IoCリスト拡張でBlackEnergyによるDDoS攻撃を緩和

目次

要旨

BlackEnergyが最初に登場したのは2007年のことです。DDoS攻撃を仕掛けたり、カスタマイズされたスパムや銀行データを盗むプラグインをダウンロードしたりするように設計されており、昨年5月にはジョージア州の州弁護士会が標的にされました。

そのサイバー攻撃により、同弁護士会事務所は対応を終えるまで通常業務を停止せざるを得なくなりました。そして、事件後すぐに行われた調査の結果、BlackEnergyの使用が明らかにされ、8つのドメイン名（clusteron[.]ru、svdrom[.]cn、fumpic[.]org、logartos[.]org、pizdos[.]net、webror[.]cn、h278666y[.]netおよび inattack[.]rub ）がセキュリティ侵害インジケーター（IoC）として特定されました。

当社は上記のIoCを出発点とし、WHOISおよびDNSのデータを活用してさらに調査を広げました。その結果、以下を発見しました。

- IoCとされたドメイン名が名前解決した49個のIPアドレス
- IoCとされたドメイン名の登録に使われた未編集のメールアドレス2つ
- IoCと同じ登録者メールアドレスまたはIPアドレスを使っていた6,003個のドメイン名。そのうち141個は複数のマルウェアエンジンで「悪意がある」と確認

IoCのリストを拡張

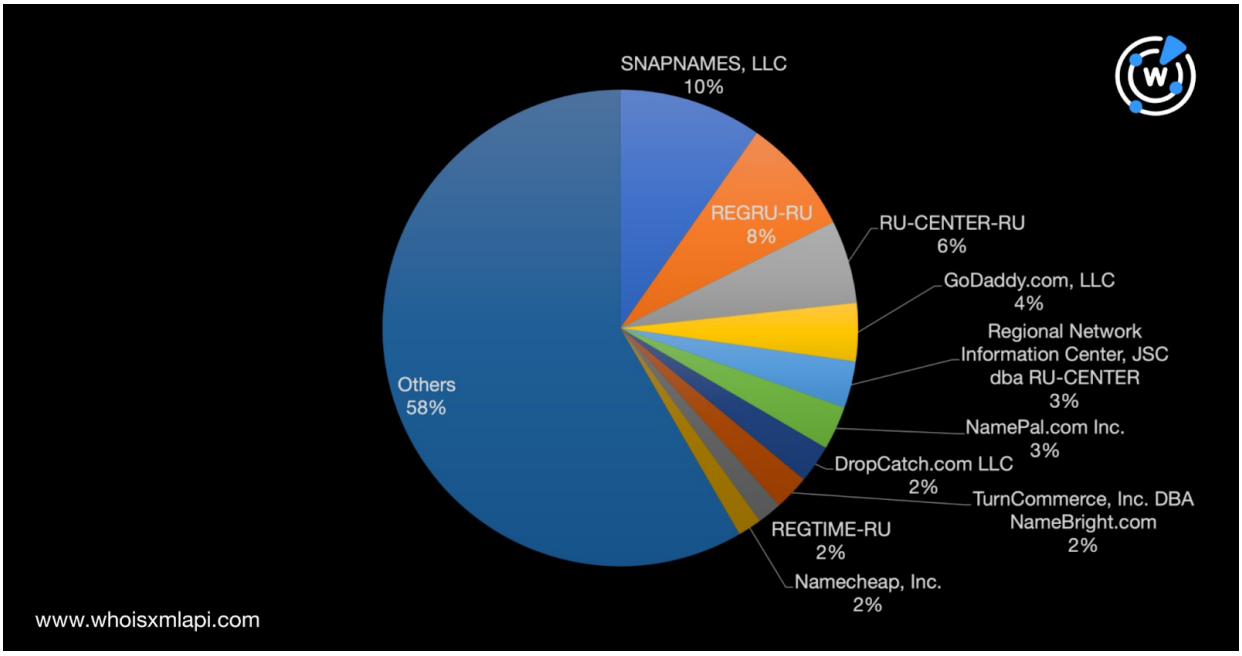
BlackEnergyを利用した攻撃からネットワークを保護するため、WHOISとDNSのデータからIoCと関連している可能性のあるアーティファクトをできるだけ多く特定しました。

IoCとされたドメイン名を検索キーワードとしてDNS lookupで調べたところ、名前解決した49個のIPアドレスに辿り着きました。それらのアドレスの地理的位置は、米国、オランダ、ロシア、ドイツ、シンガポールを中心に11カ国に分散していました。

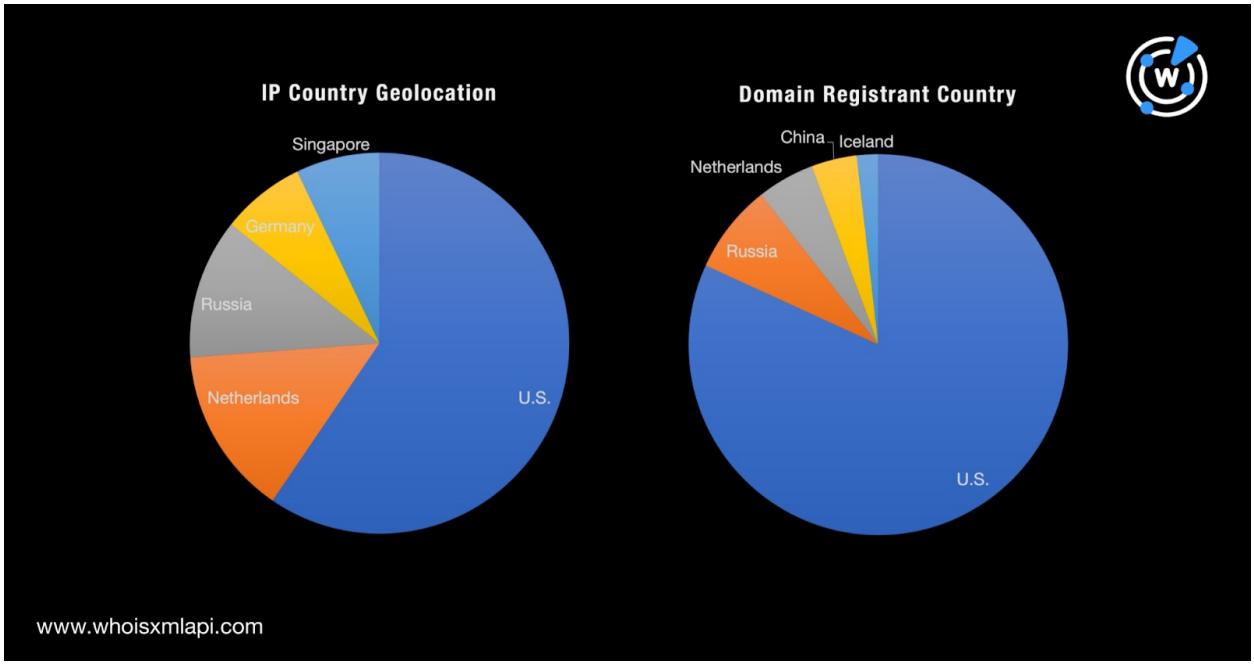
当社が実施したマルウェアチェックでは、どのIPアドレスもその時点で危険とは見なされませんでした。しかし、一部のアドレスはIoCの共用ホストとして機能していたため、悪意ある活動の兆候を監視する意味はあると思われます。

また、IoCとされたドメイン名の過去のWHOISレコードを精査したところ、ドメイン名登録に使用された未編集のメールアドレス（135224*****@163[.]comとasdf9*****@21cn[.]com）を特定できました。

さらに、IPアドレスとメールアドレスを検索キーワードとしてIP逆引きとWHOIS逆引きを行ったところ、関連性のあるドメイン名が6,003個見つかりました。これらのドメイン名についてWHOIS一括検索を行った結果、その多くがSnapNames, LLCというレジストラのもとで登録されたことがわかりました。以下の通り、同社を経由して登録されたドメイン名は全体の10%を占めています。



下のチャートは、IPアドレス（左：国別ジオロケーション）とドメイン名（右：登録者の所在国）の登録が集中した国を比較したものです。



米国、オランダ、ロシアは、IPジオロケーションとドメイン名登録の両方で常に上位5カ国にランクインしています。SnapNames、GoDaddy、NamePal、DropCatch、TurnCommerce、Namecheapが米国に拠点を置いていることを考えると、これは驚くべきことではありません。また、REGRU-RU、RU-CENTER-RU、Regional Network Information Center、REGTIME-RUは、ロシアに拠点を置いています。

さらに最終段階として、関連性のある6,000超のドメイン名を Threat Intelligence Platform（TIP）の一括マルウェアチェックにかけてみました。その結果、141個のドメイン名がマルウェアやスパムのホストとして各種マルウェアエンジンから検出されていたことがわかりました。

BlackEnergyを利用した攻撃への対策

BlackEnergyがもたらす被害、特にオペレーションの中断を回避するため、組織にはIoCとして特定されたドメイン名に加え、当社が発見した141個の関連ドメイン名へのアクセスをブロックすることをお勧めします。また、関連しているIPアドレスに悪意ある活動の兆候がないか監視することも有効です。

同様の調査をご希望のお客様、またはこの調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせ下さい。

付録：アーティファクトとIoCの例

IoCとされたドメイン名が名前解決したIPアドレス

- 72[.]233[.]60[.]254
- 34[.]229[.]158[.]240
- 103[.]232[.]215[.]142
- 124[.]16[.]31[.]152
- 50[.]117[.]120[.]251
- 127[.]0[.]0[.]1
- 103[.]232[.]215[.]129
- 104[.]201[.]25[.]77
- 203[.]117[.]111[.]52
- 195[.]24[.]78[.]242
- 79[.]174[.]72[.]81
- 185[.]162[.]9[.]224
- 64[.]32[.]8[.]69
- 109[.]70[.]26[.]37
- 209[.]99[.]64[.]18
- 185[.]107[.]56[.]60
- 194[.]85[.]61[.]76
- 185[.]107[.]56[.]57
- 31[.]31[.]196[.]200
- 65[.]19[.]157[.]227

IoCと同じIPアドレスや登録者メールアドレスを使用していたドメイン名の例

- muca-shop[.]com
- official-patch[.]com
- lemaket[.]com
- beautifulbarbado[.]com
- pclaptopapps[.]com
- raincourses[.]com
- tfldap[.]com
- beastscans[.]com
- monkeys247[.]com
- tvserialupdates[.]com
- optilux-light[.]com
- giftideascanada[.]com
- binsecret[.]com
- mapleye1994[.]com
- baguiocarmela[.]com
- dmbfccdictionary[.]com
- seduceteen[.]com
- ogormanogorman[.]com
- expunct[.]com
- mp3youtubemusic[.]com
- gherlock[.]com
- 100preanuncios[.]com
- premiumvapecarts[.]com
- bmsuniversaloficial[.]com
- fabrikborne[.]com
- hhlighter[.]com
- convergentatberkeley[.]com
- kostromasauna[.]com
- startyourclan[.]com
- wolfyshopd[.]com
- 86fans[.]com
- get699250[.]com
- mydreamkatch22[.]com
- storecharming[.]com
- polifaceticoactua[.]com
- rocketscienceandleadership[.]com
- mymerrys[.]com
- ycilka[.]com
- aktiva-knjigovodstvo[.]com
- mail[.]transmediatelevision[.]com
- gongj4[.]com
- 1bie[.]com
- directbookingonline[.]com
- brasfieldresources[.]com
- intesolrussia[.]com
- calvin-profits[.]com
- lynxurbanoutdoor[.]com
- smallrigamazon[.]com
- unicaudio[.]com
- popno-tour[.]net
- er-diagram[.]com
- tuhocielts9[.]com
- sparksthemagic[.]com
- agronegociosjewell[.]com
- familyfirstfoodservicellc[.]com
- zmbang1[.]com
- covidbelgesial[.]com
- dkcronusv2[.]com
- yogalivingarts[.]com
- kfandom[.]com
- xingbayy[.]com
- www[.]cellularmountain[.]com
- untaobao[.]com
- carolgarciapsicologa[.]com
- canadianteaparty[.]com
- deadsidemap[.]com
- aylarosemodel[.]com
- luanasweet[.]com

- breathfilmnow[.]com
- deyakannesha[.]com
- shelby-andrew[.]com
- coloradolocalbusinessdirectory[.]com
- ayhankorkmaz[.]net
- fit40andover[.]com
- boss-wow[.]com
- mischief-progress[.]com
- wujizhiji[.]com
- nomimono-showgi[.]com
- pricemy3dprint[.]com
- xn--hc0bt2ji8dd5kw6bmxpq8qlic[.]com
- mdkglass[.]com
- osteriasgarzarie[.]com
- knklim[.]com
- nguyenquoclong[.]com
- modelivylee[.]com
- igpreview[.]com
- knownclouds[.]net
- rootforum1[.]com
- lachgod[.]com
- starwaygames[.]com
- treelyrics[.]com
- eliteveloelectrique[.]com
- eluosi-liwu[.]com
- 735486[.]com
- windsculpturesartworks[.]com
- uprexbit[.]com
- mikutools[.]com
- estrategiasclubhouse[.]com
- hedonisteshop[.]com
- binghechina[.]com

悪意あるドメイン名の例

- binsecret[.]com
- loginpp[.]com
- profsoundsystem[.]com
- paintrightcincy[.]com
- pandemic-covid-19[.]net
- magicpod[.]top
- depresjakoronawirus[.]info
- amilziswaf[.]com
- tuoka50[.]com
- playtely[.]com
- dollarpresets[.]com
- avatachi[.]u0559032[.]cp[.]regruhosting[.]ru
- 1-ea[.]u0559032[.]cp[.]regruhosting[.]ru
- mail[.]ws-amgu[.]ru
- 9kmovies[.]net
- www[.]ws-amgu[.]ru
- e-formula[.]pro
- plusgmail[.]ru
- 26x10[.]com
- pym-studios[.]com
- husseinatwi[.]com
- pagibigfundservices27[.]com
- blueberrytube[.]com
- kamawheelj[.]com
- pvaagent[.]com
- pupalley[.]com
- inattack[.]ru
- reverse-real[.]com
- ijkconsult[.]com
- tamiratiranian[.]net
- collectiblebay[.]com
- www[.]leandomain[.]com
- coronabot[.]site

- clientform[.]ref1828684[.]bbt[.]com[.]potreit[.]cn
- mixante[.]cn
- clientform[.]ref454011[.]bbt[.]com[.]potreit[.]cn
- clientform[.]ref990758[.]bbt[.]com[.]potreit[.]cn
- gcounter[.]cn
- interactsession-567309924[.]regions[.]com[.]usersetup[.]cn
- 0011[.]89111[.]cn
- clientform[.]ref5239484[.]bbt[.]com[.]potreit[.]cn
- clientform[.]ref8722996[.]bbt[.]com[.]potreit[.]cn
- www[.]loadskynet[.]cn
- www2[.]89111[.]cn
- margin-groupco[.]cn
- bemlida[.]cn
- brandnameshoppin[.]cn
- qudeteyuj[.]cn
- myvloji[.]cn
- count[.]llads[.]cn