AREA 1

The Unlikely Origins of Cyber Attacks

Intro

News headlines about data breaches today detail the amount of data stolen or the number of customer records impacted. The stories discuss how sophisticated the attackers are and how fancy their malware was. They talk about who initiated the attack and who the victim is. They try to explain how to contain the damage once it is done.

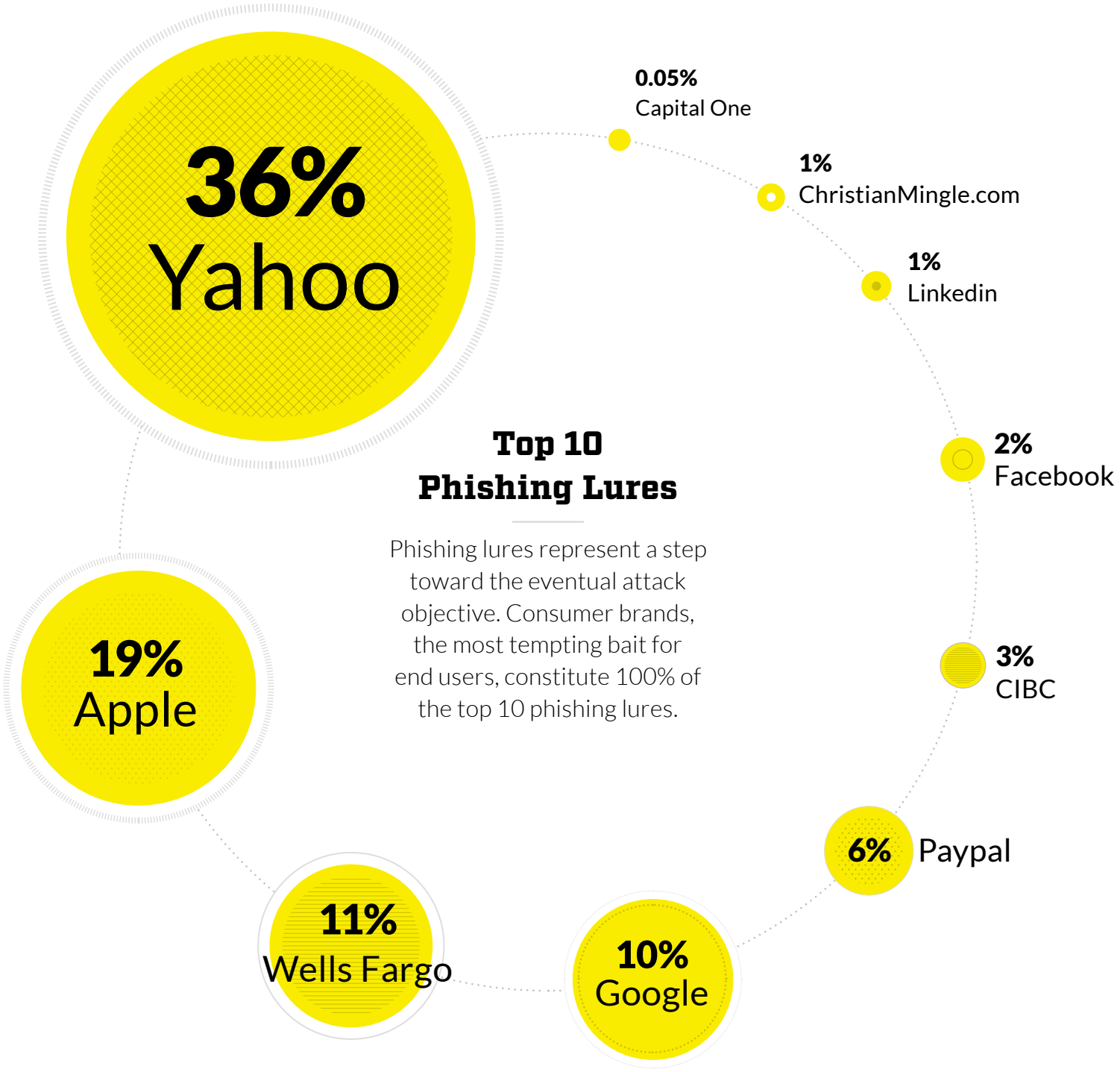
While those headlines are understandable, they prove that companies are focused on the wrong parts of cyber security: attribution and remediation. Regardless of how many attackers have been identified or how much clean up has been done, attacks continue to happen. Organizations must turn their focus toward where cyber attacks originate. Hackers always leave traces of impending attacks — traces that clue victims in on the origin of attacks.

Cybersecurity measures that can zero in on attack origins stand a much better chance of both mitigating effects of impending attacks and limiting future attacks. Discovering and understanding where cyber attacks come from is the key to developing a long-term cybersecurity solution.

© Area 1 Security 2016

Top Attacks

Analysis from **Jan 1st 2016** to date. A dataset sample of more than **2.15 million phishing attacks** across that period.



Top 10 Phishing Lures

Phishing lures represent a step toward the eventual attack objective. Consumer brands, the most tempting bait for end users, constitute 100% of the top 10 phishing lures.

© Area 1 Security 2016

Top Geolocation Cities

Major metropolitan areas host the most attacks and have the most victims.

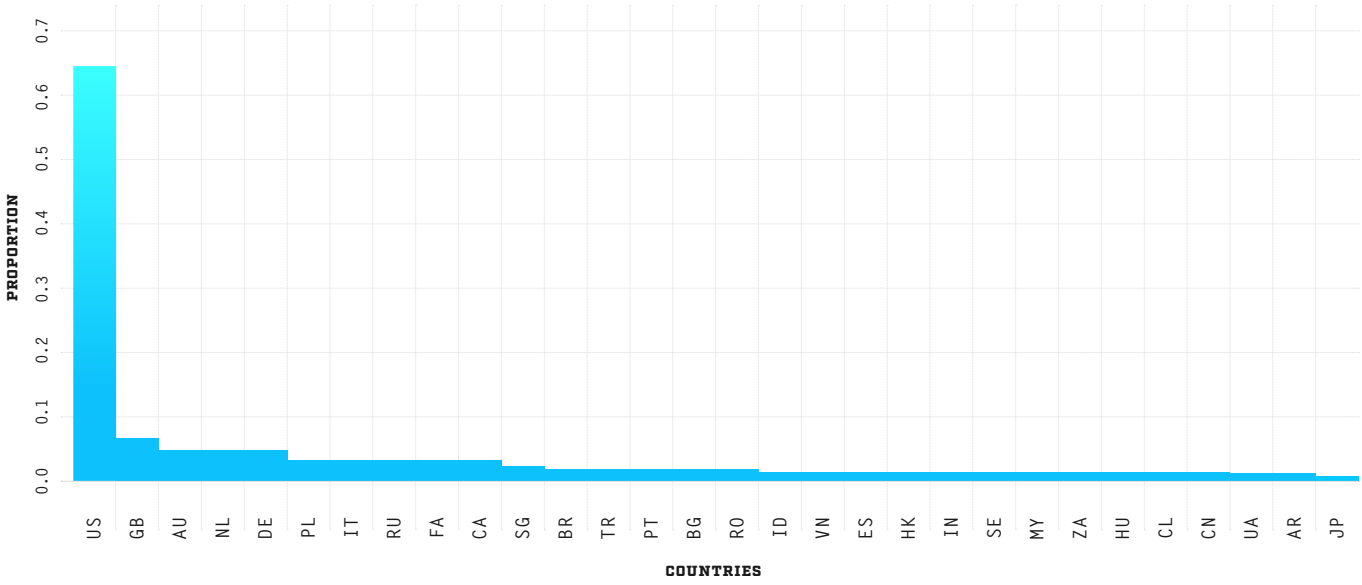
AREA 1

© Area 1 Security 2016

Top Geolocation Countries

Attacks have a massive long tail. Most are aimed at US targets and are hosted within the US.

HOST COUNTRIES OF PHISHING WEBSITES



PHISHING URLS ANALYZED

2,150,280

DETECTED FROM THE US

63%

Top 10 ASNs by Country

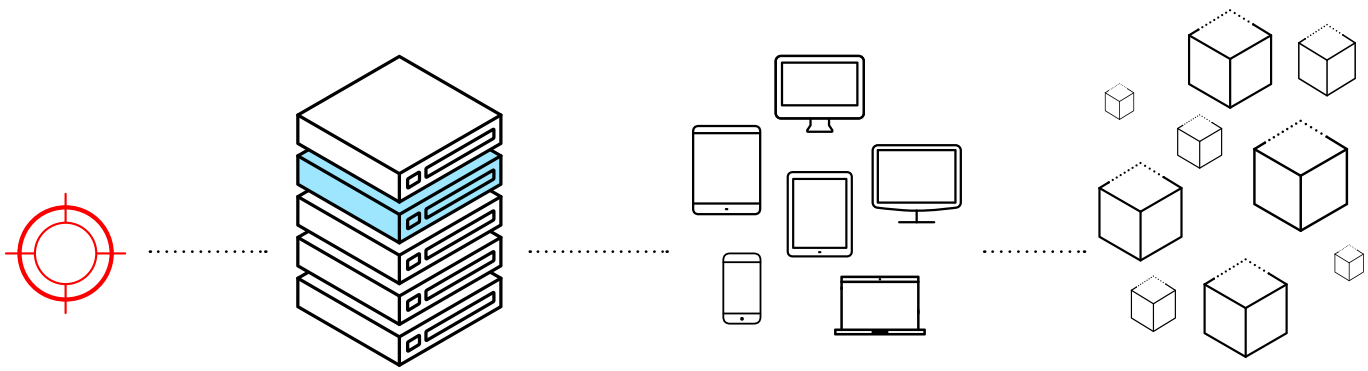
Most attack relay points are in the US, following the pattern of where these sites are hosted. Bad guys repurpose innocent servers, which is why attacks often come from unlikely origins.

It's fairly common knowledge that users tend to repeat their credentials. Once an attacker gets hold of a set of working credentials for an end user, those credentials get used at other target systems the user has accounts.

1. GoDaddy (US)
2. Cyrs-As (US)
3. Unified Layer (US)
4. DimeNOC (US)
5. NetRegistry (AU)
6. Softlayer (US)
7. E-xpedient (US)
8. SingleHop (US)
9. Amazon (US)
10. LiquidWeb (US)

© Area 1 Security 2016

The Attack Trifecta



Existing cybersecurity defenses focus on constructing a perimeter around the potential victim and identifying the payload in order to stop attacks from getting through. Area 1 takes a different approach. We focus on the attacker's history, behavior, delivery mechanism, and infrastructure. When you can identify and neutralize those, the payload doesn't matter. And there is no victim.

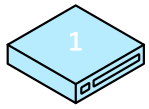
© Area 1 Security 2016

In the Wrong Hands, Any Server Is a Weapon

When we think about targeted attacks such as phishing and remote exploitation, many of us assume that they emanate from large data centers. This is not necessarily the case. Attackers, well aware of the cat and mouse game they play with security teams of Global 2000 organizations, often proxy their command and control (C2) through one or more intermediary nodes on the Internet.

These nodes, often belonging to small-to-medium-sized organizations, serve as the intermediary hop points in what is often referred to as a "stepping stone attack."

Over the last two years, globally-distributed Area 1 sensors have seen hundreds of such organizations breached by these attacks. In this section, we outline some of the most interesting and unique attack proxy points.



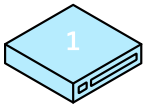
The Saddle Maker

The Public School

The Social Club

The Industrial Automation Equipment Manufacturer

© Area 1 Security 2016



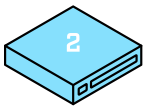
The Saddle Maker

In late 2015, Area 1 surveilled the compromise of a Saddle Maker by an actor sponsored by a foreign country. Small companies are at risk from large, national spy programs because their compromised servers can hide attacks on other organizations. The breach occurred as a result of the Saddle Maker running outdated Windows 2003 Servers on the Internet with poor perimeter security, including weak passwords. Once breached, the actor made quick lateral movement, exploiting all of the core server infrastructure. The actor installed a backup backdoor as well as C2 management software to be used to communicate with the main targets as soon as the actor exploited them successfully. After breaching the company's email server, the attacker created a fake user and email account on the server. The accounts were used to send a wave of over 100 targeted phishing emails across multiple industry verticals.

Verticals that were included in the attack included United States Department of Defense contractors. Once these targets opened the weaponized office documents attached to the malicious emails, malware was silently installed and began beaconing back to the C2 server running on the Saddle Maker's systems for further instruction.

While DoD contractors often have a significant budget for defense against targeted attacks, proxying an attack through the servers of a legitimate U.S.-based company can fool even the most sophisticated IT security teams.

© Area 1 Security 2016



The Public School

In early 2016, threat actors began to leverage a then-recently disclosed exploit, Jexboss, against a myriad of public school servers throughout the world who managed their libraries with vulnerable versions of the JBoss web application server. In this case, it was open source software and services that were used to detect vulnerabilities within the public school systems.

After compromising the targets, the actors executed Visual Basic scripts on the compromised machines using Microsoft PowerShell commands. These scripts were used to install a variety of webshell backdoors to ensure that access to these systems was maintained. The actors then leveraged the open source tools Mimikatz and Powercat: a PowerShell version of Netcat, a network tool with legitimate applications. Mimikatz was used to steal credentials to enable lateral movement within the breached networks while Powercat was used to launch n-map, another network tool with legitimate uses, which attacked internal hosts within each public school network. Reverse shell connections were initiated to download backdoors which stole credentials and executed commands. Downloader scripts sent a "download successful" status message back to the C2 server to track the progress of the campaign as it unfolded. To manage all the compromised servers, the attackers leveraged Twiddle, a command execution capability in the JBoss server, to execute additional scripts and to interrogate the JBoss server to divulge critical system information.

Some of the compromised hosts were turned into proxies after the attacker installed a configurable tool for filtering and redirecting network traffic. This allowed traffic to be bounced around within this network of compromised systems to hide the backend C2 server owned by the actor.

Second-stage backdoors were installed on other compromised hosts and the actors used them to attack their actual targets, outside of the school networks. The compromised hosts were used to carry out the attacks since without knowledge of a breach, the attack appeared to the victim as benign traffic from a reputable server.

Interestingly, but not surprisingly, none of the educational institutions were targeted for any of their own data. Their vulnerable systems were simply compromised by opportunity and used as pawns to attack the actor's main targets, providing the attacker with a protective layer of anonymity.

Over the last two years, Area 1 has observed several public schools that serve as email phishing senders, exploit servers, and C2 servers for malware. Often lacking the IT budget necessary to defend against targeted attacks, many public school systems are easily and unknowingly conscripted in targeted attacks against enterprises. Even well-resourced public school systems in the top 10 US major metropolitan areas face challenges in detecting and preventing compromises from sophisticated attackers.

© Area 1 Security 2016

The Social Club

The Social Club used to be a place where acquaintances met to have a drink, but now it has a virtual side, offering seemingly harmless Internet access to its members as well. "Watering hole attacks" on the web typically encompass compromising legitimate, frequently-visited sites in order to distribute malware to their visitors. The Social Club, however, serves as a virtual watering hole for the club's clientele via the club's network. The Social Club's clientele are often individuals with Ivy League degrees who work at major enterprises worldwide across multiple verticals. With an attacker in full control of the club's entire computer network, the members are mere victims in the enterprise cybersecurity arms race.

As members enter the club to relax for a few hours, they open up their laptops, joining the club's network to check email or the browse the web. Unaware of the systemic breach, the club's WiFi Internet connection puts each member in front of a watering hole that specializes in unintentional "drive-by downloads." Unfortunately for the companies they work for, some club members are using their corporate laptops. A drive-by download distributes malware on the corporate laptop, and as the user connects to their Virtual Private Network, the attacker suddenly finds himself inside a Fortune 500 organization.

It doesn't end there. Today is the attacker's lucky day. The user is part of the organization's information technology department and has administrator access to the company's Windows network. Over the next 24 hours, the attacker moves laterally within the network to effortlessly gain access across the Windows Domain and begin the trivial task of exfiltrating thousands of files from the organization. To add insult to injury, since the user's passwords are compromised, the attacker then connects to the user's email account using a common email client configured with the victim's credentials and proceeds to perform a sync of the entire mailbox's contents.

This is a key exfiltration technique: theft of email content via mailbox sync using IMAP and POP3 mail protocols over SSL and access to cloud-based email services over SSL that are not protected with two-factor authentication.

Since the breach of The Social Club, the club acts as a revolving door for members to effectively walk in, be breached, and walk back out. By attacking a common hub where many people working at a myriad of corporations conglomerate, **the actor gains access to a vast number of organizations much more easily than attacking each organization individually.**

© Area 1 Security 2016

The Industrial Automation Equipment Manufacturer (SCADA)

In early 2016, a global industrial equipment manufacturer in the SCADA space was compromised. Following mass data exfiltration, the attacker began to reuse the victim for anonymity as it attacked other targets. It is quite common to see attackers use compromised systems from successful hacks to attack other organizations.

Because of the special relationship that exists between industrial partners, there is a higher success ratio associated with attacks that originate from trusted networks. This is commonly known as a "supply chain attack."

In this case, the actor began using the compromised infrastructure in their attack chain to target companies in a different region of the world via spear phishing, fake emails that appear to be from someone the target knows. The attacker deployed the well-known Scanbox framework, a web-based reconnaissance kit. Scanbox provided the attacker with two key tools:

1. Keylogging capabilities
2. Version numbers for all installed software on the system.

Keylogging allowed the actor to obtain credentials for login masquerades, which let them access the site's administration functions remotely. The list of installed software allowed the actor to identify vulnerable software that could be exploited either directly or through spear phishing with weaponized documents.

Attackers use the proxy chain not only to manage their C2 infrastructure for future attacks, but also to take vast amounts of sensitive data from their victims.

© Area 1 Security 2016

Conclusion

Attackers make use of a variety of delivery techniques to target different types of victims. While they can change the servers they use to launch attacks, they can't change their return address, the location where they are actually based. Compromising existing small-to-medium-sized organizations not only gives attackers anonymity, but also eliminates the long and costly process of fabricating an online identity. It is cheaper and easier for attackers to use someone else's infrastructure than to rely on their own servers.

© Area 1 Security 2016

Appendix

Top N Data

ASN	ASN_Name	Count	Country
26496	GODADDY	17162	SG,NL,US
20013	CYRS-AS	12787	US
33182	DimeNOC	6555	US
46606	UNIFIEDLAYER-AS-1 - Unified Layer, US	5943	US
36351	SOFTLAYER	5217	
13335	CLOUDFLARENET-AS	2473	EU,CR,US
17054	E-xpedient	1881	US
24446	NETREGISTRY-AS-AP	1873	AU
47583	HOSTINGER-AS	1646	LT,US
16276	OVH	1450	FR,CA,IT
24940	HETZNER-AS	1407	DE
54641	IMH-EAST	1387	US
32244	LiquidWeb	1380	US
21840	SAGONET-TPA - Sago Networks, US	1308	US
42410	PTP-AS	1272	
36024	COLO4-CO - Colo4, LLC, US	1184	US
11042	LANDIS-HOLDINGS-INC - Landis Holdings Inc, US	1122	US
20454	ASN-HIGHHO	1061	US
39729	REGISTER-AS	1044	IT
13768	PEER1	1035	CA,GB,US
24961	MYLOC-AS	1014	DE
12824	HOMEPL-AS	1006	PL
22611	INMOTION-1	826	US
30496	COLO4 - Colo4, LLC, US	818	CA,US
38001	NEWMEDIAEXPRESS-AS-AP	718	
22878	ASACENET1 - ACENET, INC., US	684	US
55660	MWN-AS-ID	683	ID

© Area 1 Security 2016

32613	IWEB-AS	678	CA
10316	CODERO-AS - Codero, US	661	US
23352	SERVERCENTRAL	571	US
32475	SINGLEHOP	570	BG,PA,US
9198	KAZTELECOM-AS	549	
20738	AS20738	542	GB
45753	NETSEC-HK	532	HK
20860	IOMART-AS	506	GB
33494	IHNET	500	US
7506	GMO-INTERNET	471	JP
5588	GTSCE	445	CZ,RO,HU
23456	NO_NAME	445	LT
14618	Amazon-AES-IAD	414	US
6428	CDM - CDM, US	414	US
50673	Serverius-as	396	UA,NL,RU
54290	HOSTWINDS-1	392	US
29802	HIVELOCITY-1	389	US
12876	AS12876	371	FR,GB
20473	ASN-CHOOPA	348	US
29550	SIMPLYTRANSIT	346	GB,IT
30764	PODA-AS	322	
38186	FTG-AS-AP	304	
60376	LEVONLINE-NET	295	
37153	HETZNER-AFRICA-37153	293	ZA
8342	RTCOMM-AS	284	RU
198047	UKWEB-EQX	283	GB
57746	MACOSOFT-AS	265	RO
13147	NETINFO	265	BG
52270	X-Host SRL, AR	261	AR
55293	A2HOSTING-AS	249	US
28299	IPV6-INTERNET	242	BR
30083	SERVER4YOU - Hosting Solutions International, Inc., US	237	US
18229	CTRLS-AS-IN	234	IN
62698		234	
16509	Amazon	231	IE,US
46055	ROKA-AS-ID	227	

© Area 1 Security 2016

13237	LAMBDANET-AS	223	EU
26347	DREAMHOST-AS - New Dream Network, LLC, US	221	US
14259	ASN-GTD-INTERNET	219	CL
53755	INPUT-1	210	US
36352	Colocrossing-AS	209	US
25504	CRONON-AS	208	
29757		207	
31815	MEDIATEMPLE	199	US
54600	PEGTECHINC	198	US
24085	QTSP	196	
32953	MHCV	196	
31034	ARUBA-ASN	196	IT,US
19318	NJIIX-1	188	US
51559	NETINTERNET	186	TR
52048	DATACLUB	181	
8560	ONEANDONE-AS	180	DE,US,ES,GB
8304	ECRITEL-INC	179	FR
6327	ASN-SHAW	172	CA
200000	Ukraine-AS	171	UA
63976	GND2AIR-AU	170	
16265	Leaseweb-Network	169	NL
3786	LGDACOM	167	KR
26094	BTP - Baltimore Technology Park, LLC, US	166	US
19066	WIREDTREE	162	US
33070	RACKSPACE-DFW	161	US
46475	LIMESTONENETWORKS	160	US
45839	PIRADIUS-AS	160	MY
29854	WESTHOST-US	159	US
51167	CONTABO	158	DE
15418	FASTHOSTS-INTERNET	155	
46015	EXABYTES-AS-AP	155	MY
62904		153	
20718	AS_ARSYS-EURO-1	152	
9116	GOLDENLINES-ASN	151	IL
15967	NAZWAPL	149	PL
198414	BIZNESHOST-AS	147	PL
3595	AS-GNAXNET-AS	147	US

© Area 1 Security 2016

© Area 1 Security 2016

Report design by TM
www.weare.tm