MuddyWaterの進展の兆しをDNSで発見

目次

要旨

ハッカー集団「MuddyWater」または「Mercury」による最初の大規模なキャンペーンが行われたのは、2012年のことでした。しかし、サイバーセキュリティの領域では常にそうであるように、脅威グループ、特に悪名を馳せる脅威グループは、時と共に現れては消えるというものではありません。

MuddyWaterの場合は、消え去るどころか毎回より大規模・巧妙になって戻ってきます。その顕著な例はMuddyWaterの最新フレームワークであるPhonyC2です。Deep Instinctが最近、このPhonyC2に関する詳細な調査結果を発表しました。

WhoisXML APIはこのたび、Deep Instinctが公表したPhonyC2のIoC（27個のIPアドレスと12個のドメイン名）を出発点として、DNSデータを徹底的に調査しました。その結果、以下のアーティファクトを新たに発見しました。

- IoCとして特定された一部のドメイン名が名前解決する3個のユニークなIPアドレス
- IoCとされたドメイン名と同じ専用IPアドレスを共用する3個のドメイン名
- IoCとされたドメイン名と同じ文字列を含む152個のドメイン名
- IoCとして特定されたIPアドレスを使うドメイン名と同じ文字列を含む22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により悪意あるドメイン名と確認

また、最近のランサムウェアキャンペーンを掘り下げるため、攻撃へのMuddyWaterの関与をDEV-1084が隠すという、MuddyWater・DEV-1084間の協力関係を分析しました。ここではMicrosoftが公開した14個のIoCのリストをもとに調査し、以下を明らかにしました：

- IoCとして特定された一部のドメイン名が名前解決する3個のユニークなIPアドレス

- IoCとされたドメイン名の専用ホストを共用する294個のドメイン名。そのうち1つは、マルウェアの一括チェックにより悪意あるドメイン名と確認

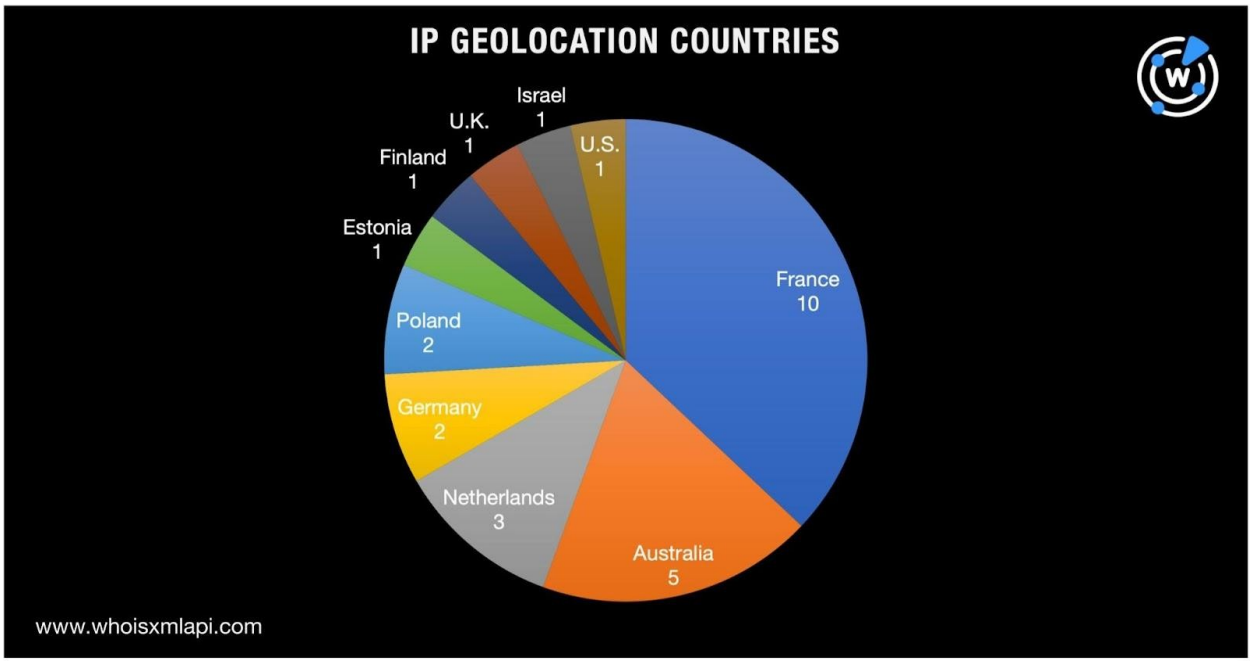
パート1：DNSに残されたPhonyC2の痕跡

PhonyC2のIoC

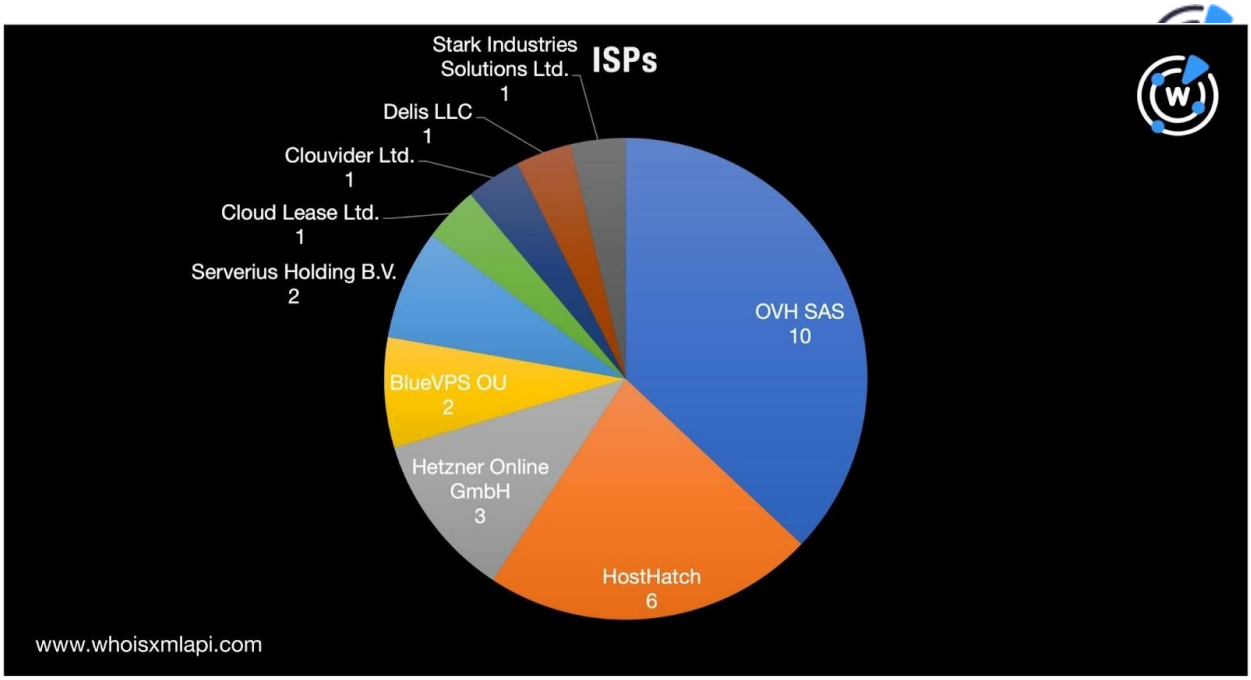
前述の通り、PhonyC2のIoCとして合計39個がDeep Instinctにより公表されていますが、それらは全てMuddyWaterの新しいC&Cフレームワークの一部です。WhoisXML APIでは今回、自らの広範なDNSインテリジェンスを駆使して、これらのIoCを詳しく調査しました。

IoCとして特定されたIPアドレスをBulk IP Geolocation Lookupにかけたところ、以下が判明しました。

- IPアドレスが地理的に位置していた国の上位は、フランス（10個）、オーストラリア（5個）およびオランダ（3個）。残りの9つのIPアドレスは7カ国に分散



- 最も多くのIPアドレスIoCを管理していたのはOVH SAS（10個）。次いでHostHatch（6個）、Hetzner Online GmbH（3個）



PhonyC2のIoCリスト拡張

まず、PhonyC2のIoCとして特定されたドメイン名に見られる以下の文字列を[Domains & Subdomains Discovery]で検索しました。

- **edc1.**
- **pru2.**
- **nno1.**
- **nno3.**
- **kwd1.**
- **kwd2.**
- **kwd3.**
- **qjk1.**
- **qjk2.**
- **qjk3.**
- **tes2.**
- **pru1.**

その結果、上記の文字列で始まるドメイン名が152個見つかりました。内訳は以下の表の通りです。

文字列	文字列を含んだドメイン名の数
edc1.	19
pru2.	10
nno1.	13
nno3.	9

kwd1.	11
kwd2.	7
kwd3.	14
qjk1.	11
qjk2.	13
qjk3.	14
tes2.	20
pru1.	11

いずれのドメイン名も悪意があることを確認できなかったものの、一部は非常に悪質なキャンペーンで使用または悪用されたウェブプロパティと共通の文字列を含んでいました。その例を以下に示します。

- **Adobe:** edc1[.]adobeaemcloud[.]com。Adobeのソフトウェア開発者やAdobe製品のユーザーを標的としたサイバー攻撃に使われた可能性があります。

- **ClouDNS:** edc1[.]cloudns[.]info。このドメイン名は、ClouDNSに帰属していることが公開のWHOIS情報から確認できませんでした。ClouDNSまたはその顧客を標的とした攻撃に使われた可能性があります。

- **Yandex:** kwd3[.]storage[.]yandexcloud[.]net。脅威アクターがYandexまたはそのユーザーに対して不正行為を働くために使った可能性があります。

次に、Deep InstinctがIoCとして特定した27個のIPアドレスをReverse IP Lookupで検索したところ、3個は専用ホストであることがわかりました。それらは、IoCリストに含まれていない3個のドメイン名（rare-upload[.]top、urbancritters[.]org[.]uk、s2-store[.]com）をホストしていました。

そこで、**rare-upload**、**urbancritters**または**s2-store**を含むドメイン名が他にないか探してみました。 その結果、**urbancritters**または**s2-store**を含む22個のドメイン名を特定しました。一括マルウェアチェックにかけたところ、そのうち2個は悪意あるドメイン名に分類されました。

本稿執筆時点で、2個の悪意あるドメイン名は両方とも到達不能でした。なお、そのうちの1つであるrefund-orderdc50kfcs2-store-apple[.]cfはAppleが所有していることを連想させますが、WHOISレコードを調べたところ、同社への帰属は確認できませんでした。

パート2：DNSに残されたMuddyWater・DEV-1084間協力の痕跡

MuddyWater・DEV-1084のIoC

MuddyWaterに関連するもう一つの最近の動きは、「DEV-1084」として知られる別の脅威グループとの連携です。

MuddyWaterが主導したと思われる最近の攻撃で、DEV-1084はDarkBitという人格を名乗り、前者の関与を隠していました。しかし、Microsoftの研究者がこの協力関係を暴露し、IoCとして4個のドメイン名と10個のIPアドレスを公表しました。

MuddyWater・DEV-1084のIoCリスト拡張

MuddyWater・DEV-1084の攻撃に関連したアーティファクトを見つけるために、MicrosoftがIoCとして特定したドメイン名を当社のDNS Lookupで検索しました。その結果、3個のドメイン名（pairing[.]rport[.]io、vatacloud[.]com、ehorus[.]com）が名前解決する合計4個のユニークなIPアドレスが見つかりました。それらのうち1個はすでにIoCリストに含まれていましたが、残りの3個（49[.]12[.]228[.]207、172[.]67[.]181[.]250、104[.]21[.]80[.]130）はリストに含まれていないものでした。

その3個の未公開IPアドレスとIoCのIPアドレス10個を合わせた13個をDNSで逆引きしたところ、3個の専用IPホストを294個のドメイン名が共用していたことがわかりました。また、その294個のドメイン名のうち1個（sdtvcs[.]ru）はマルウェアホストと判明しました。

その294個のドメイン名とIoCとして特定済みのドメイン名について、Bulk WHOIS Lookupの結果を照合したところ、以下が明らかになりました。

- IPアドレスを共用する294個のドメイン名のうち36個のレジストラは、IoCであるrport[.]ioのレジストラと同じ。4個はehorus[.]comと、50個はvatacloud[.]comと同じレジストラを使用
- IPアドレスを共用する294個のドメイン名のうち18個は、rport[.]ioと同じ年に登録。7個はehorus[.]comと、60個はvatacloud[.]comと登録された年が同じ
- IPアドレスを共用する294個のドメイン名のうち105個はrport[.]ioと同じ国で登録。1個はehorus[.]comと、44個はvatacloud[.]comと登録された国が同じ

—

今回のMuddyWaterの調査で、PhonyC2およびMercury・DEV-1084連携との関連が疑われる477個のウェブプロパティを特定できました。また、注目すべき3個の悪意あるドメイン名の発見にもつながりました。

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

Deep Instinctが特定したPhonyC2のIoC

- 45[.]159[.]248[.]244
- 91[.]121[.]240[.]104
- 195[.]20[.]17[.]44
- 45[.]86[.]230[.]20
- 137[.]74[.]131[.]30
- 178[.]32[.]30[.]3
- 137[.]74[.]131[.]24
- 46[.]249[.]35[.]243
- 185[.]254[.]37[.]173
- 194[.]61[.]121[.]86
- 87[.]236[.]212[.]22
- 91[.]235[.]234[.]130
- 157[.]90[.]153[.]60
- 157[.]90[.]152[.]26
- 65[.]21[.]183[.]238
- 45[.]132[.]75[.]101
- 51[.]255[.]19[.]178
- 103[.]73[.]65[.]129
- 103[.]73[.]65[.]225
- 103[.]73[.]65[.]244
- 103[.]73[.]65[.]246
- 103[.]73[.]65[.]253
- 137[.]74[.]131[.]16
- 137[.]74[.]131[.]18
- 137[.]74[.]131[.]25
- 164[.]132[.]237[.]67
- 164[.]132[.]237[.]79
- edc1[.]6nc051221c[.]co
- pru2[.]6nc110821hdb[.]co
- nno1[.]6nc060821[.]co
- nno3[.]6nc060821[.]co
- kwd1[.]6nc220721[.]co
- kwd2[.]6nc220721[.]co
- kwd3[.]6nc220721[.]co
- qjk1[.]6nc051221c[.]co
- qjk2[.]6nc051221c[.]co
- qjk3[.]6nc051221c[.]co
- tes2[.]6nc051221a[.]co
- pru1[.]6nc110821hdb[.]co

PhonyC2のIoCとして特定されたドメイン名と同じ文字列を含むドメイン名の例

- edc1[.]xn--fiqz9s
- edc1[.]ru
- edc1[.]aquila[.]it
- edc1[.]adobeaemcloud[.]com
- edc1[.]cn
- edc1[.]net
- edc1[.]vg
- edc1[.]club
- edc1[.]xn--node
- edc1[.]com
- edc1[.]tk
- edc1[.]win
- edc1[.]com[.]au
- edc1[.]kz
- edc1[.]cloudns[.]info
- edc1[.]com[.]br
- edc1[.]store
- edc1[.]xyz
- edc1[.]2038[.]io
- pru2[.]omniwe[.]site
- pru2[.]com
- pru2[.]lolipop[.]io
- pru2[.]net
- pru2[.]townnews-staging[.]com
- pru2[.]com[.]de
- pru2[.]filegear-de[.]me
- pru2[.]us
- pru2[.]tk
- pru2[.]ws
- nno1[.]now[.]sh
- nno1[.]df[.]gov[.]br
- nno1[.]static[.]observableuserconten t[.]com
- nno1[.]square7[.]net
- nno1[.]hb[.]cldmail[.]ru
- nno1[.]com
- nno1[.]panel[.]gg
- nno1[.]cn
- nno1[.]xn--fiqz9s
- nno1[.]ru
- nno1[.]user[.]srcf[.]net
- nno1[.]readthedocs[.]io
- nno1[.]resindevice[.]io
- nno3[.]onza[.]mythic-beasts[.]com
- nno3[.]shopitsite[.]com
- nno3[.]fastly-terrarium[.]com
- nno3[.]com
- nno3[.]user[.]srcf[.]net
- nno3[.]ga
- nno3[.]vg
- nno3[.]hu[.]net

PhonyC2のIoCとして特定されたIPアドレスを共用するドメイン名と同じ文字列を含むドメイン名の例

- urbancritters[.]net
- urbancritters[.]com
- urbancritters[.]org
- urbancritterssd[.]com
- urbancritters[.]store
- avsurbancritters[.]com
- plus2-store[.]com
- airpods2-store[.]com
- darksouls2-store[.]fr
- darksouls2-store[.]com
- shoppinguss2-store[.]com

- refund-orderdc50kfcs2-store-apple[.]cf

Microsoftが特定したMuddyWater・DEV-1084のIoC

- cybercom[.]mil
- pairing[.]rport[.]io
- vatacloud[.]com
- ehorus[.]com
- 46[.]249[.]35[.]243
- 45[.]86[.]230[.]20
- 45[.]56[.]162[.]111
- 194[.]61[.]121[.]86
- 193[.]200[.]16[.]3
- 192[.]52[.]166[.]191
- 146[.]70[.]106[.]89
- 141[.]95[.]22[.]153
- 104[.]194[.]222[.]219
- 192[.]169[.]6[.]88

MuddyWater・DEV-1084のIoCとIPアドレスを共用していたドメイン名の例

- 000037c[.]com
- 030tt[.]com
- 195806[.]cc
- 22setrabettv[.]com
- 420cannabisonline[.]net
- 7jrl1x[.]com
- adrainburdettevu[.]buzz
- advantagebell[.]com
- afsdf44[.]com
- al5drawing[.]shop
- albertsbridgemusical[.]co[.]uk
- amacolumbus[.]com
- ampliface[.]com
- anhoatech[.]vn
- aptenodytes[.]nl
- arshashokri[.]eu[.]org
- artlifedigital[.]ru
- asgdl[.]life
- asrelaterco[.]beauty
- azennamtirama[.]cf
- baba-behtarin10000[.]buzz
- balenciagatrendy[.]com
- barriranstighredbte[.]cf
- bbppxtn[.]info
- bestairpurifier[.]reviews
- bigchange[.]tokyo
- bisamaxwin[.]pro
- bitficompdupati[.]cf
- bizenglish-edu[.]net
- blanks[.]eu
- bloomodeliving[.]shop
- botza1m[.]online
- britos[.]net
- budapest-travel-tips[.]com
- cadija[.]com
- camphotsell[.]store
- canteenrepertoire[.]cn
- caprode[.]top
- casino-gang[.]cl
- casinogate[.]io
- cbs79[.]com
- cetuw[.]online
- charmchange[.]online
- chassed[.]bar
- cnleotradepart[.]space
- col-kofpqw[.]shop
- coniksho[.]lol
- contact[.]jobild[.]com
- copperbringer[.]sa[.]com
- cwpuser[.]newmediafactor[.]com