Visualizing Cybersecurity Events

G. Markowsky[1] **and L. Markowsky**[1]
[1]School of Computing & Information Science, University of Maine, Orono, ME, USA

Abstract— *The old adage "a picture is worth a 1,000 words" is relevant to cybersecurity because professionals must deal with large amounts of data in a very short period. It is also relevant to cybersecurity educators who must convey the complexity of cybersecurity events to students and to members of the general public who might have little or no background in cybersecurity. Fortunately, there are many fine tools now available for visualization and there will be more such tools in the future. This paper discusses some of the tools that are available and highlights some work that deserves to be better known by cybersecurity educators.*

Keywords: visualization, cyberattacks, DoS, honeypots, Wireshark, Netstat, cybersecurity event

1. Introduction

In 1983 Edward Tufte created a stir in the area of information display by publishing his book *The Visual Display of Quantitative Information* [1]. The book went through seventeen printings before a second edition came out [2]. Tufte's book sparked a lot of interest in graphic design and the visual display of information. Since then there have been quite a few books published in the area. Some examples include books by William Cleveland [3], [4], [5], and [6]. While computers have improved tremendously over the past several decades, humans have stayed pretty much the same, so it is important to follow well-established design principles when designing effective visualizations for people.

Cleveland [3, pp. 4-15] and [4, pp. 4-22] show some examples where inadequate visualizations of data helped exacerbate problems and where clever visualizations led to the discovery of new scientific effects. These examples are of value and will help most people concerned with visualization.

We use the term *cybersecurity event* to describe any event that has implications for the cybersecurity of an individual or organization. Examples of events are the installation of a rootkit, placing malware on a system, scanning a system and even an all-out denial of service attack (DoS). Some events give little indication that they are happening and detecting them might involve the cyber equivalent of finding a needle in the haystack. Other events, like a massive distributed denial of service attack are obvious to the people involved and might involve a massive number of rapidly changing IP addresses and massive numbers of packets.

2. Static and Dynamic Images

It would appear that for visualizing cybersecurity events, dynamic images (including video) would be preferable to static images. Static images, however, have several advantages over dynamic images.

1) They can be included on ordinary paper and made available in many formats.
2) They are often easier to study and absorb than a dynamic images.
3) They are easier to produce.
4) We have many tools available for annotating static images.
5) They are less resource intensive and less expensive to produce.

Well-designed static images can tell a lot about a dynamic event. The graphic drawn by Charled Minard showing the terrible fate of Napoleon's army when it invaded Russia is shown in Figure 1. Carefully studying Figure 1 can give even the casual student a lot of information about the Russian campaign. Edward Tufte [1, p. 40] has a high regard for this graphic and states that "it may well be the best statistical graphic ever drawn."

Drawing something like Figure 1 requires a great deal of design skill. Fortunately, many ideas are relatively straightforward and can be presented effectively with much simpler graphics. Figure 2 is a graphic that we used in [7] to highlight the frequency of social engineering attacks on supercomputing clusters. We used a graphic such as this one for each of the questions on our survey. We found this to be effective for communicating the results of our survey. Graphics such as Figure 2 are relatively quick and easy to generate. Of course, the ability to make videos easily extends our ability to capture dynamic events.

Not all information that one might wish to convey is numerical in nature. Some important cybersecurity threats such as *viruses*, *worms* and *trojans* are primarily behavioral in nature and cannot be easily represented using numerical techniques. The concept of a *trojan* is derived from the well-known story of the Trojan Horse, which is some 3,000 years old. To this day, it continues to inspire stories and paintings, some of which have been used to illustrate security related concepts, e.g., Figure 3 which once was displayed on the website *www.container-it.com*.

When people adapt classical ideas to modern security concerns, they often get some of the details wrong. For example, in Figure 3 the Greeks launch their attack during

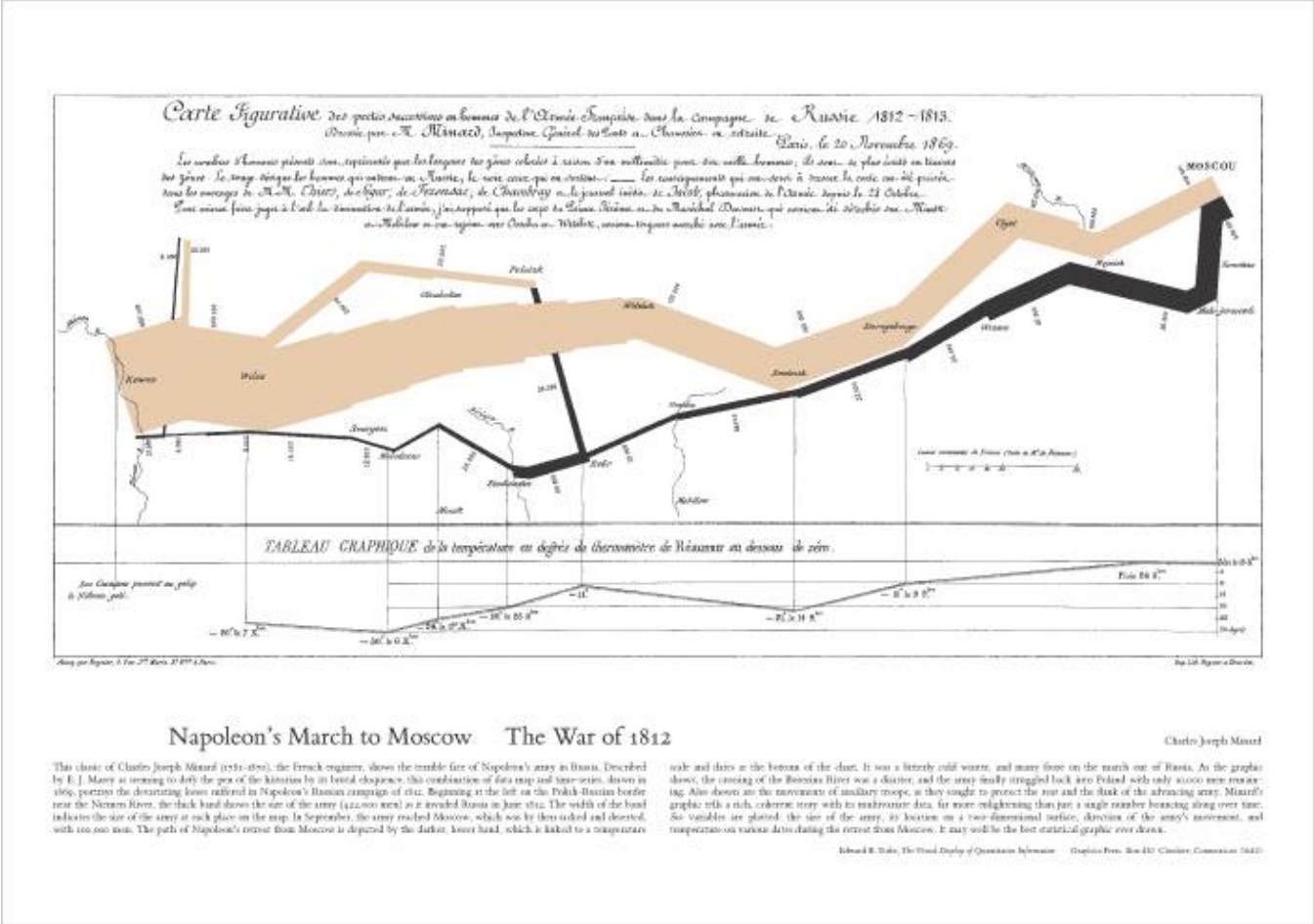


Fig. 1: A Static Image that Represents a Dynamic Event

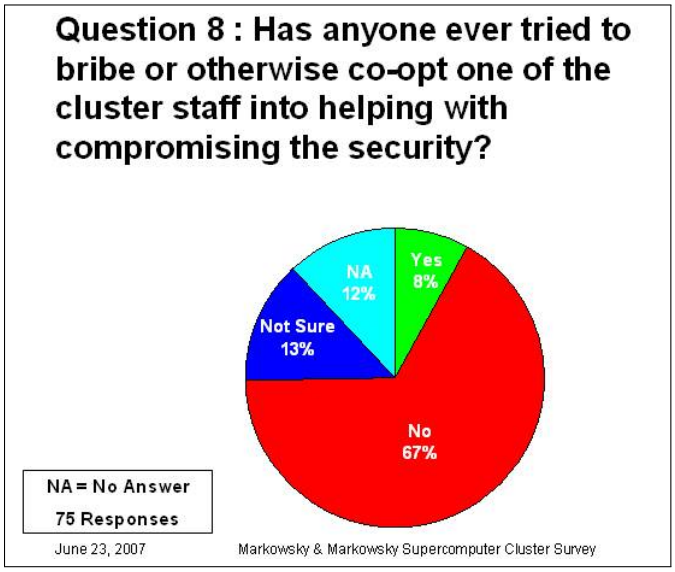


Fig. 2: The Likelihood of Insider Threats

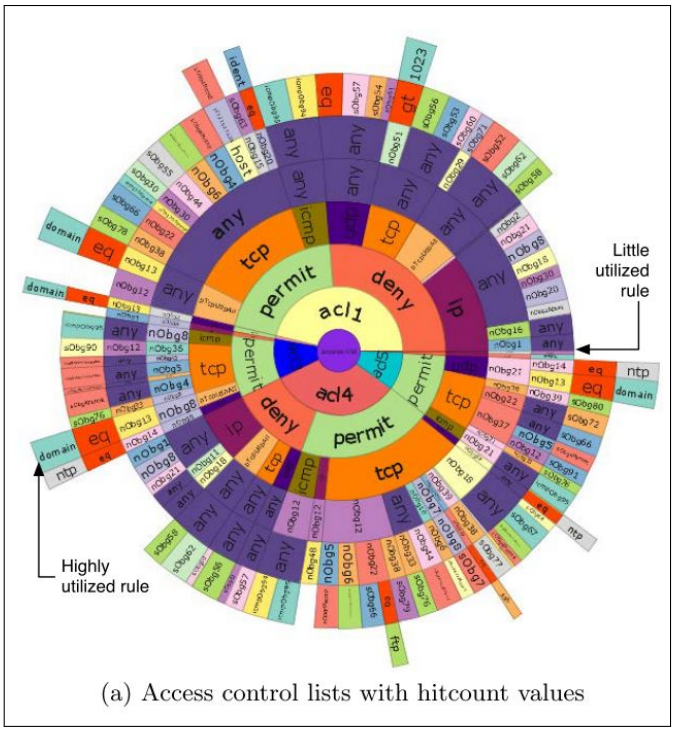
the day, whereas it clearly had to be done at night. In [8] we discussed the image on the cover of the February 22, 2010 issue of *Information Week* shown here in Figure 4. Not only was the image a very poor representation of actual castles, it was actually a very bad way to apply the castle metaphor to the problems of cybersecurity. For better ways to utilize the castle metaphor for cybersecurity education see [8]. Some very compelling ways of visualizing complex firewall configurations is discussed in [9]. A sample image from [9] is shown in Figure 5. In [10] Sven Turpe discusses some general principles for designing cybersecurity visualization tools for developers.

3. Netstat

Netstat is a standard network information gathering tool that runs on all major computing platforms. Figure 6 shows a standard NetStat display. This display carries a lot of information for people who know how to read it. In [11] we discussed how to augment the NetStat display and produce variations that are easier for novices to understand. These versions might also help experienced users use NetStat more

Fig. 3: The Trojan Horse Cargo Container

Fig. 4: A Misleading Representation of a Castle



(a) Access control lists with hitcount values

Fig. 5: Visualizing Complex Firewall Rules

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.0.114:1177        STUDYSTORE:microsoft-ds ESTABLISHED
  TCP    10.0.0.114:1269        v-client-1b:https      CLOSE_WAIT
  TCP    10.0.0.114:1399        ec2-107-20-249-77:https CLOSE_WAIT
  TCP    10.0.0.114:6500        ec2-50-18-181-105:https ESTABLISHED
  TCP    10.0.0.114:61199       sjc-not13:http         ESTABLISHED
  TCP    10.0.0.114:61280       v-d-1a:https           CLOSE_WAIT
  TCP    10.0.0.114:64201       vb-in-f103:https       ESTABLISHED
  TCP    10.0.0.114:64213       qa-in-f84:https        ESTABLISHED
  TCP    10.0.0.114:64215       lga15s28-in-f22:https  ESTABLISHED
  TCP    10.0.0.114:64422       lga15s28-in-f14:http   ESTABLISHED
  TCP    10.0.0.114:64423       lga15s28-in-f4:http    ESTABLISHED
  TCP    127.0.0.1:1030         NewtonII:5354          ESTABLISHED
  TCP    127.0.0.1:1243         NewtonII:27015         ESTABLISHED
  TCP    127.0.0.1:5354         NewtonII:1030          ESTABLISHED
  TCP    127.0.0.1:27015        NewtonII:1243          ESTABLISHED
  TCP    127.0.0.1:64225        NewtonII:64226         ESTABLISHED
  TCP    127.0.0.1:64226        NewtonII:64225         ESTABLISHED
```

Fig. 6: A Basic NetStat Display

effectively. Figre 7 illustrates the output of such a NetStat-Python combination.

Similar in style are two programs available for Windows machines called TCPview and Process Explorer. Screenshots of these programs can be seen in Figures 8 and 9. Both can be used to make valuable points about cybersecurity events.

4. Wireshark

Wireshark is a free protocol analyzer available from wireshark.org. It runs on all major computer platforms and is widely used by cybersecurity professionals. Simply running it, as illustrated in Figure 10, provides a user with a sense of how much traffice is seen by even a single computer. For

```
PORT: 135
    ('TCP', '0.0.0.0', '0.0.0.0', '0', 'LISTENING')
    ('TCPv6', '[::]', '[::]', '0', 'LISTENING')
PORT: 137
    ('UDP', '10.0.0.114', '*', '*', '')
    ('UDP', '192.168.56.1', '*', '*', '')
PORT: 138
    ('UDP', '10.0.0.114', '*', '*', '')
    ('UDP', '192.168.56.1', '*', '*', '')
PORT: 139
    ('TCP', '10.0.0.114', '0.0.0.0', '0', 'LISTENING')
    ('TCP', '192.168.56.1', '0.0.0.0', '0', 'LISTENING')
PORT: 445
    ('TCP', '0.0.0.0', '0.0.0.0', '0', 'LISTENING')
    ('TCPv6', '[::]', '[::]', '0', 'LISTENING')
PORT: 500
    ('UDP', '0.0.0.0', '*', '*', '')
    ('UDPv6', '[::]', '*', '*', '')
PORT: 546
    ('UDPv6', '[fe80::dc3:d544:ad26:ef9a%24]', '*', '*', '')
    ('UDPv6', '[fe80::58ef:5bcf:ebd6:a6db%10]', '*', '*', '')
```

Fig. 7: Using Python to Augment NetStat

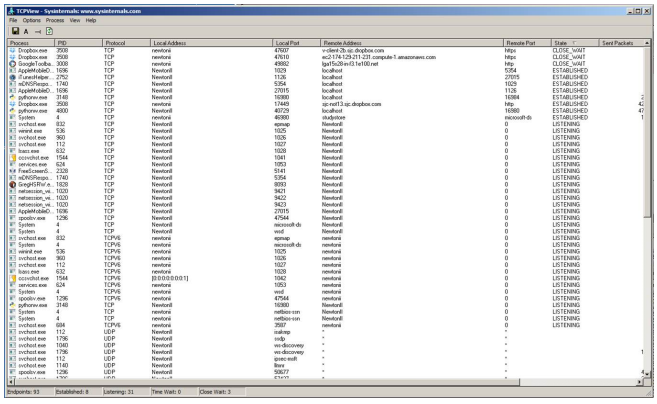


Fig. 8: A Screenshot of TCPview

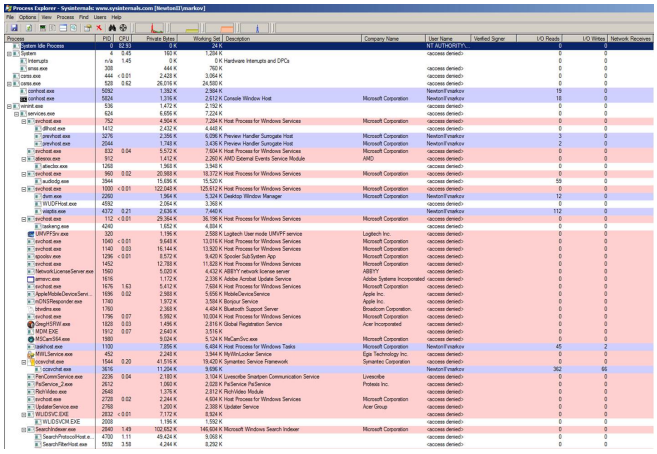


Fig. 9: A Screenshot of Process Explorer

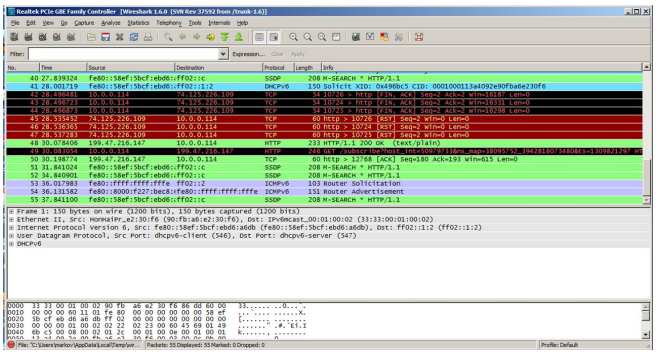


Fig. 10: A Basic Wireshark Display

Port	Protocol	State	Service	Version
139	tcp	open	netbios-ssn	
445	tcp	open	netbios-ssn	
1025	tcp	open	msrpc	Microsoft Windows RPC
1026	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	msrpc	Microsoft Windows RPC
1028	tcp	open	msrpc	Microsoft Windows RPC
1045	tcp	open	msrpc	Microsoft Windows RPC
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8093	tcp	open	http	Indy httpd 9.00.10 (.NET 1.0.2001.0; Acer Registration Service; greghsrw.exe)
47544	tcp	open	msrpc	Microsoft Windows RPC

Fig. 11: A Basic NMap Display

most effectiveness, a sequence of Wireshark screenshots can provide a compelling story of network activity.

5. NMap

NMap is a free security scanner available from nmap.org. Like Wireshark, NMap runs on all major computer platforms and is widely used by cybersecurity professionals. A basic display is shown in Figure 11. One of the nice features of NMap is its ability to produce a useful picture of a network's topology. A sample picture is shown in Figure 12. Figure 13 shows some of the memorable icons that NMap uses to describe the security rating of various systems and also icons that it uses to represent different operating systems. For maximum effectiveness a variety of NMap images can be combined to tell the story of a cybersecurity event.

6. The Radar Page

The "Radar Page" can be found at www.securitywizardry.com/radar.htm. It is shown in Figure 14. This page is designed for viewing in real time since many of the panels scroll. Nevertheless, static screenshots of this page are of great value in visualizing cybersecurity events. This page is so highly regarded that the Pentagon used it as a backdrop when briefing President George W. Bush on cybersecurity (Figure 15).

7. Honeypots

Honeypots are widely used to glean information about cyberevents. They are especially useful when organized

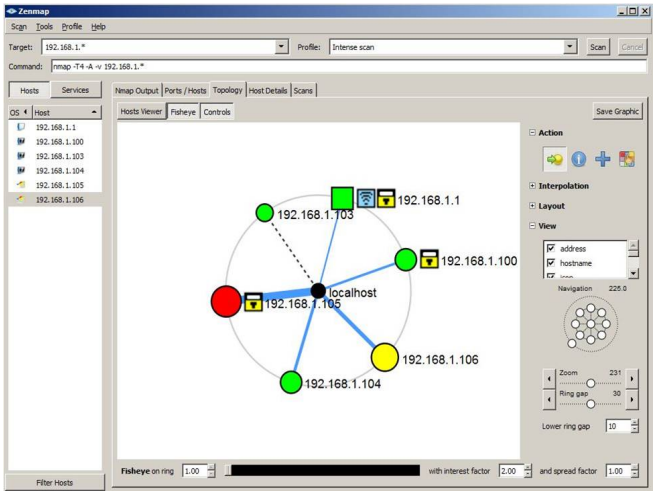


Fig. 12: An NMap Topological Display

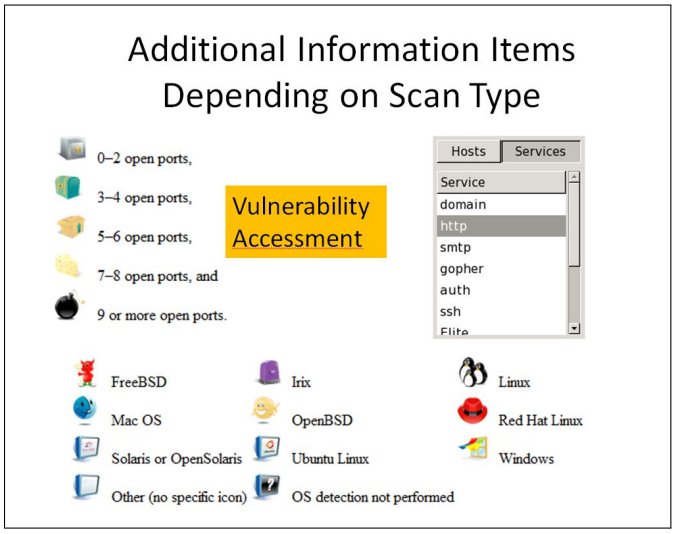


Fig. 13: NMap's Memorable Icons

Fig. 14: The "Radar Page"

Fig. 15: The Pentagon Showing Off for President Bush

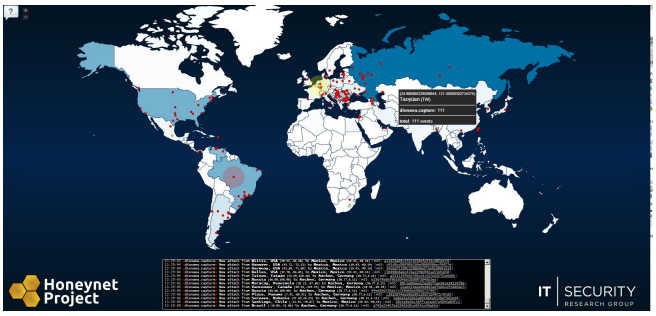


Fig. 16: Honeypots under Attack

into a distributed network that can collect data over a wide region. An interesting project of this sort can be found at www.honeynet.org. They have a web page at http://map.honeynet.org/ that displays what they call the "Honey Map." This map, which can be found at map.honeynet.org, provides a real-time indication of activity on the World Wide Web. A sample display is shown in Figure 16. There are periods when the map shows little activity. Of course, the map illustrates the activities on the World Wide Web that involve the honeypots operated by the project. This map is best viewed dynamically, although static screenshots also convey a lot of information to cybersecurity professionals.

8. Imaginative Displays

Figure 17 visualizes a distributed denial of service attack. It can be found at http://honeynet.org.au/?q=node/67. While a static image gives some flavor of the visualization, for best results we recommend that you view the video. A variant that can be found at https://code.google.com/p/logstalgia/ adapts the game of Pong to defend against a distributed denial of service attack. This is shown in Figure 18.

The visualizations in Figures 17 and 18 were produced using the Google Project tool called Logstalgia. More information about this tool is available at https://code.google.com/p/logstalgia/. Another interesting visualization project is called Gouse. It uses advanced

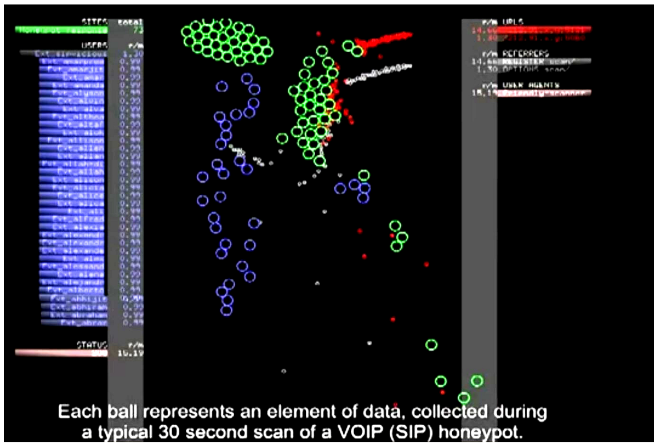


Fig. 17: Visualizing a DDoS Attack

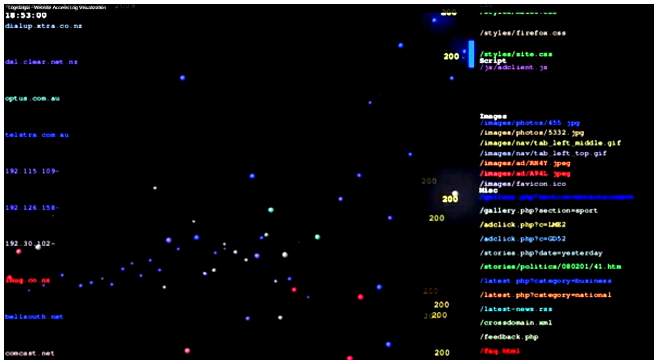


Fig. 18: Adapting Pong to Defending Against a DDoS Attack

techniques for software version control visualization. More information about this project can be found at https://code.google.com/p/gource/.

9. Three Dimensional Displays

Given the very dynamic nature of cybersecurity events, especially when dealing with cyber attacks, it seems clear that three dimensional visualizations might be very helpful. Daedalus, a tool that produces such visualizations, was produced by Japan's National Institute of Information and Communications Technology (NICT). More information about this project can be found at http://www.nict.go.jp/press/2012/06/06-1.html and also in [12]. Figure 19 shows the system in action. Using all three dimensions, the system clearly shows used and unused IP addresses. It is rightly assumed that activity involving unused IP addresses is suspicious and should be examined in more detail. Figure 20 shows a closeup of this system.

Another interesting use of three dimensional graphics can be found in [13]. Figure 21 from that paper shows how to analyze spam campaigns launched by various botnets.

Fig. 19: A 3D Visualization of Cyberevents

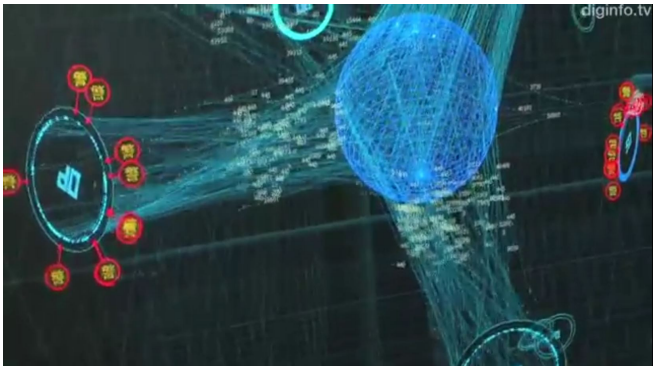


Fig. 20: A Closeup of a 3D Visualization System

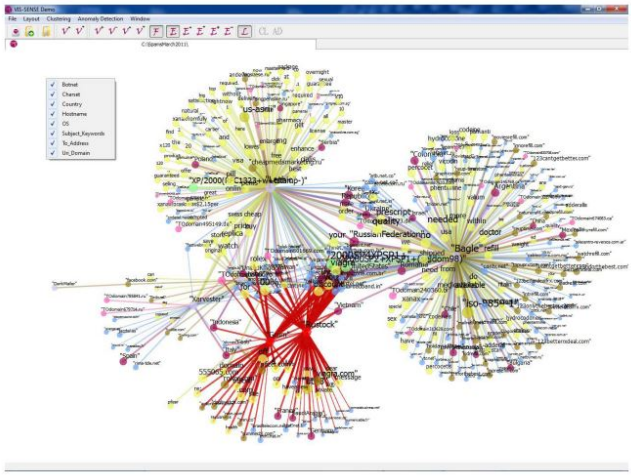


Figure 5: The big picture that is created by taking into account 8 features of spam emails sent during March 2011: *Botnet, Subject Keywords, Uri Domain, Country, Recipient Address, Charset and Hostname.* Rustock and Grum are higlighted in red.

Fig. 21: Analyzing Spam Campaigns Launched by Botnets

10. Symposium on Visualization for Cyber Security

A wonderful source of cutting edge cybersecurity related visualizations can be found in the various Symposia on Visualization for Cyber Security. The website for this organization can be found at http://www.vizsec.org/. Their 2013 meeting, Visualization for Cyber Security (VizSec 2013) will be held on October 14, 2013 in Atlanta GA, USA in conjunction with IEEE VIS.

11. Conclusions

There are many promising tools that can produce very fine visualizations that can be of great help in communicating cybersecurity concepts to a wide range of audiences. We urge people to use the existing tools more widely and to add new visualizations for others to use.

References

[1] Edward R. Tufte, *The Visual Display of Quantitative Information*, Cheshire, CT, USA: Graphics Press, 1983.

[2] Edward R. Tufte, *The Visual Display of Quantitative Information*, 2nd ed., Cheshire, CT, USA: Graphics Press, 2001.

[3] William .S Cleveland, *Visualizing Data*, Summit, NJ, USA: Hobart Press, 1993.

[4] William S. Cleveland, *The Elements of Graphing Data*, Summit, CT, USA: Hobart Press, 1994.

[5] Antony Unwin, Martin Theus, and Heike Hofman, *Graphics of Large Datasets*, New York, NY, USA: Springer Science+Business Media, 2006.

[6] Nathan Yau, *Visualize This*, Indianapolis, IN, USA: Wiley Publishing, 2011.

[7] George Markowsky and Linda Markowsky, "Survey of Supercomputer Cluster Security Issues," in *Proc. SAM'07*, 2007, pp. 474-480.

[8] George Markowsky and Linda Markowsky, "Using the Castle Metaphor to Communicate Basic Concepts in Cybersecurity Education," in *Proc. SAM'11*, 2011, p. 507-511.

[9] Florian Mansmann, Timo Gobel, and William Cheswick, "Visual Analysis of Complex Firewall Configurations," in *Proc. VizSec'12*, 2012, pp. 1-8.

[10] Sven Turpe, "Point-and-Shoot Security Design: Can We Build Better Tools for Developers?," in *Proc. VizSec'12*, 2012, pp. 27-41.

[11] George Markowsky and Linda Markowsky, "Who's Knocking at Your Cybercastle's Gate?," in *Proc. SAM'12*, 2012, pp. 206-212.

[12] Daisuke Inoue, Koei Suzuki, Mio Suzuki, Masashi Eto, and Koji Nakao, "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System," in *Proc. VizSec'12*, 2012, pp. 72-79.

[13] Orestis Tsigkas, Olivier Thonnard, and Dimitrios Tzovaras, "Visual Spam Campaigns Analysis using Abstrac Graphs Representation," in *Proc. VizSec'12*, 2012, pp. 64-71.