Health Care Cyberthreat Report

Widespread Compromises Detected, Compliance Nightmare on Horizon

A SANS Analyst Whitepaper

Written by Barbara Filkins

February 2014

Sponsored by

Norse

Table of Contents

Executive Summary

Real Threats, Real Compliance Nightmares

As an organization that provides the largest global network of cybersecurity training, certification and research information, SANS understands the impact that cyber attacks have on organizations of all types and sizes. With research analysts dedicated to studying the effects of cyber attacks on multiple industries, SANS repeatedly sees how cybercriminals and nation-backed operators are constantly devising new ways of leveraging the Internet of Things (IoT) and expanding the attack surface to carry out advanced persistent threats (APTs), DDoS attacks, malware infections, cyber espionage, and data and intellectual property theft. All of these activities are causing organizations to spend billions[1] to mitigate every year.

The IoT has the potential to cause significant out-of-pocket losses for businesses and consumers. Results from the 2014 SANS Securing the Internet of Things Survey[2] support the prediction that the health care/pharmaceutical space will be among those that experience the highest level of near-term deployment and use of IoT devices. As compared to traditional IT systems, incidents involving Things, such as a hacked MRI machine, can carry physical consequences, as well as policy and financial impacts.

Health Care Cybercrime: Now a Reality

Virtually all software, applications, systems and devices are now connected to the Internet. This is a reality that cybercriminals recognize and are actively exploiting.

Some 94 percent of medical institutions said their organizations have been victims of a cyber attack, according to the Ponemon Institute.[3] Now, with the push to digitize all health care records, the emergence of HealthCare.gov and an outpouring of electronic protected health information (ePHI) being exchanged online, even more attack surfaces are being exposed in the health care field.

A SANS examination of cyberthreat intelligence provided by Norse supports these statistics and conclusions, revealing exploited medical devices, conferencing systems, web servers, printers and edge security technologies all sending out malicious traffic from medical organizations. Some of these devices and applications were openly exploitable (such as default admin passwords) for many months before the breached organization recognized or repaired the breach.

The intelligence data that SANS examined for development of this report was specific to the health care sector and was collected between September 2012 and October 2013. The data analyzed was alarming. It not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen.

[1] www.healthcareitnews.com/news/healthcare-data-breaches-trend-upward-come-potential-7b-price-tag

[2] www.sans.org/reading-room/analysts-program/survey-internet-things

[3] www.healthcareitnews.com/news/healthcare-data-breaches-trend-upward-come-potential-7b-price-tag

Organizations of All Types/All Sizes

During the sample period, the Norse threat intelligence infrastructure—a global network of sensors and honeypots that process and analyze over 100 terabytes of traffic daily—gathered data. The intelligence data collected for this sample included:

- 49,917 unique malicious events
- 723 unique malicious source IP addresses
- 375 U.S.-based compromised health care-related organizations

Appendix A, at the end of this document, provides the specifics on how the captured data was analyzed against the criteria we set. The data provided offered intelligence as to the source of the suspicious traffic (source IP address and port) and possible attack characteristics through the network service associated with the destination port on the Norse network. We identified the top 10 ports and associated network service by frequency of events represented in the data. Appendix B provides a description of these "ports of compromise," including a brief overview of their standard usage and commonly associated threats. Appendix C provides a more detailed timeline of how activity around these ports and services varied across the duration of the captured data.

SANS analyzed almost 50,000 events captured between September 2012 and October 2013.

About a third of the organizations represent small providers, while the rest represented clearinghouses, health plans, pharmaceutical companies and other types of medical organizations. Some of these providers were also quite large, with renowned research centers and teaching hospitals among the sources sending out the malicious packets. (See more in-depth discussion in the "Organizations Out of Compliance" section.

Many of the organizations were compromised and, therefore, out of compliance for months, and some for the duration of the study—meaning they never detected their compromises or outbound malicious communications. Although the types of organizations were vast, this is the breakdown of the organizational types detected as compromised and the percentage of malicious IP traffic emanating from them:

- **Health care providers**—72.0% of malicious traffic
- **Health care business associates**—9.9% of malicious traffic
- **Health plans**—6.1% of malicious traffic
- **Health care clearinghouses**—0.5% of malicious traffic
- **Pharmaceutical**—2.9% of malicious traffic
- **Other related health care entities**—8.5% of malicious traffic

There is also a more detailed case study examination of our top three sites toward the end of this document. See the section titled "Case Study Examination of the Top Three Entities."

Conclusions Based on the Data

The unique events detected revealed that multiple connected device types, applications and systems can be compromised, including radiology imaging software, video conferencing systems, digital video systems, call contact software, security systems and edge devices such as VPNs, firewalls and routers. Percentages of each are explained in the "Biggest Culprits: Internet of Things and Security Devices" section.

There are many reasons why these findings are cause for alarm:

- The sheer volume of IPs detected in this targeted sample can be extrapolated to assume that there are, in fact, millions of compromised health care organizations, applications, devices and systems sending malicious packets from around the globe.
- Current security practices and strategies around endpoints in general, but especially those that are health care related, are not keeping pace with attack volumes. In fact, results from the 2014 SANS Endpoint Security Survey indicate that attackers are bypassing perimeter protections en-masse and do not need to use stealth techniques to do so.[4] These results show that, once compromised, these networks are not only vulnerable to breaches, but also available to be used for attacks such as phishing, DDoS and fraudulent activities launched against other networks and victims.
- Personal health care information (PHI) and organization intellectual property, as well as medical billing and payment organizations, are all increasingly at risk of data theft and fraud because of these attacks and breaches. Poorly protected medical endpoints, including personal health devices, become gateways, exposing consumers' personal computers and information to prowling cybercriminals.
- Today, compliance does not equal security. Organizations may think they're compliant, but this data shows that they are not secure.
- The costs of failed compliance or compromises are increasing. These costs go far beyond the regulatory fines, the burden of notification to victims or immediate remediation costs—there are legal risks from class-action lawsuits incurred following a breach, potential fallout in stock prices and the intangible costs of brand damage when word gets out about the company's missteps.

[4] The 2014 SANS Endpoint Security Survey is expected to be published in March 2014 and will be available at www.sans.org/reading-room/analysts-program.

Compliance Nightmares Looming

From a compliance standpoint, the findings demonstrate that health care organizations could continue to find themselves in the same situation as health care companies such as WellPoint Inc. found itself in—on the receiving end of HIPAA fines reaching almost $2 million after exposing hundreds of thousands of ePHI.[5]

These deep fines aren't the only costs health care providers need to be concerned with. According to the 2013 Ponemon Cost of a Data Breach report,[6] expenses related to a breach, such as incident handling, victim notification, credit monitoring and projected lost opportunities, cost health care organizations globally in the range of $233 per compromised record. Additional recovery actions, such as legal actions, recovery, new security control investments, extended credit protection services for victims and other related costs, actually push the cost much higher—amounting to an astronomical $142,689,666 in the case of the WellPoint incident.

If action isn't taken, the proliferation of ePHI will exacerbate the situation. It is not unthinkable that a database, such as the one connected to HealthCare.gov, will eventually be breached. Indeed, new attention and standards for security and reporting are now being applied to this federal health care exchange,[7] which could put health care breach damage on par with or well above what enterprises such as Target are now experiencing. In such highly publicized breaches, it has been estimated that the personal information of as many as 110 million payment card holders have been breached.

From a providers' standpoint, the value of this research is evident: It serves as an ominous warning that should be heeded and provides useful guidance on how to reduce related risks.

It is equally important to point out that, in addition to the extreme inconvenience that identity theft, stolen information and fraud can place on individual, there are additional costs associated with cybercrime that consumers may not have the ability to recover. Unlike e-commerce–related theft and fraud expenses from which most consumers are shielded, consumers are responsible for costs related to compromised medical insurance records and—costs that reached $12 billion in 2013.[8]

[5] www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html

[6] www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[7] www.dailytech.com/Cyber+Security+Experts+HealthCaregov+Isnt+Secure+Governments+Doing+Nothing+About+It/article34149.htm

[8] www.infosecurity-magazine.com/view/34540/medical-id-fraud-costs-consumers-12bn-in-outofpocket-costs

The Federal Exchange—Key Events

MARCH 2010 — The Patient Protection and Affordable Care Act (PPACA) is signed into law.

SEPTEMBER 2011 — CGI Federal is awarded the originally $93M contract to build the HealthCare.gov website.

AUGUST 2012 — The Center for Medicare and Medicaid Services (CMS) publishes "Harmonized Security and Privacy Framework—Exchange Reference Architecture," which defines the risk-based security and privacy framework for use in the design and implementation of the federal exchanges and the foundational requirements for protecting the individual information on the exchanges, information that includes absolutely everything required to commit both financial and medical identity theft against that individual.[9]

FEBRUARY 2013 — Twenty-five states declare that they will depend on the federal exchange, 18 will create their own, and 8 will participate in partnership with the federal government.

JUNE 2013 — The Health and Human Services inspector general reveals that Quality Software Services Inc. (QSSI), responsible for building the data hub, allowed workers to connect unsanctioned devices to USB ports, which posed a risk to the personally identifiable information of over 6 million Medicare beneficiaries.

AUGUST 2013 — Concern continues to be voiced that both HealthCare.gov and the data hub, which provides the interconnections between key federal (HHS, Treasury, and IRS) and state systems used to determine individual eligibility, suffers from security concerns and lack of adequate testing.

OCTOBER 2013 — HeathCare.gov opens for business and immediately fails because of site performance issues exacerbated by unanticipated demand. This is followed by discovery of various security flaws, such as the site's password-reset functionality, which would allow an attacker to view information such as the email address associated with an account and the security questions a user had selected to answer.

NOVEMBER 2013 — The Verizon Terremark outage takes down HealthCare.gov and the data hub.

DECEMBER 2013 — Corrective actions continue. A "tiger team" for resolution and mitigation of the problems is put in place, the site kept open, and registration/enrollment deadlines extended.

JANUARY 2014 — Four highly regarded cybersecurity experts testify before Congress about data security problems with the HealthCare.gov website. They recommend that the site remain offline until problems can be fixed and that the public not be allowed to use the site.[10]

The House passes the Health Exchange Security and Transparency Act, which contains one sentence that says HHS must notify all individuals whose personally identifiable information is exposed in a data breach of a health care exchange within two days of discovering the breach.

CGI is replaced by Accenture; QSSI is retained; and hosting is moved from Verizon Terremark to another hosting service.

[9] www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Harmonized-Security-and-Privacy-Framework-ERA-Supp-v-1-0-08012012-a.pdf

[10] www.trustedsec.com/files/CONGRESS_Hearing_Security-Testimony_v1.4.pdf

Biggest Culprits: Internet of Things and Security Devices

Let's start with the devices and applications emitting malevolent traffic caught in the Norse sample. The security that health care organizations most rely on to protect them, along with nontraditional medical endpoints, represent the largest sources of malicious traffic. These include:

- **Connected medical endpoints.** The findings of this study indicate that 7 percent of traffic was coming from radiology imaging software, another 7 percent of malicious traffic originated from video conferencing systems, and another 3 percent came from digital video systems that are most likely used for consults and remote procedures. Connected medical devices, applications and software used by health care organizations providing everything from online health monitoring to radiology devices to video-oriented services are fast becoming targets of choice for nefarious hackers taking advantage of the IoT to carry out all manner of illicit transactions, data theft and attacks. This is especially true because securing common devices, such as network-attached printers, faxes and surveillance cameras, is often overlooked. The devices themselves are not thought of as being available attack surfaces by health care organizations that are focused on their more prominent information systems.
- **Internet-facing personal health data.** The study shows 8 percent of malicious traffic was emitted through a web-based call center website, backed by a VoIP PBX, in use by a medical supply company. Also we found indications of a compromised personal health record (PHR) system. In a PHR system, consumers' personal health records are not necessarily tethered to an electronic health record (EHR) system and, therefore, are neither certified under the U.S. standards[11] nor regulated under HIPAA/HITECH legislation. Consumers may find that they have no recourse under HIPAA or other jurisdictional privacy breach legislation if personal information in an untethered PHR is compromised, leaving the consumers to bear the costs. In its 2013 Survey on Medical Identity Theft,[12] Ponemon estimates that nearly 2 million Americans will spend over $12 billion out of pocket this year alone to deal with the consequences of their compromised medical or insurance files.
- **Security systems and edge devices.** In this study, most of the malicious traffic passed through or was transmitted from VPN applications and devices (33 percent),[13] whereas 16 percent was sent by firewalls, 7 percent was sent from routers and 3 percent was sent from enterprise network controllers (ENCs). This indicates that the security devices and applications themselves were either compromised, which is a common tactic among malware families, or that these "protection" systems are not detecting malicious traffic coming from the network endpoints inside the protected perimeter—inside the firewall or behind the VPN concentrator. If they are not detecting, they are not reporting—and that means they are out of compliance with privacy and security regulations for patient data.

[11] www.healthit.gov/policy-researchers-implementers/onc-hit-certification-program

[12] www.ponemon.org/blog/2013-survey-on-medical-identity-theft

[13] Cisco technology accounted for 62% of all VPNs generating malicious traffic with the majority of this being Cisco SSL VPN, Dell Sonicwalls accounted for 21%, and the remaining 17% was a mix of lesser known technologies.

VoIP and mail servers were also among the devices and applications emitting malicious traffic, and a very small fraction (1 percent or less) came from different types of Internet connected monitoring systems, cameras and printers, as shown in Figure 1.

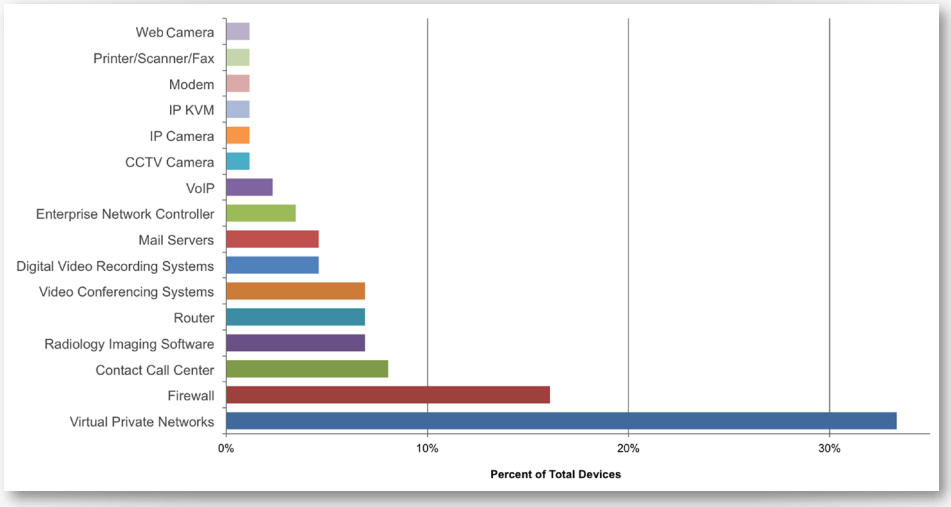
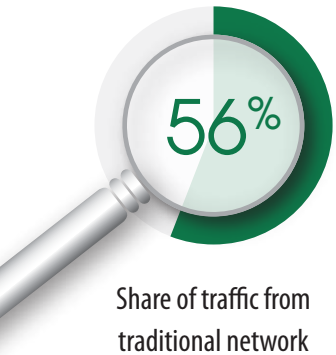


Figure 1. Devices Emitting Malicious Traffic



Share of traffic from traditional network edge devices, including firewalls, routers and VPN systems

The fact that security devices and applications are emitting the most malicious traffic caught in the sensors is particularly troubling. In a recent SANS survey, IT professionals working for health care-related industries still think their network perimeter defenses are their most effective security and compliance measures, as shown in Figure 2.[14]

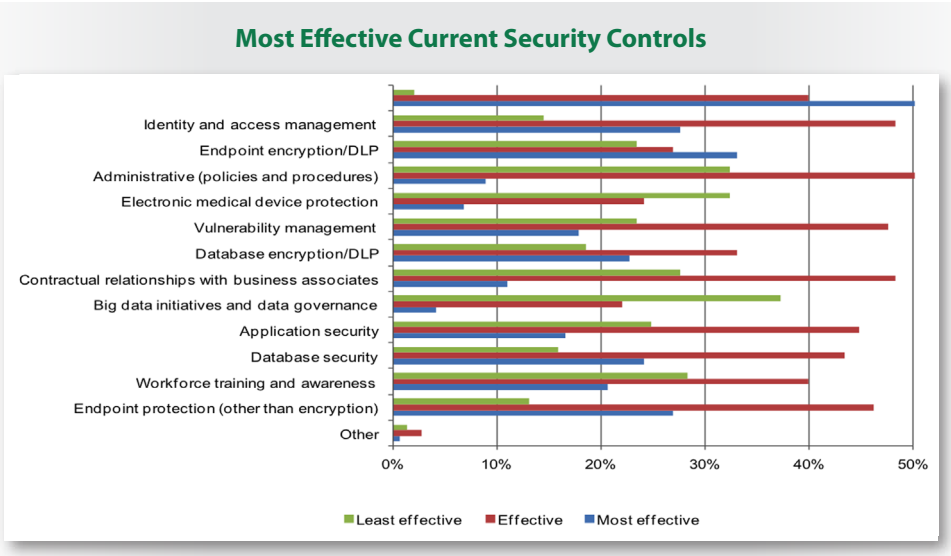


Figure 2. Effectiveness of Security Controls[15]

[14] www.sans.org/reading-room/analysts-program/2013-healthcare-survey

[15] www.sans.org/reading-room/analysts-program/2013-healthcare-survey, page 16

This perception of being secure, when organizations are clearly being breached and emitting malicious traffic, is troubling from both the risk and compliance perspectives. This gap in reality versus practice indicates that compliance legislation, such as HIPAA or the Health Information Technology for Economic and Clinical Health (HITECH) Act, and related regulations are not enough, by themselves, to serve as a blueprint for health care organizations wishing to adequately secure themselves. In some cases, regulations that surround medical devices actually make it difficult to secure and upgrade such items, even if manufacturers can develop adequate security for them.

Misconfigurations, Public-Facing Logins and More

Many of the exploits discovered in the analyzed data take advantage of misconfigurations. Today, almost every network-attached device is shipped from its vendor in an insecure configuration with defaults that can be discovered easily through an Internet search.[16] Many of these devices, such as surveillance cameras, are apparently not secured at implementation. These exploits (and their related costs and privacy violations) could have been reduced by practicing good configuration control and monitoring for signs of compromise and malicious communications. Figure 3 shows examples of the actual vulnerabilities and entities revealed by our analysis of source IP addresses.

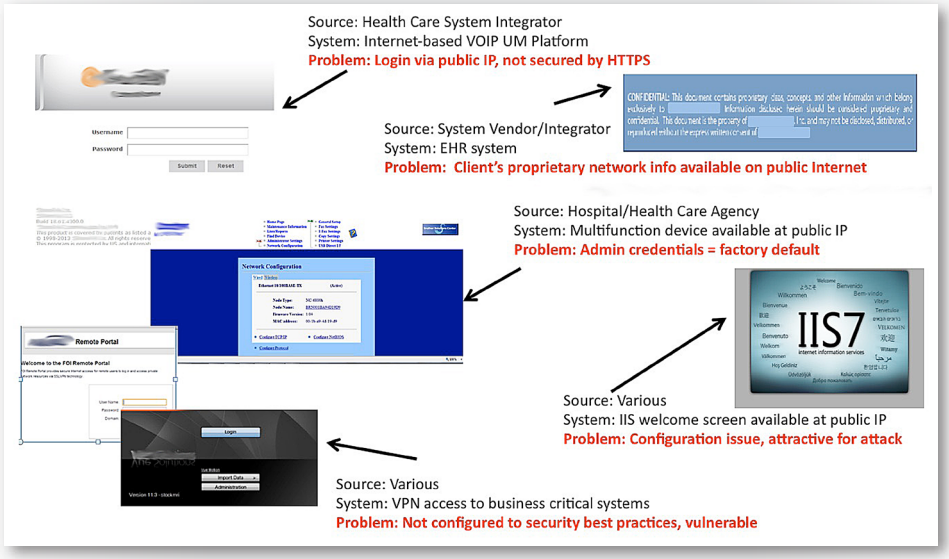


Figure 3. Noncompliant, Vulnerable Endpoints Represented

[16] Just one example is www.routerpasswords.com.

Most network admins change the factory defaults (sometimes as simple as Username: admin, Password: password) for router firewalls, but they often overlook other network-attached devices, such as surveillance cameras and network-attached printers or fax machines. The default usernames and passwords for these often overlooked endpoints can be easily procured by an Internet search on "type of device" plus "default password." See Figure 4 for a particularly chilling example.

Medical Endpoints Detected

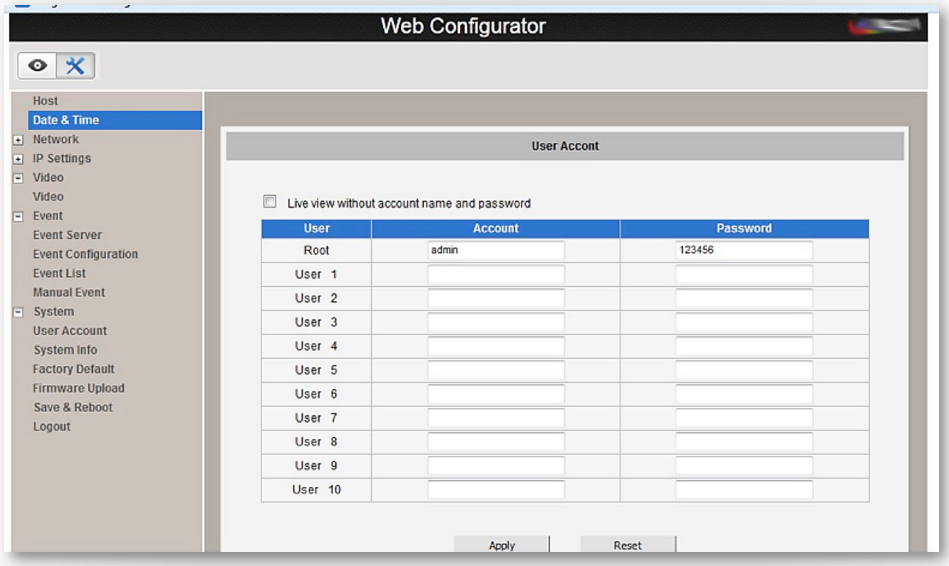


Figure 4. Surveillance Camera Interface Exposed to Internet with Default Credentials

Access from this configuration screen can be extended to other devices on what the affected organization would consider its private network. This isn't even hacking!

Organizations Out of Compliance

We also discovered multiple types of organizations associated with each source IP address, including their relationship to the health care industry and the Internet service provider (ISP) being used (see Appendix A, "How Captured Traffic Was Analyzed"). Compromised system traffic emitting from health care providers, health plans, clearinghouses, business associates and pharmaceutical and health care-related organizations (including nonprofit and emergency services), fell into the "other" category, as shown in Figure 5.

Security is a problem for organizations large and small.

Organizations Compromised

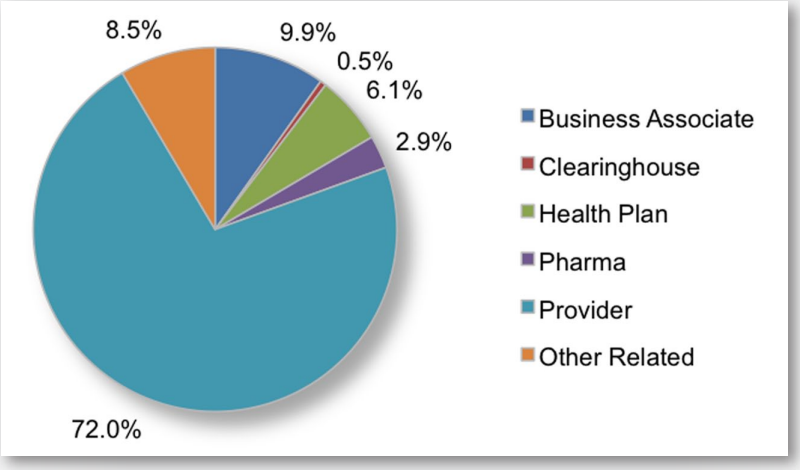


Figure 5. Type of Organizations Compromised

From our analysis of the Norse data, SANS estimates roughly a third of the provider organizations caught in the Norse network represent small providers, either individual practices or small groups with fewer than 10 providers. Also implicated were prominent university hospitals known for cutting-edge medical treatment and education, large health systems (one with 9,000+ providers across 350 locations), national associations that set industry policy and practice, several global pharmaceutical firms with revenues measured in the billions, health plans (including both major carriers) and at least one state human services agency.

How does this impact the industry in terms of employees, patients and profit? In 2005, the national provider/patient ratio was around 2,300 patients to one provider.[17] That means one individual provider has access to 2,300 individuals. Even in today's environment, this ratio serves as a starting point for estimating potential compromise. From our dataset alone, given that a third of the provider organizations were small providers, and assuming one provider per organization, a minimum of over 200,000 individuals could potentially have had their records compromised. For the state agency implicated in our intelligence data, the estimated number of new Medicaid enrollments due to the Patient Protection and Affordable Care Act (PPACA) is close to half a million new individuals, creating both eligibility and health care records that can be compromised within that entity. And theoretically, the effects of an ePHI compromise could potentially touch almost every person in the United States if the goal set by President Bush in 2004 that every American would have an electronic health record by 2014 comes anywhere close to reality.

Many of the compromised entities are categorized under the so-called "HIPAA Privacy Rule," which is made up of multiple regulations and provisions for different types of providers.[18] Here's a brief description of the organization types (as described by HIPAA) we found among the malicious actors:

- **Providers (72.0% of malicious traffic captured).** The HIPAA Privacy Rule applies to all health care providers, regardless of practice size, provided that they transmit health information electronically. This category can include doctors, clinics, psychologists, dentists, chiropractors, nursing homes or pharmacies.[19]
- **Business associates (9.9% of malicious traffic captured).** These are persons or entities that create, receive, maintain or transmit protected health information on behalf of a covered entity or another business associate as defined under the HIPAA Omnibus Rule.[20] The rule now specifically includes those who provide data transmission services, such as health information exchanges, electronic prescribing gateways or networks, or electronic health record hosting services.
- **Health plans (6.1% of malicious traffic captured).** These include medical, dental, and vision plans; HMOs; state and federal health care supplement insurers; long-term care insurers; veterans' health plans and company health plans.[21] This category also includes Medicare and state programs as health plans with large and extensive claims databases that represent a treasure trove for criminals.
- **Clearinghouse (0.5% of malicious traffic captured).** These entities process nonstandard health information they receive from another entity into a standard format (i.e., standard electronic format or data content), or vice versa.

[17] www.ncbi.nlm.nih.gov/pmc/articles/PMC1490281

[18] The provisions making up the HIPAA Privacy Rule are located at 45 CFR Part 160 and Subparts A and E of Part 164, www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/content-detail.html.

[19] www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/entityhipaa.html

[20] The final rule, published in January 2013 and effective September 25, 2013, is available at www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf and implements most provisions of the HITECH Act.

[21] www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/entityhipaa.html

In addition to the entities listed in the HIPAA Privacy Rule, we also captured malicious data from two additional categories:

- **Pharmaceutical (2.9% of malicious traffic captured).** The dataset also contained several major pharmaceutical/biotech firms and several companies that support human clinical trials. These organizations are not normally considered HIPAA-covered entities or business associates, but their data can be just as valuable to criminals.
- **Other related (8.5% of malicious traffic captured).** Several organizations did not fall into one of the preceding categories, including some nonprofit agencies, emergency relief associations and other organizations providing services to health care system employees.

Figure 6 shows the geographical distribution of these types of organizations that were sending the malicious data.

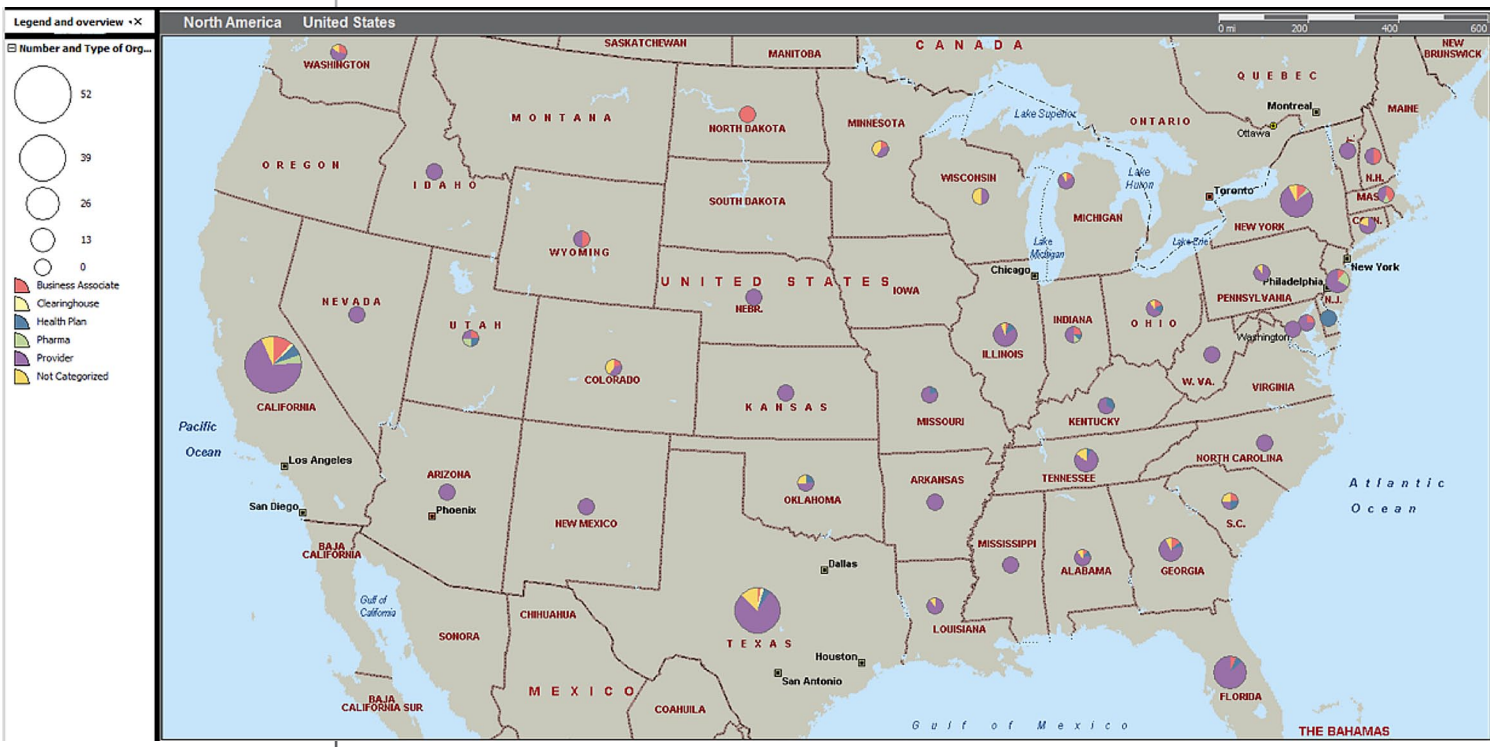


Figure 6. Locations and Types of Organizations

When we correlated the geographic distribution of source IP addresses with the associated organizations and organizational types, we found the highest concentration of compromised organizations in California, Texas, New York and Florida, which are also states known for the highest rates of medical fraud.[22] It is also interesting to note that this correlation may be a good indication of how ineffective compliance and privacy regulation is. California, Texas and New York are noted for their stringent privacy laws, many of which continue to affect national privacy and security policy.

Figure 7 provides another view of compromised organizations, this time the total number of organizations per state as shown by the circles overlaid on the shading representing overall population for each state.

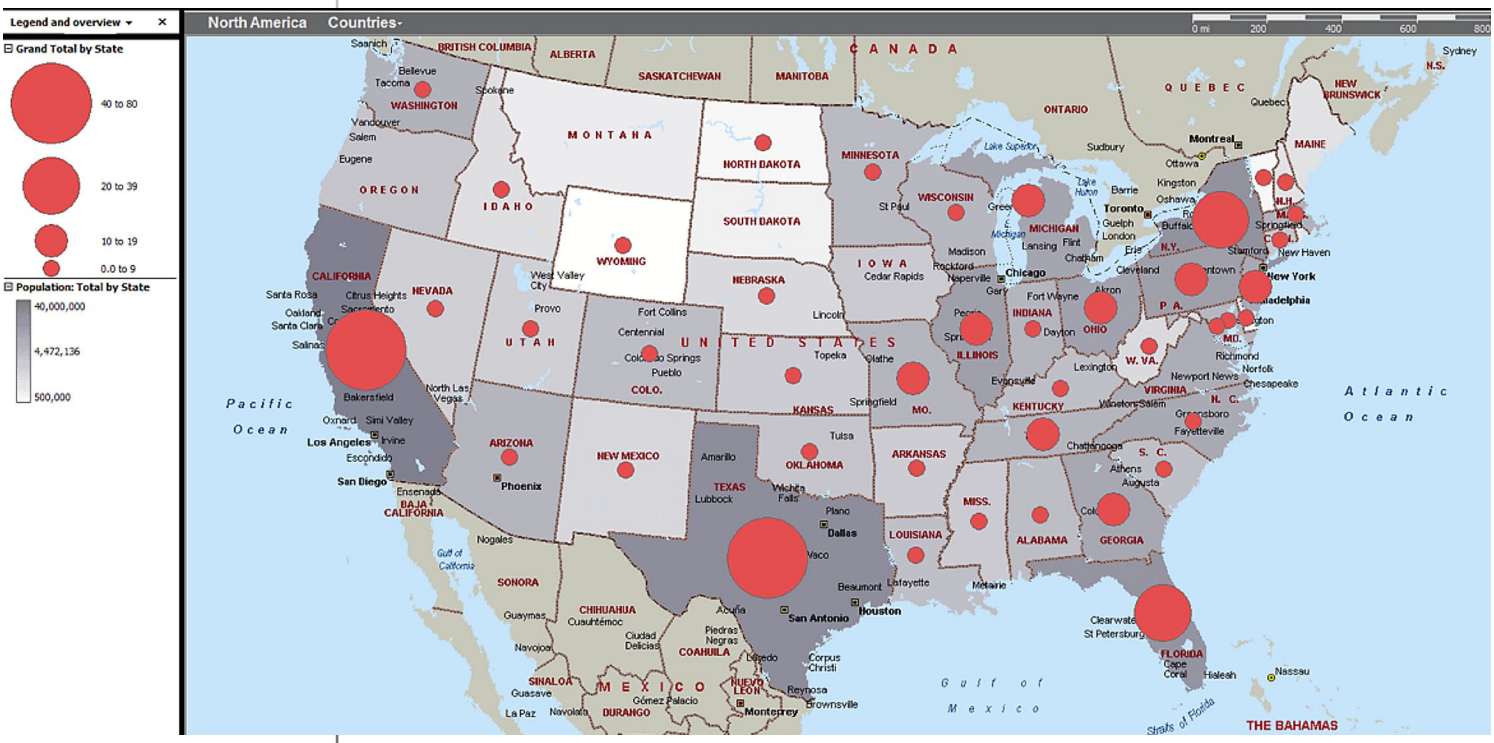


Figure 7. Locations and Types of Compromised Organizations

High populations are darker gray. Note many organizations that are compromised are in those states with higher populations such as California, Texas, Florida and New York. Activity is less pronounced in those states, such as Montana, South Dakota and Maine, with lower population densities and fewer large metropolitan areas.

In the next section, "Case Study Examination of the Top Three Entities," we will provide case studies of the top three entities responsible for the largest volumes of malicious traffic.

[22] www.beckershospitalreview.com/legal-regulatory-issues/10-states-with-the-most-medicaid-fraud-investigations-convictions.html (FY 2011 statistics) and http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2012.pdf

The Regulatory Climate

Evolution of HIPAA

- **1996:** Initial enactment of HIPAA mandates that regulations regarding privacy and securing of PHI be promulgated by HHS, but they are not consistently enforced.
- **2009:** HITECH gives teeth to HIPAA through the breach notification rules, likewise promulgated by HHS; however, it provides enforcement resources and enhanced penalties for violation.
- **2013:** The Omnibus Rule strengthens HIPAA/HITECH with additional requirements to ensure compliance with the privacy, security and breach notification rules of HIPAA/HITECH including:
  - Business associates are accountable for meeting HIPAA/HITECH privacy and security regulatory requirements same as Covered Entities.
  - Breach notification depends on objective risk assessment as opposed to the more subjective analysis laid out in the Interim Final Rule, often interpreted as "guilty until proven innocent" by many in health care industry.[23]
  - Penalties are increased.[24]

Trends, Enforcement and Penalties

- Harmonization of privacy and security, building on fair practice principles, is fueled by the creation of insurance exchanges that are not covered entities and are not governed by HIPAA.
- An increase in the volume of breaches and penalties is due to the following:
  - Wider reach of the HIPAA Omnibus Rule and higher penalties
  - Enforcement, not just breach related, such as the $1.7M penalty paid by the State of Alaska for compliance violations in June 2012
- Enforcement may not just be through the Office of Civil Rights (OCR) as indicated by Federal Trade Commission (FTC) actions against LabMD and Accretive Health Inc. for breaches.[25] (Note: The FTC can launch health data breach investigations on its own or through referrals from other agencies, including referrals by the Department of Health and Human Services' OCR.)

New Laws for Transparency[26]

- **January 2014:** The federal government is demanding accountability for the Target breach, which could have sweeping implications for all institutions, including health care organizations, regarding PII protections.
- **January 24, 2014:** The California Attorney General sued Kaiser Foundation Health Plan for 2011 alleged violation of California's breach notification law (California Civil Code section 1798.82, subdivision (a)) for late notification by Kaiser for a personal information security breach.

The outcome of this "first of a kind" case could impact when and how companies subject to California's breach notice law provide notice to affected individuals, especially on the heels of the Target breach, where people are questioning Target's three-week delay in providing initial notification. Considering California's influence in the privacy regulatory space, the outcome of this case could have nationwide implications.

[23] Breach notification is not required under the Final Rule if a Covered Entity or Business Associate demonstrates through the risk assessment that there is a low probability that the protected health information has been compromised, rather than having to demonstrate that there is no significant risk of harm to the individual, as was provided for in the Interim Final Rule.

[24] www2.idexpertscorp.com/blog/single/1156

[25] www.healthcareinfosecurity.com/lab-shutting-down-in-wake-ftc-case-a-6451?goback=%2Egde_2473393_member_583469618319643443 2

[26] www.courthousenews.com/2014/01/28/64916.htm

Several sites were of immediate interest due to the overall volume of activity and the traffic patterns revealed during the period between September 2012 and October 2013. We analyzed each site to determine how long it had been sending malicious traffic, the volume of traffic and the types of vulnerabilities associated with the source IP addresses. Through that analysis, we were able to gather the following characteristics of the top three sites putting forth the majority of traffic during the capture period.

Site One

A medical supply company in Florida with more than 12,000 events recorded from November 2012 through end of the data collection period

This company deals mainly with direct marketers of point-of-care and self-testing diagnostic products, but it has been a supplier of durable medical equipment as well. Both types of companies are targets of criminals. Florida is noted for being a hotspot of Medicaid and Medicare fraud, including the sale of durable medical equipment and HIV infusion therapy pumps, making the number of malicious traffic events recorded of even greater concern.[27]

Malicious traffic sent from this entity came from 28 contiguous IP addresses and five destination ports with IANA-assigned network services. This sample includes 4 of the top 10 ports associated with threats detected by Norse. (See Appendix A, which explains the specific vulnerabilities associated with these ports.)

From our findings, it appears that attackers were initially using Site One for reconnaissance. In Figure 8, you can see a small amount of the activity involving destination port 0. This is a reserved port, technically not allowed in normal network traffic, that is often used to fingerprint machines by recording how different operating systems respond to this port. Presence of this type of traffic often heralds the first step in the start of an attack.

Events by Month for Site One

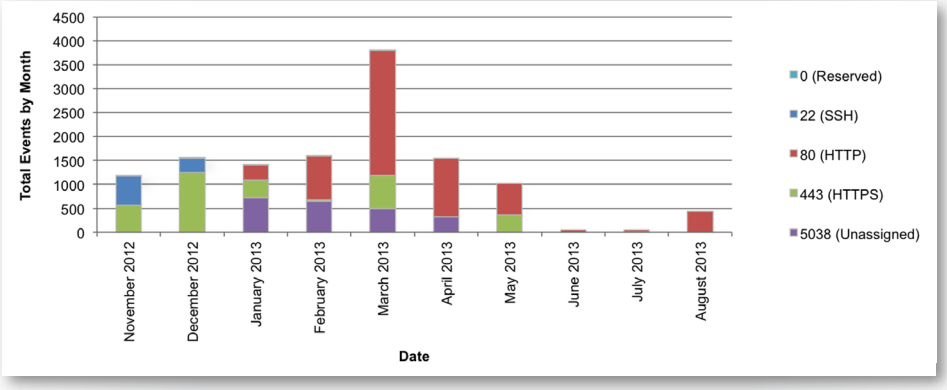


Figure 8. Events by Destination Port by Month for Site One

[27] Durable equipment sales discussion from www.finance.senate.gov/newsroom/ranking/release/?id=bff00d29-2753-458b-bae5-41ab581bb786; therapy pump sales: http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2012.pdf, p. 12

It is quite possible that the activity profile from November 2012, starting with the port 0 activity, could be indicative of a compromise of the medical supply company's call center operations. The drop in overall traffic after May 2013 and the disappearance of port 5038 activity may coincide with the end of that compromise and/or the tightening of Site One's security controls, because the source-associated IP addresses no longer resolve to the VICIDIAL user login screen. VICIDIAL is a software suite designed to interact with Asterisk systems as a complete inbound/outbound contact center suite with inbound email support.

This site also has activity around destination port 5038, which, although an unassigned service by IANA, is commonly associated with the Asterisk open source PBX phone system. Asterisk systems are the subject of various hacks. As an example, in one Internet forum, someone describes how a hacker in Moscow made $100 worth of calls on a company's Asterisk PBX before being caught.[28] Site One's data shows a compromised installation of VICIDIAL.

Site Two

A worldwide medical conglomerate, headquartered in the Northeast, with tens of thousands of employees recording more than 8,000 events from April 2013 through the end of the data collection period

Large does not necessarily mean compliant or secure, although SANS suspects that this conglomerate has a substantial budget for both compliance and security. From the data we examined, it is clear that this entity had no idea of possible infection in its midst, given the duration of the activity as shown in Figure 9.

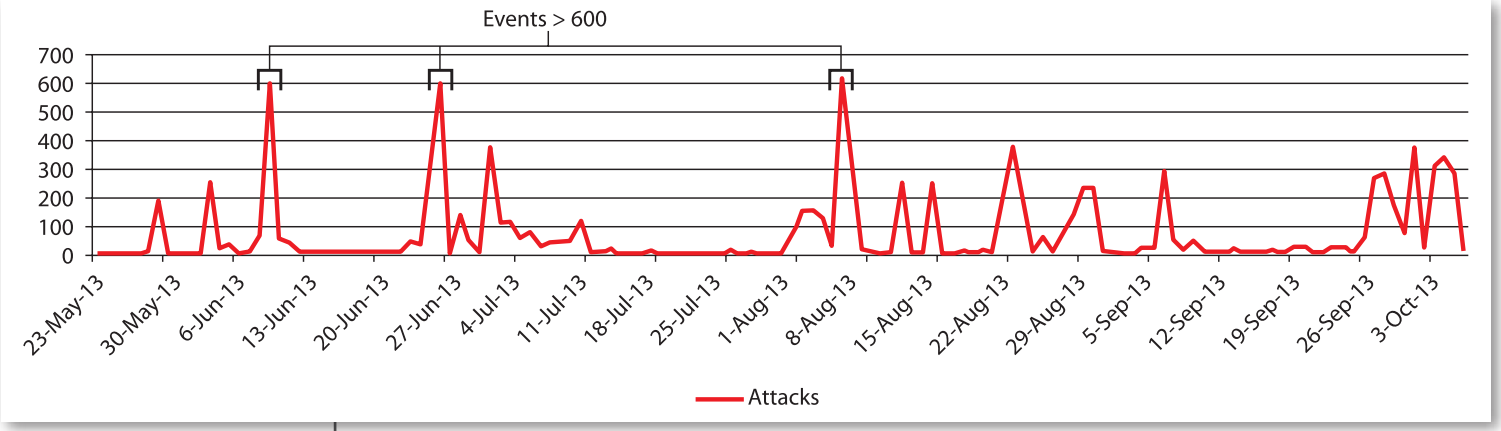


Figure 9. Daily Profile of Attacks from Site Two

[28] www.linuxquestions.org/questions/linux-security-4/asterisk-pbx-hacked-looking-to-make-sure-all-holes-are-closed-835476

Site Two's malicious traffic involved 227 contiguous IP addresses, 35 destination ports and a number of associated network services, as shown in Figure 10.

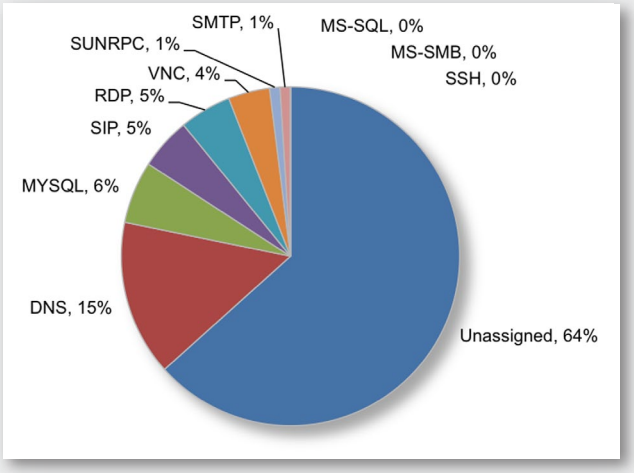


Figure 10. Site Two Network Services

The attacks involved source IP addresses that implicated affiliates and partners of the parent company, indicating the breadth of possible compromise. Among the compromises was a personal health record system owned and operated by one of the conglomerate's affiliates, raising the concerns expressed earlier about the exposure of ePHI that is not regulated by HIPAA/HITECH.

Many of the compromised addresses associated with Site Two are identified by Norse as being supported by Amazon's EC2 cloud service, raising concerns as to the exposure of remotely hosted, highly distributed information. The health care industry faces a whole new paradigm for exposure. Participating state health insurance exchanges will connect with government agencies, such as the Treasury Department, the Internal Revenue Service and other state agencies, to verify enrollees' eligibility for insurance and subsidies. If cloud-based services are sources of additional exposure, the implementation of these exchanges can unwittingly increase the ability of criminals to harvest richer datasets of PII for profitable sale and fraud.

Site Three

An ancillary medical service provider located in New Jersey with more than 2,400 events recorded during the last quarter of 2012

In this sample, malicious activity tailed off in January 2013, possibly with the implementation of stricter controls around the use of remote access by its workforce (see Figure 11).

Events by Month for Site Three

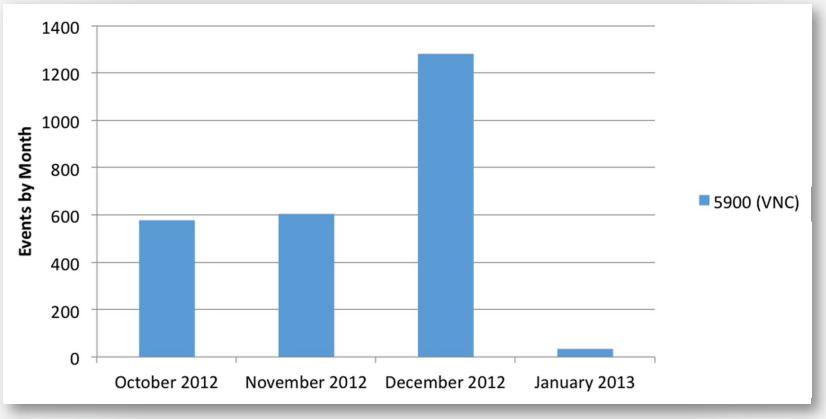


Figure 11. Site Three Events by Month

All events involved a single IP address and destination port—5900. Virtual Network Computing (VNC) is one of the services that uses the Remote Framebuffer protocol and port 5900 for remote desktop interaction with another system. Vulnerabilities associated with VNC include attackers attempting to hijack, eavesdrop or conduct denial of service (DoS) attacks through the service. VNC is subject to compromise of credentials, unless additional measures are taken to strengthen authentication and reduce vulnerability to attack.

This provider provides services for 75 to 80 percent of the primary care physicians in the area, with a daily patient load of over 300 patients and a workforce of 80. As a leading, state-of-the-art provider for the region that accepts a wide range of insurances, this provider obviously lacks the resources to respond quickly to an exposed vulnerability in its infrastructure. This presents a target of opportunity where a stealthy attacker would have time to silently compromise both patient records and insurance credentials.

This situation is also an example of how perimeters have become porous. Many health care providers, such as Site Three, don't believe their networks are compromised and feel they are secure with their current security solutions, such as firewalls. The Verizon research report "Threat Landscape: Health Care"[29] reports that attacks targeting remote desktop sessions are particularly common in health care. More diligence is required when implementing such technology, especially when the perimeter is "extended" to support staff working off-site and after hours.

[29] www.verizonenterprise.com/DL/resources/factsheets/fs_dbir-industries-healthcare-threat-landscape_en_xg.pdf

A refreshed focus on security within health care is needed, one that meets compliance requirements without compromising security, addresses computing trends—such as cloud services or mobile devices—that make traditional network perimeters more porous, and finally, that focuses on security and privacy practices that mitigate the risks outlined in this paper.

Start with enforcing best practices and controls. A good starting point to implement and enforce best policies and practices is the Critical Security Controls (CSCs), a list of 20 items for effective network defense.[30] Organizations should also consider standards for health care controls, such as two-factor authentication.

Know What's on Your Network

One of the first steps in the CSCs is assessment, which starts by gaining visibility into the enterprise and systems—including those nontraditional devices such as printers, VoIP boxes, personal medical devices and institutional medical instruments. Part of that assessment also involves determining the current state your systems. Most out-of-the-box networked devices and applications are not secure—even firewalls, VPN and other defense technologies. Organizations need to follow industry and manufacturer/vendor best practices for securing these devices. Without a strong password policy in place, even strong SSL VPN authentication can be easily compromised by brute force password guessing or dictionary attacks.

Think Like an Attacker

At a minimum, devices with default passwords, insecure ports and other inherent risks pose attack surfaces that often are not being properly configured or monitored for vulnerabilities. For example, the memory in a networked fax machine can provide attackers access to patient prescriptions that had been faxed from or to that device. Also consider physical pathways: The attacker could manipulate a vulnerable surveillance camera covering the back staircase leading to the entrance to the server room to turn off the surveillance camera or to try and capture the passcode the IT staff types into the keypad by the door. Such devices are often attached to the organization's private network and allow easy access to and compromise of that environment.

Consider Your Network Pathways

Most of us understand the need for protecting the path into our devices, systems and networks from the outside. Ingress protection, however, is not enough if internal compromise is an issue. Organizations may need egress filtering—monitoring, controlling and potentially restricting the flow of information outbound from a network—to ensure that the unauthorized or malicious traffic such as presented in this report never makes it to the Internet.

[30] www.sans.org/critical-security-controls

Cloud applications, particularly in the form of health care exchanges and medical and pharmaceutical networks, create additional attack surfaces attackers can exploit to gain access to protected patient medical and financial data. Organizations need new methods to examine and analyze the traffic flowing across their network in real time. Features such as on-the-fly decryption are increasingly important in order to look into the packets that are flowing outbound for hidden command and control channels or exfiltration of sensitive data.

Combine visualization with threat intelligence to help spot traffic trends, especially for well-known TCP and UDP ports that are commonly allowed through the network perimeter.

Assess and Attest

Assessment for system configuration and potential vulnerabilities should be an ongoing process of detection, repair, improvement and attestation that the improvements have been made.

The federally defined "Meaningful Use" criteria call for providers or hospitals that have received funding under the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program to attest to the protection of "electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities."[31]

Individuals and organizations may self-attest that they have conducted or reviewed a security risk analysis per the so-called "HIPAA Security Rule" and corrected any identified deficiencies as part of the (provider's or hospital's) risk management process. But they could still remain vulnerable to attack if they are narrowly focusing on the EHR system.[32] So it's critical not to get bogged down in the many rules and regulations for attestation. Visibility into the environment and knowledge of your systems, their maintenance and vulnerabilities can reduce the confusion and help prioritize vulnerable processes and necessary controls around them.

[31] www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

[32] The HIPAA Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164 (www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/content-detail.html); the risk management process is described at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/MU_Stage1_ReqOverview.pdf

Conclusion

The results of this analysis show that health care's critical information assets are poorly protected and are often compromised. Edge security and access systems, medical devices, video imaging systems and call centers have all been suborned in compromises that, in some cases, went on for the duration of the data collection period of 13 months.

Providers, insurers, business partners and health care exchanges of all sizes were sending malicious traffic that was caught up in Norse's global threat intelligence sensors for issuing malicious, potentially illicit traffic. Many of the organizations sending the traffic are large entities that should have the resources to conduct the basic inventory, assessment and configuration controls needed to protect their systems from being compromised and used maliciously.

This report, however, shows that the systems were compromised for long periods of time, and even when alerted to their system's actions, the organizations did not repair the vulnerabilities.

The report is a snapshot of what's happening throughout the industry. This data shows that no health care organization is immune. Reports of breaches against health care organizations, large and small, continue to rise—as do the regulatory fines they are facing for the exposure of protected patient data.

With new forms of health care taking hold, and more open exchanges of health care information between patients, insurers, doctors and pharmacists, these threats will only increase. The time to act is *yesterday*. Organizations must become aware of the many attack surfaces in their organizations and follow best practices for configuring these systems and monitoring them for abuse.

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes and people." She has focused most recently on HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system development lifecycle as well as its relation to many of the issues faced by a modern society dependent on automation—privacy, identity theft, exposure to fraud and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold) and GCIH (Gold), and the GHSC.

Sponsor

SANS would like to thank this paper's sponsor:

Appendix A: How Captured Traffic Was Analyzed

The data in this report is a sample of attacks on the Norse infrastructure from health care organizations in the contiguous United States. It was gathered by the Norse threat intelligence platform, which continuously collects and analyzes information on high-risk Internet traffic through sensors and honeypots deployed worldwide. The Norse platform focuses only on "bad" traffic, which is then analyzed, correlated and delivered to an end-user responsible for network/security management via RESTful API or a blocklist of up to 3 million risky IP addresses.

Intelligence is gathered from the darknets—places on the Internet where bad actors gather. Tor proxies, botnets, IRC chat rooms and many other areas are a haven for attackers with ill intentions, but they are also places where useful intelligence that can be used for protection against such attackers can be gathered. Once the data is analyzed, Norse delivers a simple risk score along with geolocation information, threat context (bot, anonymous proxy, bogons and so on), originating device information and more.

To properly comprehend the data, you must first have a basic understanding of how network traffic is analyzed. Although such analysis can be extremely complex, the indicators of malicious activity boil down to a few key elements:

- **Source and destination IP addresses.** These are used to distinguish attacking packets from legitimate ones. The information reported by Norse only involves publicly facing source IP addresses; there are no assumptions about the infrastructure behind each.
- **Destination port numbers.** These are often associated with a well-known network service, such as HTTP, SMTP or SSH, that can be used to disguise malicious activity. The destination port's associated services and applications identified provide a predictive clue as to the possible attack vector.
- **Activity over time.** This provides temporal clues that may identify an attack. A large number of packets being sent from the same source to the same destination, even intermittently, can signal an ongoing intrusion.
- **Latitude/longitude for source IP addresses.** This provides a snapshot of how malicious activity is distributed geographically.

Through the data provided, we were able to determine compromised ports and frequency, which helped identify the types of organizations under attack and predict basic attack characteristics. The additional information often needed for detailed analysis—such as packet structure, length and content—were not taken into account for this paper.

Appendix B: Ports of Compromise

Destination port identification is important in identifying risk and compromise. Well-known ports—those assigned by the Internet Engineering Task Force or other influential organizations—are particularly vulnerable because of their near-universal use. Attacks usually target one or more TCP or UDP ports, so the destination port can be a critical factor in identifying the potential type of attack. It is difficult to detect attacks in destination ports because they are so commonly used and, therefore, are not blocked by firewalls.

Ten destination ports, representing either TCP or UDP, were involved in more than 89 percent of compromised traffic events. They are presented in Table B-1, along with the percentage of the overall traffic they represented.

Table B-1. Top Ten Ports Associated with Events[33]

Overall Rank	Destination Port	Assigned Service	% Total Events	Use/Threat
1	80	HTTP	28%	Standard port for Internet access, not strictly monitored. Target for DDoS attacks (loss of availability for remotely hosted, mission-critical clinical systems) and various rootkits[34] (loss of sensitive information).
2	3389	RDP	13%	Widely used for remote, after-hours access. Default configuration vulnerable to man-in-the-middle attacks, brute-force attacks, and in-memory credential harvesting (unauthorized access to and transfer of sensitive information).
3	443	HTTPS	11%	Standard port for secure Internet access, not strictly monitored. New exploits emerging such as "Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext" (BREACH),[35] which bypasses SSL/TLS protections and can extract sensitive information from the message stream.
4	5900	VNC	9%	Provides remote access to computer desktops/systems. Vulnerabilities in default mode include weak authentication, making the protocol susceptible to brute force password attacks and session eavesdropping[36] (loss of confidentiality, compromised access to sensitive information).
5	5060	SIP	9%	VoIP call setup. Threats include methods based on SIP processes that govern establishment, termination and other essential elements of a call (loss [via DDoS], disruption, or degradation of service, password compromise, loss of confidentiality [eavesdropping, call interception, unauthorized forwarding] and fraud).

[33] Detailed information on ports is available at www.speedguide.net/ports.php

[34] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23412/en_US/McAfee Labs Threat Advisory-ZeroAccess.pdf, www.symantec.com/security_response/writeup.jsp?docid=2011-071314-0410-99

[35] http://thehackernews.com/2013/08/sniffing-https-BREACH-exploit-blackhat-hacking-tool.html

[36] www.dragonresearchgroup.org/insight/vnc-tac.html

Overall Rank	Destination Port	Assigned Service	% Total Events	Use/Threat
6	5038	Unassigned	5%	An open port can be compromised if a service is running on it. Threats are changing daily. Close or monitor unassigned ports for both ingress and egress.
7	445	MS-SMB	5%	Associated with several vulnerabilities that can result in compromise of the internal network and disclosure of sensitive information and/or intellectual property.
8	22	SSH	3%	Brute-force attack to obtain credentials (loss of data, system access) or compromise Internet-facing medical devices such as surgical and anesthesia devices, patient monitors and lab analysis tools[37] [38] [39] (potential loss of life).
9	8080	HTTP-alt	3%	Compromise of perimeter protective devices (broadband router, VPN) if credentials are not changed from default (compromise of internal systems, data). Several worms and Trojans open backdoors on both 8080/UDP and 8080/TCP and wait for commands on this port.
10	32767	FileNet BPM WS-Reliable Messaging	2%	Similar to port 5038. An open port can be compromised if a service is running on it. Threats are changing daily. Close or monitor unassigned ports for both ingress and egress.

In some cases, new regulation will increase the importance of standard ports. Take for example port 443. Section 1104 of the ACA mandated the creation of operating rules intended to improve the effectiveness of HIPAA transactions. The Phase I CORE Connectivity Rule defines a "Safe Harbor" transport protocol between health plans and providers over the public Internet based on the use of HTTP/S for transfer of sensitive information such as HIPAA EDI (ASC X12) transactions for claims and patient eligibility, clinical messages (HL7), zipped files, billing and other forms of sensitive information as well as for payment via electronic funds transfer (EFT) and accompanying remittance advice (ASC X12 837). Monitoring of this port needs to take into account the emergence of new exploits like BREACH to avoid disruption of provider business operations (payment) and loss of confidentiality (eligibility information).

[37] http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-034-01

[38] www.hsdl.org/?view&did=723491

[39] http://articles.washingtonpost.com/2013-06-13/national/39937799_1_passwordsmedical-devices-cybersecurity

Appendix C: Overall Traffic Trends in Time

Figure C-1 presents the overall growth in traffic volume relative to the growth in volume for each of the top 10 destination ports.

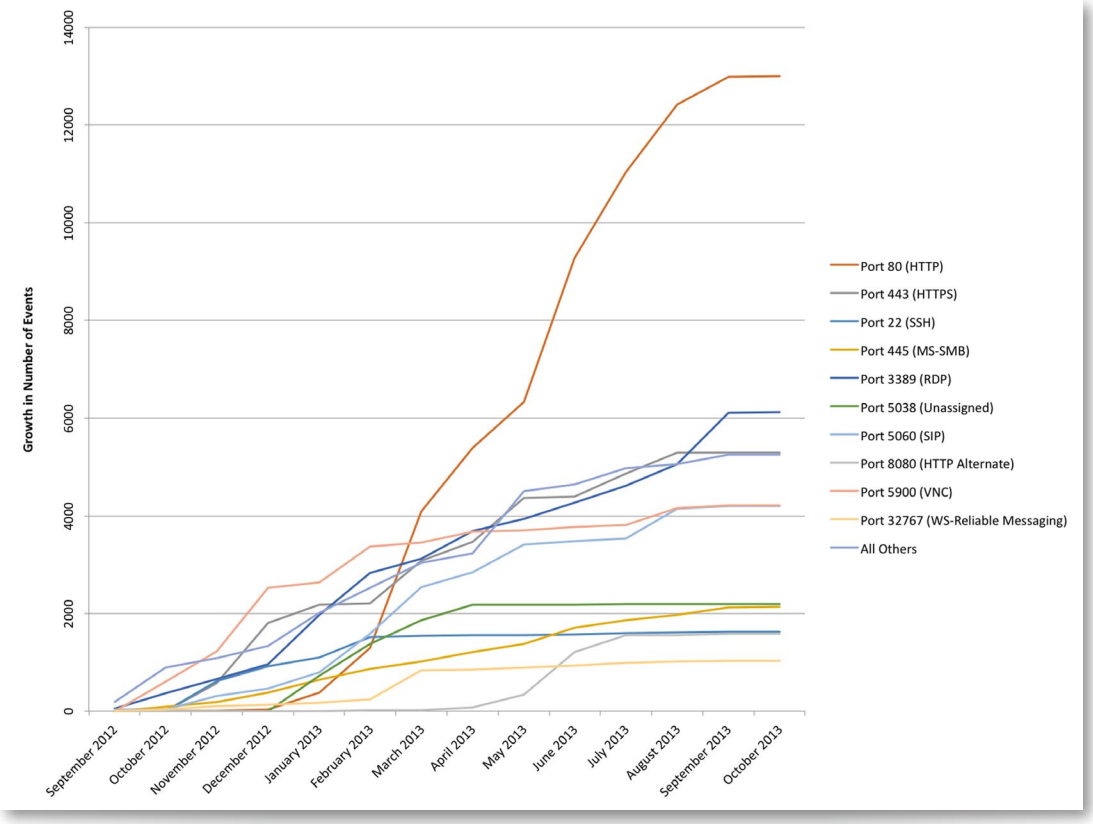


Figure C-1. Overall Growth in Event Traffic in Comparison to Destination Port Event Traffic

Activity of the First Five Top Destination Ports

The following graphics present the activity for each of the top 10 destination ports, first relative to the specific date/time the event occurred followed by the total events per month. We examine ports 22 (Figures C-2 and C-3), 80 (Figures C-4 and C-5), 443 (Figures C-6 and C-7), 445 (Figures C-8 and C-9) and 3389 (Figures C-10 and C-11). These plots represent the activity for all sites/IP addresses involved in the dataset provided by Norse. They also present some interesting trends that SANS noted but did not fully correlate with other activities occurring at that time except as noted.

Appendix D provides a further detail at the activity over time for over time for three sites selected for the volume and type of traffic associated with each site. Sites One, Two, and Three are also further described in the main body of the paper.

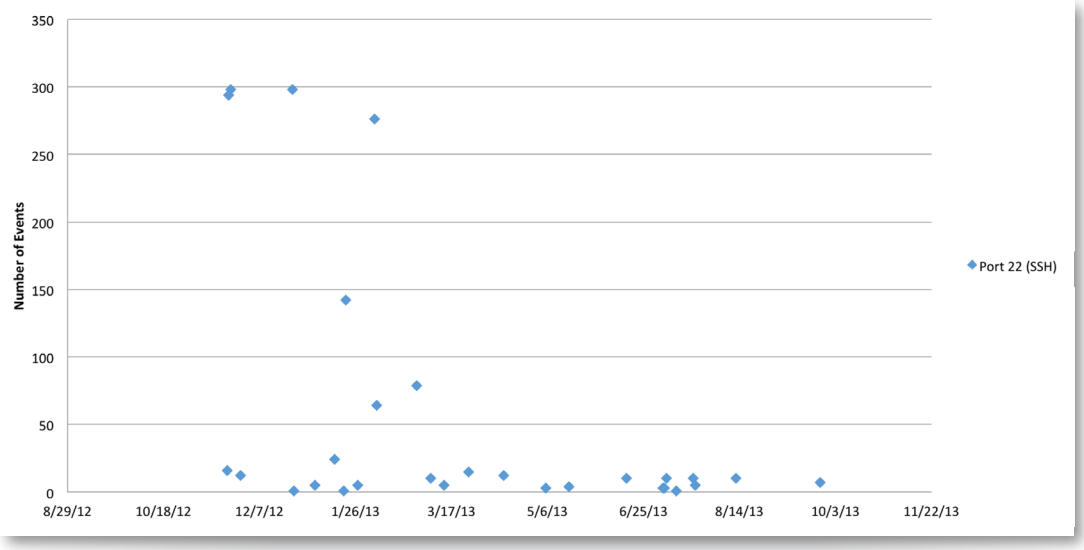


Figure C-2. Port 22 by Specific Date/Time

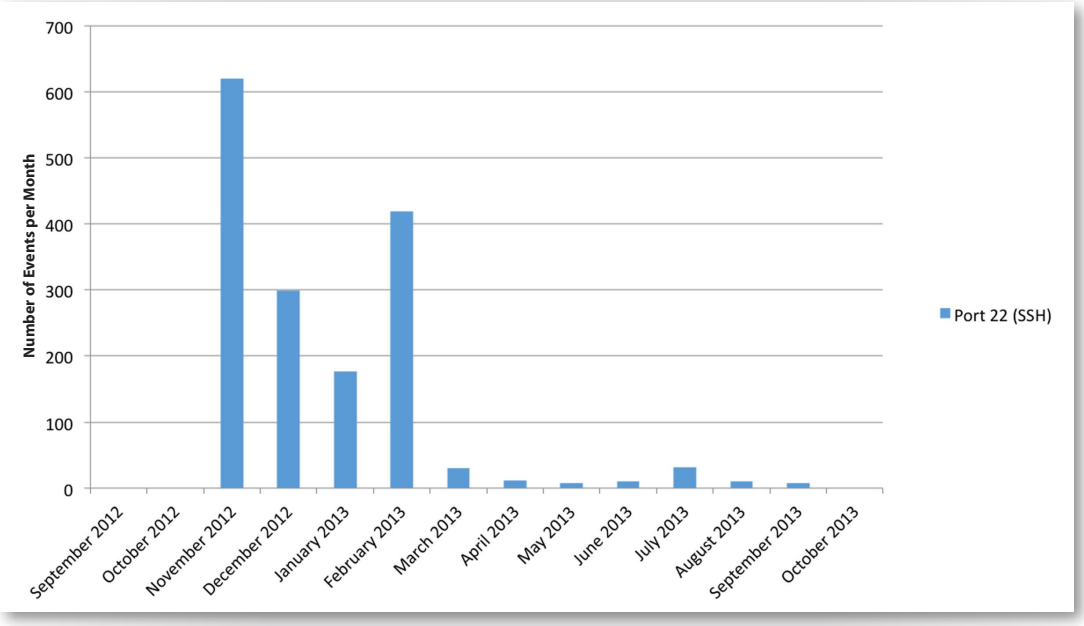


Figure C-3. Port 22 by Month

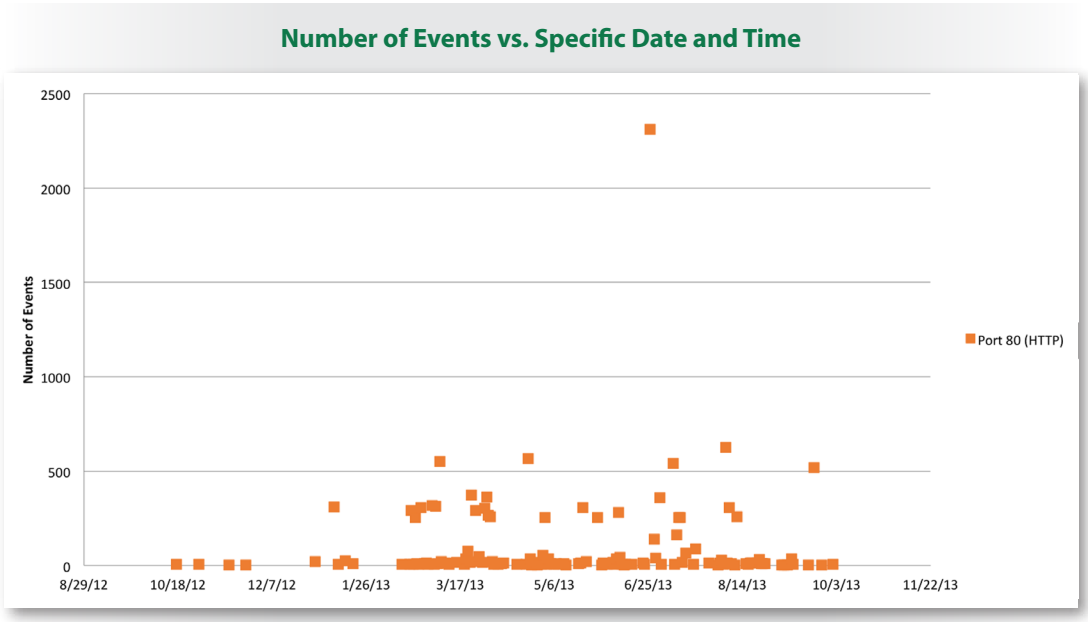


Figure C-4. Port 80 Traffic by Specific Date/Time

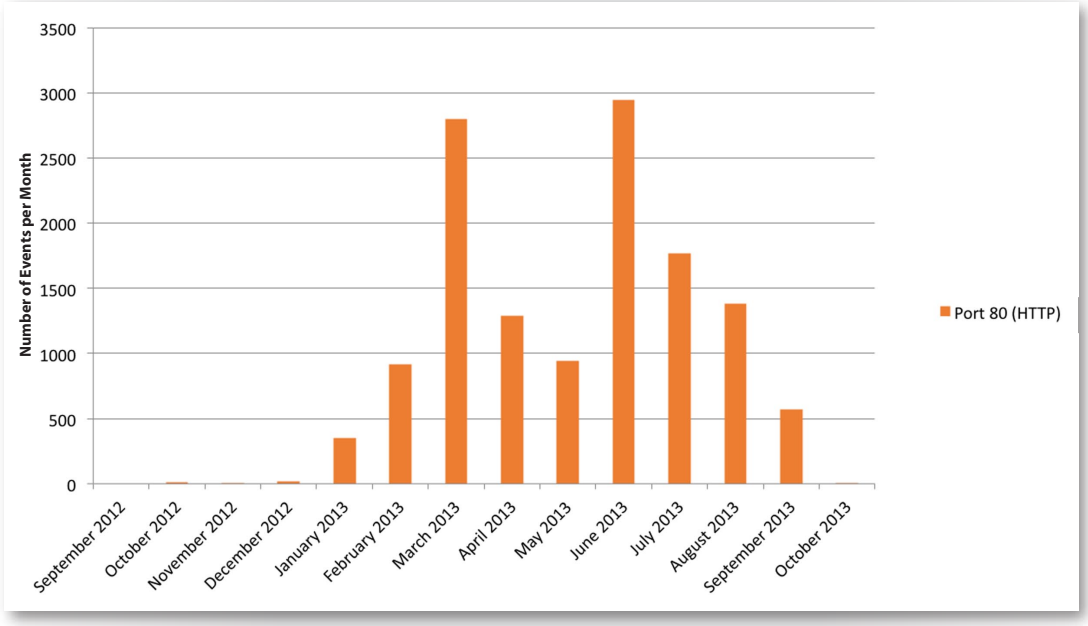


Figure C-5. Port 80 by Month

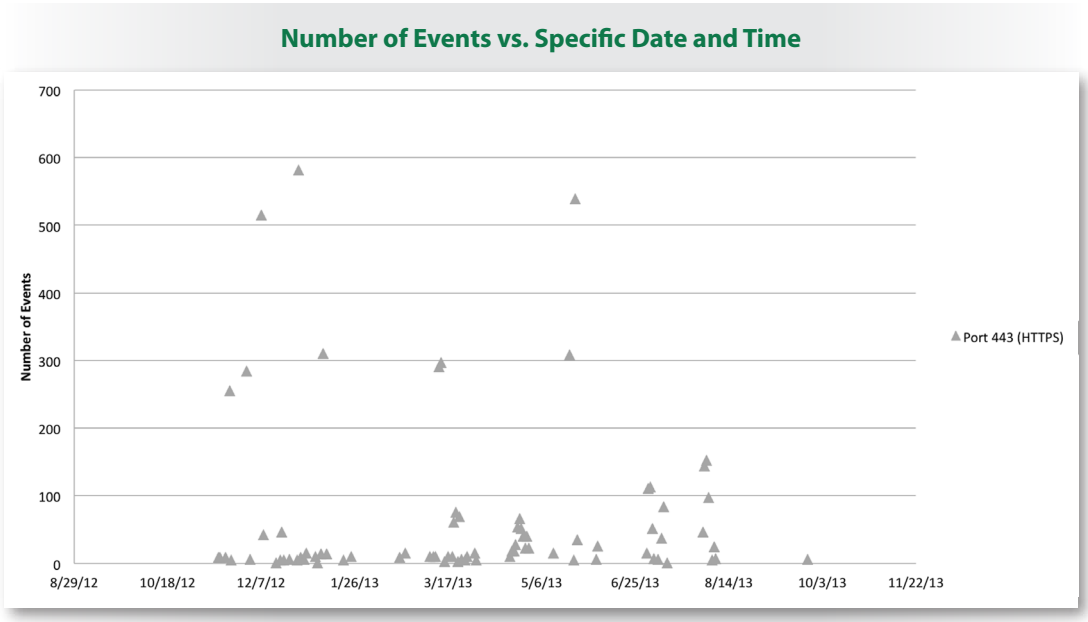


Figure C-6. Port 443 by Specific Date/Time

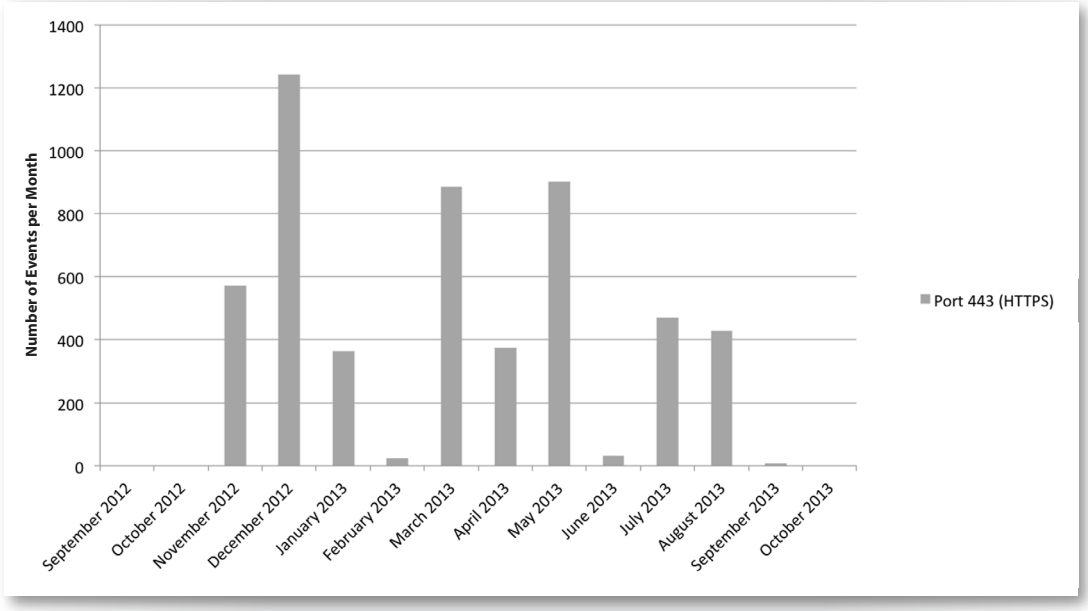


Figure C-7. Port 443 by Month

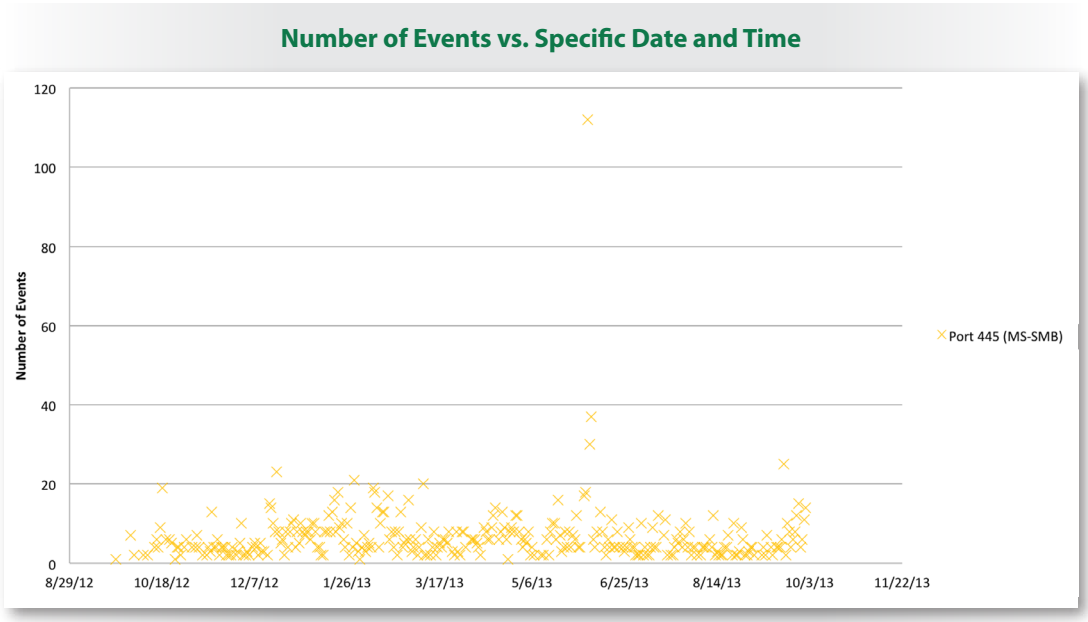


Figure C-8. Port 445 by Specific Date/Time

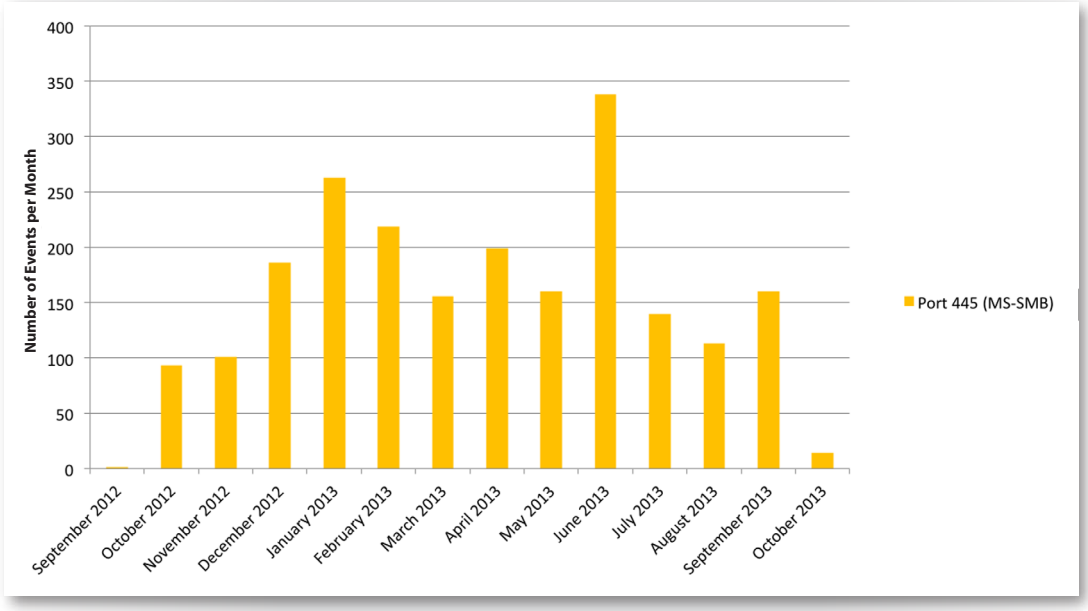


Figure C-9. Port 445 by Month

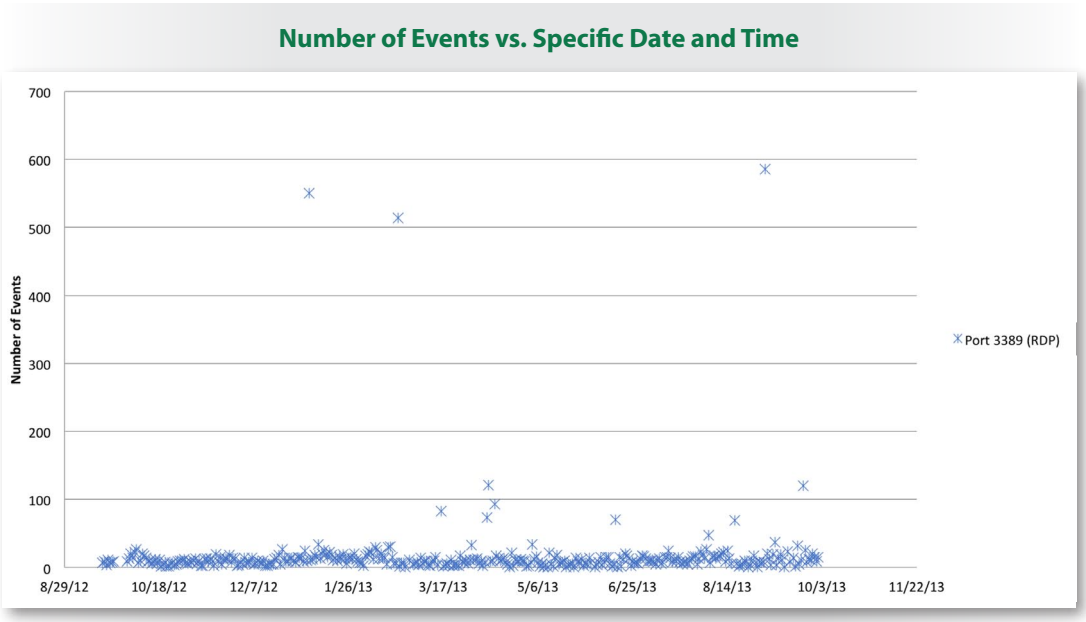


Figure C-10. Port 3389 by Specific Date/Time

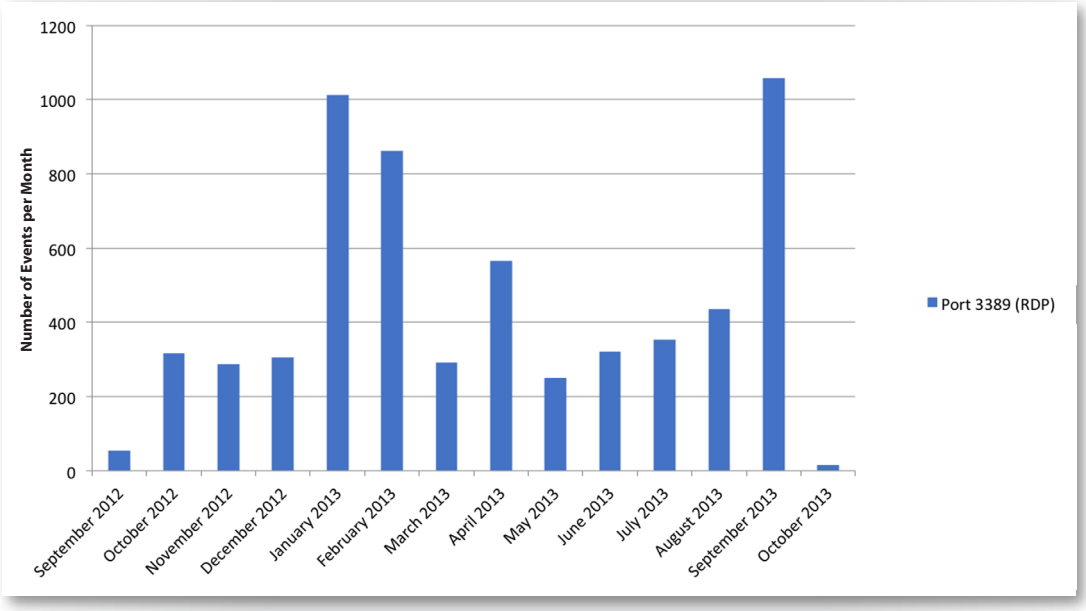


Figure C-11. Port 3389 by Month

A Quick Analysis of RDP (Destination Port 3389)

Remote computing is of special interest with respect to health care. Many organizations use remote desktop computing for its convenience in allowing busy providers to work remotely yet securely. But remote computing protocols can be one of the greatest sources of compromise. We therefore looked a little closer at what the Norse data was revealing here.

Generally, remote computing events related to RDP (destination port 3389) came from a variety of sources, with daily events averaging under 17 per day. However, the higher monthly trends in January, February and September were driven by large daily spikes in activity involving single organizations on specific days, all close to major federal holidays:

- **January 5, 2013:** A large, well-respected ear, nose and throat practice in California with over 20 providers has an activity storm with 540 events involving RDP on the Saturday after New Year's Day. A few events (12) were first seen on Thursday, January 3, and may have been a precursor to this storm. This event was followed by a few events (2) on Monday, January 7, and again (10) on Sunday, January 27.

  At this point, SANS can only speculate as to the cause of the activity on the 5th; however, because the event storm occurred on the first Saturday, early in the new year of 2013, we surmise that it may be correlated with upgrades or enhancements to the practice's infrastructure over the weekend that opened a temporary, albeit serious, vulnerability in the practice's perimeter defenses.

- **February 21, 2013:** This organization, a leading provider of pharmacy and related services to specialized health care settings, experienced an activity storm of 510 events. This is a single day, single protocol event for the firm occurring on the Thursday of President's Day week.

  SANS is not speculating as to what may have triggered this one-time event, but apparently the organization promptly recognized and suppressed the malicious activity.

- **September 3, 2013:** A group practice located in a major east coast metropolitan area suffered an activity storm of 578 events the day after Labor Day. No events preceded the storm on the 3rd, but threat intelligence identified events on the following weekend as well: 12 on Saturday, September 7, and 20 on Sunday, September 8.

  Again, the only protocol involved was RDP, port 3389. A review of the source IP reveals that these events emanated from an address that resolves to the web-based administrative login for their mail server.

These activity diagrams should be a warning to organizations that they should take proper measures to ensure that RDP services are not accessible from the public Internet unless they have taken proper measures to secure it against compromise. The specific examples provided here also indicate that organizations should pay special attention to monitoring traffic at or around holiday and weekends.

Activity of the Final Five Destination Ports

Returning to the top 10 destination ports, let's examine ports 5038 (Figures C-12 and C-13), 5060 (Figures C-14 and C-15), 5900 (Figures C-16 and C-17), 8080 (Figures C-18 and C-19), and 32767 (Figures C-20 and C-21).

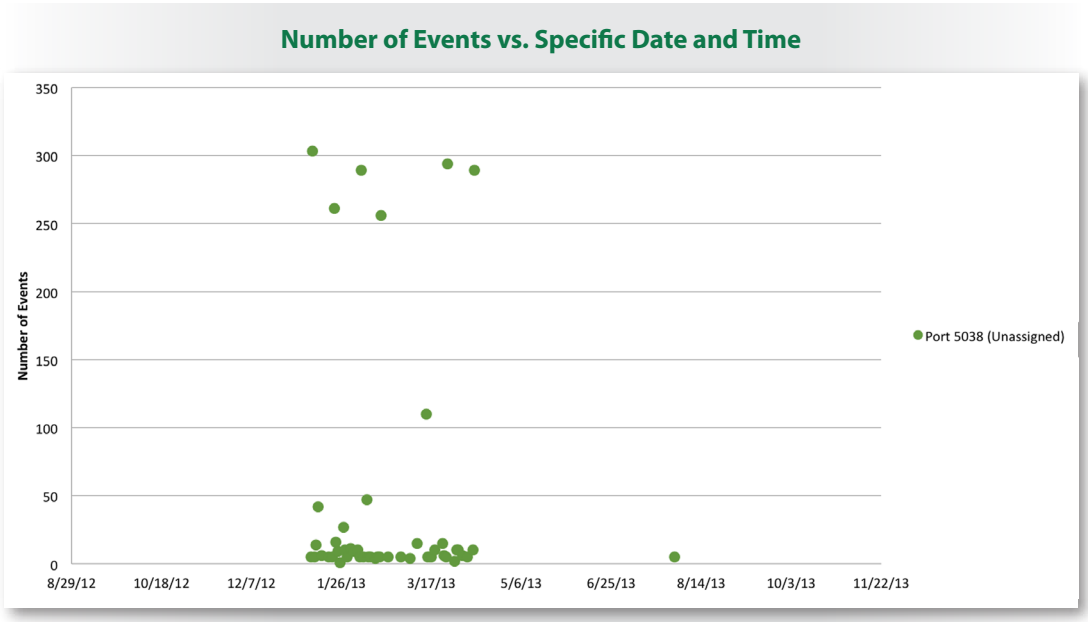


Figure C-12. Port 5038 by Specific Date/Time[40]

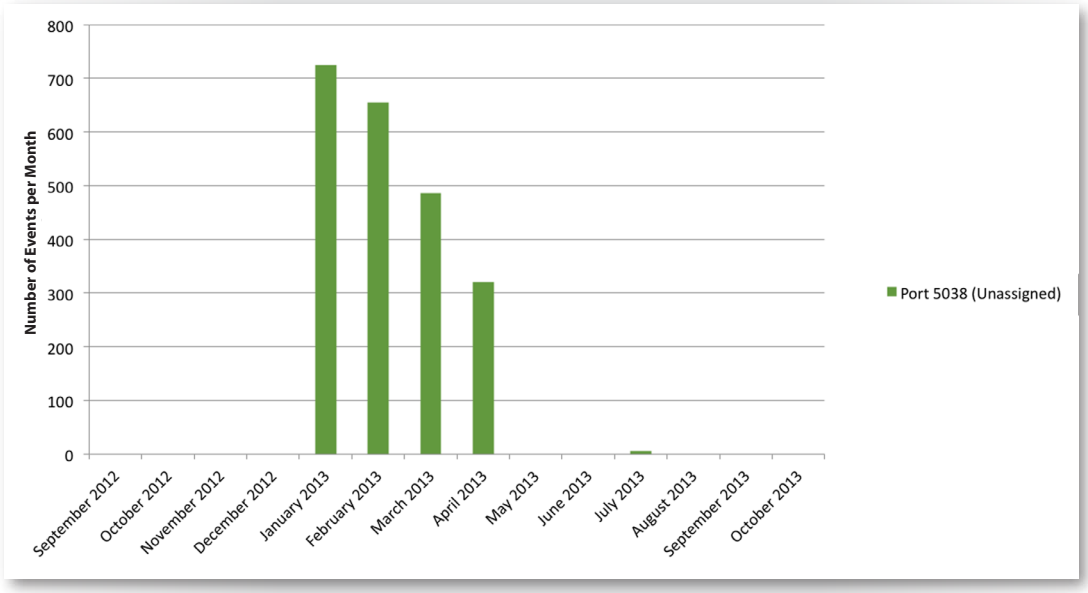


Figure C-13. Port 5038 by Month

[40] Port 5038, although considered "Unassigned" by IANA, is associated with a VoIP-based solution. Malicious activity related to this port was definitely of interest as SANS explored the mechanisms around its use. We further analyze this port in our discussion of Site One in the main body of the report.

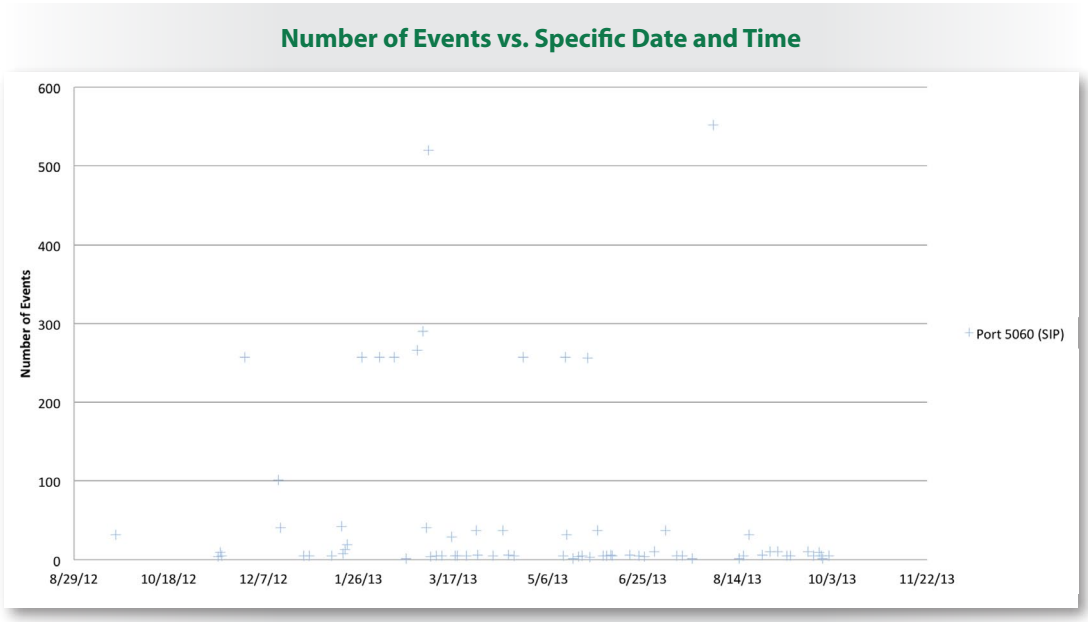


Figure C-14. Port 5060 by Specific Date/Time

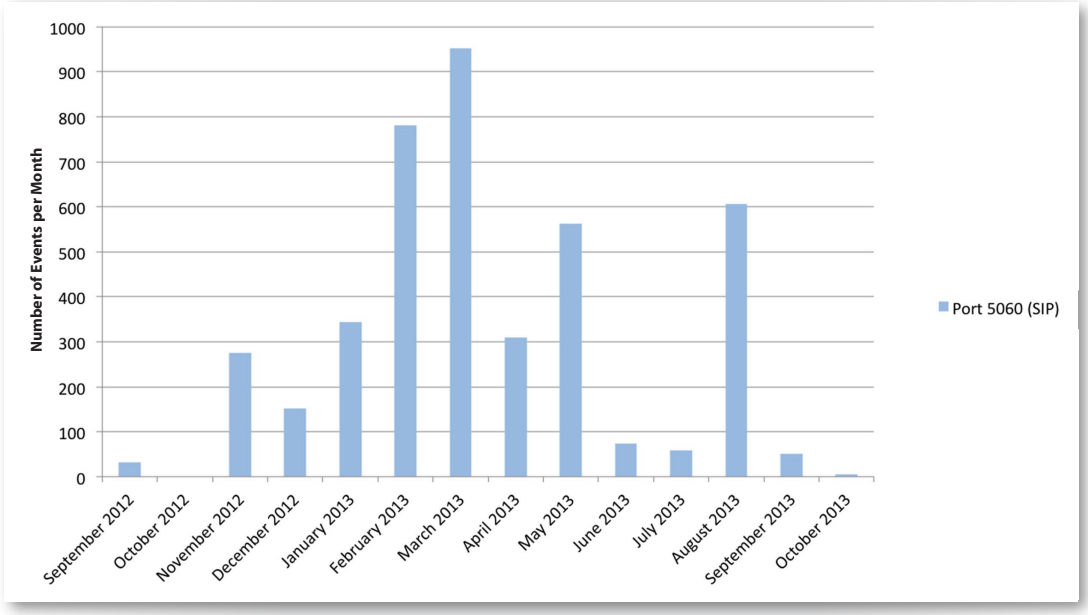


Figure C-15. Port 5060 by Month

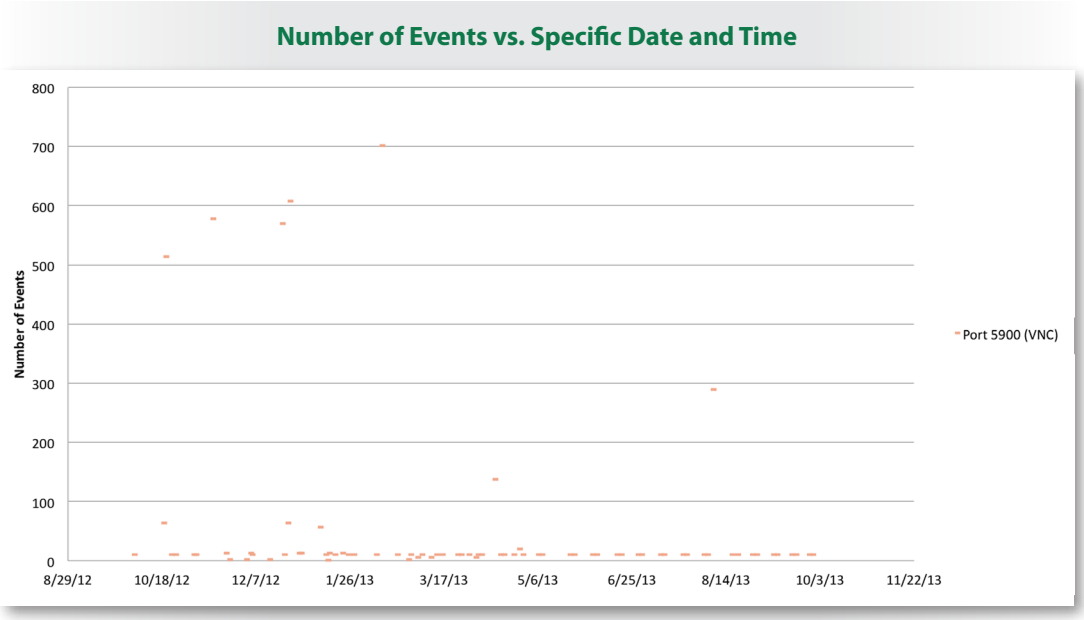


Figure C-16. Port 5900 by Specific Date/Time

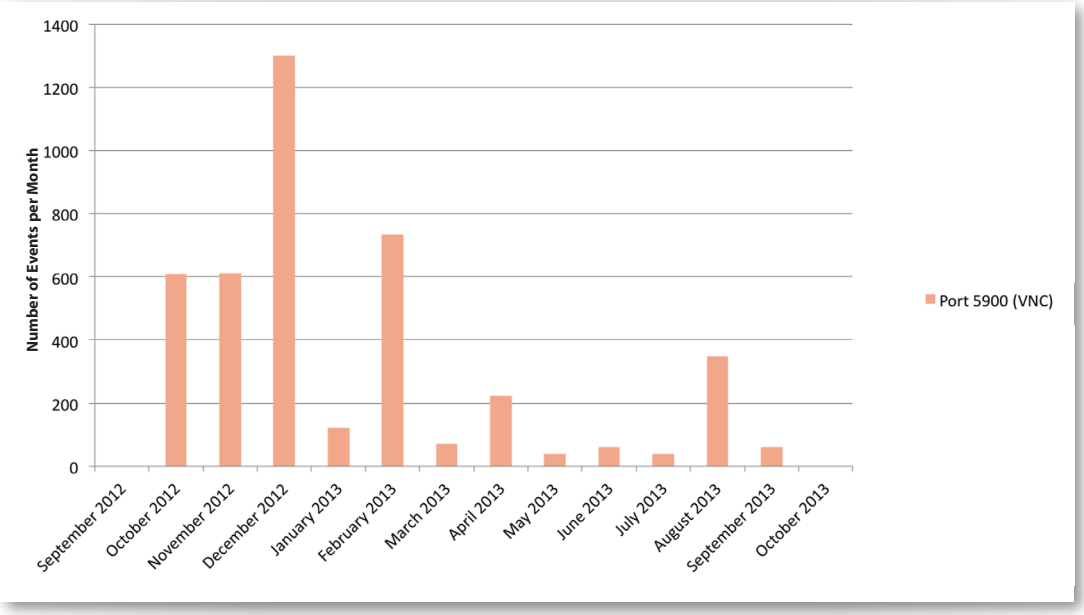


Figure C-17. Port 5900 by Month

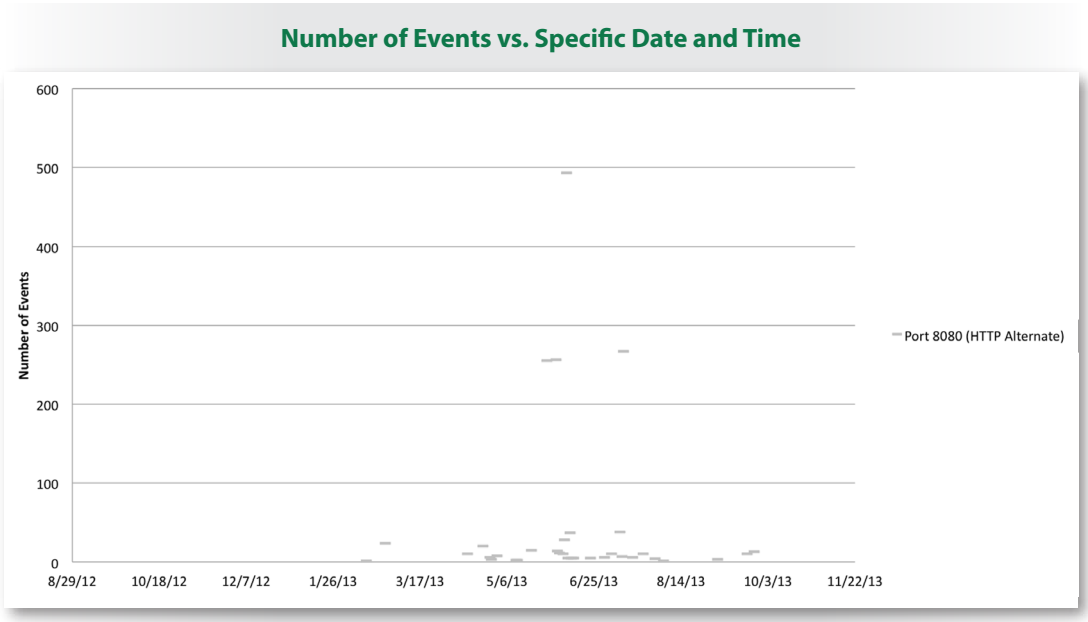


Figure C-18. Port 8080 by Specific Date/Time

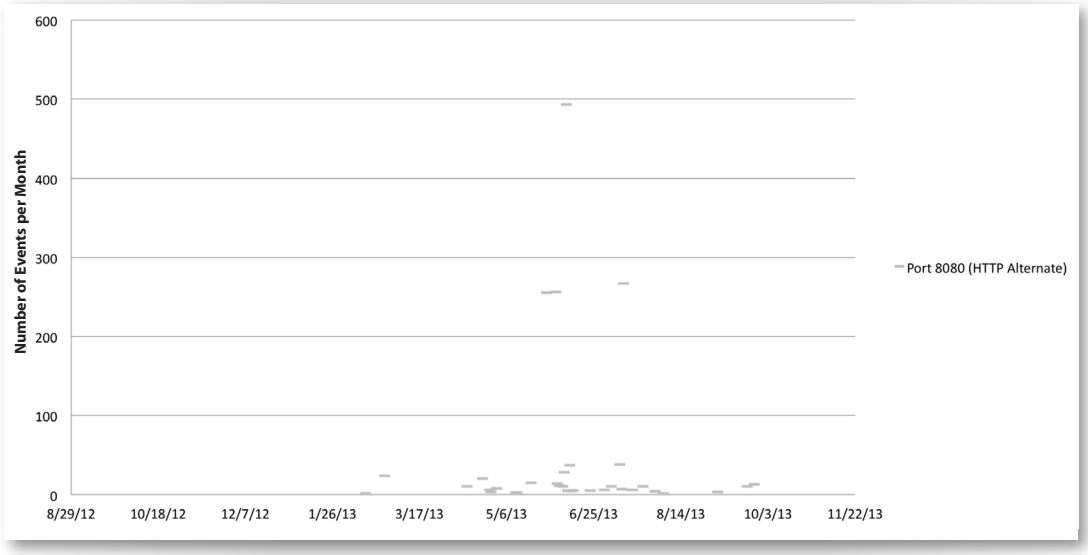


Figure C-19. Port 8080 by Month

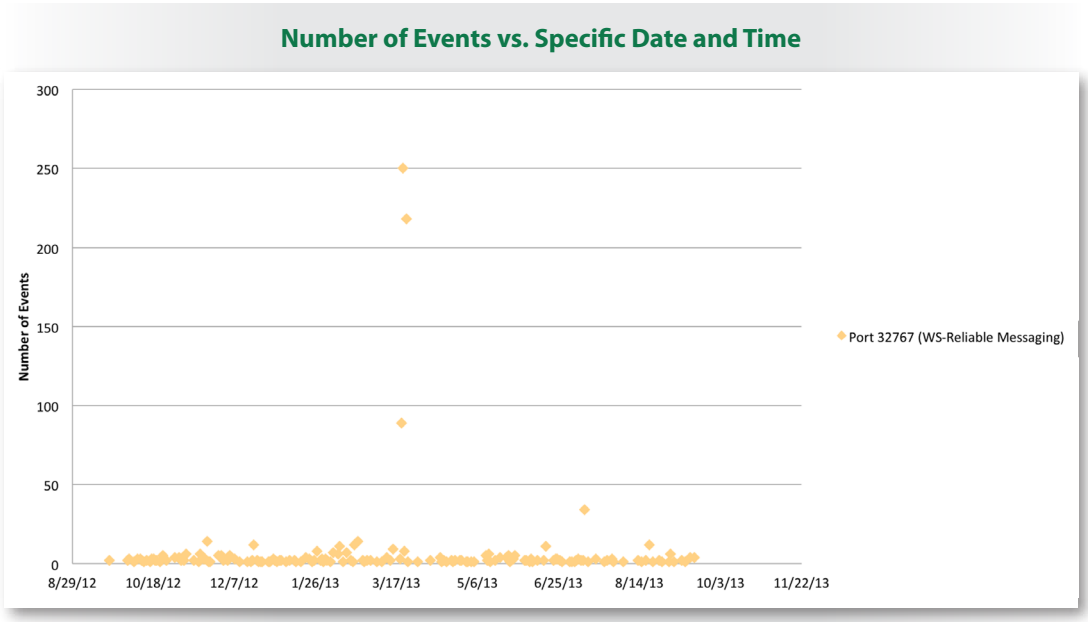


Figure C-20. Port 32767 by Specific Date/Time

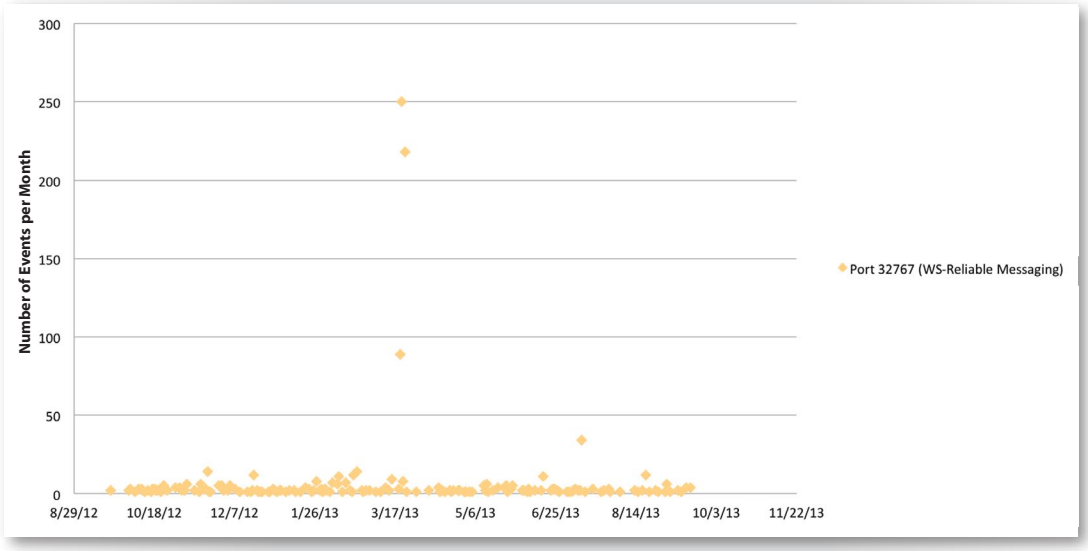


Figure C-21. Port 32767 by Month

Appendix D: Top Three Sites Traffic Trends in Time

The activity for the three most active sites in the dataset—Site One, Site Two and Site Three in the main body of the paper—is presented here, both by the date/time that an event actually occurred (Figures D-1, D-3, and D-5), as well as by the total events per month for the overall traffic and the top 10 ports that are applicable to that site (Figures D-2, D-4, and D-6).

Site One: 12,000+ events

The analysis of this site is provided in the body of the main report.

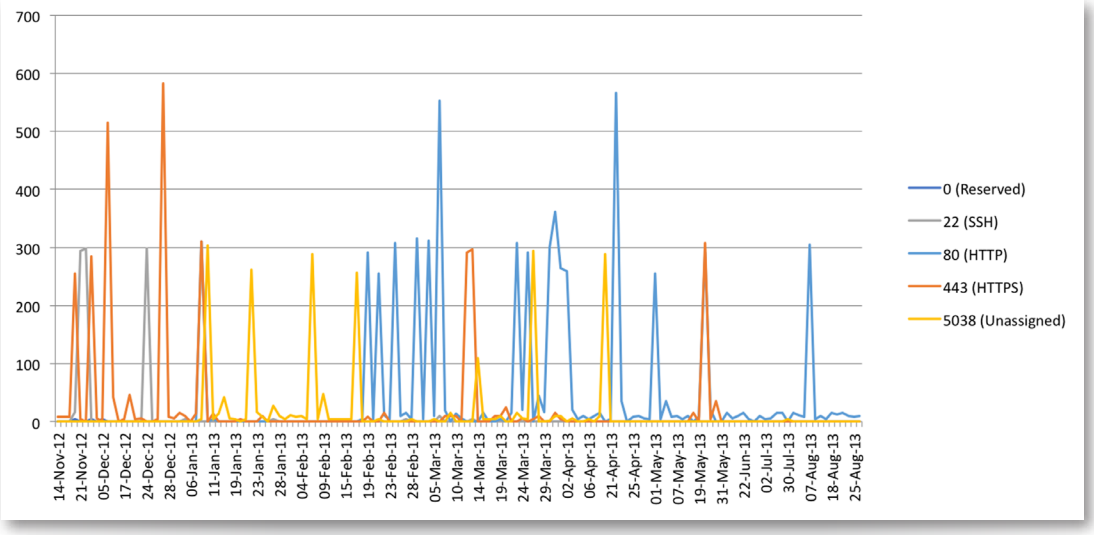


Figure D-1. Site One Events by Date/Time

Events by Month for Site One

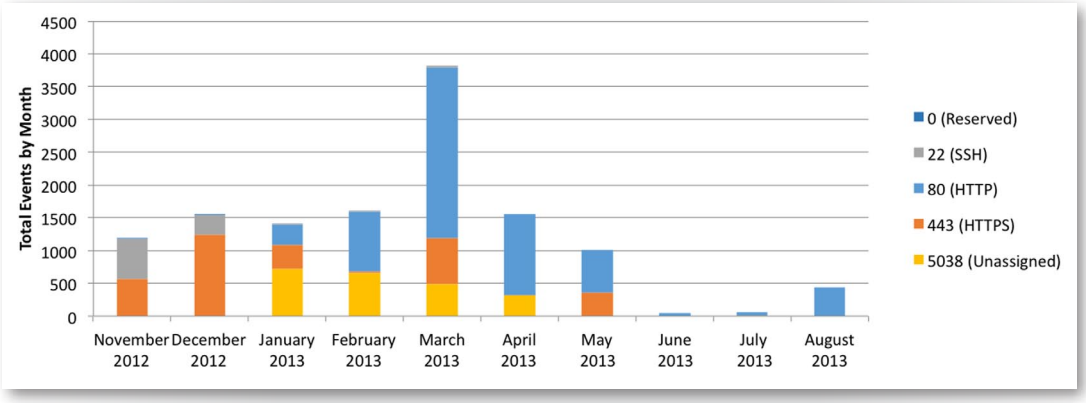


Figure D-2. Site One Events by Month

Site Two: 8,000+ events

Traffic from Site Two represents a large set of destination ports and network services. What is interesting is the growth of suspicious port 80 traffic in the second half of the year, starting with a gigantic spike on June 26, 2013, coinciding with the announcement of second quarter profits, settlement of a large class action suit involving the giant and pending concerns over reductions in the workforce.

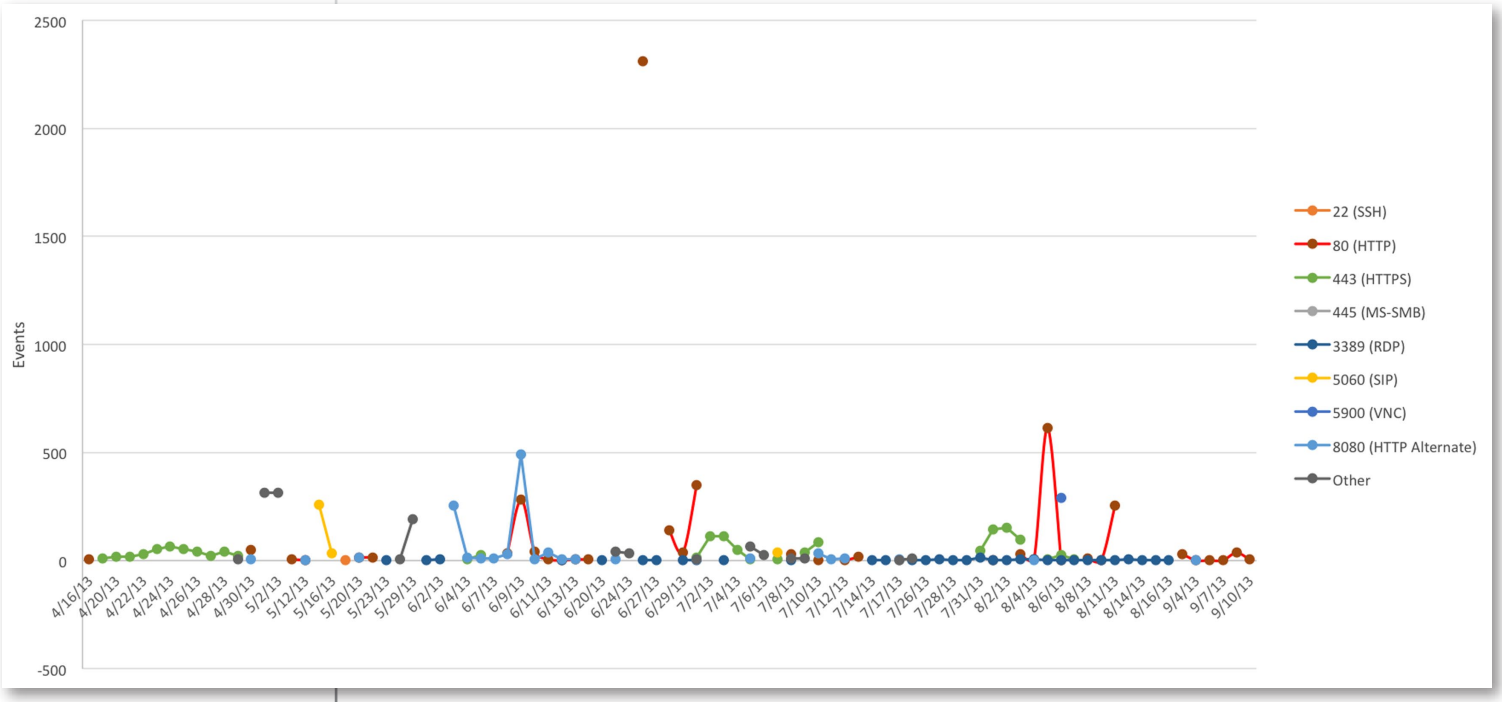


Figure D-3. Site Two Events by Date/Time

Events by Month for Site Two

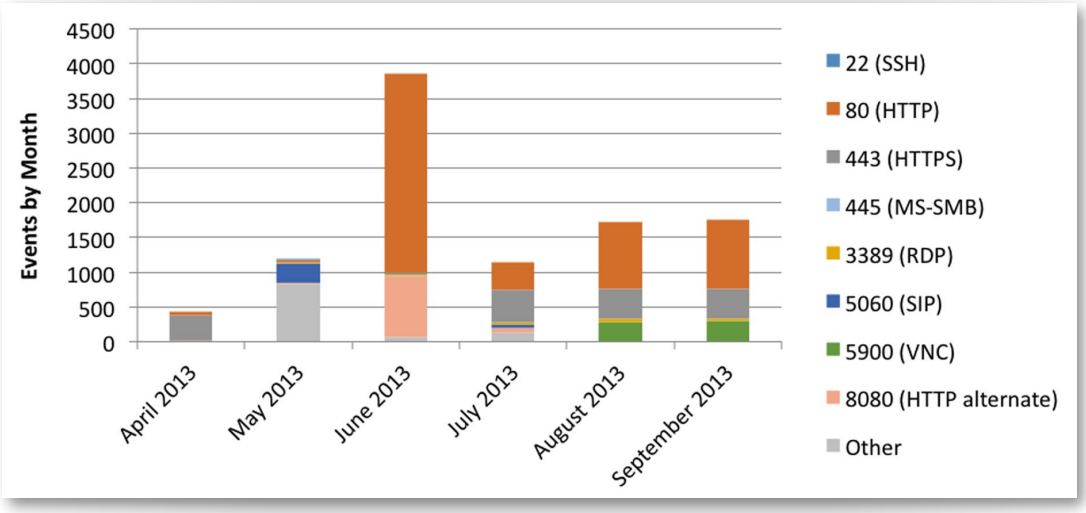


Figure D-4. Site Two Events by Month

Site Three: 2,400+ events

What is interesting about this plot is the correlation with the time of year. November 22, 2012, was Thanksgiving, and Figure D-5 shows a lull in Port 5900 activity during that long weekend and into the first two weeks of December. The increased volume in later December may reflect that most of the staff may have been working off-site or from home over the holidays. The decline of activity in January may be due to a return to work and/or a realization that there was a problem—and the subsequent creation and enforcement of better security measures for off-site employees.

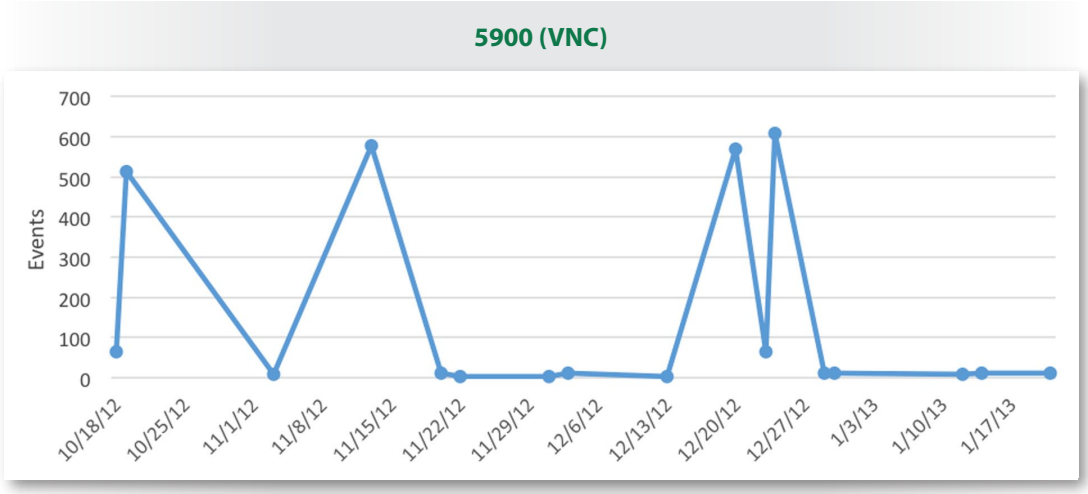


Figure D-5. Site Three Port 5900 Events by Date/Time

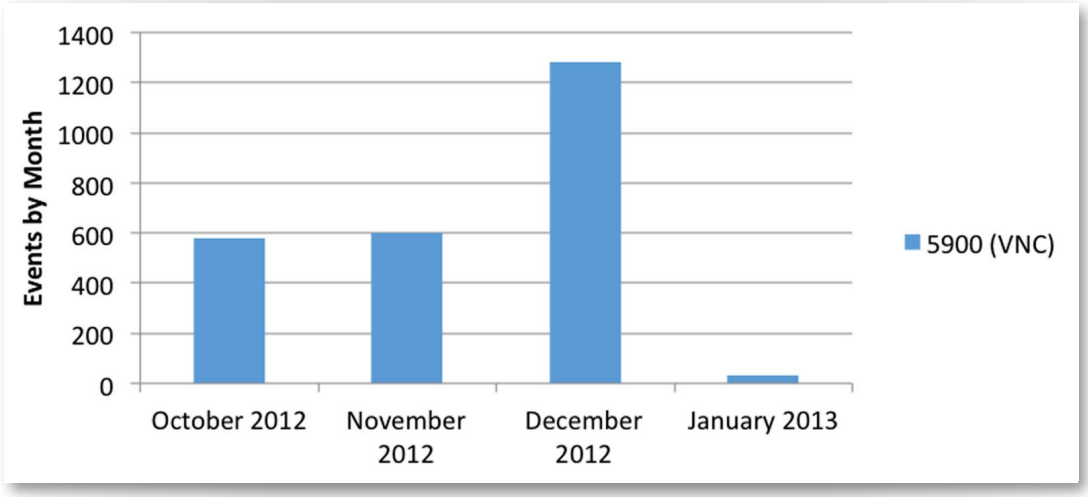


Figure D-6. Site Three Port 5900 Events by Month