に関連
104[.]21[.]30[.]25	8,176の脅威に関連
172[.]67[.]182[.]141	8,271の脅威に関連
172[.]67[.]147[.]71	8,195の脅威に関連
172[.]67[.]150[.]110	8,196の脅威に関連

- 7個のIPアドレスのうち、所在国や管理ISPがIoCのそれと共通しているものはありませんでした。

特定済みのIPアドレスIoC 1個に上記の7個を加え、Atomic Stealerに関連するIPアドレスは合計8個となりました。当社の調査により、7個のIPアドレスは共用ホストらしいことがわかりました。また、1個は名前解決しませんでした。

過去10年ほどの間に登録された関連プロパティを洗い出す最終ステップとして、6個のドメインIoCに見られるテキスト文字列を含む他のドメイン名とサブドメインをDomains & Subdomains Discoveryで探しました。その結果、下表の通り17個のドメイン名と14個のサブドメインが見つかりました。

ドメインIoCに見られるテキスト文字列	DOMAINS & SUBDOMAINS DISCOVERYでヒットしたドメイン名の数	DOMAINS & SUBDOMAINS DISCOVERYでヒットしたサブドメインの数
thebestthings1337	1	0
chalomannoakhali	1	0
jaminzaidad	4	2
royaltrustrbc	2	0
wifi-ber	9	12

重複、ドメインIoC、共通のメールアドレスまたはIPアドレスを使用していたドメイン名を取り除いた後、共通の文字列を含むドメイン名12個、共通の文字列を含むサブドメイン14個が残りました。

そのうち1個のドメイン名（royaltrustrbc[.]online）は、Royal Bank of Canadaをサイバースクワッティングしている可能性があります。先に見つけたタイポスクワッティングらしいドメイン名と同様に、royaltrustrbc[.]onlineはRoyal Bank of Canadaへの帰属を公開のWHOIS情報から確認できませんでした。このドメイン名のWHOISレコードに、同銀行の登録者メールアドレスは記載されていませんでした。

—

今回WhiosXML APIがAtomic Stealerのインフラを調査した結果、他のレポートで特定されていない64個の関連アーティファクトが新たに発見されました。その中には、Costco Wholesale Canada、Royal Bank of Canada、Scotiabank Canadaを標的としたフィッシングキャンペーンの攻撃ベクトルとなり得るドメイン名が含まれています。

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

Malwarebytes Labsが特定したAtomic StealerのIoC

ドメイン名	IPアドレス
• longlakeweb[.]com • thebestthings1337[.]online • chalomannoakhali[.]com • jaminzaidad[.]com • royaltrustrbc[.]com • wifi-ber[.]com	• 194[.]169[.]175[.]117

共通のメールアドレスを使用していたドメイン名の例

- accept-ca-interac[.]com
- antarshowbiz[.]com
- bc-hydrotrust[.]com
- bcelectricitytrust[.]com
- bonochhayabd[.]com
- canada-costco-redeem2percent[.]com
- canadascotia-sign-intrust[.]com

- communicatorbd[.]com
- comvalitsolutions[.]com
- cra-interac-mobil[.]com
- deshi[.]fr
- deshihost[.]net
- globalsurrogacyconsultancy[.]com
- interactrustweb[.]com
- irc-bd[.]com
- localmobileshops[.]com

IPアドレスの例

- 104[.]21[.]43[.]174
- 34[.]98[.]99[.]30
- 104[.]21[.]49[.]159

共通の文字列を含むドメイン名の例

- free-wifi-berlin[.]de
- jaminzaidad[.]in
- jaminzaidad[.]online
- open-wifi-berlin[.]de
- ricjaminzaidad[.]com
- royaltrustrbc[.]online

共通の文字列を含むサブドメインの例

- 3623-privatapartment-wifi-bernhard-jordens-weg[.]gravelytravel[.]com
- 5809-privatapartment-wifi-berliner-strasse[.]gravelytravel[.]com
- almikez-iphone-wifi-bernhard[.]h6[.]xiaoeknow[.]com
- jaminzaidad[.]allexamonline[.]com
- mail[.]wifi-bersama[.]mikkcloud[.]my[.]id
- wifi-beroun-ded[.]bluetone[.]cz
- wifi-bersama[.]mikkcloud[.]my[.]id