Alleviating BlackEnergy-Enabled DDoS Attacks

Table of Contents

Executive Report

BlackEnergy first appeared in 2007. Designed to launch distributed denial-of-service (DDoS) attacks or download customized spam or banking data-stealer plug-ins, it was again used to target the State Bar of Georgia last May.

Following the most recent cyber attack, the office had to suspend normal operations until the issue was addressed. Investigations that ensued soon after the incident revealed the use of BlackEnergy along with the identification of eight domains—clusteron[.]ru, svdrom[.]cn, funpic[.]org, logartos[.]org, pizdos[.]net, weberror[.]cn, h278666y[.]net, and inattack[.]ru—as indicators of compromise (IoCs).

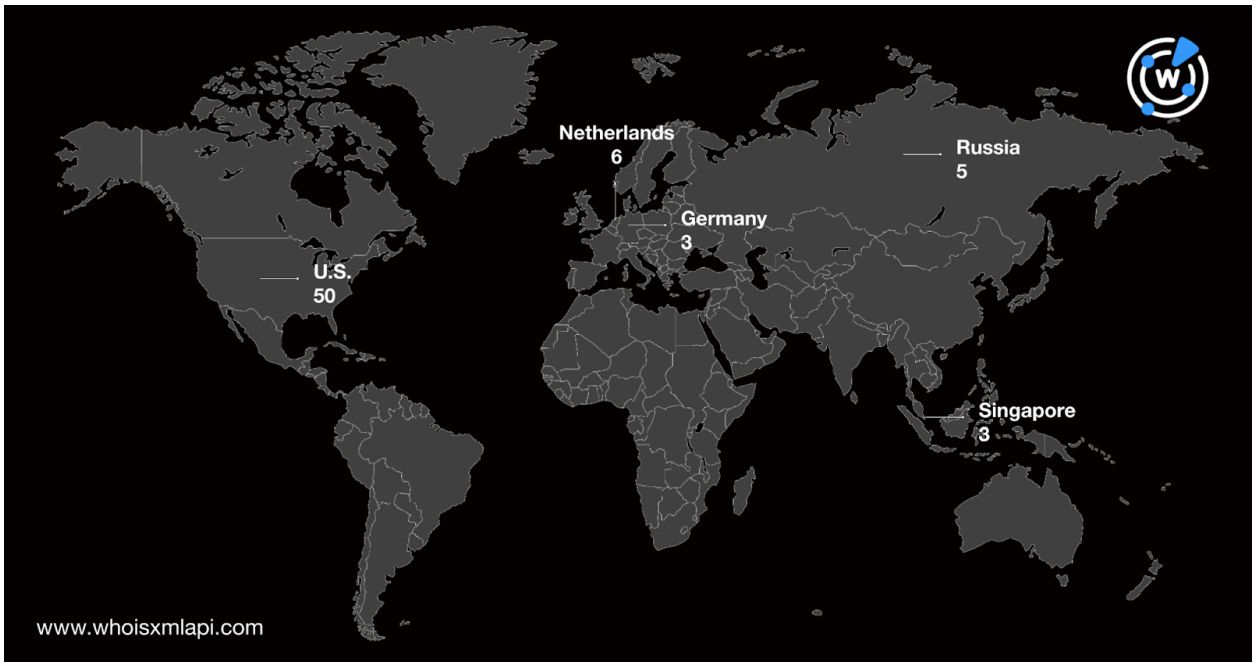
Using these web properties as jump-off points for a deep dive enabled by WHOIS and Domain Name System (DNS) data led to the discovery of:

- 49 IP addresses to which the domains identified as IoCs resolved
- Two unredacted email addresses used to register the domains tagged as IoCs
- 6,003 domains that shared the IoCs' registrant email addresses or IP addresses, 141 of which were dubbed "malicious" by various malware engines

Expanding the List of IoCs for Better Protection

To help organizations to protect their networks from BlackEnergy-enabled attacks, we identified as many possibly related artifacts with WHOIS and DNS data.

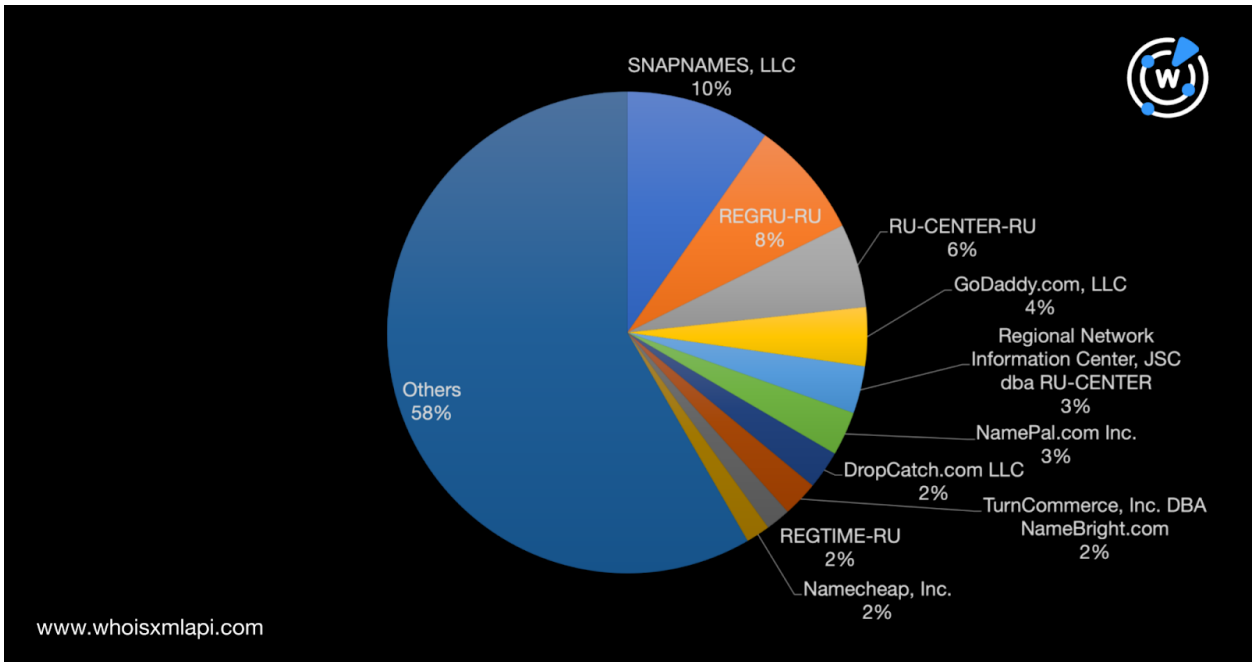
Using the IoC domains identified as DNS lookup search terms led to the discovery of 49 IP addresses to which they resolved. These were spread across 11 countries led by the U.S., Netherlands, Russia, Germany, and Singapore.



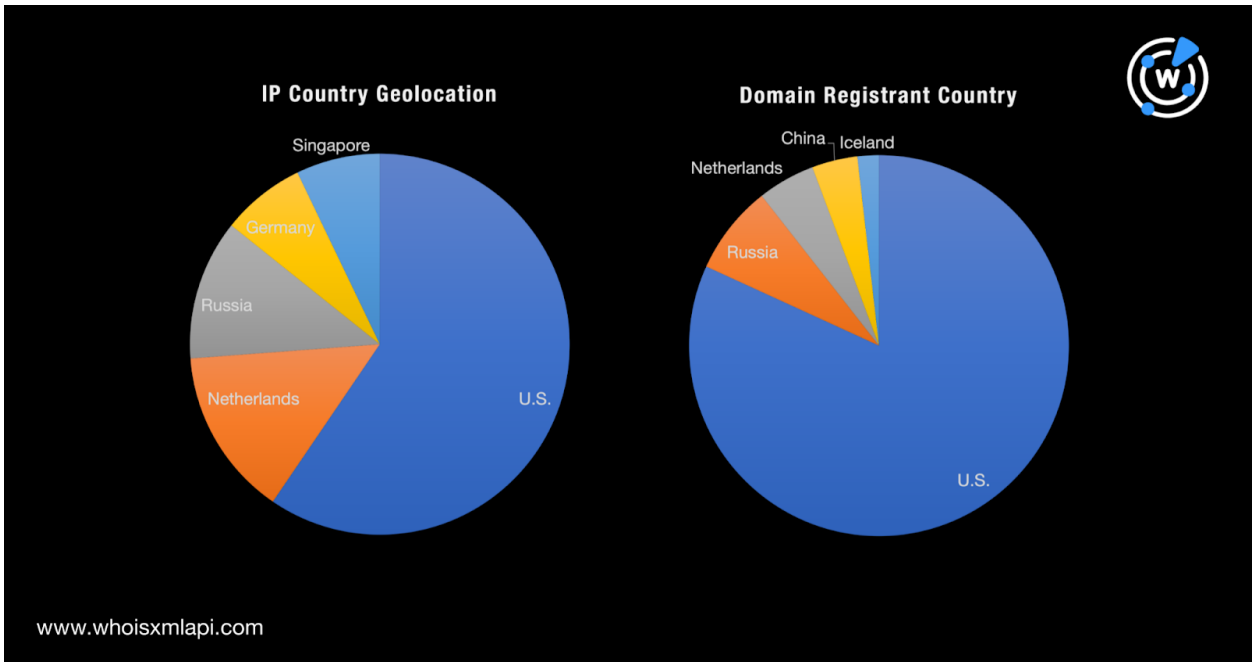
While none of the IP addresses are currently considered dangerous as per malware checks we conducted, monitoring them for signs of malicious activity may still be worth doing as some of them served as shared hosts to the IoCs.

A closer scrutiny of the historical WHOIS records of the domains tagged as IoCs, meanwhile, allowed us to uncover two unredacted email addresses—135224*****@163[.]com and asdf9*****@21cn[.]com—used to register them.

Reverse IP and reverse WHOIS lookups using the IP addresses and email addresses, respectively, as search terms further provided 6,003 possibly connected domains. A bulk WHOIS lookup for these showed that a majority of them were registered under SnapNames, LLC, which accounted for 10% of the total domain volume, among other registrars shown in the figure below.



The following chart compares the countries where most of the IP addresses (left: country geolocation) and domain registrations (right: registrant country) were concentrated.



The U.S., Netherlands, and Russia consistently figured in the top 5 countries in terms of both IP geolocation and domain registration. That isn't surprising given that SnapNames, GoDaddy, NamePal, DropCatch, TurnCommerce, and Namecheap are based in the U.S., while REGRU-RU, RU-CENTER-RU, Regional Network Information Center, and REGTIME-RU are based in Russia.

As the final step, we subjected the 6,000+ possibly connected domains to a bulk malware check via the Threat Intelligence Platform (TIP) and found that 141 of them were detected by various malware engines as malware or spam hosts.

BlackEnergy-Enabled Attack Prevention

Organizations that want to avoid the unwanted consequences that BlackEnergy poses, specifically an operational disruption, may want to block access to the domains identified as IoCs and the additional 141 possibly connected domains we found. Monitoring the connected IP addresses for signs of malicious activity may also help.

If you wish to perform a similar investigation or get access to the full data behind this research, please contact us.

Appendix: Sample Artifacts and IoCs

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 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

Sample Domains That Shared the IoCs' IP Addresses or Registrant Email Addresses

- 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

Sample Malicious Domains

- 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