# CYBER GREEN RESEARCH PAPER

Prepared on behalf of JPCERT by Invincea Labs

Winter, 2015

## Table of Contents

## Summary

Cybersecurity metrics, specifically for Cyber Health, have long suffered from a lack of statistical rigor. The origin of this omission is multi-fold, including issues in collection, the inability to cross compare data, and a failure to apply normalization techniques. The absence of statistically meaningful cybersecurity metrics prevents the ability to compare organizations, efforts over time, and blocks an effective evaluation of cybersecurity investments.

To address this, we propose the Cyber Green Initiative, a multi-stakeholder effort that at its core is focused on a statistically meaningful evaluation of cybersecurity data. The Cyber Green portal will be a key element of this analysis, utilizing third party data to generate metrics and indicators about global Cyber Health. These statistics will enable an evaluation of cybersecurity investments over time and between countries.

This report outlines the existing state of cybersecurity data collection and metrics, and the problems they have that prevent the derivation of statistical indicators. This report then outlines an approach that could yield such statistics, and then gives technical details of the operation of the Cyber Green portal. This report closes with a brief summary, recommendations for data collection and sharing to achieve the Cyber Green vision, and a list of benefits for the Japanese taxpayers who fund JPCERT, the sponsoring agency for Cyber Green.

## Overview

The modern economy is highly dependent on the Internet, which itself is dependent on information and network security. Threats to the Internet's security and stability can have effects on the global economy. Reports have been made that estimate billions of US dollars per year for the U.S. alone can be tied to Internet security incidents. Recent estimates state that approximately 5 percent of PCs connected to the Internet may be affected by malware.

Central to this concern is how to address Internet security. A number of efforts have been made to attack specific problems such as Conficker and other botnets or to address specific vulnerabilities such as Heartbleed and the Kaminsky DNS bug, and to implement new protocols such as DNSsec. However, such efforts are limited in focus and time, and therefore the rate of Internet security incidents continues to rise.

This report has roots in the hypothesis that the common way of measuring cybersecurity risks, by counting incident reports, is flawed. The flaws arise from the disparity between *symptoms* and *causes*. Addressing symptoms is expensive and never ending; addressing causes is cheaper and longer lasting.

Seeing a parallel to the public health model, this report proposes that Internet security incidents are symptoms of underlying problems, and that by identifying the root causes and treating them we can make large-scale improvements in Internet security. Central to this premise is the idea of an **Internet health level** and what indicators exist to estimate that.

Typical cybersecurity incidents, such as botnet membership, indicate symptoms of larger cybersecurity risks, often a population of unpatched machines. For example, we postulate that when the host became a member of a botnet because botnet code was loaded onto the machine, that code may have been delivered through an exploit of a known vulnerability with an available patch. While we can address the bot executable and remove the host from that particular botnet, unless patching addresses the host's vulnerabilities, this type of incident is likely to occur again. Because of this relationship, we seek to address the risk conditions that lead to hosts becoming infected with bot executables - the known vulnerabilities they possess. System misconfigurations and the lack of security software represent two aspects of this approach in a broader sense.

This report is written from the perspective of informing a Computer Security Incident Response Team (CSIRT, generally equivalent to a Computer Emergency Response Team or CERT) serving a large customer base, for example a national CSIRT. The focus of this report is aid in helping these CSIRTs evaluating the efficacy of their investments in cybersecurity. The other targets of this research are the policymakers who review cybersecurity investment and evaluate any returns on those efforts.

This report is organized in three sections. The first section outlines the state of cybersecurity data collection and gives some insights into the roots of the challenges of performing statistical characterization of the data. The second section outlines a model for how we might relate the data we collect with statistics and indicators that would enable the evaluation of cybersecurity efforts around the world. The third section outlines the technical roadmap of the Cyber Green Initiative.

To study this relationship and understand how to affect its change, a data processing system for Cyber Green will be produced. The Cyber Green process diagram below illustrates the flow of data through the Cyber Green platform, where the data is combined and normalized. A variety of data sources will come together to capture measurements about risks and incidents; Cyber Green does not propose to make its own measurements and will rely on third-party data feeds. Reports will be created based on this data and be distributed to Cyber Green participants and members. Participants will also be able to provide risk condition data through their portals.

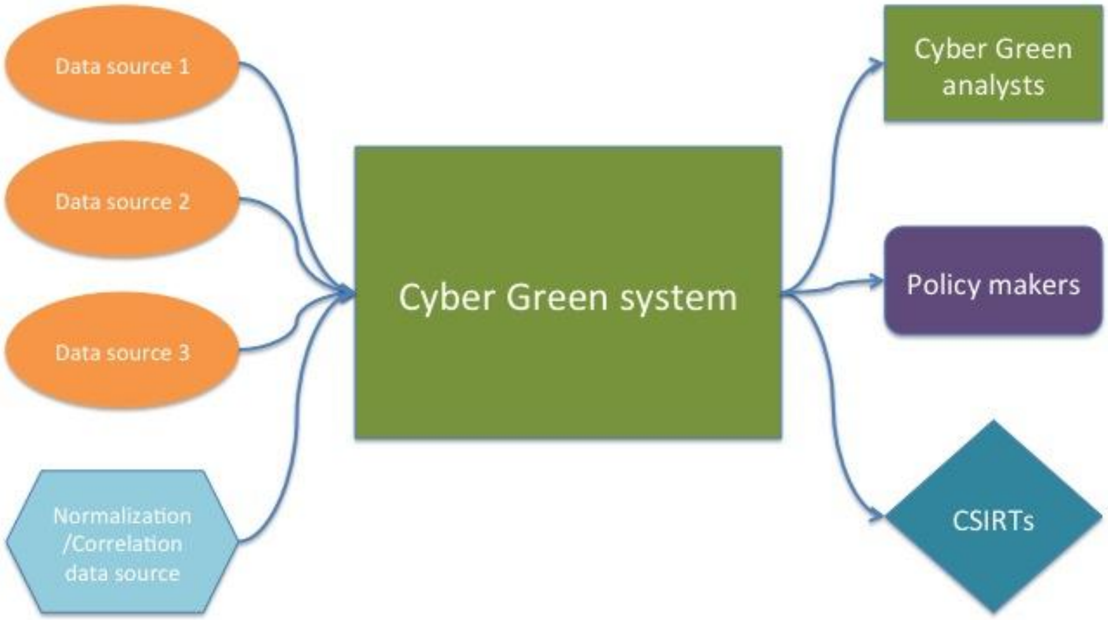


Figure 1: High-level data flow within the Cyber Green Initiative from third-party data sources to CSIRTs, policy makers, and Cyber Green analysts.

## Scope

This report seeks to understand the following questions:

- Firstly, how might we define the risk conditions that lead to cybersecurity incidents? Put another way, when we talk about cybersecurity data, what do we mean? What kinds of data points do we observe and express, how do we classify them, and how do we communicate them to achieve a common understanding?
- Secondly, how might we measure those risk conditions objectively and repeatedly?

- Thirdly, how might we help address them? Our goal is to help create a secure Internet by informing CSIRTs and policy makers about the results of their investments.

## Definitions

Quoting from RFC 2350[1], we find a suitable definition of a **Computer Security Incident Response Team (CSIRT)** that we will use in this report:

> *a CSIRT is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency (see Appendix A for a more complete definition). Any group calling itself a CSIRT for a specific constituency must therefore react to reported security incidents, and to threats to "their" constituency in ways which the specific community agrees to be in its general interest.*

Continuing from RFC 2350, we see the relationship between a CSIRT and their constituency:

> *Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. This is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.*

A **national CSIRT** is a CSIRT that serves a nationwide constituency. Some national CSIRTs may have regulatory authority, may work with police and public security organizations within the government, and generally support a broad body of government, public, and private sector entities for the national benefit.

**Risks** can include misconfigurations, such as insecure permissions, leftover installation scripts, or absent controls. Risks can also include a failure to apply patches for known software flaws, or a failure to implement remediation steps. Example risk conditions include a failure to update antivirus definitions, world readable and writable directories on web servers, or open recursive DNS servers. In most cases these are not intended and, if left unaddressed, can be abused by arbitrary third parties to further unwanted activities.

**Incidents**, in contrast, are the events that occur that are unintended uses, events or misuses of computing resources. While the security industry has labeled many broad incident classifications, they generally fall into two categories: the abuse of the end resource and its data, or an attack to another endpoint through the system. Incidents can include the emission of spam from a botnet infected PC, BGP route hijacks, or website attacks. While incidents can occur as a result of a previously unknown risk, the bulk of Internet-scale incidents occur due to previously known risks.

For the purposes of this report, cybersecurity risk conditions are defined as the existence of conditions that are often abused by attackers to carry out attacks. These risks typically arise from misconfigurations or known vulnerabilities that remain unaddressed. Risk conditions are sometimes an element of incidents, and can be measured and quantified. Cybersecurity incidents can be defined from RFC 2350 as “any adverse event that comprises some aspect of computer or network security”. Incidents can be quantified and measured.

# Part 1: Existing Cyber Security Measurement Efforts

At present, a wealth of cybersecurity data is gathered and made available. Much of the data is centered on counting incident sources, infected hosts, or identifying malicious servers on the Internet. However, this data lacks the necessary rigor for statistical purposes for the reasons outlined below.

Definitions are crucial to this effort but lack standardization. The criteria and definition of specific incident types, however, is largely driven by ad-hoc consensus within the community and not through any formal lexicon such as the MAL from CMU/SEI[34]. Sometimes the definitions are adopted from advisories or other publications. For the purposes of this report, we will use broad subjects when necessary.

## State of the Practice

### Existing data collection methods

#### Direct observation

The direct observation method is to look at the traffic or payloads being captured and to inspect them, classify them, and count malicious or unwanted traffic. This can be done by looking at normal payloads or traffic and trying to detect malicious payloads or traffic. This approach yields the highest confidence in the observations because the full context is available. Direct observation also yields the most information about the incident because the full event is visible.

#### **Indirect observation**

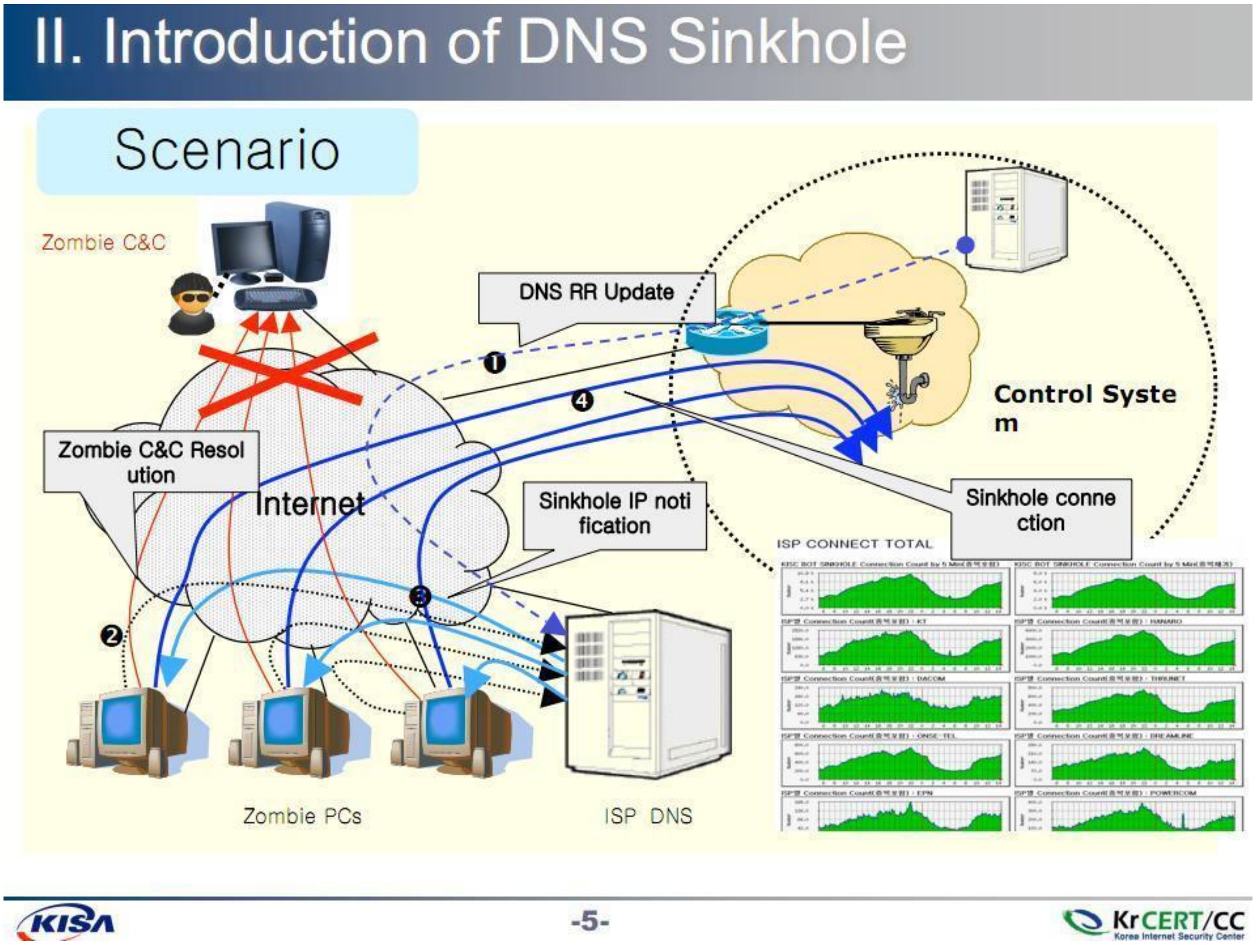
The indirect observation techniques utilize replies or other failures to classify an event based on *inference* of what could have caused it. Because of a guaranteed imperfect view, indirect methods can only yield a lower bound of the number of events of a specific type. Finally, indirect methods typically yield less data than direct measurement methods due to the way that the reply traffic is generated.

#### Data Collection Systems

#### ***Sinkholes***

One of the most popular ways to detect hosts infected with known botnet software (“bots” or “zombies”) is to create a traffic sinkhole to one or more of its command and control (CnC) servers, where the infected computers would connect to receive updates[48]. Sinkholes can be set up using web servers, for example, and record the traffic coming to them. Because of the redirection, typically done using DNS names that have been taken away from the attacker, the bots will send a communications message to the sinkhole, which records the client IP address along with the timestamp to generate a report of an infection. Typically, a domain name is used by only one type of botnet software and rarely for legitimate purposes, so the client connection is an indicator of an infection. Many sinkhole operators then sell this data to businesses and networks that wish to learn of their local infections for remediation purposes.

Figure 2 shows the common model of sinkhole operation.


II. Introduction of DNS Sinkhole

Scenario

Figure 2: DNS-based redirection for a sinkhole to detect botnet membership. From http://cdn-static.zdnet.com/i/story/13/39/307357/sinhkhole.jpg

### *Honeypots*

Honeypots are another source of infected host data that some providers use[49]. A honeypot is a system set up to resemble a legitimate resource to interact with attackers and record their behaviors. Honeypots exist to mimic many types of systems, including web servers, login servers, and even industrial control systems. Many honeypots are contacted by infected PCs trying to propagate their activities. Similar to a sinkhole, a honeypot operator can record the connections made to their honeypots and sell that data to customers who wish to learn about local infections.

A key limitation of a honeypot is that they rely on the attacker finding them and spending considerable time with them, revealing their intentions and techniques. Honeypots have found great success in malware and botnet identification, where the infected PCs try and spread to as many hosts as possible.

### *System Alerts*

Live system alerts including antispam (email, web forum comments included), network IDS sensors provide another rich data source for alerts to sell to customers. A canonical example of this is Microsoft's Smart Network Data Services (SNDS)[15], which has been in use for many years. Through their cloud email services Microsoft is able to see many Internet spam origins. They use the SNDS service and allows for domain postmasters to sign up and receive reports of spam emitters from their networks.

### *Malware Analysis*

Automated web and executable malware analysis provides another rich source for data providers. Through the large-scale analysis of thousands of malware samples a day, many threat data providers are able to identify the servers involved in spreading malware and controlling infected PCs. One of the primary purposes for this line of business is to generate data feeds for third parties to receive information about problems in their network, and also to generate outbound block lists for their firewalls, IDS systems, and DNS servers.

This data source yields the command and control addresses and URLs for malware, malware payload sites, and the sites and addresses where malware uploads stolen information.

Shadowserver's daily reports provide excellent examples of this data generation. Their sandbox systems produce a daily report of malware IRC command and control servers, which ties together malware by hash (MD5, a unique identifier of a binary) with the IRC server information such as port, hostname, IP address, channel and key, and additional information. A similar report of the URLs contacted by malware is produced every day. Zeus malware, for example, sends stolen data to a remote web server. Shutting down these servers can render the bots ineffective. Web-based DDoS bots also uses an HTTP server to coordinate attacks, a server that is revealed through malware analysis. This data can be useful in both botnet tracking and also in creating an egress block list. Shadowserver also produces reports for email addresses, which are often used to send information stolen from the infected PC to the attacker.

### Server misconfiguration surveys

Server misconfiguration surveys have been a mainstay of Internet security for many years. Historic examples include the Smurf Amplifier Registry[2] from 1998 and onwards, used in identifying systems that can contribute to DDoS attacks, and the Spam and Open Relay Blocking System (SORBS)[3] begun in 2002 to combat spam-friendly misconfigured SMTP servers. Recent examples include the OpenNTPProject[8] that tracks network time protocol (NTP) servers and the OpenResolverProject[9] that tracks open DNS servers that may contribute to DDoS attacks. Project Sonar from Rapid7[50] is another such project that performs Internet-wide scans to identify services that could be abused for amplification attacks or information leaks. More general misconfigurations, such as improperly managed permissions on web servers, can be difficult to measure reliably. While they contribute to increase Internet risk, they remain unquantified.

### Vulnerability surveys

Vulnerability surveys are carried out from time to time to estimate the remediation of large-scale bugs. Notable examples include the patching around the Kaminsky DNS bug[51] from 2008 and the OpenSSL Heartbleed bug[11] from 2014. However, this data is rarely systematically measured and made available. Only a handful of global-scale risks ever get surveyed at scale and for a significant duration (to measure remediation rates), making estimation of the accumulated risks difficult to assess.

## Current cybersecurity measurements

The table below summarizes the major types of data collected, the method by which it is collected, and the output of that measurement.

| Measurement | Method | Informs |
|---|---|---|
| Botnet membership | Direct (sinkhole) | Members of specific botnet |
|  | Direct (peer to peer enumeration) | Members of specific botnet |
| Scans and probes | Direct | Hosts trying to look for possible propa.gation points |
|  | Dark address space | Hosts trying to look for possible propagation points |
| Spam | Direct | Source hosts for spam |
|  | Dark address space | Source hosts for spam |
| Malicious links | Web crawls | URLs for drive-by download exploits |
|  | Spam inspection | URLs for drive-by download exploits |
| Phishing sites | Spam inspection | URLs for drive-by download exploits |
| Denial of service | Direct | Attack type, duration, intensity, victim, sources |
|  | Command tracking | Attack type, start time, intended victim, responsible botnet |
|  | Dark address space (backscatter) | Attack type, duration, intensity, victim, sources |
| Malware samples | Direct | Number of unique malware samples by hash, families |

*Table 1: Measurement methods for cybersecurity and the data gathered by each method.*

## Problem of cybersecurity and metrics

Current practices in cybersecurity measurement, which is incident-centric, have many flaws that prevent true metrics and comparisons from occurring. These problems can be largely grouped into two categories: a lack of clear, consistent and transparent standards, and methodology problems.

### Problems due to a lack of standards

Definitions remain one of the key challenges in sharing cybersecurity data. Many of the types of abuse noted are either subjective or have cultural or national definitions that vary from place to place. An example is spam. Every user and every vendor has slightly differing definitions of what constitutes spam. Similarly, "potentially unwanted software" is a broad category of software that covers executables that virus scanners would not otherwise indicate, but due to policy or personal preferences some users do not want on their machines.

Similarly, a lack of standard definitions for measuring events plagues cross comparisons between data sources. For example, scan and probe detection can be done in a variety of ways with no clear standard, and often data sources do not report how they captured the data or what settings they used as thresholds.

A lack of malware name standards has long plagued the cross comparison between vendors' lists of malware in the wild. One effort to standardize this was the Common Malware Enumeration (CME)[14], an effort organized by the MITRE Corporation. CME was intended to give a unique identifier to every malware family and provide a vendor neutral means to understand cross-references. While it never succeeded in its mission, it highlighted the growing problem of vendors' unique names causing confusion. This manifests itself when network defenders receive an alert referencing one name when their vendor of choice uses another.

## Problems due to measurement methods

While we can remotely measure cybersecurity issues such as vulnerable websites and compromised hosts, there remains ambiguity in detection, which can also lead to confusion. Detection in this scenario can refer to probes sent from a measurement node, such as a scan or a sweep of a network. A sensor may be a device in the middle of a connection, such as an intrusion detection system. A sensor may also refer to a server that collects inbound queries from hosts, such as a web server or a sinkhole.

Remote sensors have limitations imposed on them by the designers, often to comply with the law or other potential complications such as crashing the remote host, and also just timeliness - an exhaustive scan of a website to find all potential vulnerabilities could take a very long time. A typical scanner may try and determine a remote application version based on an advertised banner or a vendor supplied mechanism, but will often not test for the presence of a vulnerability through an exploit because to do so would cause undue risk to the system's stability, for example. Because of this, remote sensors typically make inferences about vulnerable conditions with as little information as needed; they often infer the presence of a known vulnerability based solely on the version information presented.

Finally, vantage points matter. For passive sensors, being globally visible and covering a wide enough portion of the Internet is crucial to ensure complete measurement[52, 53]. For active sensors, ensuring that the destinations are reachable and not blocked is crucial to obtain a complete measurement. In both cases unless the site performs active testing or statistical analysis of the data, the accuracy of measurement will remain unknown. This means that the data may not reflect reality, preventing cross comparison with other data sets.

## Network Factors Affecting Measurement

One of the key factors to assessing the coverage of cybersecurity measurements is a baseline value to measure against, ideally reality. This "ground truth," or actual data about the number of infected machines or systems at risk, is typically missing or inaccessible, making the evaluation of coverage impossible[28,56]. We know that two major factors affect measurement: NAT deployments and DHCP address assignments.

### NAT Effects

Network address translation (NAT) thwarts accurate remote measurements in two ways. Firstly the NAT device maps all IP addresses behind it to a single globally unique IP address, leading to undercounting. Secondly the NAT device will not let in any traffic to any IP address behind the device (from a remote perspective) without a circuit having been built. This means that vulnerable host surveys will mistakenly undercount vulnerable systems.

Some theoretical and limited work has been done to develop methods to count hosts behind a NAT device. Bellovin introduced the concept of using the IPID field as a means to disambiguate hosts behind a NAT device[25]. In this model, each host's TCP/IP stack begins at a unique IPID value and increments it at a different rate. By observing the IPID values of traffic from an IP address, distinct patterns emerge for each unique host behind the NAT device. As shown in Figure 3 the IPID values wind up making distinctive lines when plotted by packet arrival time.

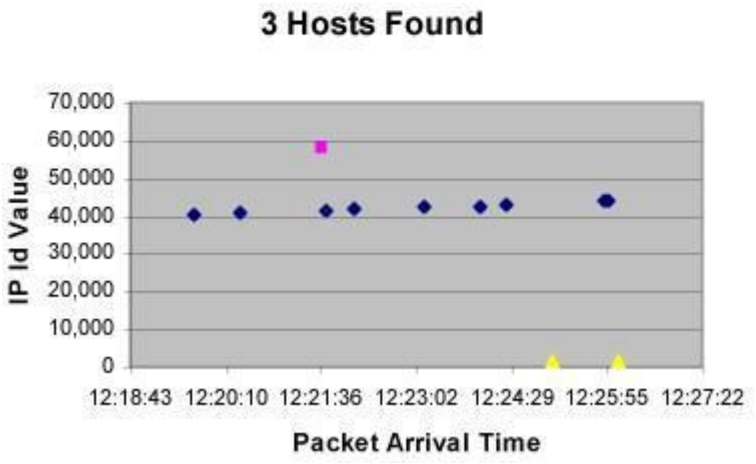


*Figure 3: Using IPID values to count hosts behind a NAT device. From http://www.sflow.org/detectNAT/images/chart.jpg*

Krmicek *et al.* introduced another NAT host counting method that uses TTL values, IPID and TCP SYN sizes[29]. Maier further modifies this by looking at the HTTP user-agent header value and is able to further disambiguate the number of hosts behind a NAT device.

Work by Maier[27] to characterize residential broadband networks shows that on residential networks 90% or more hosts are behind a NAT device, but only 38% manage more than one device. This number compares favorably to the work by Casado and Freedman[26] who found that 50% of NAT devices house at most 2-3 devices. Obviously some large NATs exist, but are extremely rare according to these two measurements.

### DHCP Effects

Dynamic host configuration protocol (DHCP) thwarts accurate remote measurements by leading to possible over counting through IP address reassignment. DHCP lease times vary around the world and from network to network, and depending on the survey duration. A single affected host could appear multiple times during the data collection. To address this many population estimates, especially botnet measurements, use a 24-hour window to perform population estimates[54,55]. As the number of networked devices has grown and IPv4 remains in widespread use, DHCP pressures have only grown.

With mobile systems, either mobile phones and tablets or mobile hotspots and dongles attached to laptops, the DHCP and NAT problems are only magnified. Mobile networks can be “oversubscribed” - meaning the ratio of devices to globally unique IP addresses available - at ratios over 100:1.

### Correcting Measurements

Few data providers do any analysis of their measurements to account for NAT or DHCP effects. Shadowserver[54], for example, ignores these effects and instead publishes the number of unique, raw IP addresses that trigger a specific event per day. This is not an uncommon approach in the industry.

## Incident Data but No Precision

Fleming and Goldstein[46] note many of these problems, and concur that this imprecision is what leads to a failure to generate statistics. While they focused on a narrow question - does information sharing decrease incident severity and count - the issues they note that plague the cybersecurity measurement community are the same ones that affect the generation of global statistical indicators.

## Part 2: A Model for Generating Cyber Health Statistics

Part 1 explored the current state of the practice in cybersecurity measurements, and explained some of the origins that prevent the generation of robust statistics about cybersecurity. In Part 2 we develop a model that we feel can provide both statistically meaningful cybersecurity data and highlight the underlying risk conditions that yield these incidents.

## Risk and Incident Relationship Model

Core to the premise that we can measure and affect Internet health is the idea of the risk and incident relationship. While people cause incidents, it is risk conditions that lead to almost all incidents. Risks provide the conditions necessary for incidents to occur.

Applying the public health model to Internet security, epidemics provide an interesting framework in which to think about Internet risks and incidents. Using malaria as an analogy, we can think of a malaria infection as an incident, and the conditions that allow for mosquitoes to breed and bite people as the risk conditions.

Risks and incidents have a *cause* and *symptom* relationship. Risks create the root causes by which incidents can manifest themselves. While some symptoms have multiple causes, addressing a cause should affect the rate of symptoms.

### Historic Examples

History can provide some illumination of the relationship between risks and incidents. Two large-scale efforts at reducing the risk conditions and symptoms are anti-spam efforts and anti-DDoS efforts. These efforts highlight how the relationship between *symptom* and *cause* can be applied to affect incidents by addressing the cause.

Anti-spam efforts in the late 1990s and early 2000s focused on mail server infrastructure, specifically open SMTP relays[3] that sent mail for any part regardless of authority, and open TCP port 25 which enabled compromised systems to send mail directly to a target's SMTP server. In both cases the conditions were relatively easy to measure; indeed registries of open SMTP relays and networks that allowed for outbound TCP port 25[62] were created and used by many mail server administrators to reject inbound mail as likely spam. Between network configuration changes by large providers blocking TCP port 25 outbound together with vendor changes that disabled open SMTP relays by default made a significant impact on the spam landscape. Spam from networks that block port 25 outbound went down significantly, and spam sent through open relays also dropped significantly. The spam emitter landscape was forced to compensate by migrating to botnets.

Similarly, denial of service (DDoS) attacks that relied on ICMP echo amplifiers in the "Smurf" attack were a nuisance in the late 90s[2]. To combat this, a small number of network operators began to test addresses for the misconfiguration condition and created the open Smurf amplifier registry. This list was used in conjunction with secure configuration templates to contact site owners to address the problem. From thousands of open Smurf amplifiers in the registry the number is now much smaller, and Smurf attacks are no more.

## Applying Root-Cause Analysis to Internet Health

These two efforts suggest that applying remediation to the root cause of global cybersecurity situations can lead to a tremendous impact when the root cause is addressed, greater than simply treating the symptoms. Furthermore, because the underlying cause is addressed, multiple symptoms may be addressed for a longer period of time, which can also lead to a cost savings.  A larger set of relationships between symptoms (for example attacks), causes and root causes (second order causes) is below. For reference, the example of malaria is shown first showing the relationship between the disease, mosquitos and swamps.

| **Symptom** | **Enabling factor or transmission vector** | **Root cause** |
|---|---|---|
| *Malaria* | *Mosquito (transmission vector)* | *Swamps (mosquito breeding grounds)* |
| DDoS | Amplifiers | Misconfigured servers |
| | | Lack of access control lists at the application layer |
| | | Source IP spoofing is possible |
| | Bots | Lack of patched hosts |
| | | Misconfigured servers |
| | | No AV on endpoints |
| Spam | Open relays | Misconfigured servers |
| | Bots | Lack of patched hosts |
| | | Misconfigured servers |
| | | No AV on endpoints |
| Drive by downloads | | Unpatched servers |
| | | Misconfigured servers |
| | | Rogue DNS names |
| | | Weak passwords |
| Phishing sites | | Unpatched servers |
| | | Misconfigured servers |
| | | Rogue DNS names |
| | | Weak passwords |
| Bots | Unpatched PCs | Pirated software |
| | No AV | Pirated software |
| Exploit attempts | | Bots |
| | | Humans |
| Port and host scans | | Bots |
| | | Humans |

*Table 2: Relationship between Internet risks as causes and root causes, and incidents. The malaria example is shown as an illustration of the relationships of enabling factors.*

Zhang *et al.*[32] examined the correlation between mismanagement and maliciousness. For their purposes they defined mismanagement as a lack of following best practices across a variety of externally testable parameters such as open recursive DNS resolvers, DNS source port randomization, and untrusted HTTPS certificates. They measured maliciousness by looking at externally measured symptoms as indicators, such as spam rates, phishing and malware, and active attacks. Their findings are that the correlation between some indicators of the quality of network management is stronger than others, but overall mismanaged networks are likely to show signs of abuse and victimize third-party networks when normalized by IPv4 address space. The paper examines possible root causes such as country GDP, network customers and peers and finds some correlation there, but does not delve deeper into the relationships between these factors and mismanaged networks.

The Zhang paper, however, strengthens the hypothesis that the relationship between symptoms and management is real, and that the application of best efforts to network management should have a positive effect on the symptoms emanating from the network. This research suggests that the hypothesis of the Cyber Green project is valid. We seek to extend that line of work in time, scope, and participation to affect Internet health levels.

## Useful Cyber Health Statistical Markers

Insights into the scope and severity of issues will be highlighted through a number of analyses of the data once it has been normalized. All of these statistical analyses are based on population analysis methods from other sciences. When appropriate, the analysis will assume *constant* growth or decay rates.

### Specific Incident Doubling Time

The growth rate of issues and problems is a key insight the Cyber Green portal can highlight. When coupled to the population estimate of an incident type, the growth rate can be used to highlight problems that are likely to grow bigger. Some botnets and malware infections have doubling times on the order of days or, in the case of the Witty[57] and SQLSlammer[58] worms, minutes.

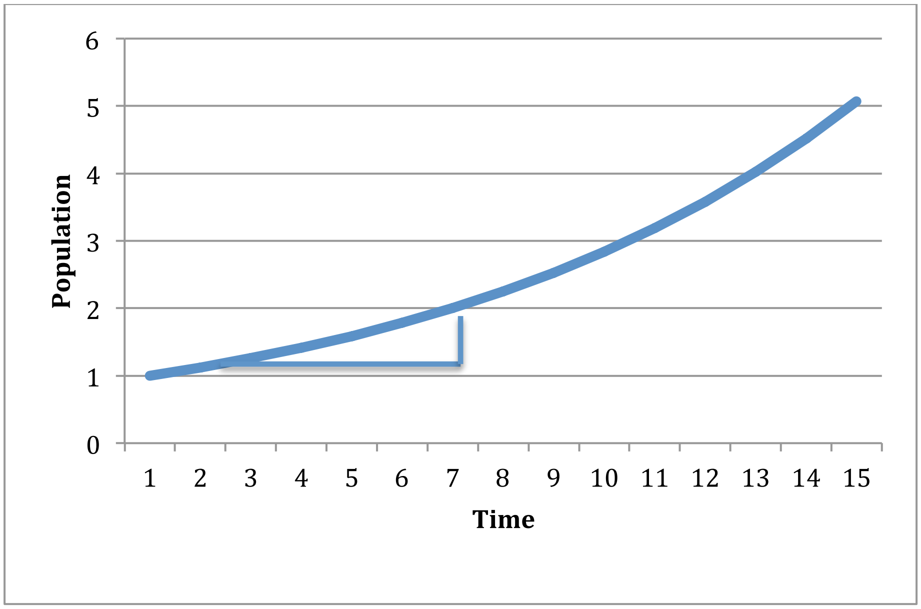


*Figure 4: Doubling time illustration showing how fast a population can grow, and how to visually estimate the doubling time.*

Using the following equation[59], we can calculate doubling times from using population data per issue (e.g. per-distinct malware infection or per-issue type) over time:

$$T_d = (t_2 - t_1) * \frac{log(2)}{log(\frac{q_2}{q_1})}$$

for quantities $q_1$ and $q_2$ at time points $t_1$, $t_2$.

The insights this analysis would yield would be to identify which regions of the Cyber Green community are likely to be facing massive issues of potential risk, and how best to address them. It would also help yield insights into the efficacy of preventative measures. Of interest would be the doubling time for specific infections per country when compared to ICT and CSIRT education budgets, software piracy rates and endpoint security installation rates.

## Specific Incident Half Life

The half-life of a population is defined as the time it takes for a population to decrease by half, and is useful for large populations over a long duration. This measurement is especially useful for populations such as botnet membership or malware infections. For example, through graphical analysis of the Conficker sinkhole data, early on in the malware's response time (in early to mid 2009) the half-life of the Conficker botnet was approximately 300 days. The data that would be used to measure this value would be malware populations through sinkhole efforts and also vulnerability population measurements. The populations by issue by day are used to feed into this analysis.

The equation to calculate a half-life[60] is given by

$$t_{1/2} = e^{-kt}$$

where *e* is the natural logarithm, *t* is the time elapsed, and $t_{1/2}$ is the population half life. The half-life can be calculated using the time series data of a specific measured problem; individual problems would be measured separately.

The purpose of this analysis is to provide insights into how fast the community is responding to pressing issues such as vulnerability populations, malware infections, or major botnets. A low half-life is a desired value, hopefully on the order of days not months.

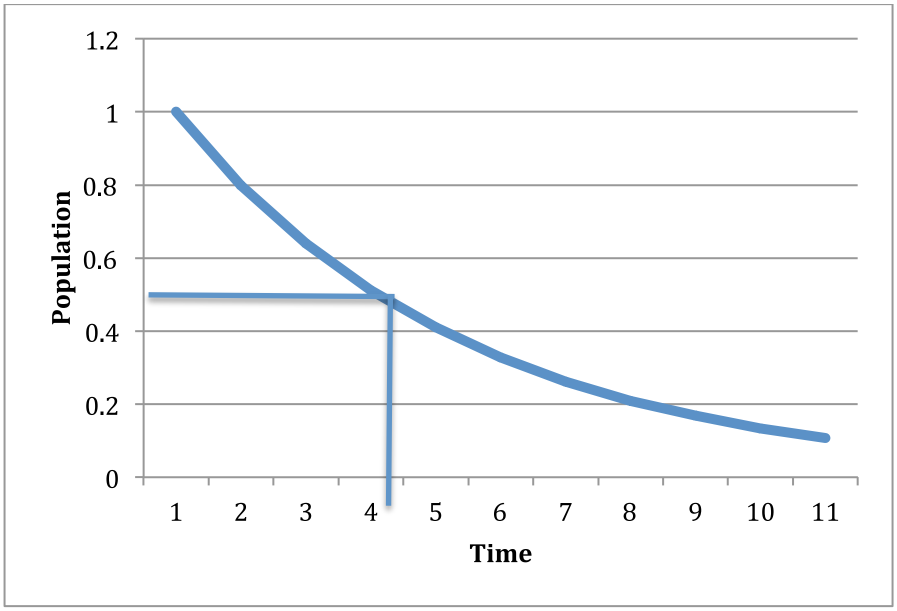


*Figure 5: Half-life illustrated through an example population decay measurement. A graphical solution is shown from the Y-axis to the X-axis to yield the approximate half-life.*

Second order analysis of the half-life can be performed after some time to yield insights into any improvements into the efficacy of responses. By analyzing a series of half-life measurements over time, we can gain insights into how effective global and CSIRT eradication efforts are - and if we are improving our eradication efforts. A desired outcome would be a falling $t_{1/2}$ rate over time, showing that the cycle of identifying problems and deploying counter-efforts to the affected populations has improved.

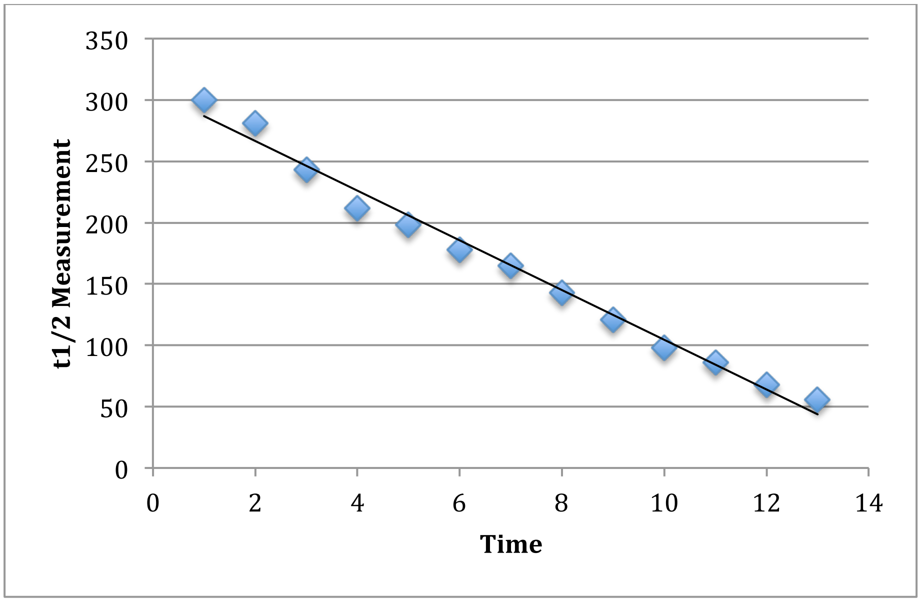


*Figure 6: Second order analysis of $t_{1/2}$ rates over time, hopefully showing a decrease as time progresses.*

Because Cyber Green is measuring the rate of incidents such as infections and vulnerabilities that require remediation, a half-life measurement is a practical, valuable statistical tool to gain insights. Both the first and second order analysis can be used to measure response rates for various infections and issues. Correlations between the $t_{1/2}$ value and ICT or CSIRT budgets to determine what kind of impact such efforts have on addressing infected populations. An additional correlation to look for would be high $t_{1/2}$ values and high software piracy rates or low AV adoption rates to assess the impact of those behaviors on applying vendor remediation steps.

## Mean Time to Resolve Incidents

One of the insights that Cyber Green can yield is the response rate of various countries, or even providers within countries, through the captured data. One statistic that can be used to measure this response rate is the mean time to resolve (MTTR) these issues. This measurement is done by looking at the active lifetimes of issues grouped by specific issue and by country, for example the lifetime of phishing sites in the US. The lifetime of an issue can be calculated by taking the difference between the last observation of a specific issue (such as a phishing URL) and the first observation of that same issue. This list of lifetimes is then analyzed to find the mean lifetime, giving a mean time to resolve. This lifetime should be a measure of the complete cycle of issue genesis, discovery, notification to the appropriate party, and resolution of the issue. Note that the data captured does not contain any information about when the responsible parties were notified. As an example, previous work in 2008 by the author at Arbor Networks found that globally, fast flux domains had a mean lifetime of 18.5 days[61].

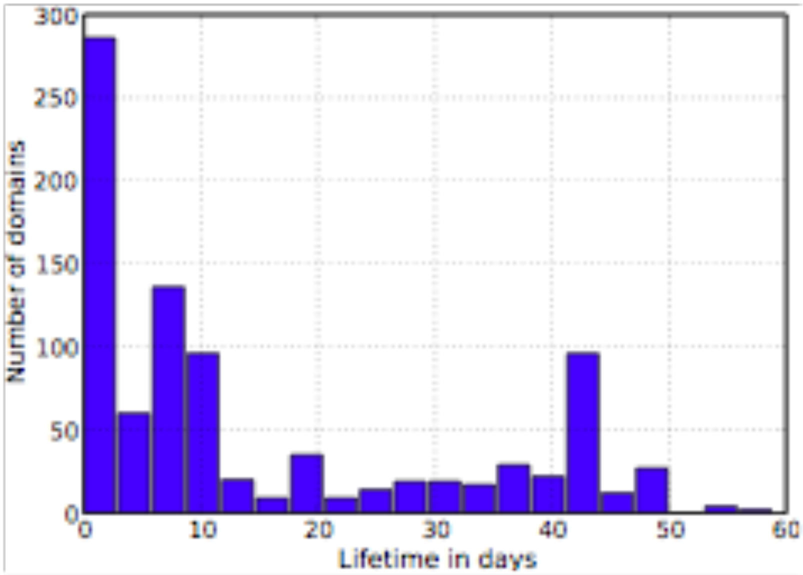


*Figure 7: Fast flux botnet lifetimes from [61] using data from Arbor Networks' ATLAS observatory. The mean time to resolve the fast flux domain, based on the domain's active lifetime, was 18.5 days globally.*

The utility of this measurement is to assess how rapidly various CSIRTs are responding to the attacks on their infrastructure through the abuse of their resources. CSIRTs with low MTTR values, even if they have a high incident count, show effective detection and response mechanisms. It would be interesting to look for any correlations between MTTR values and ICT or CSIRT budgets.

## Target Cyber Health Indicators

In economics, two major kinds of indicators are used to understand the world: leading and lagging indicators. Leading indicators are metrics that appear before environment or condition changes; leading indicators can be used to predict changes and trends. Lagging indicators, in contrast, are metrics that change only after a change has been made; lagging indicators confirm trends but do not predict them. In cybersecurity, lagging indicators could be derived from incident data. For the purposes of Cyber Green, these indicators will be useful in assessing cybersecurity investment efforts. Positive movement of lagging indicators such as incident counts per capita can be used to confirm that cybersecurity efforts are working as intended.

The Cyber Green Initiative does not plan to gather its own data but instead rely primarily on third parties for their data. This requires that the data be well understood to ensure proper merging with related data sets, and a proper merging to avoid counting duplicate observations. From this we can combine the data as shown in Table 2 and yield an understanding of the risk landscape, and from there begin to generate target indicators of cyber health.

## Cyber Health Level Measurement

No single value can adequately capture the health levels of the Internet, it is a concept with a number of different dimensions. However, a combination of values can reveal the status of the Internet per quarter. The three high-level measurements in this section are *aspirational*, meaning we cannot yet achieve them but we are aiming to calculate them. As such, these metrics serve as guides to indicate what data to gather and how to combine that data to yield measurements and insights.

Looking at the WHO website, their "Data and Statistics"[42] page reveals three key indicators about global health and the effect of actions and policy on public health and safety. Cyber Green's goals are similar, and we should be able to distill cyber health into a handful of key metrics that reveal the impact of investment efforts and the potential for major incidents. The values that could serve as Internet health indicators include:

- **Percent traffic that is made of unwanted traffic**. Unwanted traffic is broadly defined but includes spam and attack traffic, anything the system was not designed to explicitly handle. Example results include: in 2008, Arbor Networks suggested that approximately 2-3% of Internet traffic was attack traffic[43,63]; in August, 2014, Senderbase shows that approximately 14% of mail is legitimate compared to 85% that is spam[44]. This metric over time should reveal the balance between wanted and unwanted (spam, attack, etc) traffic.
- **Percent of the Internet population that is infected with malware.** This can include the fraction of websites that are being abused for attack traffic and botnet infection rate estimates. This metric over time should reveal the effect of efforts to combat infections.
- **Percent of the Internet population that is vulnerable and creates a risk for other Internet users.** This can include the fraction of systems vulnerable to major, high profile issues such as Heartbleed[11] or the Kaminsky attack[51], or PCs and common vulnerabilities. This statistic may be difficult to gather with currently available data. This metric over time should reveal the risk profile of the Internet and the success of efforts to lower risk conditions.

Much of the data we are able to gather shows incident counts, but is based on factors such as externally visible IP addresses or partial views of the Internet. As such, these values do not represent absolute numbers but instead relative numbers; more importantly, their relationship to any ground truth is unclear and constantly changing. *Trends* are more accessible, therefore. If we assume that the measurement methodologies remain largely constant, we can watch the changes in the values over time to assess impact of investment efforts.

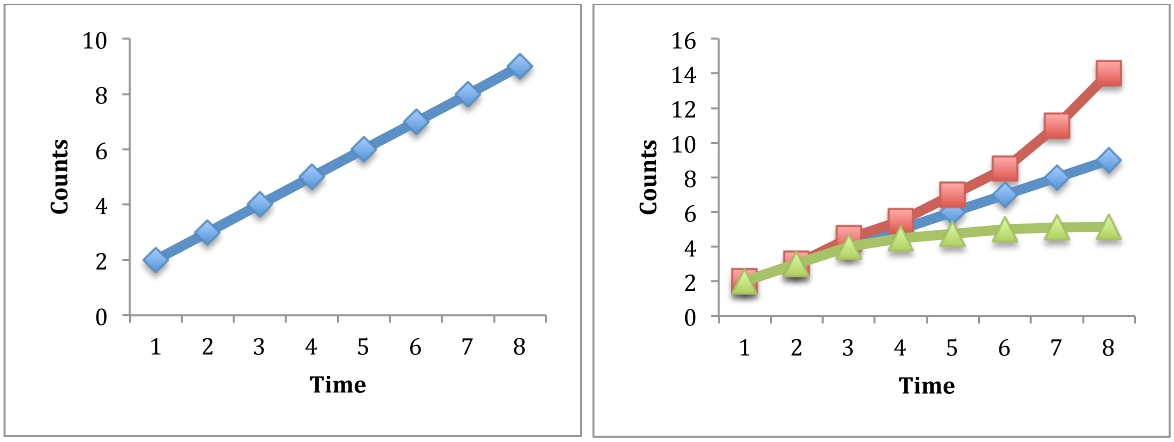


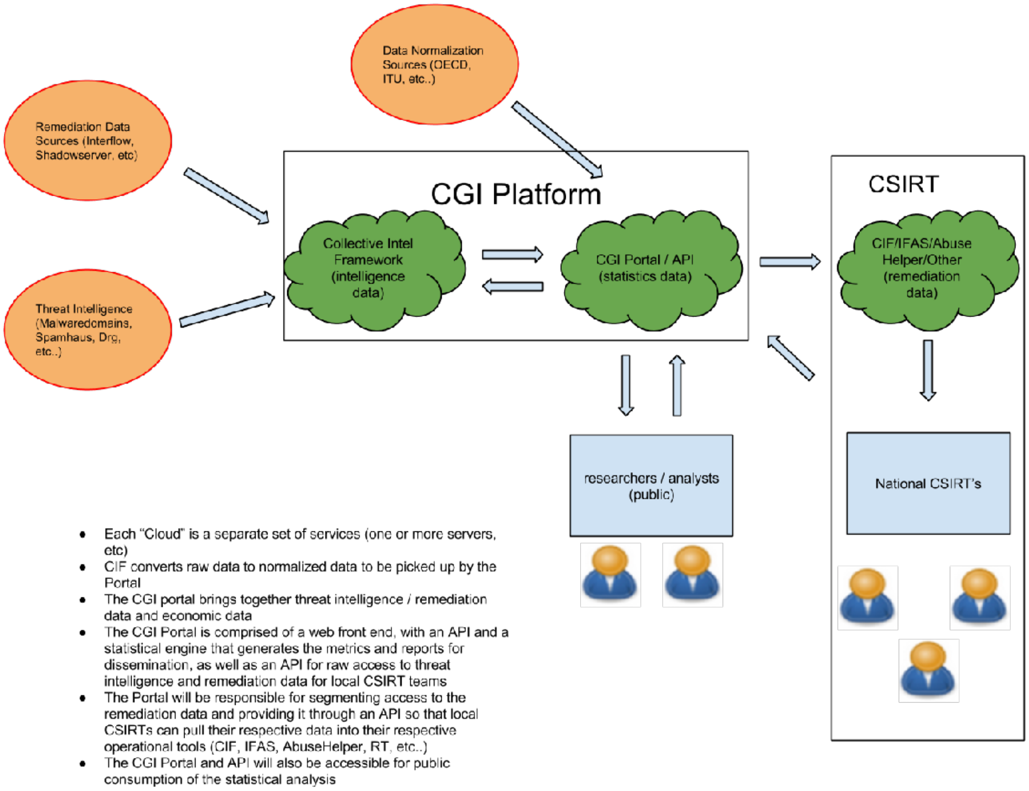
*Figure 8: Interpreting metrics to understand trends in global cybersecurity metrics, after normalization, for a hypothetical data set. In the left-side figure, the original trend line is shown. In the right-side figure, two new lines have been added. The curve that continues above the original trend line shows that the problem is getting worse (after normalization) by growing at an increasing rate. The bottom line shows that despite the continued movement upwards, it is growing more slowly than the original trend line would have predicted, suggesting some progress is being made against that aspect of cybersecurity.*

Trends are useful because we can extrapolate them in the near future and use that extrapolation to understand the impact cybersecurity efforts. Figure 8 shows how we might interpret these trend lines. The upper panel shows the original trend line for a growing problem, while in the lower panel two lines diverge from the original trend line. The upper line would be expected if the problem is growing in intensity, that is growing faster than the expected rate; the lower line shows the problem growing more slowly than expected, perhaps even dropping. This is how we can use trends in cybersecurity to assess investments and understand what works and what investments failed to affect the needed change.

Cybersecurity Health levels are thus a combination of these values. For example, a healthy Internet would have lower attack traffic rates than historic norms (and trends that continue downward), along with low infection rates and high current patch rates. An unhealthy Internet would have growing attack traffic rates, growing infection rates and low patch rates, all suggesting future attacks could grow worse.

## Part 3: Cyber Green Technical Overview

With the goals broadly outlined in Part 2, we can now walk through the Cyber Green system that is designed to generate statistically robust indicators about cyber health. The Cyber Green portal is a web-based system that collects data from multiple sources, combines them, and yields statistical indicators from this data. As shown in Figure 1, data is then made available to CISRTs, policy makers and Cyber Green analysis in the form of raw incident data and reports. Figure 9 below shows a more detailed data flow within the system.


Data Normalization Sources (OECD, ITU, etc..)
Remediation Data Sources (Interflow, Shadowserver, etc)
Threat Intelligence (Malwaredomains, Spamhaus, Drg, etc..)
CGI Platform
Collective Intel Framework (intelligence data)
CGI Portal / API (statistics data)
CSIRT
CIF/IFAS/Abuse Helper/Other (remediation data)
researchers / analysts (public)
National CSIRT's

- Each "Cloud" is a separate set of services (one or more servers, etc)
- CIF converts raw data to normalized data to be picked up by the Portal
- The CGI portal brings together threat intelligence / remediation data and economic data
- The CGI Portal is comprised of a web front end, with an API and a statistical engine that generates the metrics and reports for dissemination, as well as an API for raw access to threat intelligence and remediation data for local CSIRT teams
- The Portal will be responsible for segmenting access to the remediation data and providing it through an API so that local CSIRTs can pull their respective data into their respective operational tools (CIF, IFAS, AbuseHelper, RT, etc..)
- The CGI Portal and API will also be accessible for public consumption of the statistical analysis

*Figure 9: Cyber Green process diagram showing data flow through the system.*

# Cyber Green Design

## Data Aggregation Methodology

Data will be aggregated into the following buckets for each type of incident or metric, as well as any further breakdowns available such as botnet family.

1. Unique IP addresses seen per day. In the absence of device counts, and owing to dynamic or mobile addresses, a count of unique IP addresses seen per day is a commonly accepted metric. Example values would be "186129 unique IP addresses seen in the Conficker sinkhole in the past 24 hours, 2962 unique IP addresses seen in the Qakbot sinkhole in the past 24 hours, etc".
2. Unique IP addresses per country per day, using geolocation services such as MaxMind or Quova to do the mapping of an IP address to the country. Example values would be "8761 unique IP addresses seen for Colombia in the past 24 hours, 21986 unique IPs seen for the United States in the past 24 hours, etc".

While these aggregations do not permit measurement of the absolute number of affected subscribers, devices or installations, the trend of these numbers over time and between entities can be useful. These aggregations permit normalization using external data about per-capita statistics for each country.

## Data Normalization Methodology

The Cyber Green portal will collect raw measurement data about incidents and risk conditions and then perform transformations of that data on demand as part of its reporting. This transformation will include normalization, which will permit cross comparisons between countries and over time. The choice of the normalization parameters should reveal both where problems lie, both in terms of locations and sub-populations, and also indicate the scale of effort required to affect measurements. As noted above, because we were unable to find global, updated data sets exist for the number of online devices we cannot normalize against that value. Instead we will normalize data against meaningful and available statistics from outside parties: the size of the Internet connected population and the number of Internet connections per country.

Normalization will occur with the appropriate timeframe of the data; for example 2014 data sets would be normalized against the 2014 statistics from the ITU on Internet subscriptions by country.

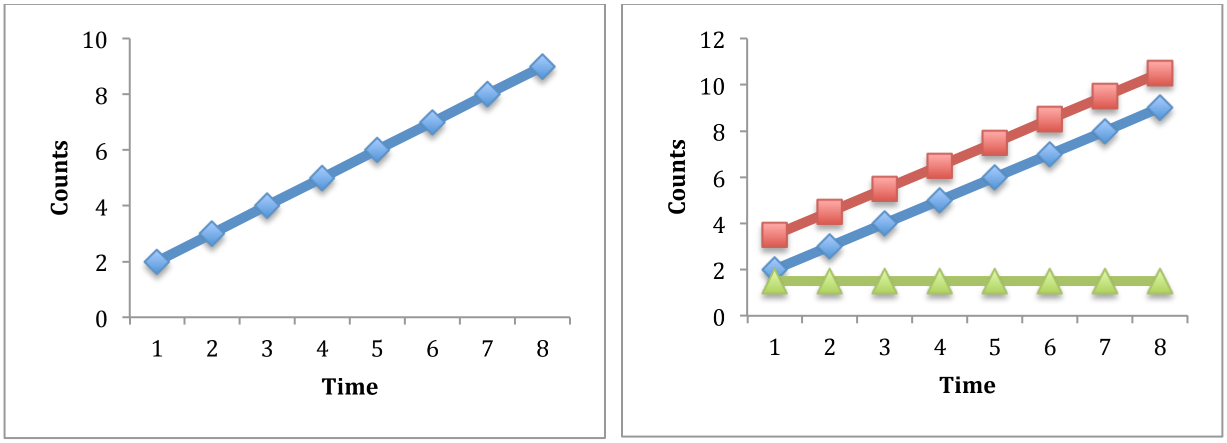


*Figure 10: Value of data normalization with a hypothetical data set. In the top figure, the raw trend line indicates a growing count of events. Once we also plot the population (e.g. devices, Internet subscriptions, or Internet population) in this time frame and normalize the data, we see that the actual trend is level.*

As new data sets become available, the Cyber Green portal will be updated to include them. This includes updated measurements of existing data sets (for example the next year's data sets from ITU and OECD for Internet adoption rates) and also new data sets (for example if the OECD is able to collect data on ICT and CSIRT budgets).

Possible errors that could be introduced include from IP geolocation, DHCP and NAT effects. IP geo-mapping services (such as MaxMind, Quova, etc) have varying degrees of accuracy around the world. These services build maps based on IP block allocations, reverse DNS names, and routing path information, but mistakes can be introduced, especially for developing and non-western areas of the world. As noted earlier, DHCP leases affect the assumption in counting unique IP addresses per day that a device will have a stable IP address assignment in that time period. Because leases are volatile, a single device in one location may have multiple IPs in a 24-hour time window. This is further complicated by devices on the move, such as laptops that go from home to work to a coffee shop; in such as scenario a single infected laptop could appear as three distinct IPs and be over counted in a 24-hour time window.

Finally, NAT effects, as noted earlier, reduce device visibility by masquerading as a single globally unique IP address; multiple infected devices behind a NAT device will appear as a single IP address, undercounting. Finally, errors may appear in the survey data from the OECD or ITU, which may be uneven across the survey area (global). All of these factors may contribute errors in measurements.

To address this, the Cyber Green portal will keep the raw data as it is received in order to permit re-analysis if errors are found and corrected.

## Data Lifecycle in the Cyber Green System

It may be useful to explore the lifecycle of data within the Cyber Green system. Data can take a couple of major paths. The first is the raw incident data that goes from data sources, through Cyber Green, and onwards to the CSIRTs who have responsibility for that collection of networks. The second major path is an analysis and reporting path, mainly for Cyber Green analysts.

In both cases, data must be gathered. Data sources are identified by Cyber Green stakeholders and analysts, with an emphasis on reliable data where it is economically feasible to re-share for the purposes of remediation and feasible in generating more accurate statistics. The system will regularly aggregate the data from each source by polling the data source (e.g. pulling a data feed from a URL). The system will annotate data as needed to add geolocation, ASN data and perform DNS lookups as needed, completing the data. Finally, the system will store all data indefinitely or until space concerns become a challenge. All of this data is what feeds into the next two stages.

A key activity of Cyber Green is the production of cybersecurity statistics. To do this, data will have to be normalized against some factor, for example the number of IP addresses per country, the number of Internet users per country, etc. This normalization will permit the cross comparison of statistics, and will also enable historic comparisons. This normalization data will be imported regularly, because it is only updated periodically. It does not make sense to attempt to import it more on a schedule.

### For CSIRTs: Incident Reporting

For data feed recipients, each will have a unique key that identifies their authorization to get a particular data feed of their data. This data feed can be accessed over HTTPS in a poll fashion. For a particular CSIRT's data feed, when polled the system will gather all recent data (from the last 24 hours) for that CSIRT (identified by their unique key and mapping to a country code or a list of ASNs) and deliver the data to them.

### For Cyber Green: Reports

Cyber Green reports will have a type and duration. They can be generated on demand, for a specific page (e.g. a global dashboard), or during scheduled reports using a template. In all cases the data flow is the same.

For the duration of the report, the system will gather all report-relevant data across the time frame and group by bucket and geolocation. For example, a report may about the number of bot-infected PCs in a particular country; another report may be about bot infections around the world. The system will combine and merge all of this data to remove duplicates (see below for the mechanism by which it will do this). The system will then normalize data by the appropriate factors (e.g. IP address space or number of Internet users, see below for specifics). The system would then display the report asked for by the user.

## Cyber Green Data Sources

A large amount of cybersecurity data is already captured, which we plan to use in Cyber Green. Criteria for inclusion in the Cyber Green system include:

- Global visibility, free of bias
- Reliability
- Accuracy
- Transparency

Below are the categories of data used in Cyber Green, what they inform, and how they are collected.

### Denial of Service Attacks

- What: DDoS attacks
- How: Direct traffic observation, botnet tracking
- Data yielded: Type of attack, victim, duration, and Mbps
- Sources: (None so far)

Distributed denial of service (DDoS) attacks are measured in three ways: direct network measurement of the inbound attack traffic, botnet monitoring, and network backscatter measurement. Each of these methods yield different information about the attack, complementing each other.

Direct measurement is performed by observing the attack traffic, typically at the ingress point of the victim’s site or network. Arbor Networks’ Peakflow products are a canonical example of this. NetFlow monitors are able to build a model of normal network traffic, including a mix of protocols, rates, and geographic distributions for the time of day. Static thresholds for rates of fragments, ICMP traffic, TCP SYNs and other kinds of low-frequency packets are coupled to this dynamic model. When that model is violated, the system creates an alert describing the anomaly. These anomalies may be attacks, or they may be traffic events such as a rapid uptick in normal web traffic. Operators then mark attacks and track their intensity, duration, and mitigation. Similarly, DDoS defense services such as dedicated mitigation clouds (e.g. Prolexic, Verisgn) or content distribution networks (e.g. Akamai) can see the traffic destined to a customer’s network and analyze the attack traffic. From this direct observation the attack duration, type, intensity (bandwidth), and, for non-spoofed attacks, sources can all be gathered.

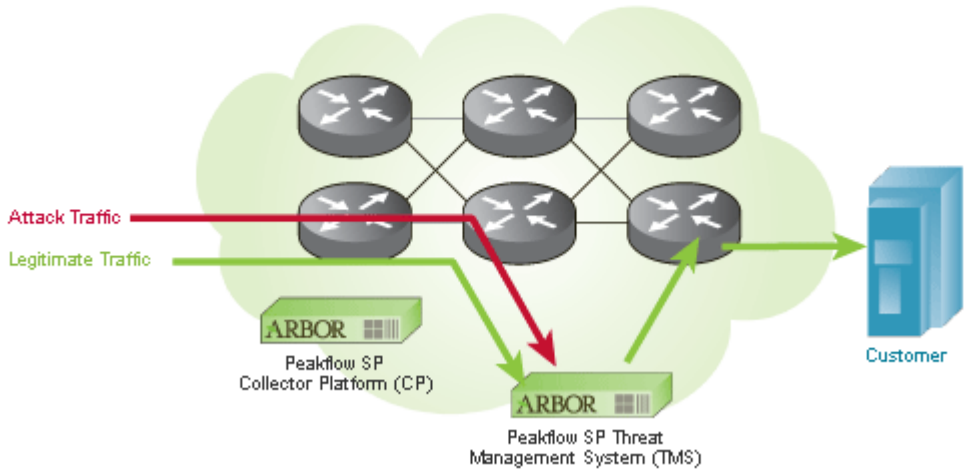


*Figure 11: Denial of service attack measurement at the customer network edge. From: http://www.hostkey.com/images/arbor_sp_tms1.gif*

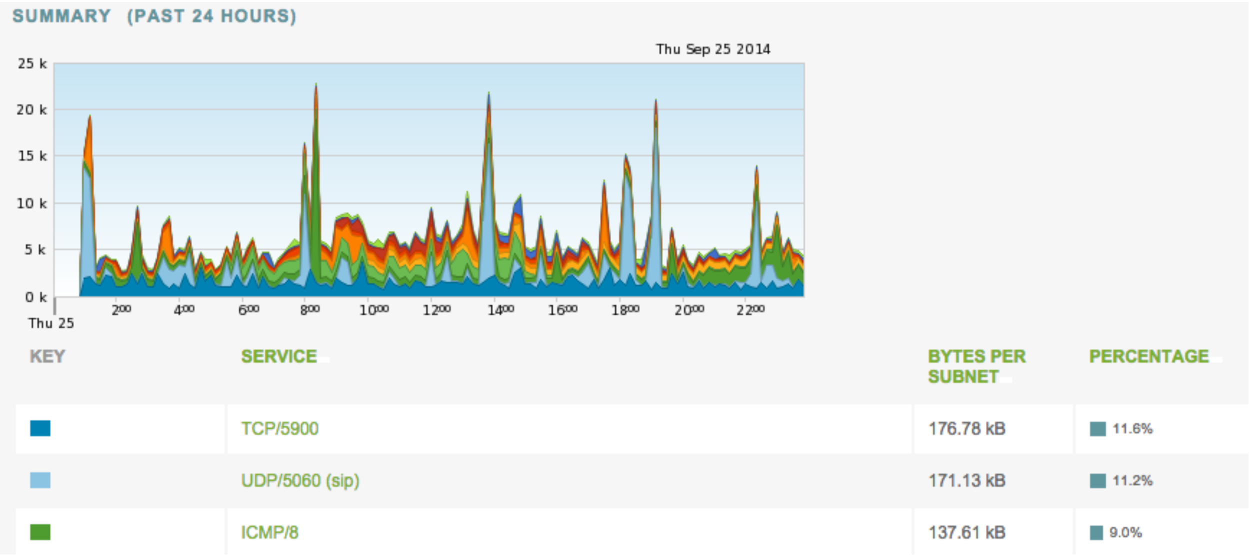
Botnet monitoring, described earlier, relies on joining multiple attack botnets and logging the commands they act upon and discovering the attacks that way[22]. By performing large-scale automated malware analysis, the botnet trackers perform botnet discovery, sending in code that mimics the behavior of the bot but only logs the commands while not acting on them. This "lurking" in the botnet gives the operators visibility into the start of the attack, the type of attack, and the responsible botnet, but little else. Botnet tracking is useful for root-cause analysis, and also for inter-attack correlation, discovering which botnets perform what other attacks. This kind of analysis has been useful for understanding ideologically motivated attacks, for example.

DDoS data is provided by a handful of parties, including Arbor Networks (direct measurement, giving full traffic characterization), Prolexic and Cloudflare (who provide cloud mitigation services for sites under DDoS attack), and Shadowserver (botnet tracking, giving responsible botnet and timestamps). Cyber Green has been negotiating with them, and others, for access to the data.

## Scans and Probes

- What: Probes for vulnerabilities and hosts
- How: Direct measurement
- Data yielded: Service and vulnerability being scanned, source IP
- Who: Arbor, SANS ISC, Dragon Research Group

Scans and probes are typically indicative of a person, or more commonly an infected PC, attempting to discover additional vulnerable systems to attack. Because scan detection requires a block of contiguous IP addresses, sites that capture that data typically do so using darknet sensors, or large-scale firewalls and IDS sensors.



| KEY | SERVICE | BYTES PER SUBNET | PERCENTAGE |
|---|---|---|---|
| 🟦 | TCP/5900 | 176.78 kB | 11.6% |
| 🟦 | UDP/5060 (sip) | 171.13 kB | 11.2% |
| 🟩 | ICMP/8 | 137.61 kB | 9.0% |

*Figure 12: Host scan data collected by Arbor ATLAS, showing top scanned services in the past 24 hours.*

Scan and probe data data is provided by few parties, including Arbor Networks (via darknet measurement), Dragon Research Group, and SANS ISC (via a distributed sensor network of their users).

## Spam

- What: Senders of spam or unwanted email
- How: Direct measurement at the SMTP server
- Data yielded: Spam source IP
- Who: Spamhaus

Broadly defined, spam is the general term for unsolicited and unwanted messages. Spam can include mail, social media updates, SMS messages, or any other communication means. Spam messages can be commercial, malware or phishing related, or just a nuisance designed to waste time and resources.

Spam is typically measured at one of three points: the message servers for popular destinations, spam traps designed to receive only spam messages, or the end users' own classification in their inbox. Spam statistics are typically either the rate of spam as a percent of volume, or the number of unique spam senders. Both are useful measures of the spam problem.

Spam sources have historically included dedicated networks, open relays, and increasingly compromised machines that have been co-opted into a botnet. In the late 1990s to the mid-2000s, the spam problem was combated through blocklists of networks known to send spam or open relay mail servers[3]. This had tremendous impacts on the ability of spam senders to utilize those strategies, forcing them to adapt. As noted by Stone-Gross *et al.*[38], since the mid-2000s, botnets have increasingly been used to send spam, enabling monetization of compromised machines through leasing service space. The reaction against blacklists of known spam origins has been to disperse to as many possible addresses as possible. This has placed pressure on such blacklists and forced them to be queried as a service instead of distributed as a static file. Additionally, content screening an effective means to detect spam regardless of origin[39]. Algorithms such as Bayesian inference have been in use since the early 2000s to categorized mail as spam based on the preponderance of "spammy" tokens and topics. This approach has been extended with other machine learning algorithms and additional message features, and is now widely incorporated into mail servers and clients around the world through technology such as SpamAssassin[40]. As of 2014, while spam sources remain prevalent, spam is largely considered a solved problem as far as end users are concerned - they see less spam in their inboxes than they used to.

Due to the intimate relationship between spam and botnets, spam source counts are a useful proxy for botnet infections. Specific botnet measurements are made by several security companies, who are able to trackback spam campaigns and volumes to specific botnet families by looking at templates and template servers. An example from the week of July 27, 2014, of one of these weekly measurements made by Trustwave is shown below.

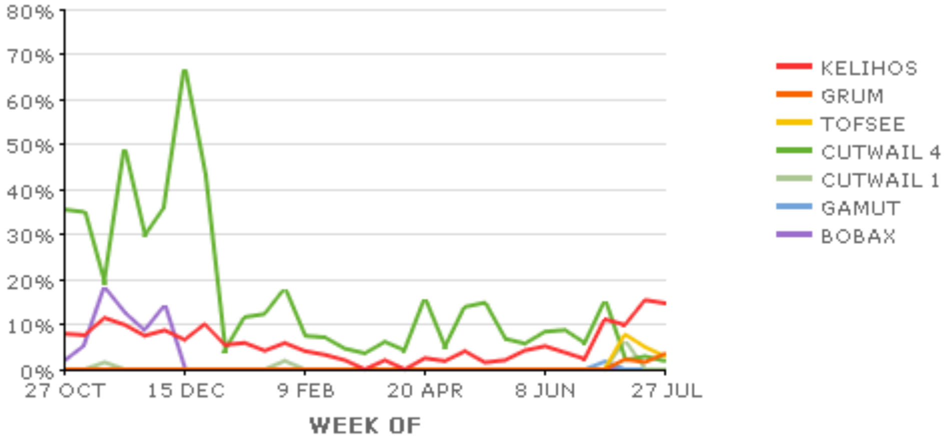
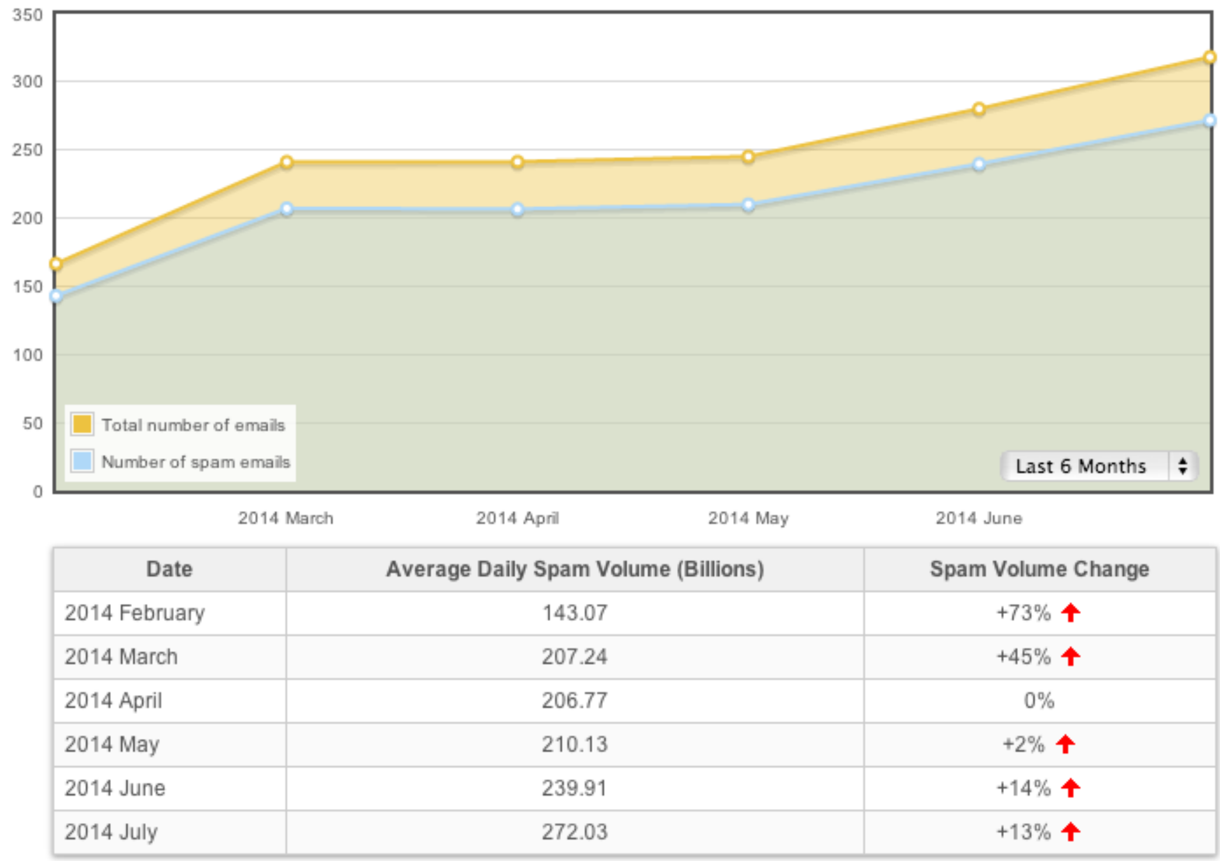


*Figure 13: Spam volumes by botnet per week as measured by Trustwave, showing the most prevalent 7 botnets. From https://www3.trustwave.com/support/labs/spam_statistics.asp .*



| Date | Average Daily Spam Volume (Billions) | Spam Volume Change |
|---|---|---|
| 2014 February | 143.07 | +73% ↑ |
| 2014 March | 207.24 | +45% ↑ |
| 2014 April | 206.77 | 0% |
| 2014 May | 210.13 | +2% ↑ |
| 2014 June | 239.91 | +14% ↑ |
| 2014 July | 272.03 | +13% ↑ |

*Figure 14: Global spam statistics from Cisco SenderBase show spam volumes per month. From http://www.senderbase.org/static/spam/#tab=1*

## Phishing Sites

- What: Phishing site URLs
- How: Lure mail analysis
- Data yielded: URLs of servers hosting the site, likely compromised server
- Who: PhishTank, OpenPhish

Phishing is a type of attack designed to socially engineer the victim into revealing their credentials to an attacker. Messages, dubbed "lures", typically warn of a negative consequence if the user does not act on the request to fill out a form. Users then submit their credentials that are then abused by the attacker; they can be sold to another user or abused right away for the attacker's immediate gain.

To complete the attack, the attacker must present to the user a website that appears to be convincing enough that the user will submit their credentials. This website can be on a server the attacker controls or it can be a server owned and operated by someone else and compromised by the attacker. To gain control of the server, the attacker typically finds a weakness into the system, often through a web application flaw, misconfiguration, or weak passwords on the system.

The number of phishing sites seen over time is available from PhishTank[41], an open community-based group dedicated to tracking phishing sites. Users submit URLs to PhishTank, whereupon they are then verified by another member. The community provides a feed of phishing URLs that can be used to integrate into a web proxy, for example, or into an email filter.

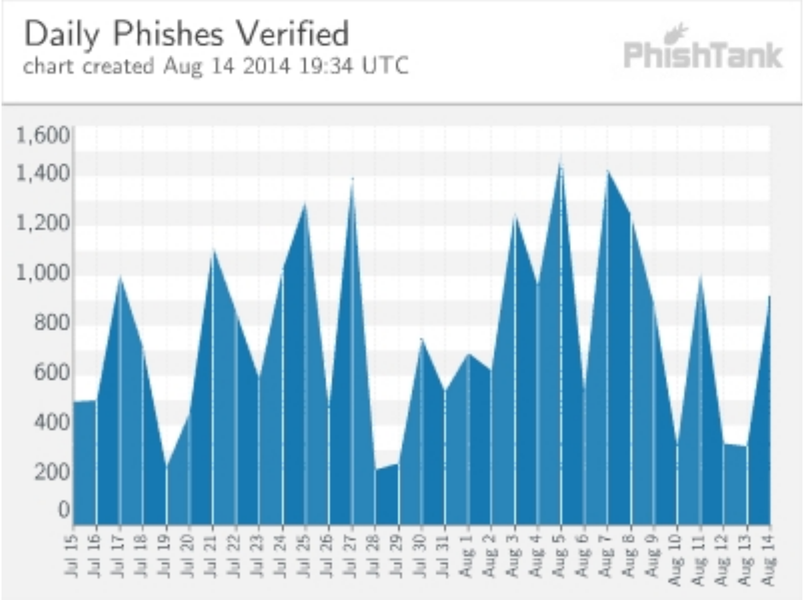


*Figure 15: Phishing sites per day for the past month seen by the PhishTank community. From https://www.phishtank.com/stats.php .*

Phishing statistics can be useful as a lagging indicator of third-party website security. Furthermore, phishing site lifetimes can be a useful measure of the responsiveness of various ISPs.

## Drive by Download Sites

- What: Malicious URLs
- How: Scanning and fingerprinting
- Data yielded: URL of malicious server, possibly compromised
- Who: Malware Domains List, Malekal, URLQuery, Siri-urz, CleanMX

Similar to phishing sites, drive by download sites can be advertised in lure messages in an attempt to draw users to visit the site[33]. Once visited, the site presents to the user's browser a series of exploit attempts targeting browser and extension flaws, such as PDF, Flash and Java exploits. The browser's error handling enables the software to operate even if one attack fails, giving the attacker multiple attempts at an exploit until one works. The purpose of these exploits is to command the victim's host to download a malware payload and infect their system.

Drive by downloads have become widespread through the use of kits, where attackers can obtain a packaged set of exploits to deploy their malware. The sites presented by these kits typically use obfuscated scripts to thwart analysis, although those features also yield detection.

Search engines employ web crawlers to collect and catalog website contents. Part of the capability of these crawlers is the ability to scan content and flag potentially malicious sites. After an outbreak of web-borne malware, major search engines began marking search results as potentially harmful to visit, augmenting host-based measures such as in-browser blacklists or local gateway URL blacklists. As noted by Provos *et al.*[33], signatures for commonly seen exploit kits and exploit pages can be inserted into the content checks for the web crawler.

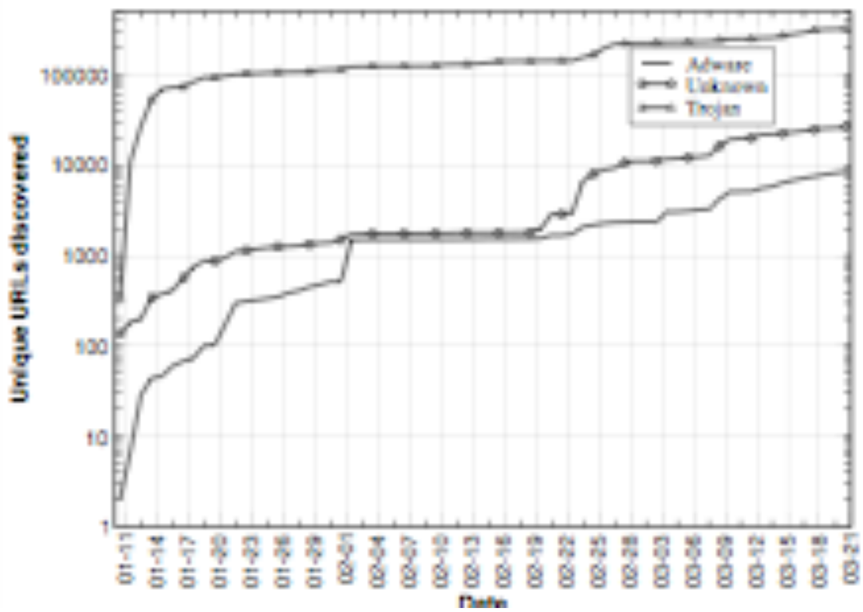


*Figure 16: Number of unique drive-by download URLs over a 60 day period in early 2007, from Provos et al.[33].*

Similar to phishing, drive-by download statistics can be useful as a lagging indicator of third-party website security. Furthermore, phishing site lifetimes can be a useful measure of the responsiveness of various ISPs.

## Botnet Membership

- What: Hosts part of a botnet
- How: Sinkhole, direct measurement
- Data yielded: Client IP address
- Who: Microsoft, AlienVault

Botnets are groups of computers affected by the same family of malware and acting on behalf of an attacker, who typically communicates with them through a server. Botnets are widely considered to be the fuel for modern Internet attacks. Their ubiquity, flexibility, and great numbers facilitate low cost, high impact attacks[35].

Botnet membership is typically measured through the use of sinkholes[48], which can give the number of endpoint members of a botnet, or by counting the number of command and control servers discovered by malware analysis.

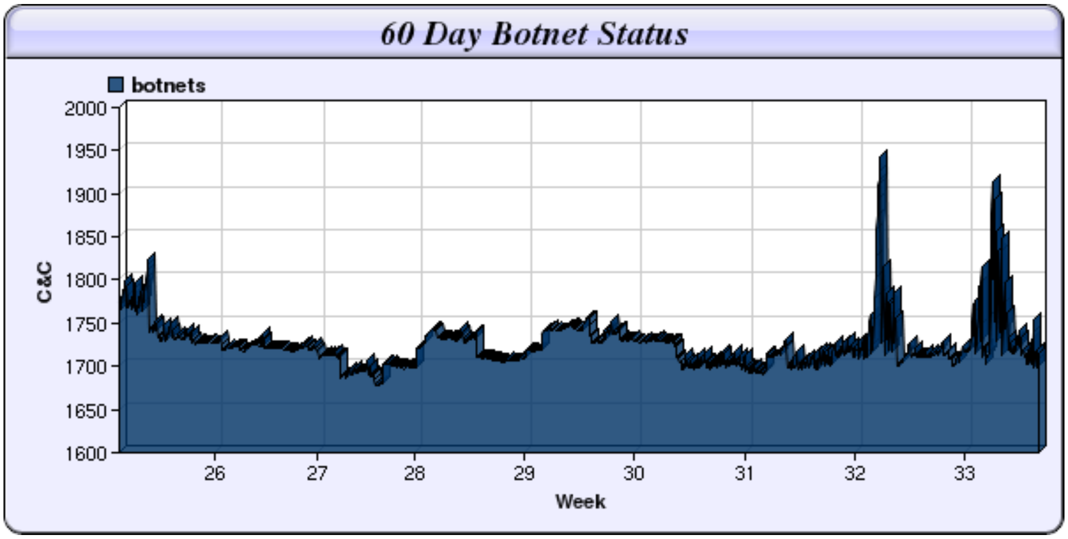


*Figure 17: Number of botnet command and control (C&C) servers seen per day by Shadowserver.*

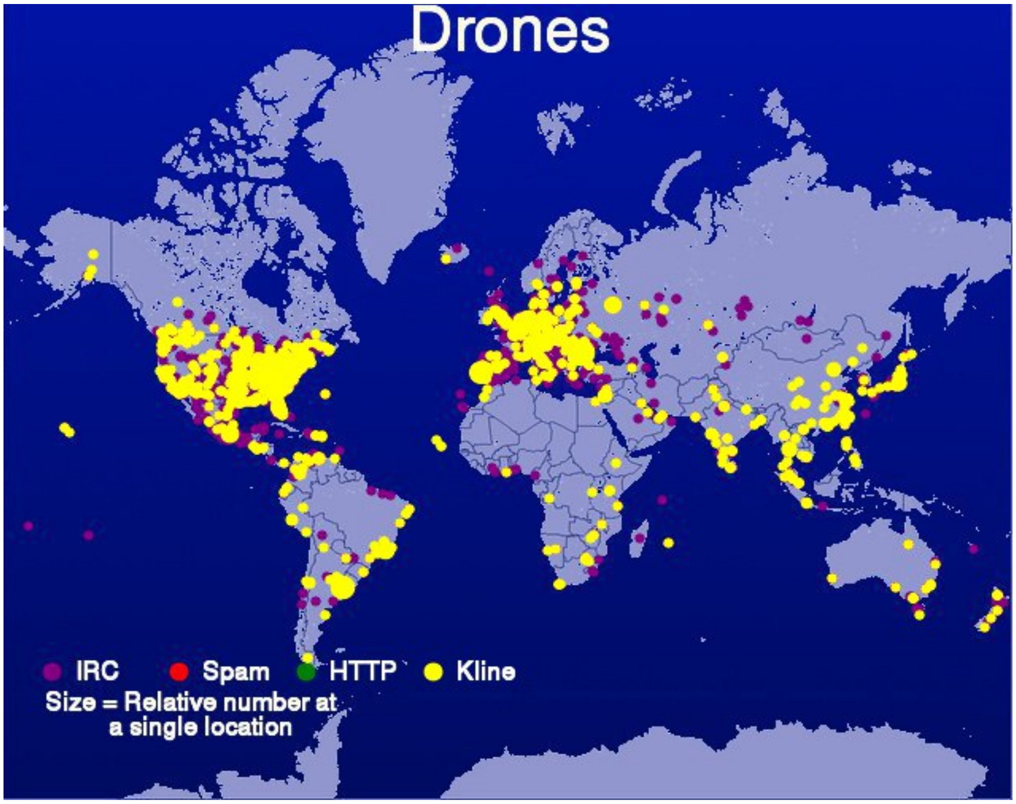


*Figure 18: Location of bots (drones) as measured by Shadowserver on August 15, 2014.*

## DDoS Amplifiers

- What: Misconfigured servers that can enable a DDoS attack
- How: Active scans and tests
- Data yielded: IP of misconfigured server
- Who: Shadowserver, Project Sonar

As noted earlier, one of the necessary elements of a DDoS amplification attack are the traffic amplifiers. These are services that generate significantly (six-fold or more) more traffic in an unauthenticated reply than the request consumed. Two major vectors for traffic amplification are DNS and NTP servers, both yielding significant amplifications of traffic as well both being popular for attackers. In a DNS amplified DDoS attack, the attackers repeatedly issue requests for a record with many resource records, such as a DNS ANY request or a request for the DNSSec keys[31]. In an NTP amplified DDoS attack, the attackers repeatedly make a small request for the NTP monlist, a list of hosts the NTP server is interacting with[65]. Because the size of list can be quite large, this can yield a significant amplification factor.

To test for these conditions, a remote sensor probes the network for the TCP/IP service port (UDP port 53 for DNS, UDP port 123 for NTP)[8]. Once it finds a server that appears to provide the service, the probe then performs a simple, single packet probe to test for vulnerable conditions. For DNS tests, the probe is for an example amplifier query with the "recursion desired" bit set (e.g. ". ANY" or "isc.org SOA" queries, both of which yield substantially larger responses than the original query). If it receives a positive result, the server is marked as being both an open recursive name server and a possible amplifier. For NTP tests, the probe simply asks the remote server for its "monlist". If it receives a reply, the server is marked as a likely amplifier.

Amplifier counts over time are shown in Figure 19, which also shows the effects of various organizations' advisories on NTP reflection and amplification attacks on the number of NTP monlist servers. From a peak of over 1.6 million servers, the number was reduced to less than 2000 around the world in the spring of 2014. According to the study, the bulk of the remaining NTP monlist servers are in the US, South Korea and Russia, with the smallest reductions occurring in Taiwan, the Netherlands and France.

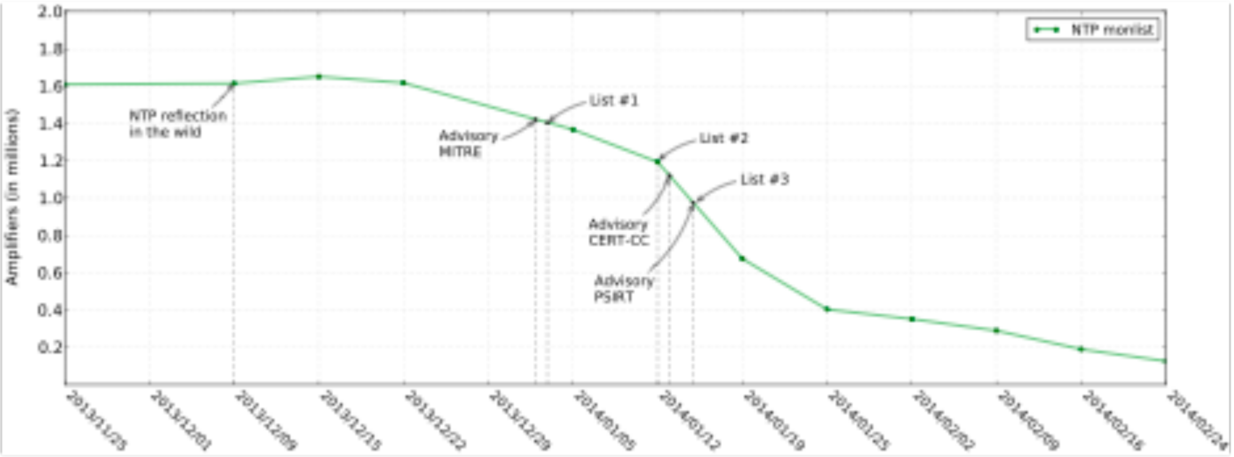


*Figure 19: The number of NTP servers vulnerable to amplification through the abuse of the monlist feature over 3 months, showing the dates of 3 major advisory efforts. From Kuhrer et al.[31].*

One of the challenges with DDoS amplifier data (and misconfiguration data such as BCP 38 adoption rates) is that the impacts of these risk conditions are externalized, meaning the costs are borne by outside parties. As such there is often little economic or financial incentive for an ISP or an organization to address these issues.

## Website Vulnerabilities

- What: Websites with known vulnerabilities
- How: Scanning and fingerprinting websites
- Data yielded: IP address of vulnerable host, list of identified vulnerabilities in server and web application software.
- Who: W3Techs, internally developed methods.

Website vulnerabilities are often the root cause of data breaches, such as community password leaks and the like, as well as follow on attacks such as phishing and drive by malware campaigns. These vulnerabilities mainly exist in web applications, such as blogging or forum software. A number of these weaknesses can be found under SANS Critical Security Controls (CSC) 6[4] as well as a number of CWE entries[66]. To understand the risk this population poses, it would be worthwhile to have an assessment of the number of websites that are vulnerable to particular attacks. The goal of this data would be to remediate the vulnerabilities and thwart the attacks before they begin. If this hypothesis is correct, we would expect a decrease in breaches, phishing and drive by attacks.

We have found one source of this data, W3Techs, who provides a commercial feed based on fingerprinting the Alexa top sites list. Their list captures both web applications (e.g. WordPress, Joomla, etc), and also server software and version together with specific PHP versions. These all represent possible intrusion points for an attacker to alter a website. We have also developed a prototype tool that can fingerprint websites, discovering the same data as the W3Techs: web applications and versions, and web server software and versions. The tools can operate on either malicious URLs to identify what a compromised site may have been running and also the Alexa top site list.

The table below shows a list of web applications from the bottom 1000 websites from Alexa's top 1 million sites for December 2014, showing known vulnerabilities as of January 1 2015. The prevalence of vulnerable or possibly vulnerable software is immediately obvious. This table was generated using the website scanning tools developed as a prototype for this Cyber Green Metrics feature.

| Count | Web Application and Version | Vulnerable? |
|---:|---:|---:|
| 1 | (c) by xt:Commerce v3.0.4 SP2.1 http://www.alu-werbetraeger.de | Y |
| 1 | 3.2.2.183 | Unknown |
| 1 | AlphaCMS - Powered by AlphaCMS 3.4 | N |
| 1 | Blogger | Unknown |
| 18 | blogger | Unknown |
| 1 | cEasy SE 4.11.2 (3337) by hitcom new media gmbh [www.hitcom.de] | N |
| 1 | Consisto.CMS V4.0.0.0 CORVI-20141231114306 | N |
| 1 | DataLife Engine (http://dle-news.ru) | Unknown |
| 1 | Discuz! 7.0.0 | Y |
| 1 | Discuz! X3.1 | Y |
| 1 | Divi Child v.0.1 | N |
| 1 | Divi v.1.9.1 | N |
| 2 | Drupal 7 (http://drupal.org) | Y |
| 1 | Edlio CMS | Unknown |
| 1 | Fable v.1.1 | N |
| 1 | Homestead SiteBuilder | Unknown |
| 1 | http://www.typepad.com/ | Unknown |
| 1 | HubSpot | Unknown |

| | | |
|---|---|---|
| 11 | Joomla! - Open Source Content Management | Unknown |
| 6 | Joomla! 1.5 - Open Source Content Management | N |
| 1 | KpopNews24-Nexus v. | Unknown |
| 1 | MagicFreebies | Unknown |
| 1 | Movable Type Pro 4.27-ja | Y |
| 524 | N/A | Unknown |
| 1 | Nexus Themes \| plumbing | Unknown |
| 1 | Onedesign | Unknown |
| 1 | OpenNemas - Open Source News Management System | Unknown |
| 2 | Orchard | Unknown |
| 1 | Osclass 3.5.3 | |
| 1 | PHP Link Directory 3.3.0 | Y |
| 1 | Polished v.3.9 | |
| 2 | Powered by Visual Composer - drag and drop page builder for WordPress. | Unknown |
| 7 | PrestaShop | Y |
| 3 | TYPO3 4.5 CMS | Y |
| 2 | TYPO3 4.7 CMS | Y |
| 1 | TYPO3 6.2 CMS | Y |
| 1 | vBulletin 3.8.2 | Y |
| 1 | vBulletin 3.8.7 | Y |
| 1 | vBulletin 4.2.2 | Y |
| 1 | Web Page Maker | N |
| 1 | Webflow | N |
| 1 | Webnode see http://www.webnode.pt/ | N |
| 1 | Wooden v.3.5 | N |
| 1 | WordPress 2.0 | Y |
| 1 | WordPress 3.3.1 | Y |
| 1 | WordPress 3.4.1 | Y |
| 1 | WordPress 3.4.2 | Y |
| 1 | WordPress 3.5 | Y |
| 1 | WordPress 3.6 | Y |
| 3 | WordPress 3.6.1 | Y |
| 1 | WordPress 3.8.1 | Y |
| 1 | WordPress 3.8.3 | Y |
| 2 | WordPress 3.8.5 | Y |
| 1 | WordPress 3.9.1 | Y |
| 1 | WordPress 3.9.2 | Y |
| 7 | WordPress 3.9.3 | Y |
| 1 | WordPress 4.0 | Y |
| 37 | WordPress 4.0.1 | N |
| 23 | WordPress 4.1 | N |
| 1 | WordPress 461 | Unknown |
| 5 | WordPress.com | Unknown |
| 1 | فرانسه | Unknown |

*Table 3: Bottom 1000 websites from the Alexa Top 1 Million from December 2014, showing detected web applications and their associated vulnerabilities.*

## Combining and Merging Data Sources

Multiple data feeds can become sources to inform about a particular problem. The combination of the data will increase coverage and visibility, generating a more complete picture of the scope of the problem. However, it is crucial to merge the data properly to avoid over counting the results when multiple sources report the same incident. To do this merge, each data source needs to be counted by a unique identifier. For example, multiple sources may report the same phishing website, but it is crucial to identify only one website and not more than one. The fact that multiple observations occurred does not increase the number of phishing websites at that URL.

Data normalization is also different depending on the type of data, as well. For client host counts, scaling the observations by Internet connections or populations, or by IP address, is a natural way to normalize the data. This is because the potential population is any Internet connected user or device. Malicious websites such as phishing or drive-by exploit websites have an upper bound on the number of websites per country, because to a first approximation not every host is often a web server.

Finally, the desired target value for each data bucket are all low, meaning the numbers should be as small as possible. Specific values, such as "no more than 2% Internet connected users should be infected", are impossible to express at this time. Several years of study would need to be carried out to understand what would be reasonable values.

The ways in which combinations will occur for each data bucket are shown in table 4.

| Bucket | Unique ID | Normalization | Desired Target |
|---|---|---|---|
| Spam source | Client IP | By Internet population<br>By IP address space<br>By Internet connections | Low |
| Bot/drone | Client IP | By Internet population<br>By IP address space<br>By Internet connections | Low |
| DDoS amplifier | (Server IP, service) | By Internet population<br>By IP address space<br>By Internet connections | Low |
| DDoS attack | (Type, victim) | N/A | Low |
| Malicious website | (URL, IP) | By website population | Low |
| Vulnerable host | Host IP+service | By Internet population<br>By IP address space<br>By Internet connections | Low |

*Table 4: Data deduplication strategies by data type ("Bucket") and normalization strategy, along with the desired target for the value. For the malicious website unique key, the URL will consist of only the scheme, hostname and path, omitting the query arguments and any fragments or anchors.*

The algorithm by which the data combinations will occur is shown in figure 20. In brief, for every data bucket the data sources will be gathered, but the extent of the problem, based on the size of the affected population, will only be calculated by the number of unique identifiers present in any one day time period. These are the numbers that will be aggregated by country and stored for analysis. This method also preserves any of the original data to enable its use in remediation. Furthermore, this method is applied by groups such as Shadowserver and Arbor Networks' ATLAS system.

**Input**: data_bucket, a list of data topics and feeds per topic

**Algorithm**:

```
for each data_bucket
  for each source in data_bucket
      gather data – timestamp, observation, etc
  count unique(bucket identifier) where
    timestamp > 00:00:00 and < 23:59:59
```

*Figure 20: Data merging algorithm for data sources in each data bucket. The end result is the number of unique hosts per problem per day.*

An example of this approach is shown below. In figure 21, two phishing data feeds report their observations, reporting URL, IP address of the server, and the timestamp of the observation. Through the data merging strategy for malicious servers, the unique identifier for any data value is the URL and the IP address of the server. So, in this example we have two sources giving four reports but only three unique phishing websites, one with one IP address and with the same URL on two IP addresses.

```
source, URL, server IP address, timestamp (GMT)
Source 1, http://paypal.fakesite.com/, 1.2.3.4, 17:28:34
Source 2, http://paypal.fakesite.com/, 1.2.3.4, 19:32:18
Source 1, http://amazon.fakesite.co.jp/, 5.6.7.7, 21:23:45
Source 1, http://amazon.fakesite.co.jp/, 5.6.7.8, 21:23:45
```

*Figure 21: Example data feed for phishing websites from two data sources showing multiple observations for merging. In this example, these two sources are reporting only 3 unique phishing websites.*

This data merging strategy is a best effort to marry multiple data sources without artificially inflating the counts when overlaps occur. The time window chosen is 24 hours (midnight to midnight) to account for DHCP and NAT effects as best as can be done in light of data capture limitations. The goal is to attempt to create an accurate, composite picture of Internet incidents through data fusion.

## Analyzing Cyber Health Problems by Pairing Data Sources

As shown in Table 2, the relationship between symptom and cause (and root cause) can yield insight into which datasets to compare. In Table 5 the related data sources we can use to assess Internet health are shown along with how they can be compared against each other. The input data sets are the product of merging all of the appropriate data feeds together.

| **Data set 1** | **Data set 2** | **Meaning of relationship** |
|---|---|---|
| DDoS amplifiers | DDoS attacks using amplification | Positive relationship expected: Reducing the number of DDoS amplifiers should reduce the number of DDoS attacks using amplification |
| Botnet membership | Software piracy rates | Many bots spread over known vulnerabilities, which remain unpatched in pirated software. Updating that software could hamper botnet propagation. |
| Website vulnerabilities | Phishing sites | Website vulnerabilities allow for attackers to take control of a web site and establish a malicious site |
| Website vulnerabilities | Drive by downloads | Website vulnerabilities allow for attackers to take control of a web site and establish a malicious site |
| Spam rates | Botnet membership | Bots have become a prime origin of spam. Similar to software piracy vs botnet membership rates, we can track spam rates compared to botnet membership rates as a root-cause of spam. |
| Major vulnerabilities | Incident counts | Major vulnerabilities such as the SSL Heartbleed vulnerability can be measured, although these in particular have no bearing on most incidents. However we can use them as a proxy for the upper bound of patch rates per country. |
| Antivirus rates | Incident counts | Many attacks such as botnet infections have known AV signatures. We can use AV rates per country to determine a correlation with incidents. |

*Table 5: The insights yielded by combining particular data sets.*

## Normalizing Internet Measurements

The goal of normalizing these measurements is to permit comparisons of the data to evaluate cleanup and remediation efforts. For these purposes we are interested in two kinds of comparisons: between countries and over time. Because each country is different - different sized populations, policies, development statuses, etc - we have to find normalization factors to account for that to more accurately evaluate a specific point, namely Internet health effects. Similarly, over time populations grow or shrink, Internet growth happens, and technology those networks. Because network protocols and applications that enable some form of amplification will continue to be created and deployed, one of the key problems to tackle to thwart such DDoS attacks is to prevent source IP spoofing via BCP38[37] compliant networks.

The primary use of normalized data would be to evaluate the effect of policy or technology changes. Without normalization, measurements may obscure trends or incorrectly create changes where none have occurred. In order to evaluate the effects of specific actions, typically deliberate actions such as investments or policy changes, data must also be normalized over time.

A second use of the normalization data would be to evaluate suspected relationships by examining correlations between data sets. For example, Windows piracy is often cited as an example of why many people do not patch their Windows software and remain vulnerable, leading to botnet infections and the like[67]. Normalizing bot infections by the prevalence of a specific Windows version may be useful in assessing the validity of this assumption. If this assumption were supported in the analysis, then it may reveal a new strategy to improve Internet health (in this case reduce piracy rates or Windows XP populations).

As noted below, not every possible normalization value is available. Some measurements will have to be proxies for other measurements that are unavailable at this time.

## By IPv4 and IPv6 Address Space

One possible means to normalize the number of events measured between countries would be to scale by the number of IP addresses in each country. While not every IP address is used in every country - and the rate of usage differs widely between countries - it is a commonly used measure to normalize IP-based measurements between countries.

The Country IP Blocks site[30] maintains a list showing counts of IPv4 address per country. A similar site, IP Duh, maintains a list of IP address counts per country for IPv4 and IPv6, listing both allocations and assignments[68]. This has the intended effect of scaling events by the number of connected hosts. However, in reality because IPv4 addresses are disproportionately assigned to countries around the world and are assigned based both on population and need but also *when* they were requested, addresses are not uniformly distributed around the world when correcting for population. The global average is 611 IP addresses per 1000 persons, with some countries having 5000 or more IP addresses per 1000 persons (an overabundance of addresses) while some have as few as 5 (an oversubscription of IP addresses). Because of this, normalizing events by IPv4 address per country is likely to yield uneven comparisons between countries.

## By Population

A large number of development indicators are scaled *per capita*, such as spending on medical infrastructure or GDP, making this a natural consideration for normalization. A number of sources for population counts are widely available and well accepted.

However, the fraction of a population for any country that is connected to the Internet varies widely, making this kind of normalization a poor choice. Instead, two more specific relations to the population make more sense as a normalization factor.

## By Internet Connected Population

A more appropriate scaling factor is the number of Internet connected persons in any country. This is more likely than the bulk number of a country's citizens to be reflective of the potential risk surface as connected individuals typically have one or more devices that can become involved in incidents. It is also a major factor to consider when planning for education or remediation efforts.

The ITU maintains a data set of the percentage of Internet users by country that is updated yearly[69].

### By Internet Subscriptions

One popular premise is that the growth of consumer Internet activities has been a major contributing factor to Internet security events. To measure this, the correlation of incidents to Internet subscriptions may be a valuable aide. Also, the number of Internet subscriptions can be used as a proxy for Internet adoption by country.

The OECD maintains a list showing the counts of Internet service subscriptions (fixed and wireless) by country[70]. A similar ITU data set lists the number of fixed-line broadband (DSL, cable modem, etc) subscriptions by country[69].

### By Internet Connected Device

If we assume that when we measure an incident we wish to identify the affected device, then this is an ideal measurement. However, this normalization factor lacks continuous, ongoing measurements. Limited studies have been performed to estimate the number of devices on any network, such as Maier[27], but no persistent global statistics have been found.

### By Website Count

A number of metrics useful to Cyber Green examine the prevalence of specific types of websites, such as phishing sites or drive by download URLs. To understand the rate of infection, another useful normalization factor is the total number of websites per country. This is because the number of websites per country is dependent not on population but other factors, including hosting infrastructure, ISP maturity, and IP address availability. This leads to a number of countries disproportionately hosting websites, especially for other users in countries.

Breakdowns of websites per country are not readily accessible. To create this, the Cyber Green project could use the Alexa Top 1 Million listing[71] and process it for DNS results, mapping those IP addresses back to countries using MaxMind. We believe this method will produce a more accurate result than forward or reverse DNS records could yield.

## Correlation Data

Similar to normalization data, correlation data seeks to understand the relationship of cybersecurity incidents and possible explanations that have been quantified. Correlation can be used to infer dependence between two variables. For example, we would like to see if software piracy is correlated with botnet infections. By plotting the two data sets - normalized botnet infections and piracy rates by country - we can determine if there is a possible relationship to investigate.  Shown in Figure 22 are three broad scenarios: positive correlation, negative correlation, and no correlation between two variables.

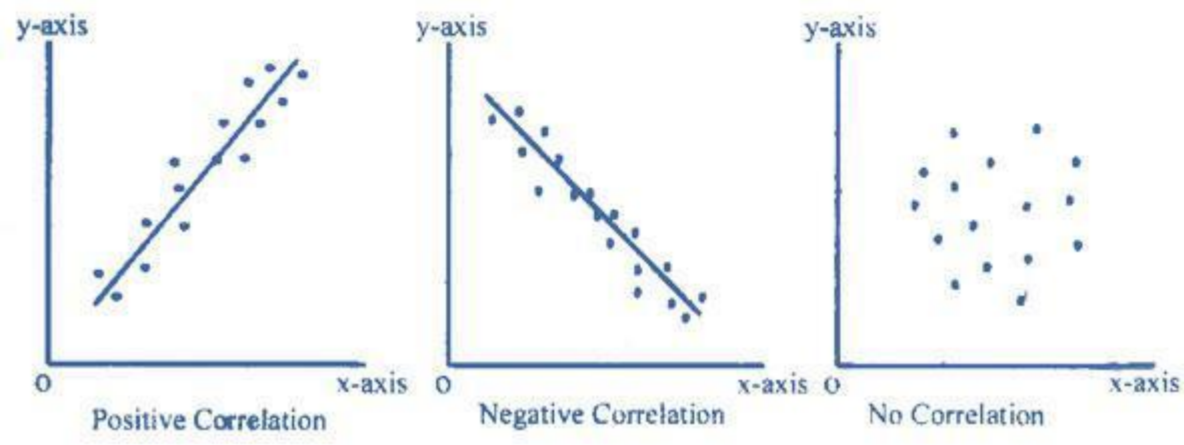


*Figure 22: Possible correlations between two variables. From http://www.emathzone.com/basic-stat/positive-negative-corr/clip_image001.jpg*

## By ICT Budget

If we accept the model that CERT and ISP activities have a positive impact on the security statistics of a country, then the amount of ICT budget spent on security efforts would provide a meaningful correlation factor. However, ICT budgets are not routinely published for various reasons, including a lack of consensus about what constitutes ICT security activities and national security concerns; some CSIRT activities for some nations are part of their domestic security apparatus. The OECD is examining if they can collect this information for member nations[72], while the World Bank may also have some data[73].

Breakdowns of the ICT budget that would be valuable to have include the amounts spent on end user education, security infrastructure spending, training, CSIRT resources, and the like. The value of this kind of breakdown would be to understand possible outcomes of particular kinds of investments, such as public outreach or additional CSIRT resources.

## By Pirated Software

The BSA (formerly the Business Software Alliance) regularly produces reports exploring the rate of software piracy around the world[5]. This will be used to explore a possible link between cybersecurity incidents, risks, and piracy rates. Microsoft has previously published a report that showed a correlation between software piracy and cybersecurity incidents[74]. The origins of this possible link come from how Microsoft and other large software organizations provide software and security updates to their clients. Some years ago, Microsoft began their “Microsoft Genuine Advantage” effort to reduce Windows piracy. This was immediately described by many as being coupled to software update availability, including security patches. As a result of this, many users of pirated software disabled security updates for fear of having their computers disabled, leaving them in a vulnerable position. Because of this, many PCs around the world lack security updates and remain at risk of attack and abuse.

## By Security Software

End host security products are one of the main lines of reducing risks that abuse endpoints such as PCs, yet protection data is often inaccessible except to vendors. For the purposes of this report, we can consider un-updated endpoint security products as we do unpatched vulnerabilities. Vendors typically release such updates to filter out newly discovered attack vectors and increase the effectiveness of their products; without such updates their products lose effectiveness. Major PC manufacturers and ISPs provide licenses to AV products, but the number of users who maintain those products is known. The AV Comparatives report[12] suggests that a wide number of users are well protected, but it relies on self selection into the survey and self assessment. As such, this study is considered flawed and is not useful for our understanding of end user protection rates.

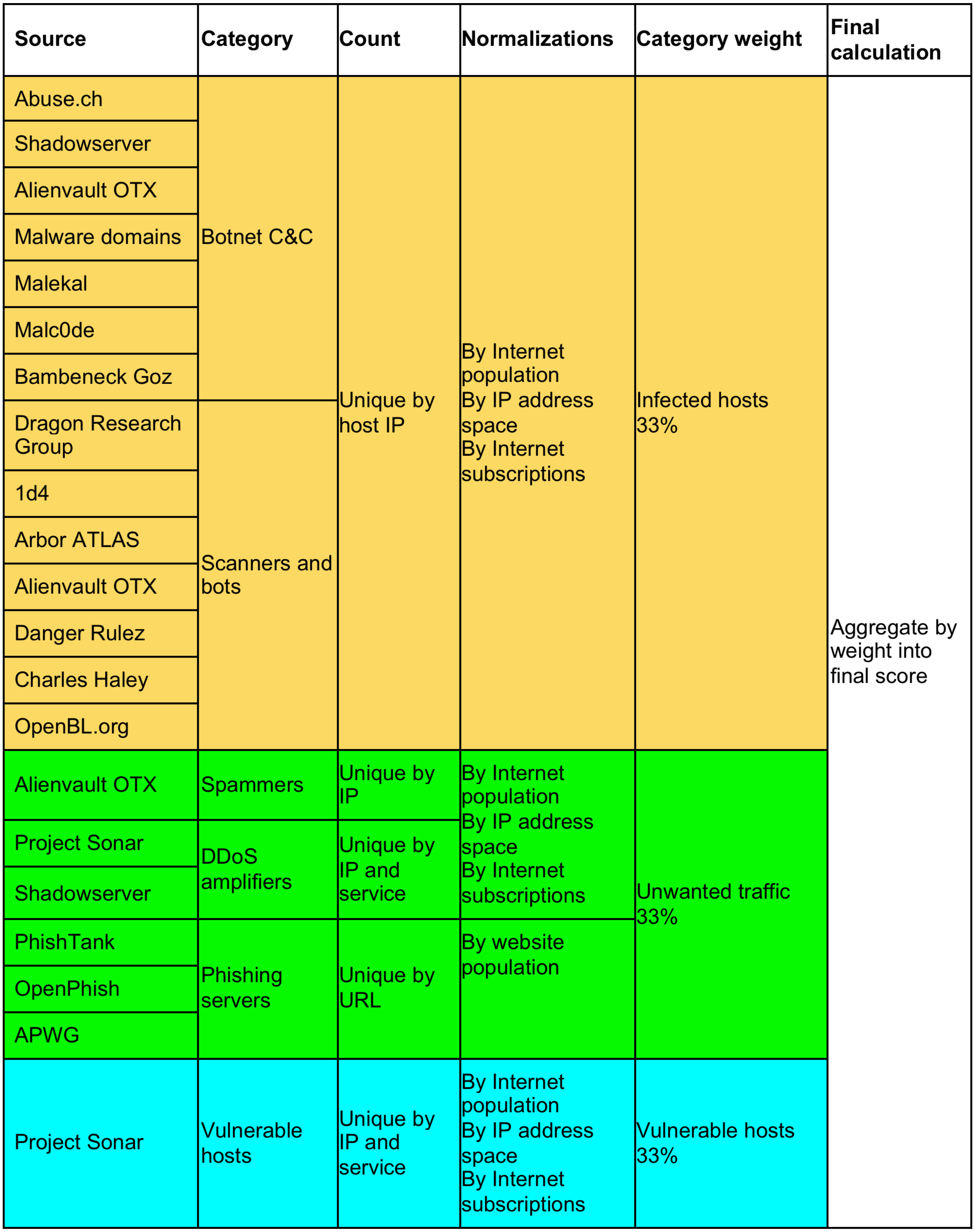
### By Vulnerability Notice

CSIRT activities are assumed to have an effect on that country's Internet health and cybersecurity position. Vulnerability notices are one of the major ways that CSIRTs communicate with their constituents. These bulletins highlight major threats that have a potentially wide impact, together with remediation steps. A natural question to explore through data set correlation, then, is *do more vulnerability notices by a CSIRT improve security noticeably?*

An example of a positive correlation is shown in Figure 19, showing the count of NTP servers that can be used as DDoS amplifiers over time. The figure shows a decrease, with the dates of several notices from high profile CSIRTs indicated. The presumption is that such an effort by a CSIRT has this kind of effect on any indicator of cybersecurity. Cyber Green will be positioned to explore this relationship by correlating Internet health measurements with the number of vulnerability notices published by CSIRTs. A positive correlation would indicate that this effort is worthwhile to continue, a negative correlation or no correlation would indicate that there is little benefit from the current practices by the CSIRT for reaching their constituents. If some geographies show a positive correlation while others do not, then this would indicate that the means by which CSIRTs reach their constituents have room for improvement.

## Overall Cyber Risk Calculation Per Region

The table below shows the mechanism by which Cyber Green will calculate the cyber risk index per country and globally. The table should be read left to right, from data source through its transformations and normalization, and then finally the cyber risk calculation. The various colors correspond to the various broad categories that are weighed together.



| Source | Category | Count | Normalizations | Category weight | Final calculation |
|---|---|---|---|---|---|
| Abuse.ch | Botnet C&C | Unique by host IP | By Internet population<br>By IP address space<br>By Internet subscriptions | Infected hosts 33% | Aggregate by weight into final score |
| Shadowserver | | | | | |
| Alienvault OTX | | | | | |
| Malware domains | | | | | |
| Malekal | | | | | |
| Malc0de | | | | | |
| Bambeneck Goz | | | | | |
| Dragon Research Group | Scanners and bots | | | | |
| 1d4 | | | | | |
| Arbor ATLAS | | | | | |
| Alienvault OTX | | | | | |
| Danger Rulez | | | | | |
| Charles Haley | | | | | |
| OpenBL.org | | | | | |
| Alienvault OTX | Spammers | Unique by IP | By Internet population<br>By IP address space<br>By Internet subscriptions | Unwanted traffic 33% | |
| Project Sonar | DDoS amplifiers | Unique by IP and service | | | |
| Shadowserver | | | | | |
| PhishTank | Phishing servers | Unique by URL | By website population | | |
| OpenPhish | | | | | |
| APWG | | | | | |
| Project Sonar | Vulnerable hosts | Unique by IP and service | By Internet population<br>By IP address space<br>By Internet subscriptions | Vulnerable hosts 33% | |

*Table 6: Data flow in the Cyber Green Index calculation.*

## Calculating the Cyber Green Score

The Green Index is a statistical model based on *percentile rank*. It is a composition of three underlying risk factors: compromised nodes, unwanted traffic and vulnerable nodes for a given country against itself over a period of time.

The percentile rank of a periodical risk condition count is the percentage of risk conditions in it's frequency distribution that are the same or lower than it within a given time period. For example, a risk condition count that is greater than or equal to 75% of the counts of other days in the period is said to be at the 75th percentile rank.

The resulting risk factor ranks are then averaged and inverted to produce an index. Countries are initially ranked against themselves for a given time period, not against each other. The higher the Green Index, the "more green" a country is currently performing against it's relative time period.

The four-step process is thus:

1. For the given country, consider the data set of distinct IP address counts for each risk factor for each day over measurement period.
2. Consider the distinct IP address data, for each risk condition we calculate the percentile rank of each risk for each day against all other days in the period.
3. A rounded average of the three risk conditions is taken.
4. To calculate the Green Index, we subtract the resulting risk condition averages from 1.0.

## Setting the Global Cyber Health Index

While it's challenging to distill a number of metrics from myriad sources and about diverse aspects of the problem into a single value, we will attempt to do so based on the values above. For the key indicators, we will use a color-coded system based on the ranges below.

| | |
|---|---|
| Less than 2% | **Blue** |
| 2%-4% | **Green** |
| 4%-10% | **Orange** |
| 10% or greater | **Red** |

Each specific key indicator will be shown with its corresponding risk level as a color. A global risk level will be calculated by combining the three key indicators evenly into a single value - .33*UT + .33*IH + .33*VH - where UT means unwanted traffic rate, IH means infected host percentage, and VH means vulnerable host percentage. The goal is to quickly, at a glance, give an impression of how close we are to the goal of a stable, secure Internet.

## Best Practices

As part of addressing the threats to Internet health at their cause - rather than their symptoms - it is important to consider established best practices that remediate the problem conditions. These may be useful for new and mature CSIRT organizations alike. Best practice efforts have been used in the past for public safety and health to great effect (Figure 25 showing one such example), and can be applied in cyber in just the same way - to improve the stability and health of a general resource, the Internet. A similar program in the United States, "Stop Think Connect", has been underway for some time now.

*Figure 24: Stop Think Connect project logo for online safety and security awareness.*

*Figure 25: Smokey the Bear poster from the US National Forest Service, part of a long-running public safety campaign to prevent forest fires.*

The figure below, from Zhang *et al.*[32], shows the larger interrelationships between societal, governance, and technical factors that contribute to network attack symptoms emanating from a network. The goal of this table of best practices is to enable the reduction of the *mismanagement* step in the graph, leading to a lower rate of attack coming from those networks. The thrust should be focused on a handful of high-reward steps with clear focus.

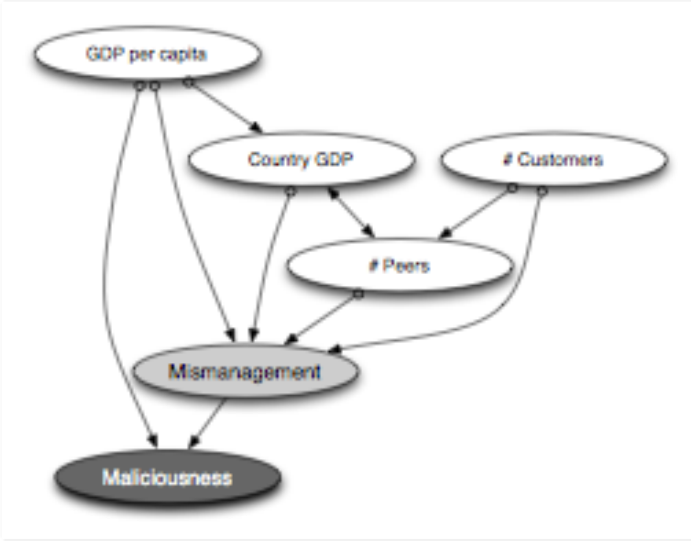


*Figure 26: The inferred cause interrelationship between societal and network effects that contribute to network mismanagement and finally maliciousness emanating from the network. From Zhang et al.[32].*

| Root Cause | Solution | Notes |
|---|---|---|
| *Mosquito transmission of malaria* | *Spray for mosquitos* | |
| | *Mosquito nets* | |
| | *Drain swamps or remove standing water* | |
| Source spoofing possible | Implement anti-spoofing ACLs | Measure deployment with the Spoofer project's tools http://spoofer.cmand.org/ |
| Traffic amplification possible | Disable features, block external access, or rate limit protocol (NTP, DNS, SNMP, etc) features | Device and service dependent |
| Exploit possible | Apply software patches as needed | |
| | Proper host or device configuration | |
| Bots send spam | Block outbound port 25 (SMTP) | Commonly suggested by MAAWG, works to stop unauthorized senders |

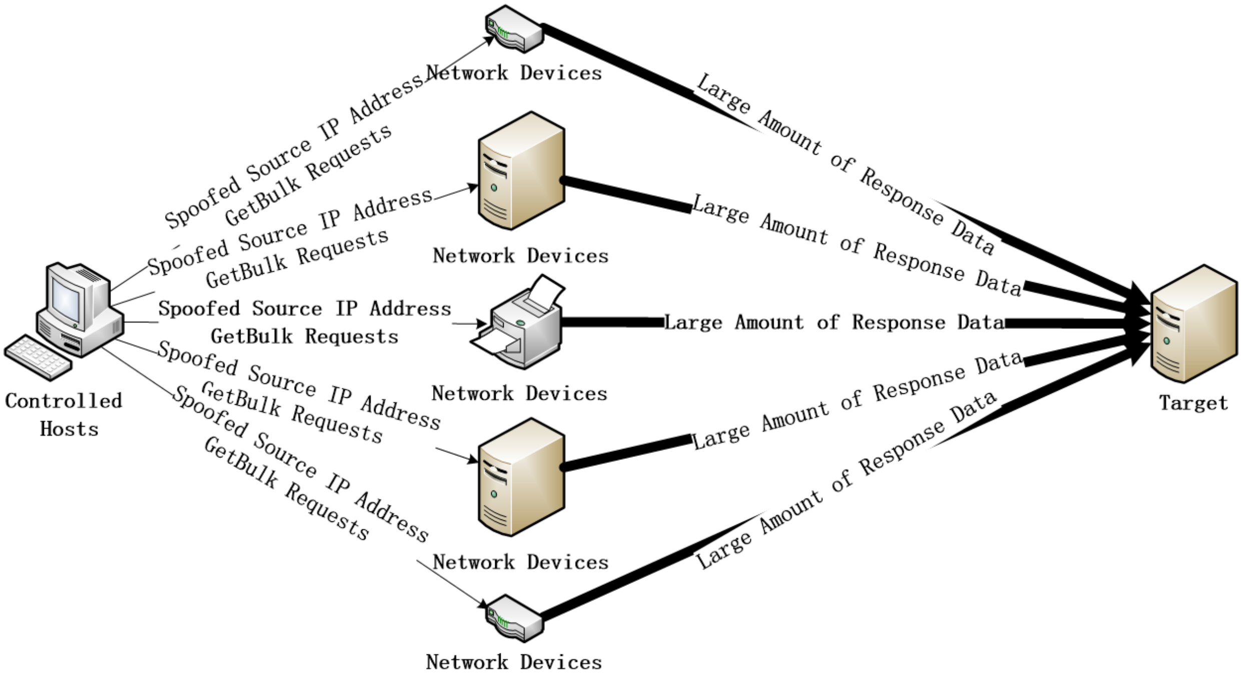
*Table 7: Best practices for specific cybersecurity issues.*

Table 2 for the root causes of the symptoms and how to address them. For completeness, the malaria example is carried over. Table 7 summarizes these solutions by root cause, with in-depth explanations in the following pages.

## Anti-spoofing

Source IP spoofing is a critical element in the ability of attackers to launch attacks via traffic amplifiers[31]. As shown in Figure 27, to launch such a DDoS attack the attacker has their bots generate traffic to the amplifier, forging the source IP address to be the victim's IP. When the amplifier responds the traffic is sent to the victim IP. Amplifiers include DNS servers, SNMP servers, NTP servers, and others, typically UDP services that respond to small requests with large replies, or send large error messages for a small malformed input.

Anti-spoofing measures are typically supported in router configurations[37], with almost all vendors supporting strict or loose source routing lookups before they would forward a packet. Strict lookups mean that the router ensures that the packet *must* have come from its observed interface; loose lookups mean that the router verifies that the packet must have come from *any* directly connected route regardless of interface. At the customer-provider edge strict route verification is preferred. The added load on the router is typically very small unless the router is already at its throughput capacity.



Controlled Hosts
Spoofed Source IP Address GetBulk Requests
Spoofed Source IP Address GetBulk Requests
Spoofed Source IP Address GetBulk Requests
Spoofed Source IP Address GetBulk Requests
Spoofed Source IP Address GetBulk Requests
Network Devices
Network Devices
Network Devices
Network Devices
Network Devices
Large Amount of Response Data
Large Amount of Response Data
Large Amount of Response Data
Large Amount of Response Data
Large Amount of Response Data
Target

*Figure 27: DDoS amplification attack using an SNMP attack vector. Via https://nsfocusblog.files.wordpress.com/2014/07/snmp-attacks-picture-1.png*

IETF best current practice (BCP) number 38 gives widely accepted information on how to implement anti-spoofing via router access control lists (ACLs)[37]. Secure router templates for a variety of router platforms (Cisco IOS, Juniper JunOS, etc) exist, and nearly all vendors have documentation on how to implement ingress filtering as described in BCP38.

The MIT-based Spoofer Project[75] has developed a small tool to test for the prevalence of networks that permit source address spoofing. Their results show that approximately 80% of all networks implement some form of ingress filtering to thwart source spoofing. This tool is available as open source and can be run very easily by nearly any operator to measure this misconfiguration that enables DDoS attacks via amplification vectors.

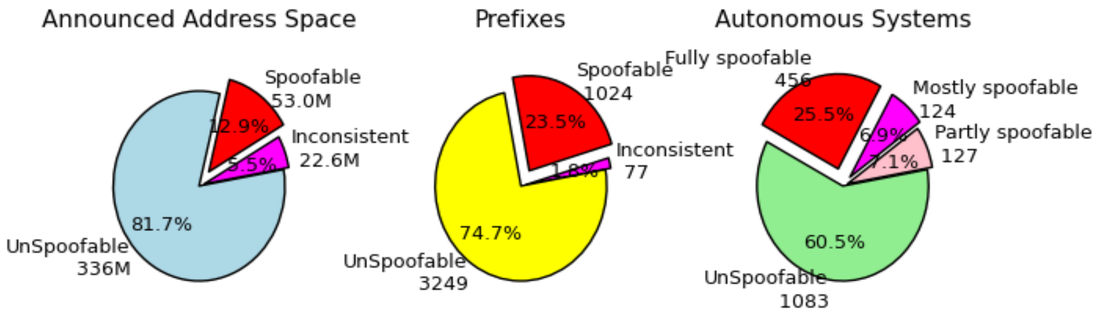


*Figure 28: Spoofer Project statistics on the amount of address space that permits source IP spoofing. Via http://spoofer.cmand.org/summary.php*

Misconfigured or poorly designed services, typically UDP-based services, are the cause of these kinds of attacks. A major contributing factor to this has been poorly designed home broadband equipment such as a cable modem router. The open recursive DNS server these devices provide is exposed to both the home network side and also the larger Internet. The solution to address this problem is to configure the device's DNS server to be authorized to receive limited network traffic on specific, internal interfaces.

# Part 4: Summary and Recommendations

## Benefits for Japanese Taxpayers

Because Cyber Green is being started by JPCERT/CC, who is itself funded through Japanese taxpayers, a key question to answer is the benefit for the Japanese taxpayer. Both direct and indirect benefits are possible if Cyber Green is successful at improving Internet health.

One direct benefit to Japan's Internet presence is readily apparent: improved Internet health means improved security for the Japanese portion of the Internet, its users and its companies' presences. Improved Internet health is expected to translate into fewer attack sources and victims, which will make the Internet for Japanese users safer, more productive, and lower cost in the long run.

An improved understanding of the objective measurement of Internet health is a second direct benefit to Japanese taxpayers. Cyber Green seeks to measure Internet health, which has been a qualitative rather than a quantitative measurement to date. If Cyber Green is able to improve cybersecurity measurements, Japanese companies, ISPs and Internet users can all benefit from improved investment of effort and resources that comes with understanding what cybersecurity efforts are effective. This would translate to lower future costs.

The indirect benefit to Japanese taxpayers is through the increased leadership of Japanese organizations in Internet security, which could translate to future benefits for companies and research organizations. It is clear to many that Internet security practices need investment around the world, but the nature and size of those investments is unclear. Cyber Green could prove to be a leading organization in this next generation of Internet security and health, drawing companies and others to the Japanese economy.

## Recommendations for Future Research

The research efforts carried out in this first year of Cyber Green have yielded some insights into possible future research directions for Cyber Green or related organizations to perform. These are described in this section.

### Vulnerability Identification

One key challenge in collecting definitive vulnerability data is in testing for the existence of the vulnerability, the test may have to actually attempt an exploit. This has obvious implications for the network being scanned - reports of intrusion attempts will litter their logs, and system instability may occur as a result. Respectable survey organizations have, in the past, refused to attempt such exploits due to these fears together with legal liability if something goes wrong.

One possible solution is for a body of trusted organizations to create and distribute vulnerability tests that are both definitive and non-harmful. These tools would then be run by the CERTs against their own customer networks to gather data. The data would also be directly comparable between participating organizations because the same methodology was used.  A major risk of this approach is that not every CERT will have the resources to run these scans and surveys on a regular basis, leading to no benefit. A major downside of this approach is that the pooling of data would be optional, thwarting Internet-wide measurements.

### Gaps in Calculating Comprehensive Cyber Health Indicators

The World Health Organization (WHO), a global body established to promote best practices health in developing and developed countries, publishes regular reports about health conditions, risks to public health, and the factors that affect health. These indicators include direct health measurements and also key environmental factors that affect health, such as access to health professionals or clean water, or the prevalence of open-air cooking, a major source of carcinogens[85]. While we do not yet have a complete set of analogs in cyber, this is an interesting exercise to discover possible cyber environmental factors affecting Internet risks per country or region. A preliminary mapping of these indicators is shown in Table 8.

| **WHO Indicator** | **Cyber Indicator Analog** |
|---|---|
| Life expectancy and mortality | (Mean time to scan/exploit) |
| Cause specific mortality | Infection data, (PC replacement data) |
| Health services coverage | (End-user service organizations) |
| Risk factors (clean water, sanitation, etc) | Vulnerability data, AV rates, piracy rates |
| Health workforce and infrastructure | (Cybersecurity population) |
| Health expenditure | ICT budget |
| Health inequities (residence, income, education) | (Census demographics) |
| Demographics | ICT demographics |

*Table 8: Mapping WHO public health indicators to possible cyber health indictors. Cyber indicators with no known source are shown in parentheses. WHO indicators taken from the sections of [85].*

Existing data captures some of these indicators on the right-hand, but many more are not quantified at all. Life expectancy, for example, is not routinely measured. Various research projects have explored the mean time to probe and exploit a honeypot, but none of these are ongoing measurements. This value is important, as it is the window of vulnerability for a new PC to get out of the box and begin patching. In this time the system may be compromised and forever set back.

Another data point that would be interesting to measure would be related to "cause specific mortality", looking at PC replacement data. Many end users simply throw away old systems that have become infected and burdened with malware leading to poor performance, meaning this PC replacement data could be a window into this aspect.

Access to health-care has a simple analog in cybersecurity: access to professionals who can diagnose and repair broken PCs, or properly set them up. While (ISC)$^2$ data is available per-country[86], other education efforts or certifications such as A+ or SANS certified professionals is not easily available. This number would be interested to correlate to cybersecurity incidents per country to discover any possible relationship; a positive relationship would indicate a return on investing in such training in a broader sense. This should lead to some understanding of the "mismanagement" node in Figure 26. In the US, the Bureau of Labor Statistics tracks the number of cybersecurity professionals as "Information Security Analysts"[88]. An international source of these numbers is being sought. A similar statistic would be the number of computer science students who graduate each year.

At present census demographics and the various inequities in them are available through statistics gathered by existing government and international bodies, but we do not include this data yet for correlation in Cyber Green. This may be a fruitful avenue to explore.

## Related Efforts

Since the start of Cyber Green, a number of related efforts have been brought to our attention. Note that in most cases these efforts address different aspects of the challenge that Cyber Green is addressing, meaning that Cyber Green is not duplicative.

### OECD Efforts

The Organization for Economic Co-operation and Development (OECD), an international body aimed at promoting development by working with policymakers, has been studying cyber security efforts for several years as part of their Working Party on Information Security and Privacy. Evidence-based cybersecurity policy making has become one of their efforts, and recent work on guidance for improving the international comparability of CSIRT statistics is being compiled in a report[72], building on a 2012 report the group produced[47]. The information to be gathered by the OECD includes CSIRT budget, staffing, training and incident capacity. The aim of this is to begin to cross-compare CSIRT organization and to understand the return on investment that countries make.

This OECD effort complements the Cyber Green Project efforts by collecting data, and standardizing the data, that may be correlated to incident and risk data gathered by the Cyber Green Project.

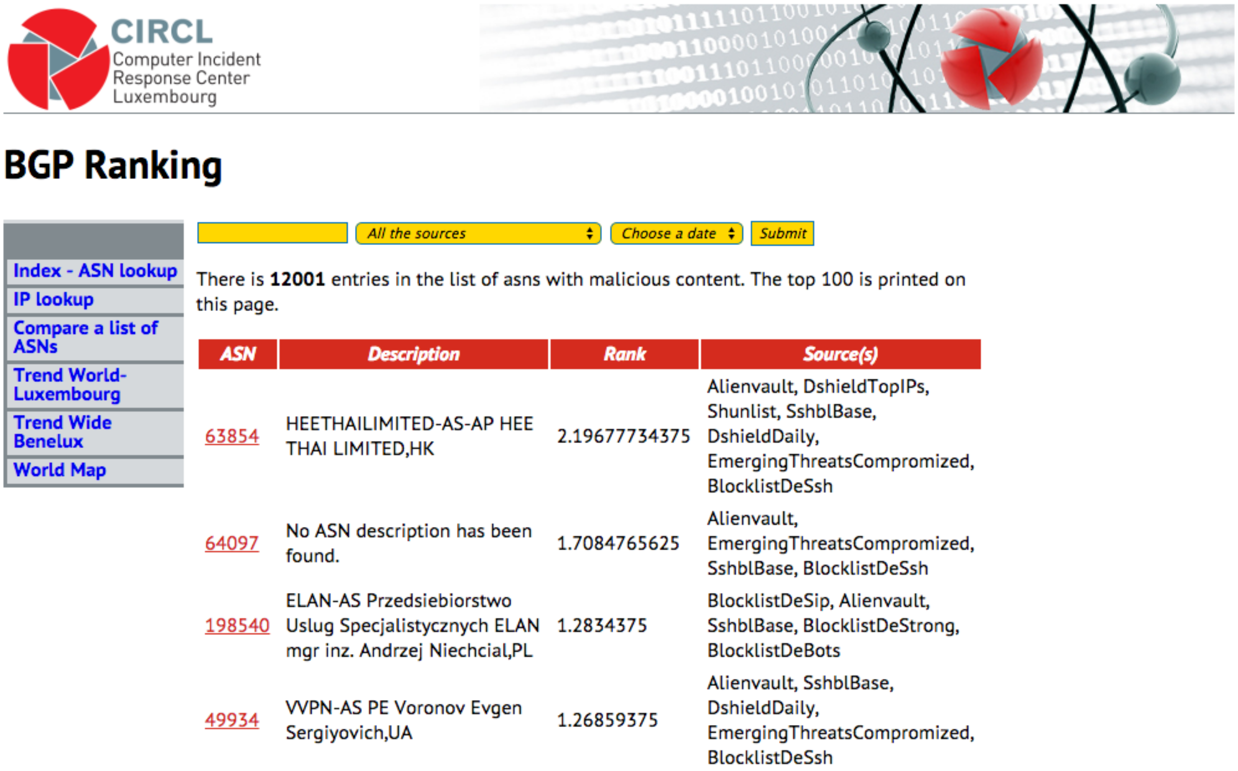
### ENISA Efforts

The European Network and Information Security Agency (ENISA), an effort set up by the European Union (EU) and assisting the European Commission (EC), has been focused on operational assistance to member CSIRTs and related CSIRTs around the world. Specifically, ENISA has produced reports in recent years focused on incident data sources, CSIRT best practices, and recently how CSIRTs may gather and utilize actionable information about security incidents[76,77]. ENISA is also funding the NECOMA project[78], focused on incident data distribution, and has developed the **n6** data interchange tool to assist this[87].

These ENISA efforts complement the Cyber Green Project data collection efforts, but do not examine any statistical analysis of the data, a key activity of Cyber Green Project.

### CIRCL BGP Ranking

The Computer Incident Response Center Luxembourg (CIRCL) BGP Ranking site[79] is an effort to rank autonomous systems (ASNs) by the frequency with which they appear in various blacklists, either by domain name (resolved to IPs) or by IP address, which are then mapped to the origin ASN.



BGP Ranking

There is **12001** entries in the list of asns with malicious content. The top 100 is printed on this page.

| ASN | Description | Rank | Source(s) |
|---|---|---|---|
| 63854 | HEETHAILIMITED-AS-AP HEE THAI LIMITED,HK | 2.19677734375 | Alienvault, DshieldTopIPs, Shunlist, SshblBase, DshieldDaily, EmergingThreatsCompromized, BlocklistDeSsh |
| 64097 | No ASN description has been found. | 1.7084765625 | Alienvault, EmergingThreatsCompromized, SshblBase, BlocklistDeSsh |
| 198540 | ELAN-AS Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz. Andrzej Niechcial,PL | 1.2834375 | BlocklistDeSip, Alienvault, SshblBase, BlocklistDeStrong, BlocklistDeBots |
| 49934 | VVPN-AS PE Voronov Evgen Sergiyovich,UA | 1.26859375 | Alienvault, SshblBase, DshieldDaily, EmergingThreatsCompromized, BlocklistDeSsh |

*Figure 29: CIRCL BGP Ranking site showing their most malicious ASNs and the data sources that combined to yield that ranking.*

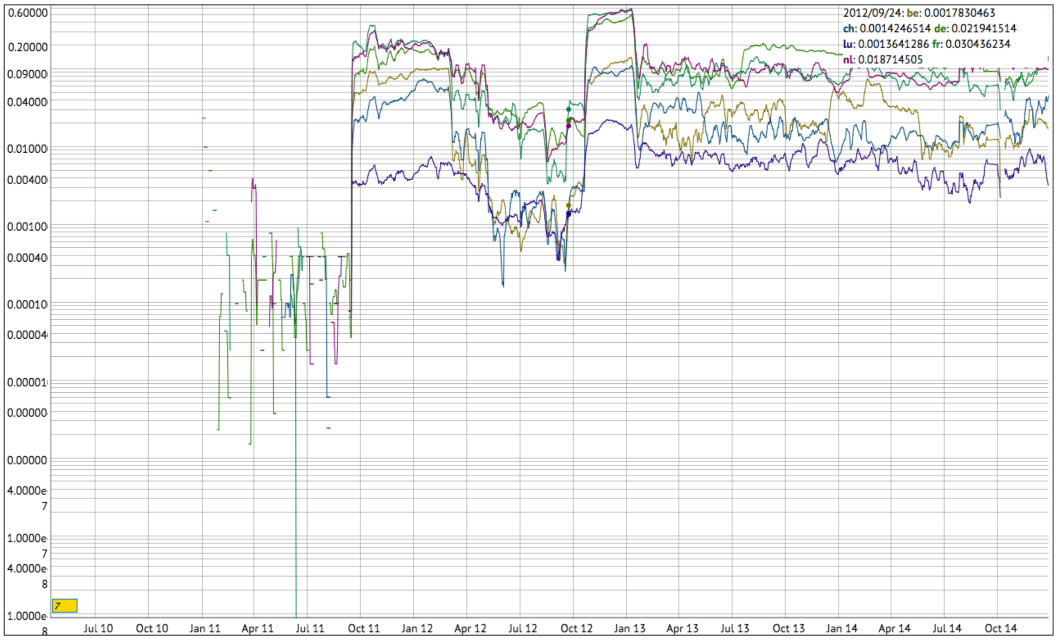
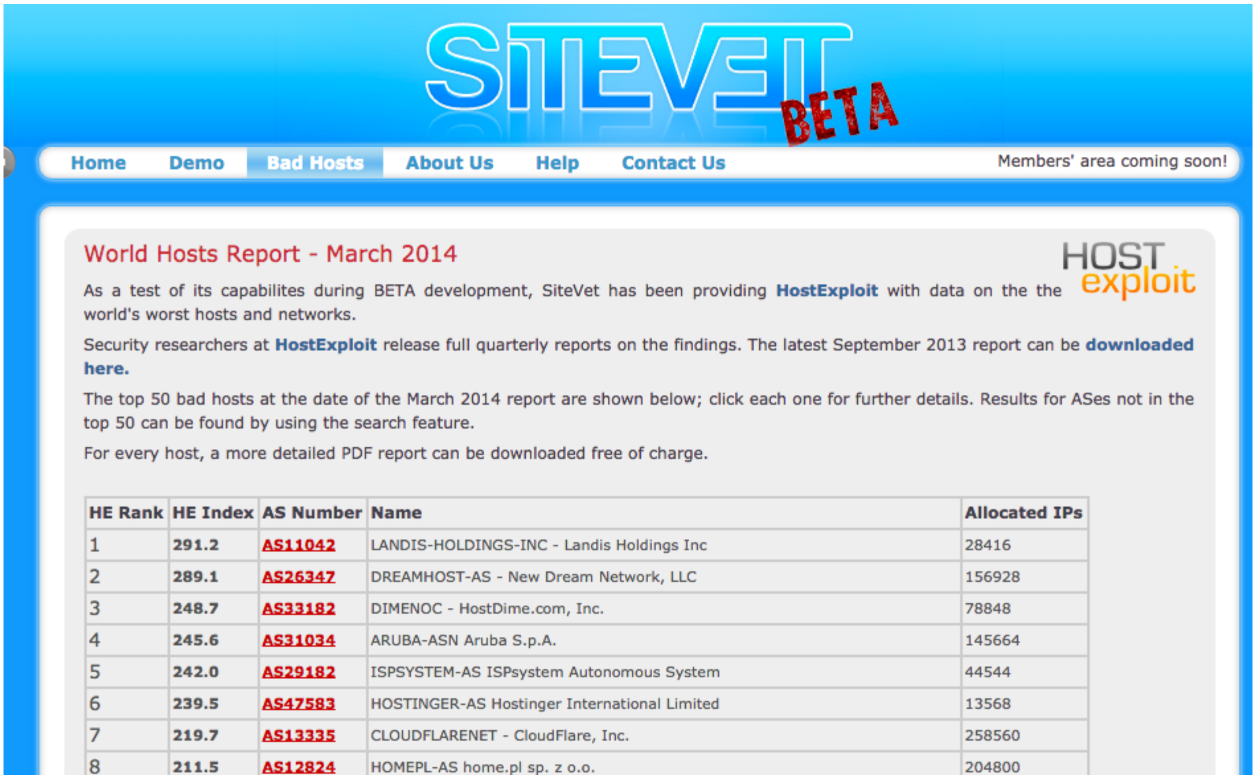


*Figure 30: CIRCL BGP Ranking scores over time for various countries. While there is some noise you can see the relative stability of those scores.*

Aside from combining blacklists as data sources to find hotspots, the CIRCLE BGP Ranking site has little in common with the Cyber Green Project's efforts. Unlike the Cyber Green Metrics data analysis, there is no statistical rigor, little transparency, and no attempt is made to do root-cause analysis in the CIRCL BGP Ranking presentation.

## SiteVet

Similar to the CIRCL BGP Ranking, the HostExploit group has created a website called SiteVet[80] that ranks ASNs by their maliciousness reported and discovered in various feeds. SiteVet is backed in part by Nominet, a UK domain registry. The goal of SiteVet is to discover which ASNs are hosting maliciousness to enable network operators to flag such traffic for further investigation.



World Hosts Report - March 2014

As a test of its capabilites during BETA development, SiteVet has been providing **HostExploit** with data on the the world's worst hosts and networks.

Security researchers at **HostExploit** release full quarterly reports on the findings. The latest September 2013 report can be **downloaded here.**

The top 50 bad hosts at the date of the March 2014 report are shown below; click each one for further details. Results for ASes not in the top 50 can be found by using the search feature.

For every host, a more detailed PDF report can be downloaded free of charge.

| HE Rank | HE Index | AS Number | Name | Allocated IPs |
|---|---|---|---|---|
| 1 | 291.2 | AS11042 | LANDIS-HOLDINGS-INC - Landis Holdings Inc | 28416 |
| 2 | 289.1 | AS26347 | DREAMHOST-AS - New Dream Network, LLC | 156928 |
| 3 | 248.7 | AS33182 | DIMENOC - HostDime.com, Inc. | 78848 |
| 4 | 245.6 | AS31034 | ARUBA-ASN Aruba S.p.A. | 145664 |
| 5 | 242.0 | AS29182 | ISPSYSTEM-AS ISPsystem Autonomous System | 44544 |
| 6 | 239.5 | AS47583 | HOSTINGER-AS Hostinger International Limited | 13568 |
| 7 | 219.7 | AS13335 | CLOUDFLARENET - CloudFlare, Inc. | 258560 |
| 8 | 211.5 | AS12824 | HOMEPL-AS home.pl sp. z o.o. | 204800 |

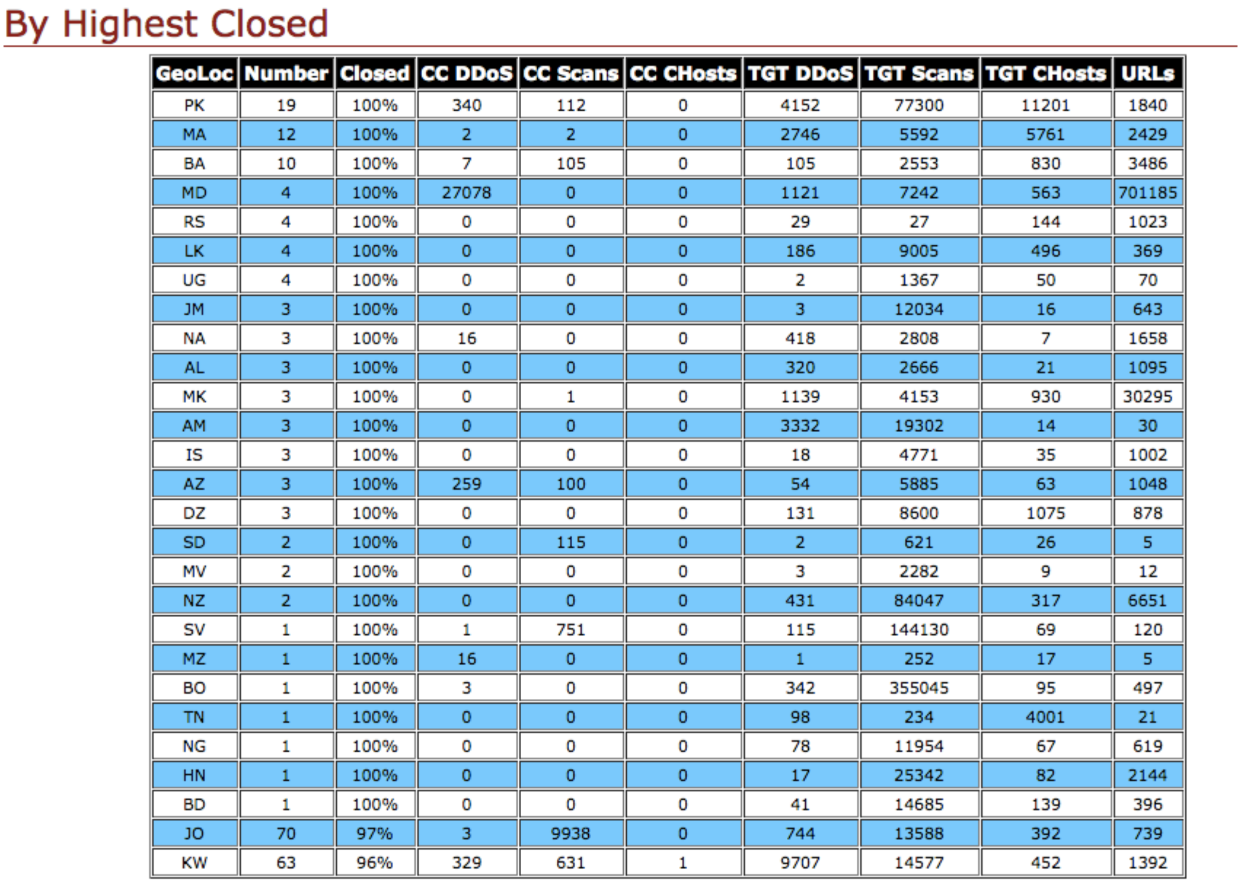
*Figure 31: SiteVet ASN ranking page.*

Similar to the CIRCL BGP Ranking tool, SiteVet has little in the way of statistical rigor, transparency, and no root-cause analysis. This means it has little in common with the Cyber Green Project's efforts.

## ShadowServer

Shadowserver, a non-profit organization that analyzes malware to discover and track botnets, produces some limited statistics on their data covering botnets, infected clients, and the like[54]. The goal of their process is to identify which countries are responsive and which ones are not, and to identify which countries they need to establish relations with.

Similar to CIRCL BGP Ranking, ShadowServer has little in the way of statistical rigor and no root-cause analysis. There is little validation of the data, little discrimination of malicious servers compared to servers that appear in executables, and the like, and no normalization or correlation. As such it has little in common with the Cyber Green Project's efforts.



By Highest Closed

| GeoLoc | Number | Closed | CC DDoS | CC Scans | CC CHosts | TGT DDoS | TGT Scans | TGT CHosts | URLs |
|---|---|---|---|---|---|---|---|---|---|
| PK | 19 | 100% | 340 | 112 | 0 | 4152 | 77300 | 11201 | 1840 |
| MA | 12 | 100% | 2 | 2 | 0 | 2746 | 5592 | 5761 | 2429 |
| BA | 10 | 100% | 7 | 105 | 0 | 105 | 2553 | 830 | 3486 |
| MD | 4 | 100% | 27078 | 0 | 0 | 1121 | 7242 | 563 | 701185 |
| RS | 4 | 100% | 0 | 0 | 0 | 29 | 27 | 144 | 1023 |
| LK | 4 | 100% | 0 | 0 | 0 | 186 | 9005 | 496 | 369 |
| UG | 4 | 100% | 0 | 0 | 0 | 2 | 1367 | 50 | 70 |
| JM | 3 | 100% | 0 | 0 | 0 | 3 | 12034 | 16 | 643 |
| NA | 3 | 100% | 16 | 0 | 0 | 418 | 2808 | 7 | 1658 |
| AL | 3 | 100% | 0 | 0 | 0 | 320 | 2666 | 21 | 1095 |
| MK | 3 | 100% | 0 | 1 | 0 | 1139 | 4153 | 930 | 30295 |
| AM | 3 | 100% | 0 | 0 | 0 | 3332 | 19302 | 14 | 30 |
| IS | 3 | 100% | 0 | 0 | 0 | 18 | 4771 | 35 | 1002 |
| AZ | 3 | 100% | 259 | 100 | 0 | 54 | 5885 | 63 | 1048 |
| DZ | 3 | 100% | 0 | 0 | 0 | 131 | 8600 | 1075 | 878 |
| SD | 2 | 100% | 0 | 115 | 0 | 2 | 621 | 26 | 5 |
| MV | 2 | 100% | 0 | 0 | 0 | 3 | 2282 | 9 | 12 |
| NZ | 2 | 100% | 0 | 0 | 0 | 431 | 84047 | 317 | 6651 |
| SV | 1 | 100% | 1 | 751 | 0 | 115 | 144130 | 69 | 120 |
| MZ | 1 | 100% | 16 | 0 | 0 | 1 | 252 | 17 | 5 |
| BO | 1 | 100% | 3 | 0 | 0 | 342 | 355045 | 95 | 497 |
| TN | 1 | 100% | 0 | 0 | 0 | 98 | 234 | 4001 | 21 |
| NG | 1 | 100% | 0 | 0 | 0 | 78 | 11954 | 67 | 619 |
| HN | 1 | 100% | 0 | 0 | 0 | 17 | 25342 | 82 | 2144 |
| BD | 1 | 100% | 0 | 0 | 0 | 41 | 14685 | 139 | 396 |
| JO | 70 | 97% | 3 | 9938 | 0 | 744 | 13588 | 392 | 739 |
| KW | 63 | 96% | 329 | 631 | 1 | 9707 | 14577 | 452 | 1392 |

*Figure 32: One of the statistics reports produced by ShadowServer, showing the closure rate for their tickets reported to ISPs and CSIRTs grouped by country.*

## SpamRankings

Professor Andrew B. Whinston of the University of Texas at Austin has begun a project dubbed SpamRankings, funded in part by the US National Science Foundation, to use spam emissions as indicators of network hygiene[83]. Prof. Whinston publishes the results, attempting to incentivize network operators to reduce their spam rates. The link between spam and network hygiene is described on their site as:

> *Outbound spam indicates botnets, botnets indicate vulnerabilities, and vulnerabilities indicate susceptibility to other malware, including phishing, DDoS, and other malware, so outbound spam is a proxy for poor organizational security on the part of any Email Service Provider (ESP), that is, any organization that sends email (not just ISPs), regardless of whether the ESP is a bank, a university, or a hospital.*

Spam rates are aggregated by network operator and country.

Comparing SpamRankings to Cyber Green, both projects are attempting to inform the debate on cyber health through the generation of metrics. Unlike Cyber Green, SpamRankings is focused solely on the volume of spam as an indicator of network hygiene, while Cyber Green attempts a more comprehensive, risk and incident model.

### Cybercrime and Economic Risks: The Italian Study

A 2014 report by the United Nations Interregional Crime and Justice Research Institute (UNICRI) looked at the impact of cybercrime at the national (Italy) and international level[89]. Conducted using interviews, the author found that the approach taken to protect small and medium-sized enterprises in Italy is uneven, and that additional safeguards must be taken to address this. The study looks mostly at the types of attacks that SMEs in Italy face, and only briefly at technical and user risks.

Comparing this study to Cyber Green, both projects attempt to understand the risk and threat landscape as they affect economies. However, this study was firstly only a single snapshot in time and is not ongoing, secondly conducted using surveys and not network measurement data, and thirdly focused largely on broad ideas rather than specific failings to defend SMEs against cybercrime.

### Patent: Method, system, and service for quantifying network risk to price insurance premiums and bonds

Patent US8494955, by Quarterman, Cassidy and Phillips, is a granted patent entitled "Method, system, and service for quantifying network risk to price insurance premiums and bonds"[84]. The patent is focused on enterprise-specific features with a specific use case of pricing insurance or bond prices. From the abstract:

> *The invention broadly comprises a method for determining financial loss related to performance of an internetwork. The method correlates input information regarding performance of an internetwork to operations of a financial entity underwriting insurance premiums and bonds and translates the correlated input information into at least one operational risk for the entity. In some aspects, the internetwork is the Internet. The method gathers secondary external information other than directly from the internetwork, correlates the input and secondary external information, and translates the correlated input and secondary external information into at least one operational risk for the entity.*

Similar to Cyber Green, the authors of this patent attempt a holistic fusion of data to understand and quantify risk. Unlike Cyber Green, however, the method is specific to the domain of enterprise security and insurance premium schedules.

### SENDS

The Science Enhanced Network Domains and Secure Social Spaces (SENDS)[81] project describes itself as “integrating across the entire scientific landscape of study a transdisciplinary effort that seeks to explain and predict the nature of emergence and connectivity that cyberspace enables.” Working with academia and operations groups, SENDS conducted studies and developed an education curriculum to explore the complexity of cyber security and connectedness.

*Figure 33: SENDS logo.*

SENDS funding has ended, but the project investigators developed a far more comprehensive and rigorous project than many others.  Unlike Cyber Green, SENDS was not specific to cybersecurity but instead focused on how organizations might realize the full potential of Internet communications.

### George Washington University Security Policy and Research Institute

The George Washington University Security Policy and Research Institute describes itself as “a center for GW and the Washington area to promote technical research and policy analysis of issues that have a significant computer security and information assurance component.”[82] Previous research projects run by the institute have looked at narrow topics such as cryptography technologies, while some have looked at broader questions such as education, privacy and civil liberties, and research coordination.

While the CSPRI looks at various technical and public policy aspects, only a handful of projects are data-driven like the Cyber Green Project effort aims to be and none are focused on risk measurement and reduction. As such it is complementary to the Cyber Green Project effort, leaving significant room for the Cyber Green Project to look at informing public policy makers with incident and risk data.

### Summary of Related Efforts

Looking at the above efforts that relate to the methods and goals of Cyber Green, it is clear that the Cyber Green Project operates in an adjacent space but with very little overlap with most efforts. The most similar project, the OECD efforts around CSIRT metrics, will complement the Cyber Green Metrics and hopefully provide some data for the Cyber Green Project for correlation. However, the Cyber Green Project appears unique in its goal of statistically meaningful results driven in part on cybersecurity measurements, with the aim of informing policymakers.

## Appendices

### List of Interview Subjects

The following individuals have been interviewed or have been involved in discussions on the topics in this paper. Discussions focused on topics such as the utility of data, data capture methods, data comparison methods, data utility in incident response, and data insights that are lacking.

Their help and insights have been greatly appreciated.

- Mike Johnson, Shadowserver
- Paul Vixie, Farsight
- Marc Eisenbart, Arbor Networks
- Marieke Kaeo, Internet Identity
- Jeff Stutzman, Red Sky Alliance
- Byron Collie, Goldman Sachs
- Chris Horsley, CSIRT Foundry
- Manish Karir, Merit Network/Quadmetrics

## Example Cyber Green Analysis: TLD Costs vs Blacklist Rates

One of the key questions in addressing cybercrime is how to apply economics to the problem. Specifically, how can we raise the costs for attackers above the returns they may enjoy, to make cybercrime less attractive. Domain name registration costs present one possible avenue for these costs.

To study the possible return on this approach, we analyzed Cyber Green data to look for a correlation between the cost to register a domain name and occurrence of blacklisting for a domain name with that TLD. Grouping the unique domain names together by TLD, we can begin to assess the likely outcome of this approach. Starting with the hypothesis that there will be a negative correlation between the two, data about blacklisted domains for several days was aggregated. These URLs and domain names represent malware and phishing, common avenues for cybercrime.

What we found, shown in the figure below, while there exists a negative correlation, it is not as absolute as we would want to justify raising domain name registration prices in an effort to combat cybercrime. The figure shows the count of unique domain names, grouped by TLD, on the x-axis and the cost to register a domain name on the y-axis. The movement of the data down and to the right across this plot (note that the number of unique domains for any TLD is on a log base 10 scale) is consistent with the hypothesis, but the crowding in the lower left corner suggests that this relationship is not absolute. An outlier, .tt, presents an interesting case, way off the trend.

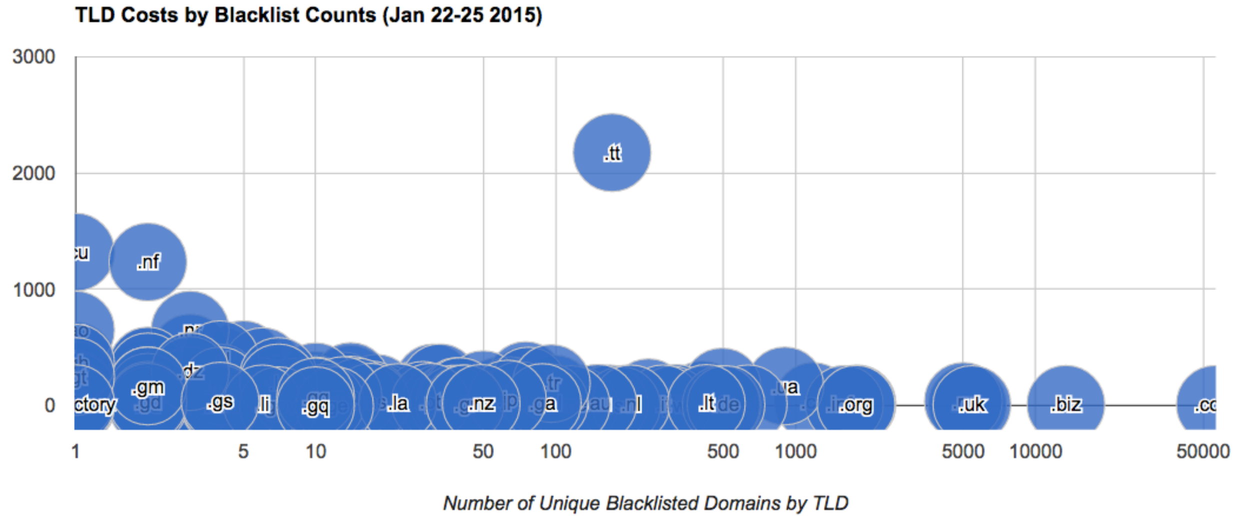


*Figure 34: TLD costs by Blacklist Counts for 3 days in January, 2015. Data sources: Domain and URL blacklists from Abuse.ch, PhishTank, CleanMX, MalwareDomains, OpenPhish, Siri-urz, and URLQuery for January 22-25 2015; TLD cost data aggregated by tld-list.com.*

Given this result, raising prices to combat cybercrime would have too great a risk on legitimate domain name registration and the resulting net-positive contributions to the economy and too little effect on cyber crime. But this simple example illustrates the power of analysis and correlation in hypothesis testing to combat cybercrime.

## References

1. Expectations for Computer Security Incident Response, https://www.csirt.org/rfc_csirt/doc/rfc2350.txt Brownlee and Guttman, 1998. Also known as BCP 21.

2. Smurf Amplifier Registry (SAR), http://smurf.powertech.no/

3. Spam and Open Relay Blocking System (SORBS), http://www.sorbs.net/

4. SANS Top 20 Critical Security Controls Version 5 http://www.sans.org/critical-security-controls

5. SHADOW MARKET 2011 BSA Global Software Piracy Study Ninth edition, May 2012, http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

6. Website Security Statistics Report, May 2013, WhiteHat Security, https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf

7. Google Hacking Database, GHDB, Google Dorks

8. OpenNTPProject, http://openntpproject.org/

9. Open Resolver Project, http://openresolverproject.org/

10. Internet-Wide Scan Data Repository, https://scans.io/

11. Heartbleed Survey, http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html

12. AV Comparatives User Survey, http://www.av-comparatives.org/wp-content/uploads/2014/03/security_survey2014_en.pdf

13. Stories as Informal Lessons about Security, Rader et al 2012

14. MITRE CME http://cme.mitre.org/about/faqs.html

15. Microsoft Smart Network Data Services https://postmaster.live.com/snds/index.aspx

16. RFC 5070, IODEF http://www.ietf.org/rfc/rfc5070.txt

17. OpenIOC Framework http://www.openioc.org/

18. MITRE CyBOX http://cybox.mitre.org/

19. MITRE STIX https://stix.mitre.org/

20. MITRE TAXII http://taxii.mitre.org/

21. Securi SiteCheck http://sitecheck.sucuri.net/

22. Freiling, Felix C., Thorsten Holz, and Georg Wicherski. Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks. Springer Berlin Heidelberg, 2005.

23. Common Crawl, http://commoncrawl.org/

24. Worldwide Infrastructure Security Report, Arbor Networks http://www.arbornetworks.com/resources/infrastructure-security-report

25. Bellovin, Steven M. "A technique for counting NATted hosts." In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, pp. 267-272. ACM, 2002.

26. Casado, Martin, and Michael J. Freedman. "Peering through the shroud: The effect of edge opacity on IP-based client identification." In Proceedings of the 4th USENIX conference on Networked systems design & implementation, pp. 13-13. USENIX Association, 2007.

27. Maier, Gregor M. "Residential broadband internet traffic: characterization and security analysis." PhD diss., TU Berlin, 2010.

28. Bailey, Michael, Evan Cooke, Farnam Jahanian, David Watson, and Jose Nazario. "The Blaster Worm: Then and Now." IEEE Security and Privacy 3, no. 4 (2005): 26-31.

29. Krmicek, Vojtech, Jan Vykopal, and Radek Krejci. "Netflow based system for NAT detection." In Proceedings of the 5th international student workshop on Emerging networking experiments and technologies, pp. 23-24. ACM, 2009.

30. Allocation of IP addresses by country https://www.countryipblocks.net/allocation-of-ip-addresses-by-country.php

31. Kuhrer, M., Thomas Hupperich, Christian Rossow, and Thorsten Holz. "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks." In USENIX Security Symposium. 2014.

32. Zhang, Jing, Zakir Durumeric, Michael Bailey, Mingyan Liu, and Manish Karir. "On the Mismanagement and Maliciousness of Networks." In to appear) Proceedings of the 21st Annual Network & Distributed System Security Symposium (NDSS'14), San Diego, California, USA. 2013.

33. Provos, Niels et al. "The ghost in the browser analysis of web-based malware." Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets 10 Apr. 2007: 4-4.

34. Mundie, David A, and David M McIntire. "The MAL: A Malware Analysis Lexicon." CERT® Program-Carnegie Mellon University, Technical (2013).

35. CARO: Basic malware definitions http://www.caro.org/definitions/

36. Stop Think Connect website http://www.stopthinkconnect.org/

37. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, Ferguson and Senie, 2000. http://tools.ietf.org/html/bcp38

38. Stone-Gross, Brett et al. "The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns." USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET) 29 Mar. 2011.

39. Graham, Paul. "A plan for spam, 2002." Available from World Wide Web: http://www.paulgraham.com/spam.html (2003).

40. McGregor, Colin. "Controlling spam with SpamAssassin." Linux J 153.1 (2007).

41. PhishTank http://www.phishtank.com/

42. World Health Organizations Data and Statistics, http://www.who.int/en/

43. Up to Three Percent of Internet Traffic is Malicious, Researcher Says, CSO Online (2008) http://www.csoonline.com/article/2122506/data-protection/up-to-three-percent-of-internet-traffic-is-malicious--researcher-says.html

44. Senderbase spam statistics, August 2014 https://www.senderbase.org/static/spam/#tab=0

45. OPSWAT Market Share Report: Antivirus, Backup, and P2P: August 2013 http://www.opswat.com/about/media/reports/antivirus-august-2013

46. Fleming, Matthew H., and Eric Goldstein. "Evaluating the Impact of Cybersecurity Information Sharing on Cyber Incidents and Their Consequences." Available at SSRN (2014).

47. IMPROVING THE EVIDENCE BASE FOR INFORMATION SECURITY AND PRIVACY POLICIES, 20 December 2012, by the OECD DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, Working Party on Information Security and Privacy. Document ID DSTI/ICCP/REG(2011)10/FINAL. Available online at http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282011%2910/FINAL&docLanguage=En

48. Yegneswaran, Vinod, Paul Barford, and Dave Plonka. "On the design and use of Internet sinks for network abuse monitoring." Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2004.

49. Spitzner, Lance. Honeypots: tracking hackers. Vol. 1. Reading: Addison-Wesley, 2003.

50. Project Sonar, Rapid7. https://sonar.labs.rapid7.com/

51. DNS and Randomness, Niels Provos, July 13, 2008. http://www.provos.org/index.php?/archives/42-DNS-and-Randomness.html

52. Cooke, Evan, Zhuoqing Morley Mao, and Farnam Jahanian. "Hotspots: The root causes of non-uniformity in self-propagating malware." Dependable Systems and Networks, 2006. DSN 2006. International Conference on. IEEE, 2006.

53. Shinoda, Yoichi, Ko Ikai, and Motomu Itoh. "Vulnerabilities of Passive Internet Threat Monitors." USENIX Security. 2005.

54. The Shadowserver Project. https://www.shadowserver.org/

55. Armitage, Grenville J. "Inferring the extent of network address port translation at public/private internet boundaries." Centre for Advanced Internet Architectures, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. A 20712 (2002).

56. Heidemann, John, et al. "Census and survey of the visible internet." Proceedings of the 8th ACM SIGCOMM conference on Internet measurement. ACM, 2008.

57. Shannon, Colleen, and David Moore. "The spread of the witty worm." Security & Privacy, IEEE 2.4 (2004): 46-50.

58. Frei, Stefan. "SQL Slammer Worm."

59. Wikipedia, Doubling time, 2015. http://en.wikipedia.org/wiki/Doubling_time

60. Wikipedia, Half life, 2015. http://en.wikipedia.org/wiki/Half-life

61. Nazario, Jose, and Thorsten Holz. "As the net churns: Fast-flux botnet observations." Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on. IEEE, 2008.

62. Messaging Anti-Abuse Working Group Issues Recommendation for Managing Port 25 MAAWG Advocates Self-Regulation to Cut Spam and Viruses, 2005. http://www.astra.cc/Client%20News/MAAWG%202005-12-Managing%20Port%2025%20BP.html

63. 2% of Internet Traffic Raw Sewage, Danny Mcpherson, 2008/ http://www.arbornetworks.com/asert/2008/03/2-of-internet-traffic-raw-sewage/

64. Cooke, Evan, Farnam Jahanian, and Danny McPherson. "The zombie roundup: Understanding, detecting, and disrupting botnets." Proceedings of the USENIX SRUTI Workshop. Vol. 39. 2005.

65. Czyz, Jakub, et al. "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks." Proceedings of the 2014 Conference on Internet Measurement Conference. ACM, 2014.

66. 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/

67. August, Terrence, and Tunay I. Tunca. "Let the pirates patch? An economic analysis of software security patch restrictions." Information Systems Research 19.1 (2008): 48-70.

68. IP numbers per County, https://ipduh.com/macro/ip/countries/

69. The ICT Facts and Figures features the latest estimates for ITU's key telecommunication/ICT indicators, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

70. OECD Broadband Portal, http://www.oecd.org/internet/oecdbroadbandportal.htm

71. Alexa Top 1 Million Sites, http://s3.amazonaws.com/alexa-static/top-1m.csv.zip

72. OECD Security and Privacy Indicators, Improving the international comparability of CSIRT statistics http://www.oecd.org/sti/ieconomy/informationsecurityandprivacyindicators.htm

73. World Bank, International surveys of ICT use in education http://go.worldbank.org/0MO795SIP0

74. The Link between Pirated Software and Cybersecurity Breaches, 2014. http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf

75. Spoofer Project: Spoofer Main, http://spoofer.cmand.org/

76. Standards and tools for exchange and processing of actionable information, ENISA, 2015. http://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information

77. Actionable information for security incident response, ENISA, http://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security

78. NECOMA, Nippon-European Cyberdefense-Oriented Multilayer threat Analysis, http://www.necoma-project.eu/

79. BGP Ranking, CIRCL, http://bgpranking.circl.lu/

80. SiteVet, World Hosts Report, http://sitevet.com/hosts/

81. Science Enhanced Network Domains and Secure Social Spaces (SENDS), http://sendsonline.org/

82. Cyber Security Policy and Research Institute (CSPRI), George Washington University, http://www.cspri.seas.gwu.edu/

83. SpamRankings, Outbound spam rankings as a proxy for organizational security, http://www.spamrankings.net/

84. Patent US8494955, Quarterman, Cassidy and Phillips, Method, system, and service for quantifying network risk to price insurance premiums and bonds, 2013.

85. World Health Statistics 2012: Part III: Global Health Indicators, World Health Organization, http://www.who.int/healthinfo/EN_WHS2012_Part3.pdf

86. (ISC)² Member Counts, https://www.isc2.org/member-counts.aspx

87. N6: Network Security Interchange, http://n6.cert.pl/

88. Occupational Employment and Wages, May 2013, 15-1122 Information Security Analysts, U.S. Bureau of Labor Statistics | Division of Occupational Employment Statistics, http://www.bls.gov/oes/current/oes151122.htm

89. Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level, Dr. Flavia Zappa on behalf of United Nations Interregional Crime and Justice Research Institute (UNICRI), http://www.unicri.it/in_focus/files/Criminalita_informatica_inglese.pdf