CHECK POINT 2013 SECURITY REPORT

JANUARY 2013

Check Point®
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT 2013 SECURITY REPORT

01 INTRODUCTION AND METHODOLOGY

“JUST AS WATER RETAINS NO CONSTANT SHAPE, SO IN WARFARE THERE ARE NO CONSTANT CONDITIONS.”[1]

ALTHOUGH THIS SENTENCE IS 2,600 YEARS OLD, SURPRISINGLY IT IS STILL VERY RELEVANT, REFLECTING TODAY’S MODERN WARFARE - CYBER WARFARE.

Hackers’ techniques are constantly changing. As these nefarious assaults become more advanced and sophisticated, security challenges are raised to new heights. Data centers, employees’ computers and mobile phones are prime targets for hackers who deploy an endless variety of malware such as bots, trojans and drive-by downloads. Hackers use ruse and social engineering to manipulate innocent users’ identities to access corporate information such as internal documents, financial records, credit card numbers and user credentials, or to simply shut down services with denial of service attacks. This modern war of advanced threats and attacks is here to stay. Corporate information stored in data centers, servers, PCs and mobile phones is ever increasing; with more data and platforms implying added risks for corporations. Finally, the list of security threats is not getting shorter, and each new attack reveals a deeper level of attacker sophistication.

What were the main security risks that your network faced last year? What are the risks it will face next year? These were the key questions that kept Check Point’s security research team busy over the past several months. While gathering answers to these questions, Check Point conducted an intensive security analysis spanning over 800 of its client organizations.

This report provides an analysis of 2012 network security events that occurred in organizations worldwide, with examples of published incidents, explanations on how some of the attacks were carried out followed by recommendations on how to protect against such assaults. The report is divided into three parts. Each part is dedicated to a different aspect of security. The first part focuses on security threats such as bots, viruses, security breaches and attacks. The second part discusses risky web applications that compromise organizational network security. The final part is dedicated to loss of data caused by unintentional employee actions.

Methodology

Check Point’s 2013 Security Report is based on a collaborative research and analysis of security events gathered from four main resources: Check Point Security Gateways Analysis Reports[2], Check Point ThreatCloud™[3], Check Point SensorNet™ network and Check Point Endpoint Security reports.

A meta-analysis of network security events at 888 companies was conducted using data collected from Check Point Security Gateways, which scanned the companies’ incoming and outgoing live network traffic. This traffic was inspected by Check Point’s multi-tier Software Blades technology to detect a variety of security threats such as high-risk applications, intrusions attempts, viruses, bots, sensitive data loss, etc. The network traffic was monitored in real time by implementing the Check Point Security Gateway inline or in monitor (i.e. tap) mode.

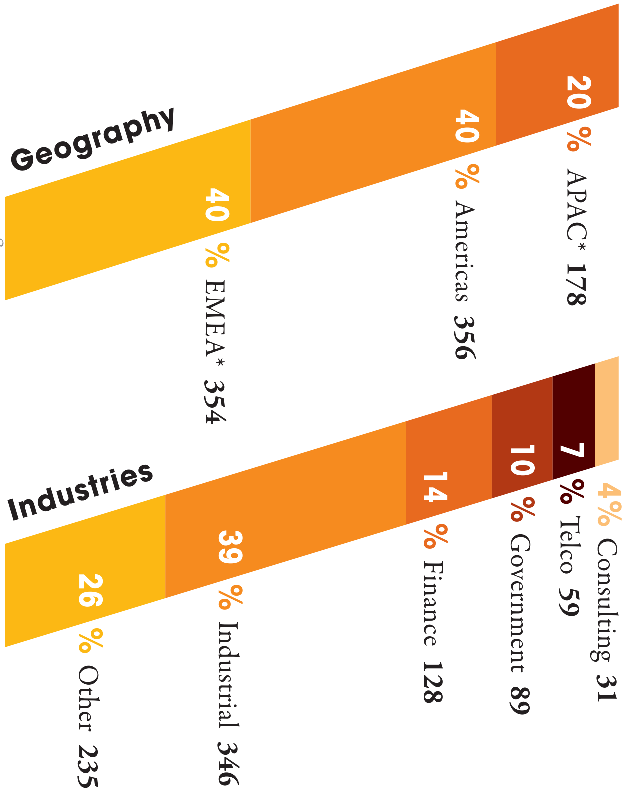
On average, each organization's network traffic was monitored for 134 hours. The companies in our research reflected a wide range of industries located globally as depicted in Chart 1-A.

In addition, over 111.7 million events from 1,494 Security Gateways were analyzed using data generated by Check Point's ThreatCloud™. ThreatCloud™ is a massive security database updated in real time and populated with data collected from a large network of global sensors, strategically placed around the globe. ThreatCloud™ gathers threat and malware attack information and enables identification of emerging global security trends and threats, creating a collaborative network to fight cybercrime. For our research, ThreatCloud™ data gathered over a 3-month period between August and October 2012 was pooled and analyzed.

Reference for threat data was gathered from Check Point's SensorNet™ for the period between July 1st and September 30st, 2012. Check Point SensorNet™ is a worldwide distributed network of sensors which provide security information and traffic statistics to a central analysis system. This data is analyzed to detect trends and anomalies, and to provide global security status monitoring in real time.

Finally, a meta-analysis of 628 endpoint security reports in a variety of organizations was conducted. This security analysis scanned each host to validate data loss risks, intrusion risks and malware risks. The analysis was done with Check Point Endpoint Security report tool which checks whether an anti-virus was running on the host, if the anti-virus was up-to-date, was the software running on the latest version, and more. This tool is free and is publically available. It can be downloaded from Check Point's public website[4].

This report is based on data gathered from these sources.



Source: Check Point Software Technologies

Chart 1-A

* APAC- Asia Pacific and Japan. EMEA- Europe, Middle East and Africa

Industry Specification

Industrial: Chemical/Refinery, Healthcare, Pharmaceutical, IT, Manufacturing, Transportation, Utilities, Infrastructure.
Finance: Finance, Accounting, Banking, Investment.
Government: Government, Military.
Telco: Telco, Services Provider, ISP, MSP.
Consulting: Consulting Services
Other: Advertising/Media, Distributor, Education, Legal, Leisure/Hospitality, Retail and Wholesale, Securities, Other

02 THREATS TO YOUR ORGANIZATION

> "THERE ARE ONLY TWO TYPES OF COMPANIES, THOSE THAT HAVE BEEN HACKED AND THOSE **THAT WILL BE."**
>
> **Robert Mueller, Director, FBI, March, 2012[5]**

Breaking News: A New Cyberattack is Exposed

In 2012, cyberattacks continued to proliferate and routinely dominated headlines. Malicious software threats, attacks and botnets made the front page news almost daily, displaying hackers' success in stealing data, paralyzing operations and spying on corporations and governments. The following represent a fraction of cyberattack events that occurred in 2012: hackers attacked the White House's network[6], hactivist group Anonymous brought down U.S. Telecom Association and TechAmerica's websites[7], cyberattacks hit Capital One Financial Corp., BB&T Corp., HSBC Bank USA[8], and many others.

Advanced Persistent Threats

Cybercriminals are no longer loose groups of amateurs. In many cases, cybercriminals belong to well-structured organizations that resemble terrorist cells. They are well-funded, highly-motivated and extremely goal-oriented. Cybercriminals seem to dedicate a considerable amount of time and resources to gather intelligence. Their villainous activities cause severe damages for organizations such as loss of confidential data, business interruptions, reputation damages and financial losses. The most sophisticated and long-term attacks work towards a specific pre-determined goal. These are referred to as Advanced Persistent Threats (APT). APTs are unlikely to be detected by traditional security systems, placing governments, enterprises, small businesses and even personal networks at risk.

BLACKHOLE AN EXPLOIT KIT FOR THE MASSES

Part of the massive increase in malicious activity in the last year can be attributed to hackers using pre-made attack tools and packages. With one click, anyone can download a full-fledged, highly sophisticated attack suite. One such suite is the BlackHole exploit kit. BlackHole is a widely-used, web-based software package which includes a collection of tools that leverage web browser security gaps. It enables the downloading of viruses, bots, trojans and other forms of malicious software onto the computers of unsuspecting victims. Prices for such kits range from $50 for a single day's usage, up to $1,500 for a full year[9].

DATA-BREACH INCIDENTS IN 2012

Numerous data-breach incidents took place in 2012. The result was that vast amounts of data stored on corporate servers such as credit card and personal information of customers, students and patients was compromised. These damaging assaults share the common goal of acquiring confidential information. The following list presents several examples.

Global Payments Inc.
A global payment processing company was hacked in June 2012. Over 1.5 million payment card details were stolen.

Clarksville Tennessee U.S.
In June 2012 hackers broke into the Clarksville-Montgomery County School System and stole names, Social Security numbers and other personal data of approximately 110,000 people. The hackers used information that employees and students posted online to gain access into the system[10].

Serco Thrift Savings Plan
In May 2012, a computer attack against Serco Inc. in the U.S. resulted in an information breach of 123,000 federal employees' information.

University of Nebraska suffered a data breach on its Student Information Systems database. This led to the theft of over 650,000 files containing personal data of students, alumni, parents and university employees.

U.S. Utah Dept. of Technology Services
In March 2012, 780,000 patient files relating to Medicaid health program claims were stolen from a server by hackers believed to be operating from Eastern Europe.

United Kingdom's National Health Service
Between July 2011 and July 2012, the United Kingdom's National Health Service experienced several data breaches that exposed nearly 1.8 million patient records[11].

In APT attacks, the typical first action is to perform reconnaissance to gather intelligence on the target's system. Then attackers make an initial intrusion into the target's network to open a back door which allows them to persistently remain in the network. This is usually accomplished by infecting a host with a bot which allows the attacker to communicate with the infected host without being detected. The attacker then strives to gain further access into the network and compromise even more nodes. After reaching the target, the attacker can further exploit the infected host to collect data or cause damage remotely while remaining undisclosed indefinitely.

BOT TOOLKITS ARE SOLD ONLINE FOR $500, THEIR DAMAGES COST BUSINESSES **MILLIONS OF DOLLARS**

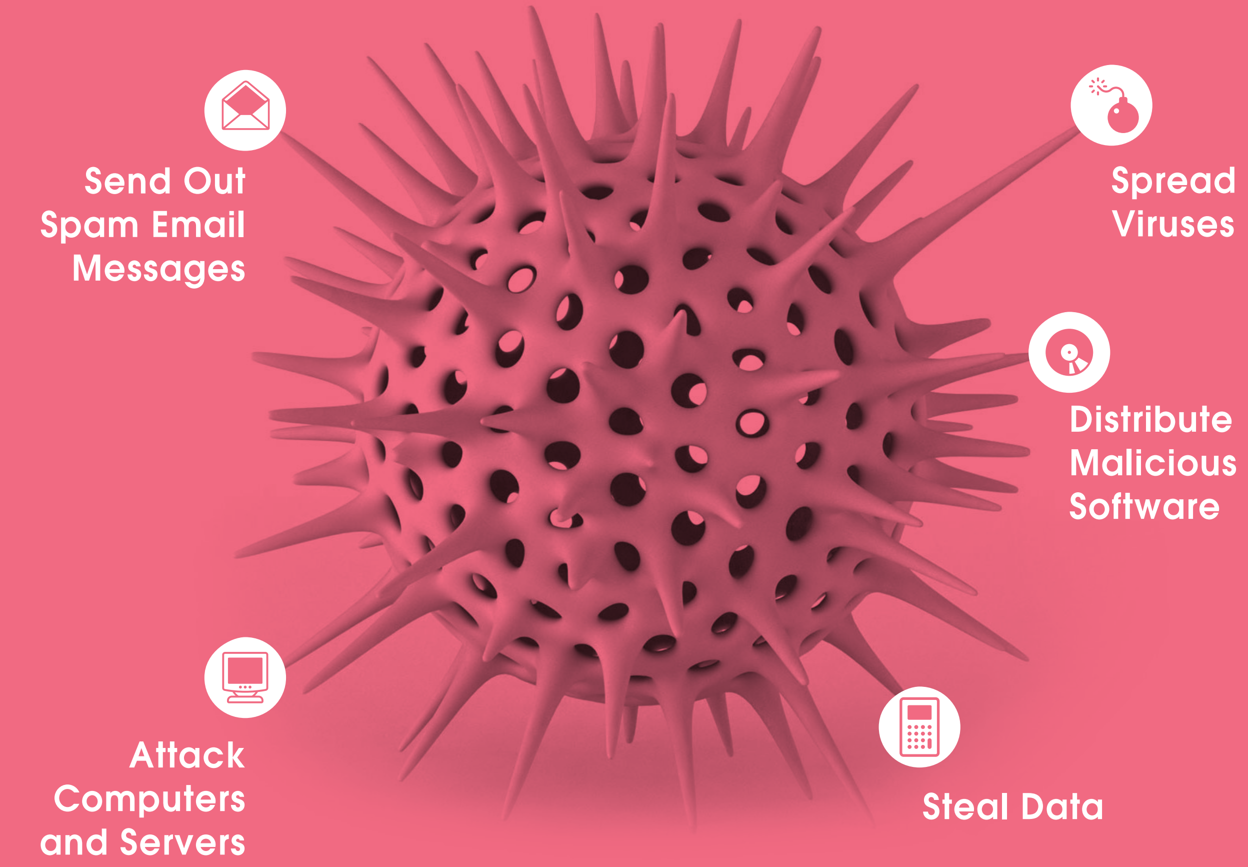
Botnets are Here to Stay

One of the most significant network security threats that organizations face today are botnets. A bot is a malicious software that invades and infects a host computer to allow cybercriminals to control it remotely. The infected host can execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DoS) attacks. The owner of the infected computer can be completely unaware of these activities. Bots also play a key role in targeted APT attacks.

There are two major trends in today's threat landscape which are driven by bot attacks. The first is the growing profit-driven cybercrime industry which includes cybercriminals, malware operators, tool providers, coders, and affiliate programmers. Their "products"(e.g. DIY malware kits, spam sending, data theft, and Denial of Service attacks) can be easily ordered online from numerous websites to cause severe damages for organizations. The second trend is the increase of ideological and state-driven attacks that target people or organizations to promote a political cause.

In any case, botnets are here to stay. As opposed to viruses and other traditional static malware types whose code and forms remain unchanged, botnets by nature are dynamic and can quickly morph form and traffic patterns. Bot toolkits are sold online for as low as $500, and their attacks cost businesses millions of dollars. The bot problem is now considered to be a major security issue.

BOTNET ACTIVITIES


Send Out Spam Email Messages
Spread Viruses
Distribute Malicious Software
Attack Computers and Servers
Steal Data

63%

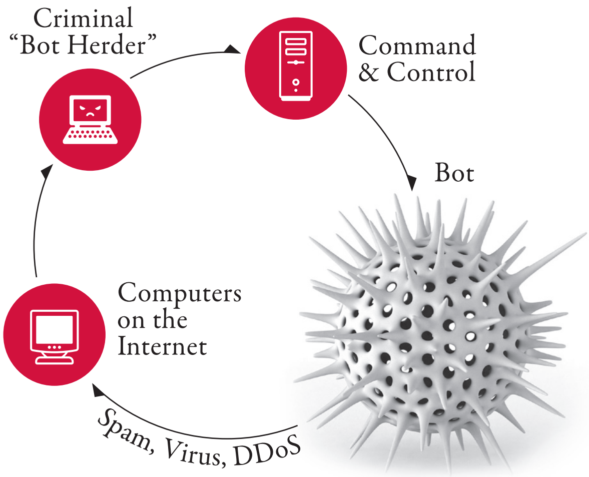
OF THE ORGANIZATIONS IN OUR RESEARCH WERE INFECTED WITH BOTS

Botnets are Everywhere, but How Critical is the Situation?

It is estimated that up to one quarter of all personal computers connected to the Internet may be part of a botnet[12]. Our research shows that in 63% of the organizations we scanned, at least one bot was detected. Most organizations were infected by a variety of bots.

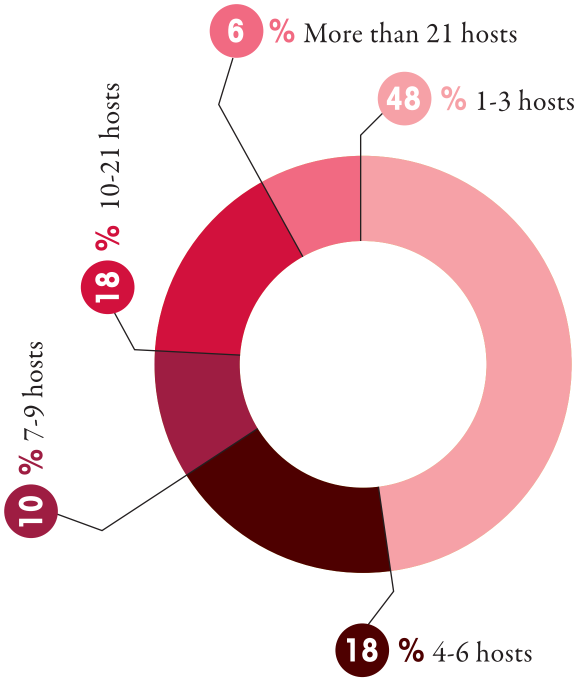
How Botnets Work

A botnet typically involves a number of computers that have been infected with malicious software. These computers then establish a network connection with a control system or systems known as Command & Control (C&C) servers. When a bot infects a computer, it takes control of the computer and neutralizes the anti-virus defenses. Bots are difficult to detect because they hide within a computer and change the way they appear to anti-virus software. The bot then connects to the C&C center for instructions from the cybercriminal who initiated the attack. Many communication protocols are used for these connections, including Internet Relay Chat (IRC), HTTP, ICMP, DNS, SMTP, SSL, and in some cases, custom protocols created by the botnet software creators.



Number of Hosts Infected with Bots

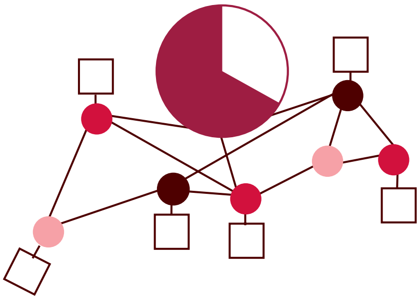
(% of Organizations)



Source: Check Point Software Technologies

Chart 2-A

ONCE EVERY 21 MINUTES A BOT IS COMMUNICATING WITH ITS COMMAND & CONTROL CENTER



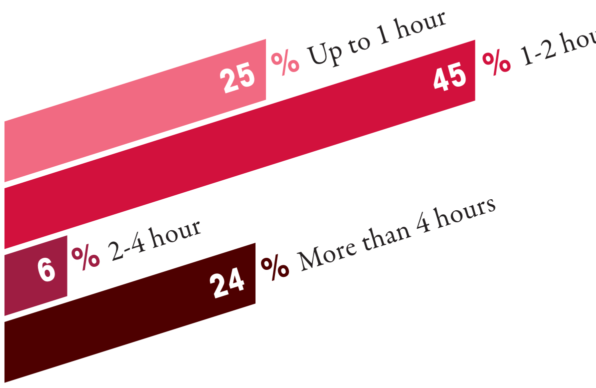
Command & Control Activity

Bots come in many shapes and forms and can execute a wide variety of activities. In many cases, a single bot can create multiple threats. Once under control of the Command & Control server, the botnet can be directed by the bot herder to conduct illegal activities without the user's knowledge. These activities include: infecting more machines in order to add them to the botnet, mass spam emailing, DDoS attacks and theft of personal, financial, and enterprise-confidential data from bots in the botnet. Bots are also often used as tools in APT attacks where cybercriminals pinpoint individuals or organizations as specific targets for attack.

Chart 2-B presents the frequency of bots' communication with their Command & Control center. 70% of the bots detected during the research communicated with their Command & Control center at least once every two hours. The majority of Command & Control activity was found in the USA, followed by Germany, Netherlands and France, as shown in Chart 2-C.

The various types of bot communication with its Command & Control center include: reports of newly infected hosts, keep-alive messages and relaying of data collected from the host system. Our research shows that on average, a bot communicated with its Command & Control center once every 21 minutes.

Frequency of Bots' Communication with Their Command & Control Center



Source: Check Point Software Technologies

Chart 2-B

Which Botnets Should We Watch Out For?

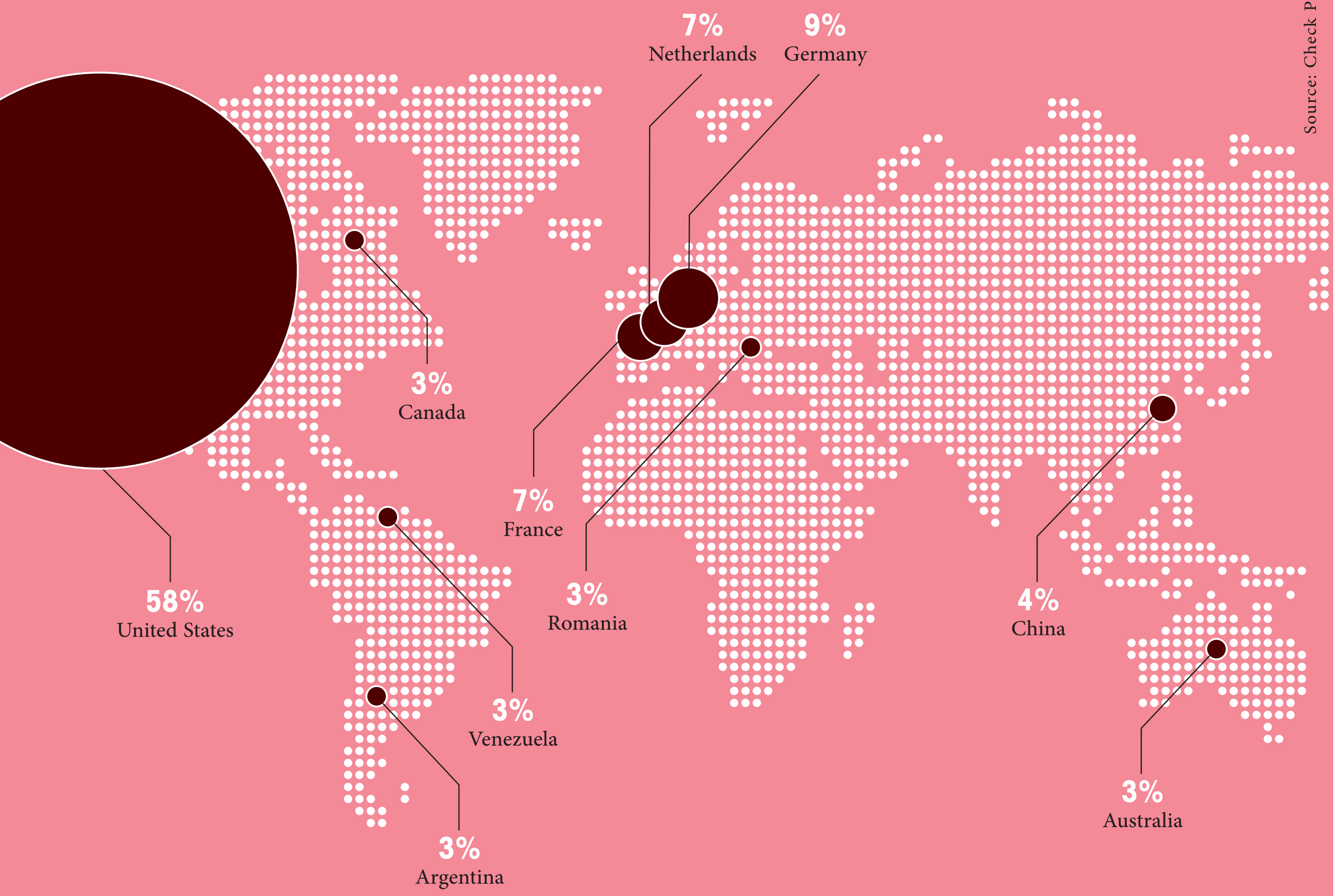
Thousands of botnets exist in the world today. The following table presents the most prominent botnets found during our research. To gain a better understanding of these stealthy threats, additional information is available at Appendix A.

How Your Organization can be Infected with Malware

Botnet Family	Malicious Activity
Zeus	Steals online banking credentials
Zwangi	Presents the user with unwanted advertising messages
Sality	Self-spreads viruses
Kuluoz	Remotely executes malicious files
Juasek	Conducts malicious actions remotely such as opening a command shell, searching/creating/deleting files and more
Papras	Steals financial information and gains remote access

See additional details in Appendix A

TOP COMMAND & CONTROL LOCATION COUNTRIES



Source: Check Point Software Technologies

Chart 2-C

IN 75% OF ORGANIZATIONS WE SCANNED, A HOST ACCESSED A MALICIOUS WEBSITE

EVERY 23 MINUTES A HOST ACCESSES A MALICIOUS WEBSITE

There are multiple entry points to breach an organization’s network defenses: browser-based vulnerabilities, mobile phones, malicious attachments and removable media, to name a few. In addition, the rapid proliferation of Web 2.0 applications and social networks used as business tools present hackers with vast new opportunities to lure victims to click on malicious links or “malvertisements“ (i.e. malicious advertisements running on legitimate websites).

Although botnets are considered to be one of the most prominent network security threats today, organizations are also facing additional security threats from damaging malware such as viruses, worms, spyware, adware, trojans, etc. Our research shows that in 75% of the organizations we scanned, a host accessed a malicious website.

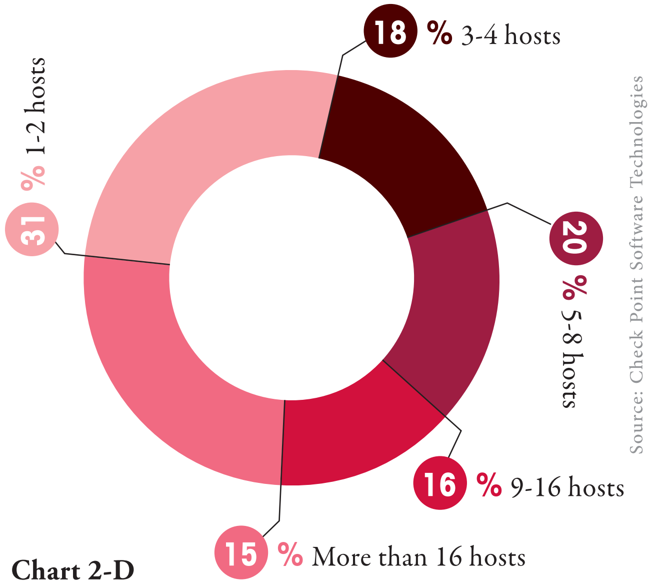
Chart 2-D presents the number of hosts that accessed a malicious website by the percentage of organizations. In over 50% of the test organizations, at least five hosts accessed a malicious website.

A malware can be downloaded by a user or by a bot located in an infected host. We found that in 53% of the researched organizations, a malware was downloaded from the corporate network. Of these organizations, over 50% had more than four hosts which have downloaded malware. Chart 2-E below presents the average frequency of malware downloads in the organizations we researched.

Chart 2-G presents the number of hosts that downloaded a malware. In more than 50% of the scanned organizations, at least five hosts downloaded a malware.

Access to Malicious Sites by Number of Hosts

(% of Organizations)

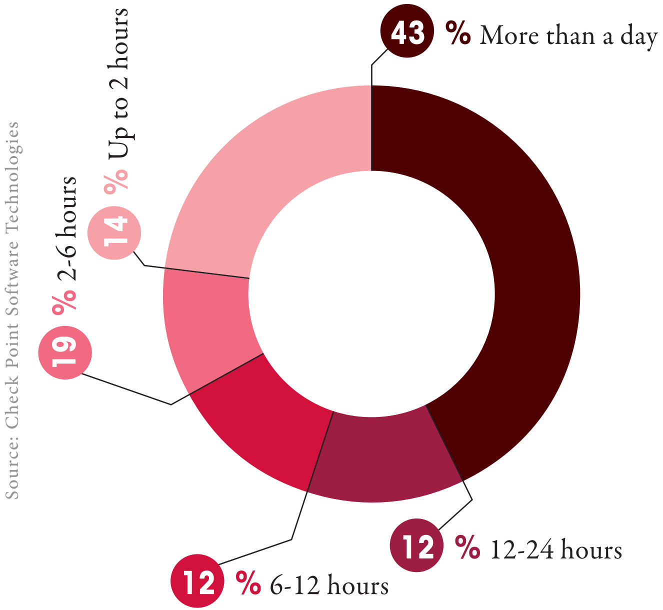


Source: Check Point Software Technologies

Chart 2-D

Malware Download Frequency

(% of Organizations)



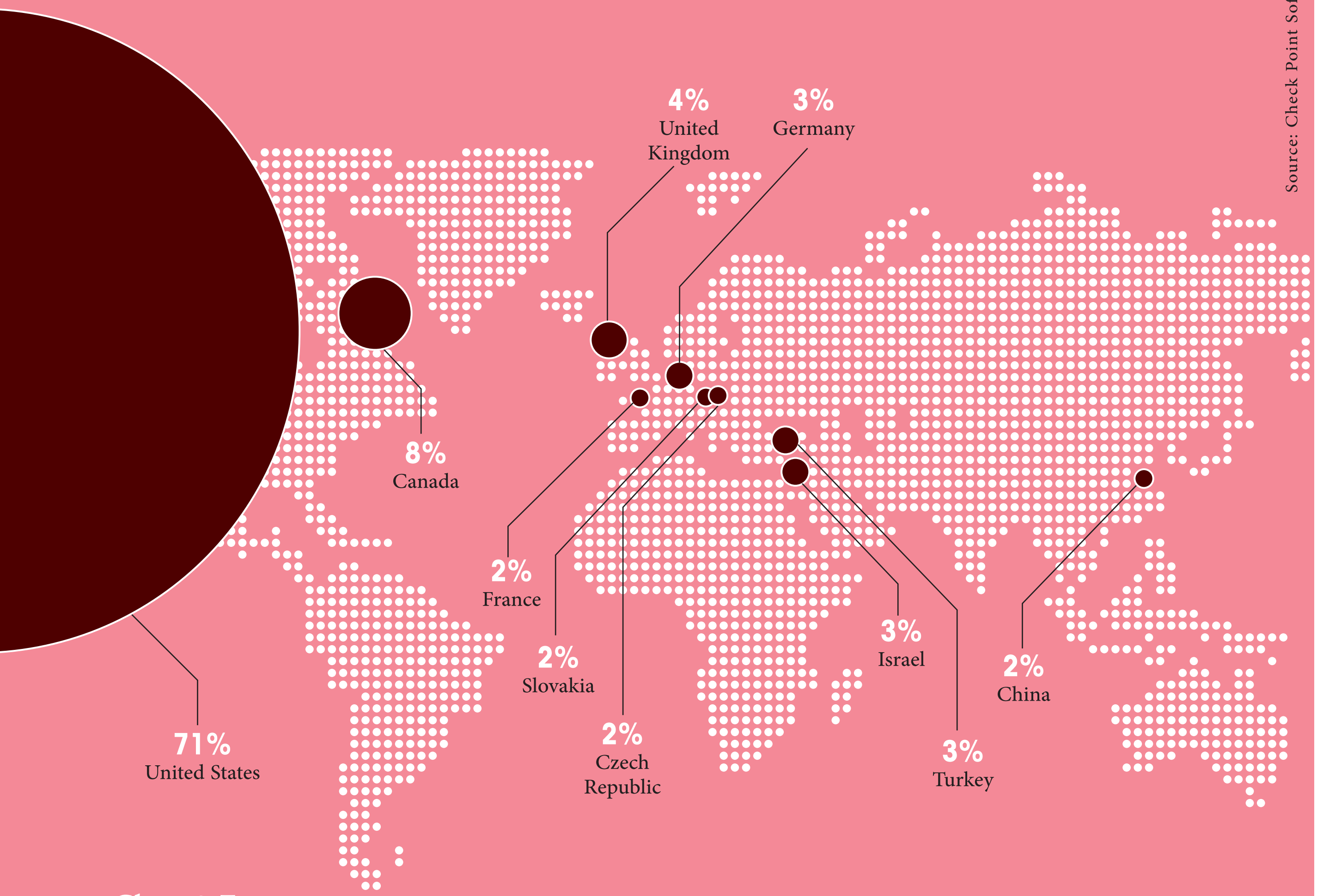
Source: Check Point Software Technologies

Chart 2-E

Our findings reveal that the majority of malware was found in the USA, followed by Canada and the United Kingdom as shown in Chart 2-F.

Anti-virus protection is one method to effectively protect against malware infections. However, our research shows that 23% of hosts in organizations did not update their anti-virus software on a daily basis. Hosts not running the latest anti-virus software are susceptible to attacks by the newest viruses. We also found that 14% of hosts in test organizations did not even have anti-virus software installed on their computers. These host computers are in extreme high risk of being infected with a malware.

TOP MALWARE LOCATION COUNTRIES

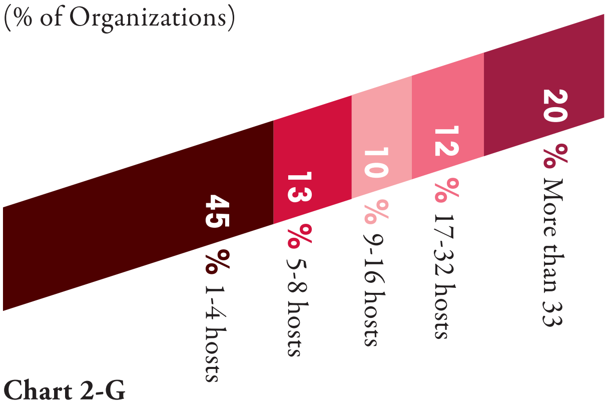


Source: Check Point Software Technologies

Chart 2-F

Number of Hosts that Downloaded a Malware

(% of Organizations)



Source: Check Point Software Technologies

Chart 2-G

Meet “miniFlame” Virus - Flame’s Smaller, More Dangerous Brother

It appears that the Flame malware that was discovered earlier in 2012 was just the beginning of a malware assault wave. Later on in the same year, a related program called “miniFlame“ was discovered. miniFlame carried out more precise attacks on targets in the Middle East and included a back door which allowed for remote control, data theft, and the ability to take screen shots.

EUROGRABBER ATTACK

36+ MILLION EUROS STOLEN FROM MORE THAN 30,000 BANK CUSTOMERS

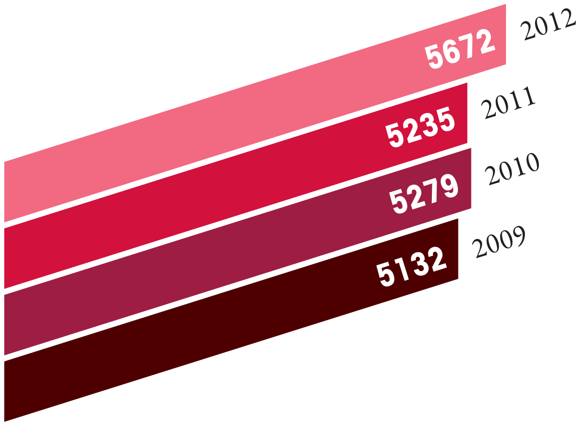
In 2012, a sophisticated multi-dimensional attack took place stealing an estimated 36+ million Euros from more than 30,000 bank customers from multiple banks across Europe. Entirely transparent to users, online banking customers had no idea that they were infected with trojans, that their online banking sessions were being compromised, or that funds were stolen directly out of their accounts. This attack was discovered and named "Eurograbber" by Versafe and Check Point Software Technologies. The Eurograbber attack employed a new and very successful variation of the ZITMO, or Zeus-In-The-Mobile trojans. To date, this exploit has only been detected in Euro Zone countries, but a variation of this attack could potentially affect banks in countries outside of the European Union. The multi-staged attack infected the computers and mobile devices of online banking customers. Once the Eurograbber trojans were installed on both devices, the bank customers' online banking sessions were completely monitored and manipulated by the attackers. Even the two-factor authentication mechanism used by banks to ensure online banking security was circumvented and was actually used by the assailants to authenticate their illicit financial transfers. Further, the trojans used to attack mobile devices were developed for both the Blackberry and Android platforms in order to attack a wider range of victims. As such, both corporate and private bank customers were infected and amounts ranging from 500 to 250,000 Euros were illegally transfered out of client accounts. Additional information on the Eurograbber attack, including a detailed review of the incident, can be found in the Eurograbber attack case study white paper[12] at the Check Point website.

More Vulnerabilities More Exploits

Hackers target well-known vulnerabilities. In fact, many rely on the fact that numerous organizations do not update their software weekly. The larger the organization, the more difficult it is for security administrators to keep all systems fully up-to-date. Thus, in many cases, a patched vulnerability that's a year old can still be used by hackers to penetrate into host systems that haven't updated their systems with the latest update patches.

The sheer volume of vulnerabilities revealed every year is overwhelming, as more than 5,000[13] new ways for hackers to cause damage and access systems were discovered in 2012 alone. Of a greater concern is that there remains numerous undiscovered vulnerabilities actively used by cybercriminals which are yet to be revealed.

Total Number of Common Vulnerabilities and Exposures

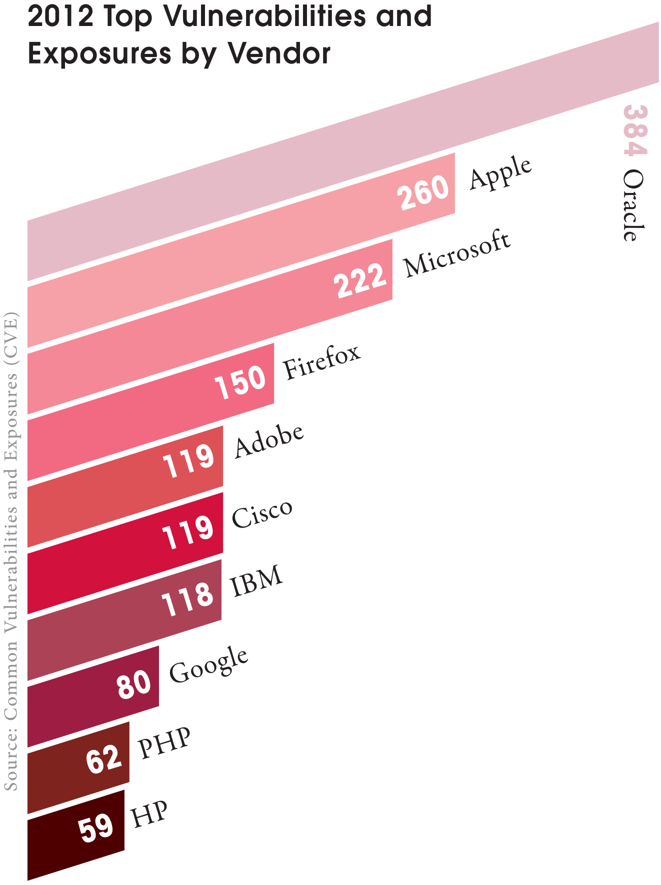


Source: Common Vulnerabilities and Exposures (CVE)

Chart 2-H

Chart 2-I demonstrates that the most popular products used by organizations were also the most susceptible to cyberattacks. Oracle, Apple and Microsoft were the most vulnerable system vendors in 2012.

2012 Top Vulnerabilities and Exposures by Vendor



Source: Common Vulnerabilities and Exposures (CVE)

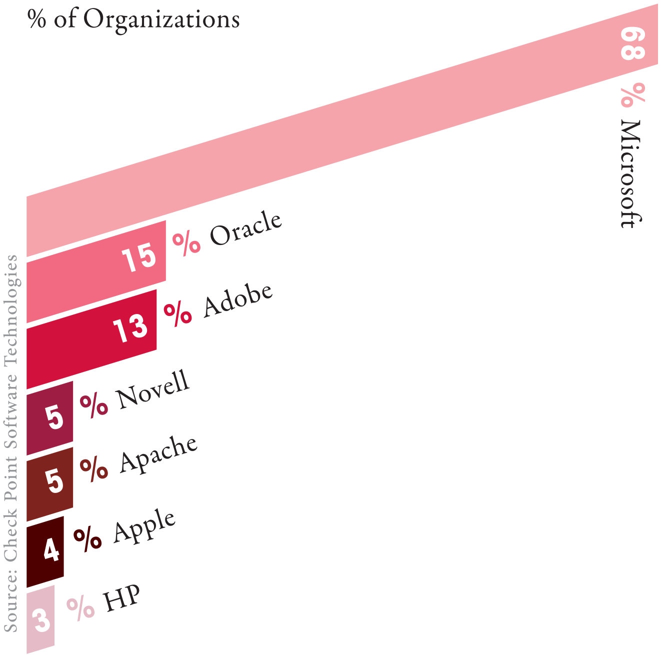
Chart 2-I

Our research shows that 75% of hosts in organizations were not using the latest software versions (e.g. Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment, etc). This means that these hosts were exposed to a wide range of vulnerabilities that could have been exploited by hackers. Our research also shows that 44% of hosts in organizations were not running the latest Microsoft Windows Service Packs. Service packs usually include security updates for the operating system. Not running the latest versions increases security risk.

Additionally, we found that Microsoft product related security events were found in 68% of the test organizations. Security events relating to other software vendors, such as Adobe and Apple, were found in significantly fewer organizations. It is interesting to note that although Apple placed second in the amount of vulnerabilities exposed, only a small percentage of organizations actually experienced security events relating to Apple products.

Security Events by Software Vendor

% of Organizations

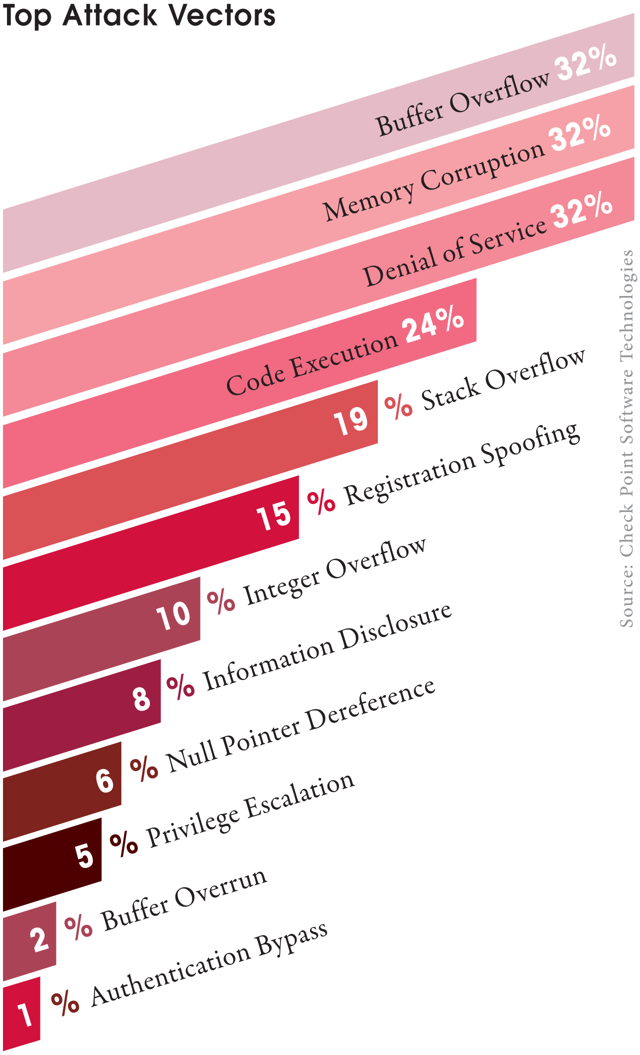


Source: Check Point Software Technologies

Chart 2-J

Hackers use various methods of attack to gain entry into the system network. These are referred to as attack vectors. Chart 2-K lists some of the more prevalent attack vectors, with the corresponding percentage of organizations that suffered from them. Memory corruption, buffer overflow and denial of service topped the list of most popular attack vectors found in our research.

Top Attack Vectors



Source: Check Point Software Technologies

Chart 2-K

What Does an SQL Injection Attack Look Like?
SQL Injection Chronicle of Event

The following case depicts an actual example of a series of SQL Injection attacks that took place between July and October 2012 at a Check Point client's system environment. The attack was detected and blocked by a Check Point Security Gateway. The case was reported by the Check Point ThreatCloud™ Managed Security Service team.

SQL Injection is a security exploit (CVE-2005-0537) in which the attacker adds Structured Query Language (SQL) code to a web form input in order to gain access to resources or to make changes to stored data. Chart 2-M shows the physical characteristics of the attack. The marked text is the data that the hacker tried to disclose with the SQL Injection (in this case, usernames and passwords). The SQL commands were: select, concat and from.

The attack occurred from 99 different IPs. Although the target organization was located in Europe, the attacks originated from a number of different locations, as presented in Chart 2-M.

SQL Injections can be manually executed via a keyboard or automatically deployed via scripted attacks. In our example, the attack peaked with a burst of 4,184 attack attempts launched within two days as depicted in Chart 2-L. These attacks used the same injecting pattern and originated from a single IP source. This was most likely an automatically deployed assault.

SQL Injection Events Rate

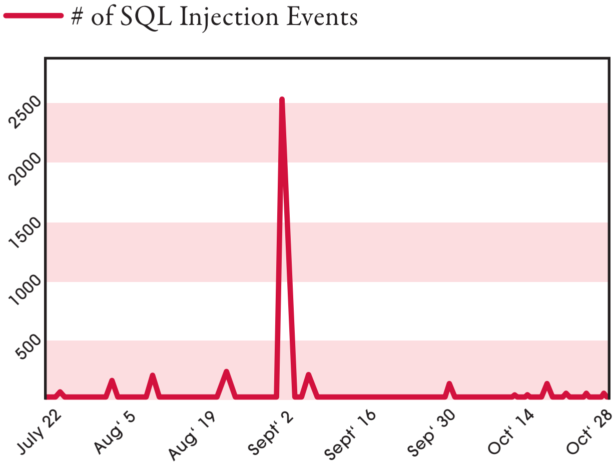
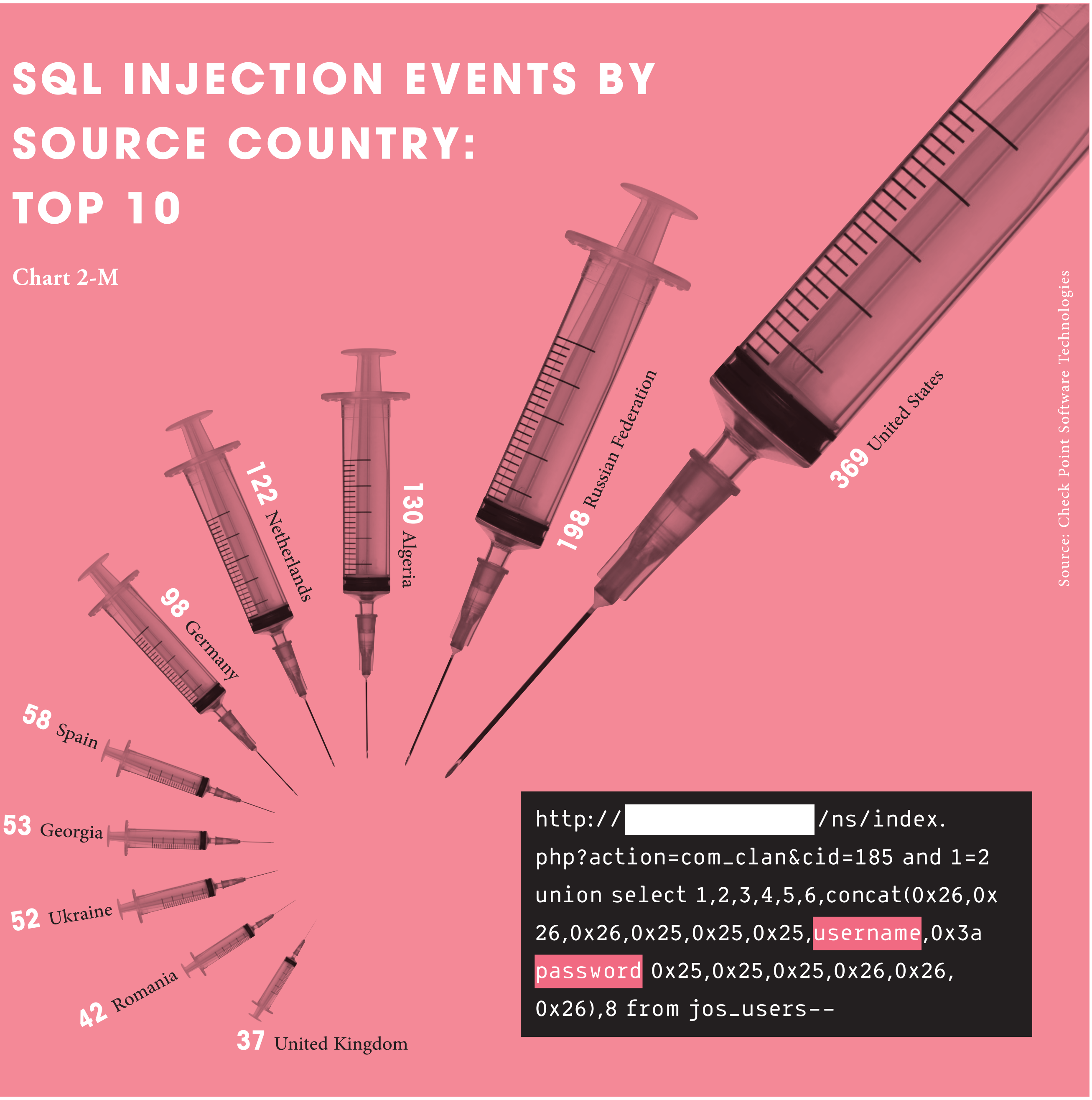


Chart 2-L

SQL INJECTION EVENTS BY SOURCE COUNTRY: TOP 10

Chart 2-M



Source: Check Point Software Technologies

```
http://[redacted]/ns/index.
php?action=com_clan&cid=185 and 1=2
union select 1,2,3,4,5,6,concat(0x26,0x
26,0x26,0x25,0x25,0x25,username,0x3a
password 0x25,0x25,0x25,0x26,0x26,
0x26),8 from jos_users--
```

SECURITY RECOMMENDATIONS MULTIPLE SECURITY LAYERS

As threats become increasingly more sophisticated, security challenges continue to grow. To maximize network security, a multi-tier protection mechanism is needed to secure against different vectors of network threats and breaches. These include:

- Anti-virus to identify and block malware
- Anti-bot to detect and prevent bot damage
- IPS to proactively prevent intrusions
- Web Control- URL Filtering and Application Control to prevent access to websites hosting/spreading malware
- Real-time security intelligence and global collaboration
- Intelligent monitoring that provides proactive data analysis

Stop Incoming Malicious Files

Organizations need an anti-malware solution that can scan files coming into the network and can also decide, in real time, if the files are infected by malware. This solution should prevent malicious files from infecting the

2012, A YEAR OF HACKTIVISM

The global political turbulence that started in 2010 with the uprisings of many Arab countries continued with different civil protests in other countries. Not surprisingly, a wave of cyberattacks based on ideological agendas followed in their wakes. As such, 2012 was marked as a year of hacktivism.

Taiwan-based Apple supplier Foxconn was hacked by the hacker collective Swagg Security. This group apparently protested over media reports of poor working conditions at Foxconn's factories in China[14].

Hacktivist group Anonymous claimed it hacked a U.S. Department of Justice website server for U.S. Bureau of Justice statistics and released 1.7GB of stolen data. The group released the following statement about the stolen data: "We are releasing it to end the corruption that exists, and truly make those who are being oppressed free"[15].

The Vatican also found its websites and internal email servers under a week-long attack by Anonymous. The group claimed that its actions were justified because the Vatican Radio System has powerful transmitters in the Rome countryside, which allegedly constituted a health risk. The group claimed that the transmitters caused "leukemia and cancer" to people living nearby. The group further justified its attack and claimed that the Vatican allegedly helped the Nazis by destroying books of historic value, and that its clergy sexually molested children[16].

In yet another cyberattack, Anonymous brought down the websites of trade groups U.S. Telecom Association and TechAmerica. These attacks were apparently conducted because of these organizations' support for the cyber security bill proposed by Rep. Mike Rogers. The bill would allow private companies and the government to share any information "directly pertaining to a vulnerability of, or threat to" a computer network[17].

internal network. It should also prevent system access to malware-infested websites that attempt to execute drive-by downloads.

Multi-Tier Bot Protection

Protection against bots consists of two phases: detection and blockage.

To maximize the ability to detect a bot in a network, a multi-tier bot discovery mechanism is needed to cover all aspects of bot behavior. A bot detection security solution should include a reputation mechanism that detects the IP, URL and DNS addresses that the remote operators use to connect to botnets. It is also very important that this protection should include the ability to detect the unique communication patterns and protocols for each botnet family. Detecting bot actions is another critical capability of bot protection. The solution should be able to identify bot activities such as sending spam, click fraud, and self-distribution. The second phase after the discovery of infected machines is to block outbound bot communication to the Command & Control servers. This neutralizes the threat and ensures that the bot agents cannot send out sensitive information nor receive any further instructions for malicious activity. In doing so, the bot-related damage is immediately mitigated. This dual-phase approach enables organizations to maintain business continuity as system users can work normally, being confident that bot-specific communications are being blocked in the background to protect their system and data without impacting productivity.

Real-time Global Collaboration

The cyberattack problem is too large and too complex for organizations to self-manage. Organizations have a better chance of overcoming this growing challenge through collaboration and professional assistance. As cybercriminals leverage malware, bots, and other forms of advanced threats, they often target multiple sites and numerous organizations to increase the likelihood of attaining success. When organizations try to address these threats independently, many attacks are left undetected because there is no effective channel for corporations to share threat information. To stay ahead of modern threats, businesses must collaborate and share threat data. Only by joining forces with other organizations can corporations strengthen their own system security.

Intrusion Prevention

Intrusion prevention is a mandatory security layer in the fight against different cyberattack vectors. An IPS solution is required for deep traffic inspection in order to prevent malicious attempts to breach security and gain access to company assets. An adequate IPS solution will provide the following capabilities:

- Protocol Validation and Anomaly Detection to identify and prevent traffic that either does not comply with protocol standards or can create device malfunction/ security issues
- Prevent transmission of unknown payloads that can exploit a specific vulnerability
- Prevent excessive communication that can indicate a Denial of Service (DoS) attack

See the Threat Picture and Take Action

Having a clear understanding of security events and trends is another key component in countering cybercrime. Security administrators must have a constant and clear knowledge of their network security status in order to be aware of threats and attacks targeting their organizations. This knowledge requires a security solution that can provide a high-level overview of the security protection systems while being able to zero in on critical information and potential attacks. The solution should also be able to conduct deep investigations on specific events. The ability to take immediate actions based on this information is another essential feature that enables real-time attack prevention and future threat avoidance. The security solution must be flexible and intuitively easy to manage in order to simplify threat analysis and reduce operational overhead of changes.

Security Updates and Support

In a constantly changing threat environment, defenses must evolve and remain one step ahead of potential threats. Security products can only effectively manage the latest malware, vulnerabilities and exploits if the security vendor is able to conduct comprehensive research and provide frequent security updates.

Excellent security service is defined as:

- Vendor conducts internal research and obtains data from multiple sources
- Frequent security updates to all relevant technologies including IPS, anti-virus and anti-bot
- Easy and convenient support that can answer questions and issues pertaining to the customer's specific system environment.

03 APPLICATIONS IN THE ENTERPRISE WORKSPACE

The Rules of the Game have Changed

The rules of the game have changed. Internet applications were once considered to be a pastime activity; a means to view pictures from our friends' photo albums or to watch entertaining videos. In recent years, Internet Web 2.0 applications have evolved substantially as the likes of Facebook, Twitter, WebEx, LinkedIn, and YouTube are quickly becoming more prevalent in enterprises and are increasingly being recognized as mainstream business facilitation tools. These tools enable companies to better communicate internally between colleagues as well as externally with clients and partners. They also serve as an effective and contemporary medium on which to share and exchange information, views and opinions amongst corporate stakeholders.

This section of our research will discuss the general risks introduced by Web 2.0 applications and their infrastructures followed by a focus on specific applications found in use at the organizations we researched. Our findings will be illustrated with actual reported incidents and examples.

Web Applications are Not Games

As technology evolves, so do security challenges. The evolution of Internet tools introduced new security risks. A number of useful Internet applications are used as attack tools against organizations to cause network security breaches. Applications such as anonymizers, file storage and sharing, peer-to-peer file sharing, remote administrative tools and social media have been used to exploit organizations.

There are myriads of web platforms and applications that could be used for personal or business purposes. Organizations need to be aware of what web applications their employees are using, and for what purposes. Then they should use this information to define their internal Internet policies.

In 91% of the organizations we scanned, web applications

SENSITIVE DATA SHARED BY P2P FILE-SHARING APPLICATIONS IN THE US

In June, 2012, the US Federal Trade Commission (FTC) charged two businesses for exposing sensitive information on peer-to-peer file sharing networks, putting thousands of consumers at risk. The FTC alleged that one of the organizations, EPN, Inc., a debt collection agency based in Provo, Utah, exposed sensitive information, including Social Security numbers, health insurance numbers, and medical diagnosis codes of 3,800 hospital patients, to any computer connected to the P2P network. The FTC also alleged Franklin's Budget Car Sales, Inc. of exposing personal information of 95,000 consumers on the P2P network. The information included names, addresses, Social Security numbers, dates of birth, and driver's license numbers[18].

In 2010, the FTC notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, had been shared from their networks and was available on peer-to-peer (P2P) file-sharing networks. Any person connected to those networks could use the data to commit identity theft or fraud[19].

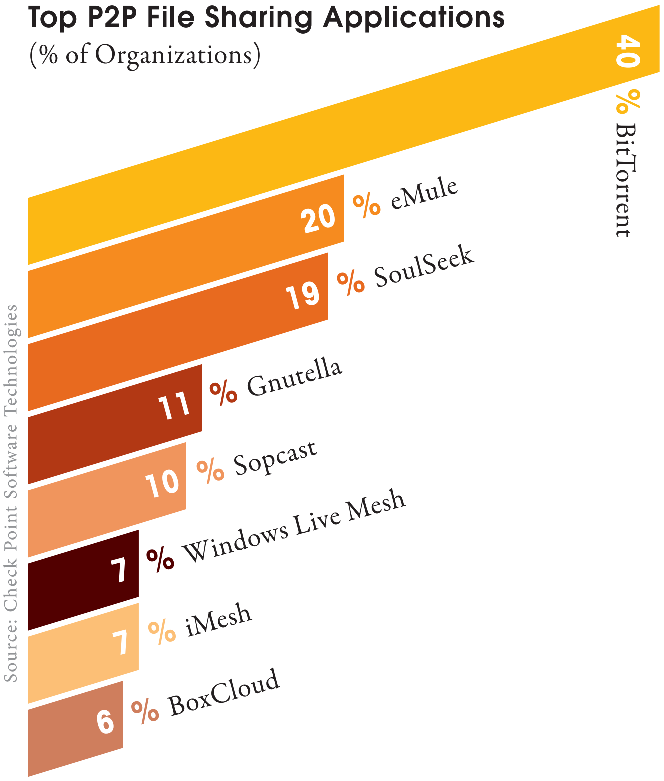
IN 61 % OF ORGANIZATIONS TESTED, A P2P FILE SHARING APPLICATION WAS USED

which could bypass security, conceal identities, cause data leakage or conspicuously introduce malware infections, were used.

P2P Applications Open Back Doors to your Network

Peer-to-peer (P2P) applications are used to share files between users. P2P is increasingly favored by attackers to spread malware among shared files. P2P applications essentially open a back door to networks. They allow users to share folders that could leak sensitive data, they also could make organizations liable for users acquiring media illegally through P2P networks. We recorded a high rate of P2P applications usage in our research as more than half of the organizations tested (61%) used P2P applications. The most prominent P2P file sharing tools used were BitTorrent clients. Chart 3-B below shows that P2P file sharing applications were more popular in Asia Pacific than in other geographical regions.

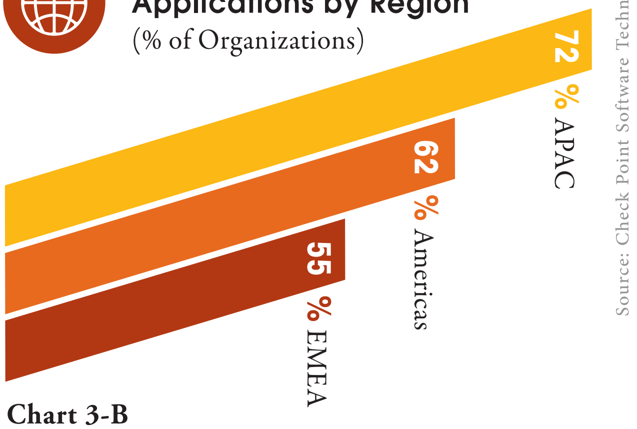
Top P2P File Sharing Applications
(% of Organizations)



Source: Check Point Software Technologies

Chart 3-A

More info on top P2P applications is available in Appendix B.



Usage of P2P File Sharing Applications by Region
(% of Organizations)

Source: Check Point Software Technologies

Chart 3-B

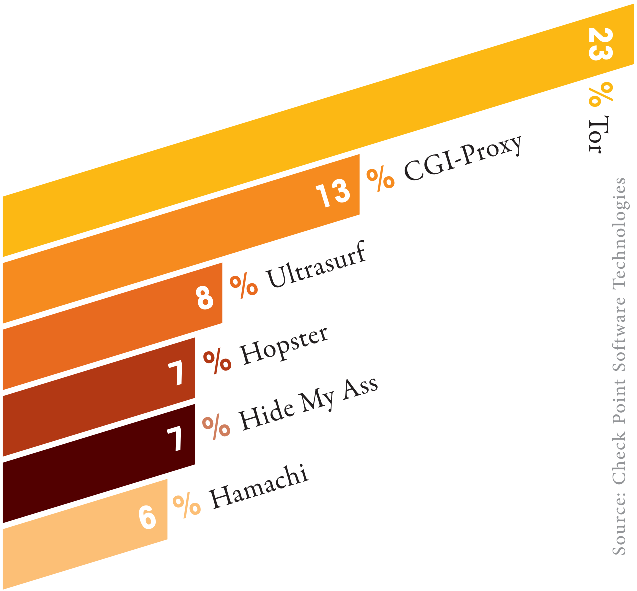
Anonymizer Applications Bypass Organization‘s Security Policy

An anonymizer (i.e. anonymous proxy) is a tool that attempts to make the user's activity on the Internet untraceable. The anonymizer application utilizes a proxy server that acts as a privacy mask between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, hiding personal information by concealing the client computer's identifying information and the destination the user is trying to reach. Anonymizer applications can be used to bypass security policies which are essentially built around users' identities and destination URLs/sites. By using anonymizers, the user appears to be on a different IP address accessing a different destination. The organization's security policies and defenses may not be able to enforce a user using an altered IP address trying to reach an altered IP destination. In some cases, anonymizers may also be used to hide criminal activities.

43% of the organizations in our study had at least one anonymizer application used by an employee, with Tor being the most prominent. 86% of the organizations where anonymizer usage was found claimed that the usage was illegitimate and that it conflicted with corporate guidelines and security policies. Closer analysis of anonymizer application usage by geographical region revealed that this type of application was most popular in the Americas and less so in Asia Pacific.

Most Popular Anonymizer Applications

(% of Organizations)



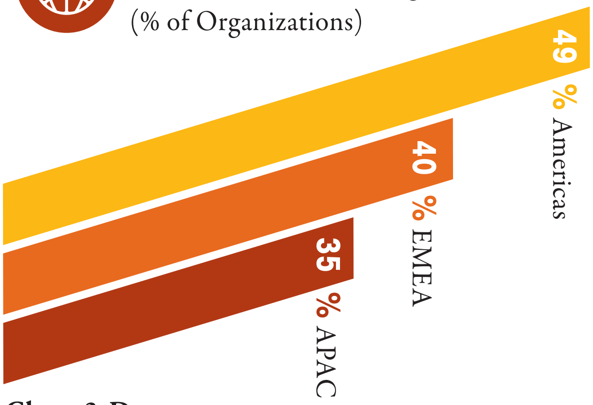
Source: Check Point Software Technologies

Chart 3-C

More info on top anonymizer applications is available in Appendix B.

Usage of Anonymizer Applications by Region

(% of Organizations)

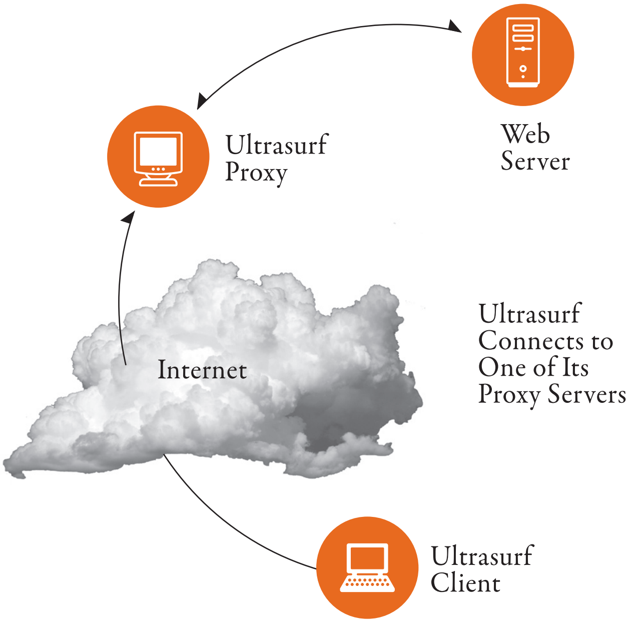


Source: Check Point Software Technologies

Chart 3-D

How does the Ultrasurf Anonymizer Work?

Ultrasurf is a very sophisticated anonymizer that works as a proxy client. It creates an encrypted HTTP tunnel between the user's computer and a central pool of proxy servers, thus enabling its users to bypass firewalls and censorship. Ultrasurf has a very advanced design for discovering proxy servers including a cache file of proxy server IPs and DNS requests. These return encoded IPs of proxy servers, encrypted documents on Google Docs and a hard coded list of proxy server IPs built into the program. Such techniques make it very difficult to detect by security devices.



IN 43% OF EXAMINED ORGANIZATIONS, ANONYMIZERS WERE USED

TOR ANONYMIZER COMPROMISES SECURITY

Recent security research has identified a botnet that is controlled by attackers from an Internet Relay Chat (IRC) server running as a hidden service inside the Tor anonymity network. The connections between users and the Tor nodes are encrypted in a multi-layered fashion, making it extremely difficult for surveillance systems that operate at the local network level or at the ISP level to determine the intended destination of a user[20]. The Tor network's (i.e. Onion Router) main goal is to provide anonymity while browsing the internet. Although it has wide support and enjoys great popularity, when used in a corporate environment it raises several security concerns. Tor can also be easily abused to bypass company security policies since it was specifically designed to provide anonymity for its users. When using Tor to access resources on the Internet, the requests sent from a user's computer are routed randomly through a series of nodes operated voluntarily by other Tor users.

81% OF TEST ORGANIZATIONS USED **REMOTE ADMINISTRATION TOOLS**

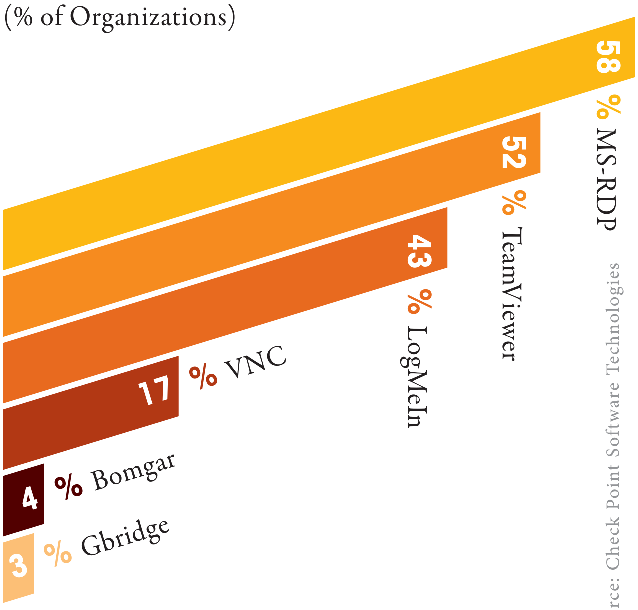
Remote Administration Tools Used for Malicious Attacks

Remote Administration Tools (RAT) could be legitimate tools when used by administrators and helpdesk operators. However, a number of attacks over the past several years leveraged an off-the-shelf RAT to remotely control infected machines in order to further infiltrate networks, log keystrokes, and steal confidential information.

Since RATs are considered to be essential business applications, they should not be categorically blocked. However, their usage should be monitored and controlled to prevent potential misuse.

Our research shows that 81% of the companies we tested had at least one remote administration application, with Microsoft RDP being the most popular.

Top Remote Administration Applications
(% of Organizations)



Source: Check Point Software Technologies

Chart 3-F

More info on top remote administration applications is available in Appendix B.

HACKED BY REMOTE ACCESS TOOLS

An attack campaign named "Nitro" took place between July to September 2011. Attackers used an off-the-shelf Remote Access Tool called Poison Ivy to steal secrets from nearly 50 companies, many of which were in the chemical and defense industry sectors. Poison Ivy was conspicuously embedded on Windows PC machines whose owners were victims of an email scam. The emails touted meeting requests from reputable business partners, or in some cases, updates to anti-virus software or Adobe Flash Player. When users opened the message attachment, they unknowingly installed Poison Ivy onto their machines. From there, the attackers were able to issue instructions to the compromised computers, troll for high-level passwords to gain access to servers hosting confidential information, and eventually offload the stolen content to hacker-controlled systems. 29 of the 48 firms attacked were in the chemical and advanced materials industry, while the remaining 19 represented a variety of business fields, including the defense sector[21]. Nitro was not the only example of RAT misuse. Other examples include RSA breach, ShadyRAT and Operation Aurora. In all these cases, Poison Ivy was utilized to carry out the crime.

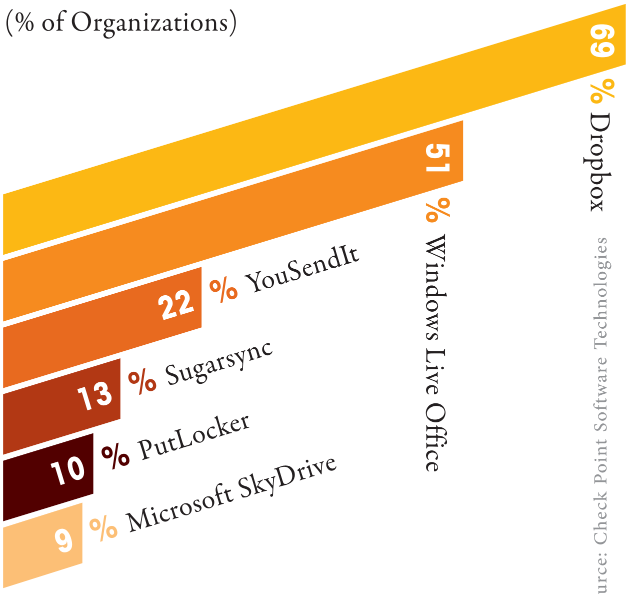
Sharing is Not Always Caring

The term 'Sharing is caring' usually means that if a person shares something with another, it's an expression of care. When sharing files using file storage and sharing appliations in workplace environments, the term may carry a different meaning. One prominent characteristic of Web 2.0 is its ability to generate content and share it, but this also presents a risk. Sensitive information can land in the wrong hands when sharing confidential files. We researched high-risk file storage and sharing applications that may cause data leak or malware infection without user knowledge. Our data shows that 80% of organizations we tested had at least one file storage or file sharing application running on their networks, and that 69% of these organizations used Dropbox. Windows Live Office was second most popular as it was used by 51% of companies.

80% OF THE ORGANIZATIONS SCANNED USED **FILE STORAGE & SHARING APPLICATIONS**

Top File Storage & Sharing Applications

(% of Organizations)



Source: Check Point Software Technologies

Chart 3-G

More info on top File Storage and Sharing Applications is available in Appendix B.

High-Risk Applications Usage by Industry

Check Point analyzed the usage of high-risk applications from an industry point of view. Chart 3-E indicates that Industrial and Governmental organizations were the most extensive users of high-risk applications. As there are legitimate business usage cases for some of these applications (such as the usage of Remote Administration Tools by the help desk), the shaded area in the chart represents the probable level of legitimate use.

PERCENTAGE OF ORGANIZATIONS USING HIGH-RISK APPLICATIONS BY INDUSTRY

(% of Organizations)

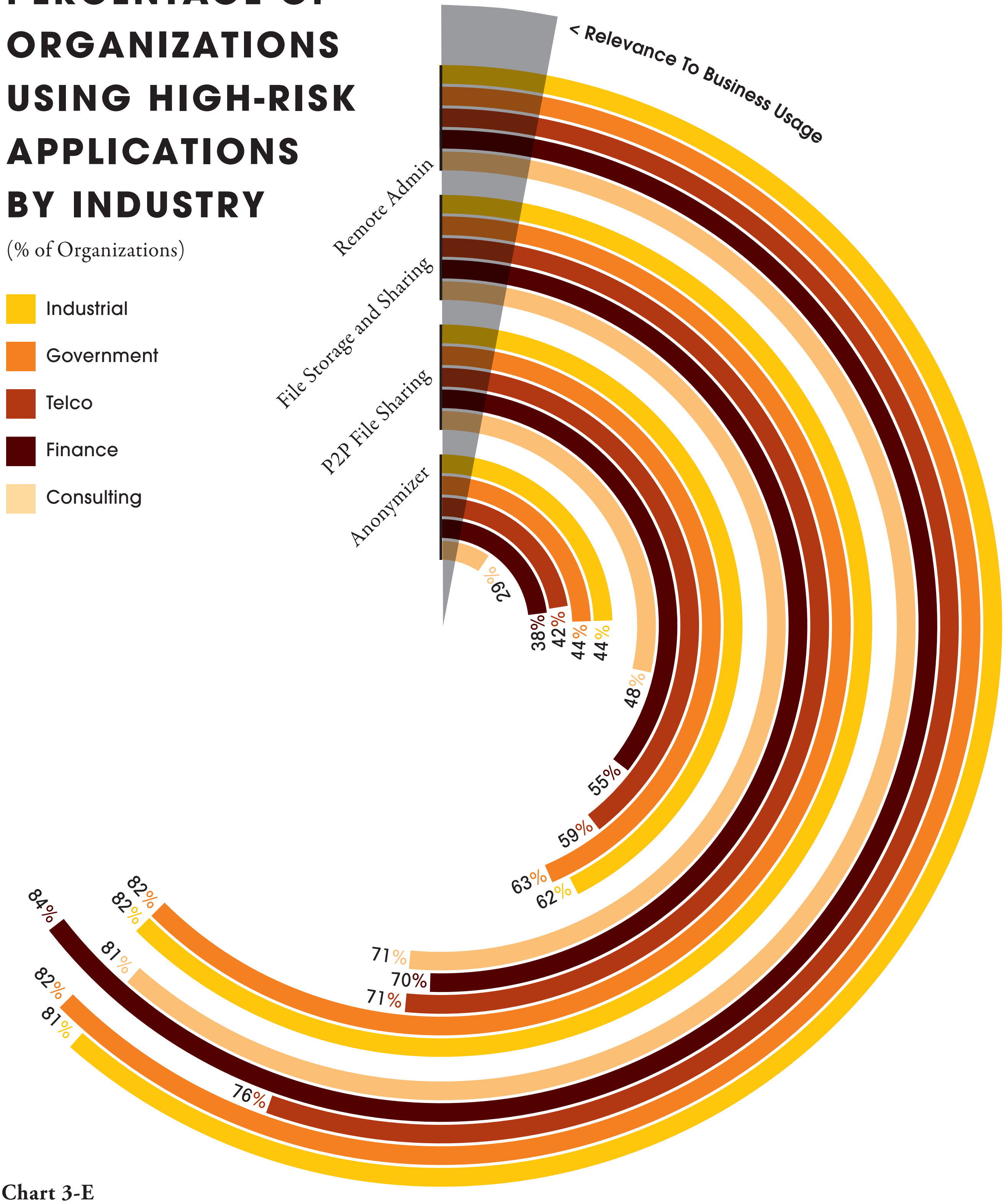


Chart 3-E

Source: Check Point Software Technologies

TWO MAJOR DROPBOX SECURITY INCIDENTS IN TWO YEARS

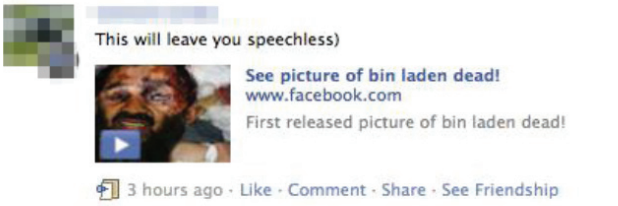
In July 2012, an attack on Dropbox users occurred. Dropbox user names and passwords exposed in breaches from another website were tested on Dropbox accounts. The hackers used a stolen password to log into a Dropbox employee's account that contained a document with users' email addresses. Spammers spammed the contacts on this list[22].

This incident illustrates a frequent tactic used by hackers. Hackers often steal user names and passwords from sites which, at first glance, may not contain any significant financial or personal information. Then, they will test the stolen credentials against websites of financial organizations, brokerage firms and apparently, Dropbox accounts, where potentially more lucrative information may be found.

In 2011, a bug in Dropbox's software update made it possible for anyone to log into any Dropbox account as long as that person had the user's email address. This bug exposed shared documents and other user information. The problem was fixed within several hours, but it served as a warning for both users and for corporations whose employees use file storage and sharing applications such as Dropbox and Google Docs, to store sensitive information appropriately[23].

Legitimate Facebook Post or Virus?

With the constant rise of social networking popularity, new security challenges are constantly introduced to organizations. Inadvertently posting sensitive project information on social networking applications could harm the reputation of an organization, cause loss of competitive advantage or lead to financial loss. Hackers are also leveraging new socially-engineered hacking techniques to drive botnet activity. Embedded videos and links in social networking pages are becoming popular vehicles for concealing malware. In addition to the security risks involved, social networking applications create a severe problem of burdening the corporate network bandwidth, slowing Internet access for network users. Facebook is the most accessed social network. Other social networks visited during work hours (but at a significantly lower rates than Facebook) include Twitter and LinkedIn. Below is an example of a Facebook link leading to a malicious site:



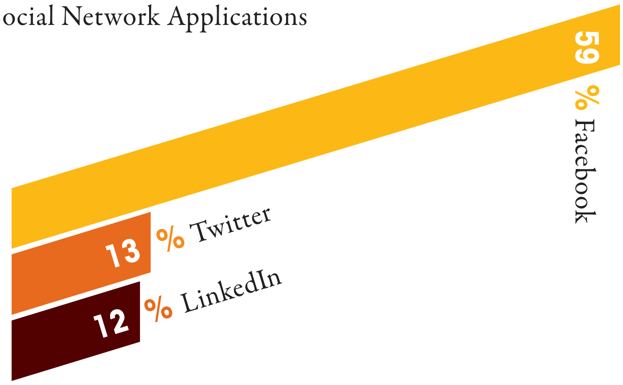
This will leave you speechless)

See picture of bin laden dead!
www.facebook.com
First released picture of bin laden dead!

3 hours ago · Like · Comment · Share · See Friendship

Top Social Network Bandwidth Utilization

Average Utilization Calculated within
Social Network Applications

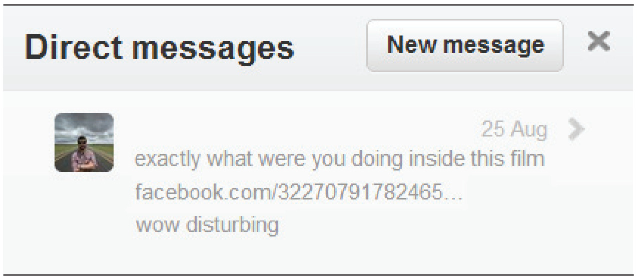


Source: Check Point Software Technologies

Chart 3-H

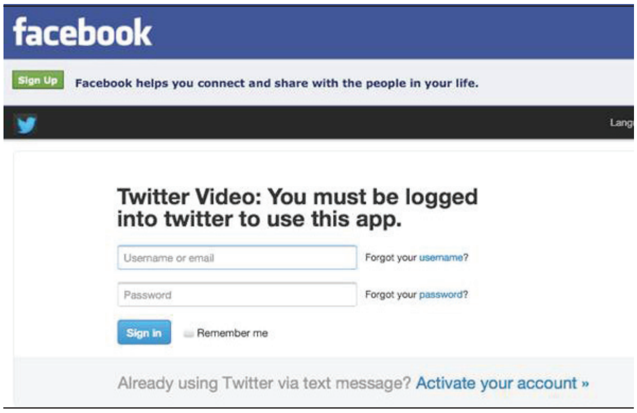
Social Engineering Attacks - Case Study

Recent attacks indicate that hackers are shifting from regular emails to social networks as their preferred malware distribution channel. The following case is based on an actual attack that took place in August 2012. Hackers used Twitter and Facebook social engineering techniques to distribute malicious content. Using a compromised Twitter account, the hacker sent the following message to all of the account's followers. "Exactly what were you doing inside this film [Facebook-URL]... wow disturbing".



25 Aug
exactly what were you doing inside this film facebook.com/32270791782465...
wow disturbing

The URL pointed to a Facebook app which required "Twitter Login". The login screen was actually a web server owned by the hacker that was used to harvest the recipient's Twitter credentials.


facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Lang

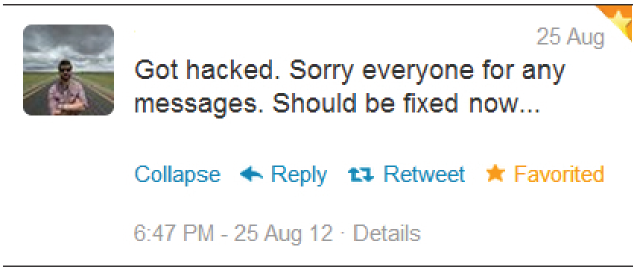
Twitter Video: You must be logged into twitter to use this app.

Username or email — Forgot your username?
Password — Forgot your password?
Sign in — Remember me

Already using Twitter via text message? Activate your account »

The hacker can repeat the process by using the newly hacked Twitter accounts to steal even more passwords. The hacker can also use the stolen credentials to access other services such as Gmail, Facebook, etc. Even worse, stolen personal credentials can be used to log into bank accounts or business-related services such as SalesForce.

After the malicious message was redistributed to the followers of the hacked account, the only effective recourse was to post a polite apology.



25 Aug
Got hacked. Sorry everyone for any messages. Should be fixed now...

6:47 PM - 25 Aug 12 · Details

RECOMMENDATIONS FOR SECURING WEB APPLICATION USAGE IN YOUR NETWORK

Enabling Effective Web 2.0 Protection?

The first step to secure web applications usage in an organization is to use a security solution that provides control and enforcement for all aspects of web usage. Full visibility of all applications running in the environment is needed, along with the ability to control their usage. This level of control has to be maintained over client applications such as Skype, and also over more traditional URL-based aspect of the web such as websites. As many sites enable the operation of numerous applications based on their URLs (e.g. Facebook runs Facebook chat and other gaming applications through the Facebook URL), it is essential to have granularity beyond the URL level. Once this is achieved, organizations should be able to effectively block applications that can endanger their corporate security.

Enabling Social Media for Businesses

There are situations where organizations block Facebook access entirely. But Facebook is considered to be an essential business tool for many businesses as companies often publish information about upcoming webinars, events, new product-related articles, pictures and videos on their corporate Facebook page. Thus a total social media ban would negatively impact business performance. So the question then becomes: How can companies enable social media usage in the workplace without compromising system security? The answer lies in controlling features and widgets within social media apps and blocking out the less business-relevant portions of the program. The combination of these actions makes it possible for corporations to utilize social media with minimal security risks.

Different Users have Different Needs

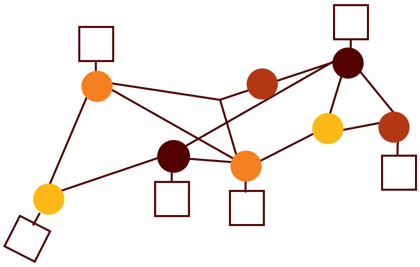
Different users in the organization have different needs, and the security policy should support the business rather than interfere with it. For example, a salesperson may use Facebook to stay in touch with customers and business partners; an IT staff member may log onto Facebook to get the latest industry news. So how do companies ensure that users have the access they need? Is it realistic to expect the security manager to know what each individual user or user group should or shouldn't be accessing?

A practical solution needs to have granular awareness of users, groups and machines in order to distinguish the difference between employees and non-employees (i.e. guests and contractors).

Another important aspect of the solution is the capability to engage and educate the end-users in real time as they use the applications. When a user lands on a questionable site or launches a questionable application, a pop-up message can ask the user to justify the business need for doing so. His or her response would then be logged and monitored. The message can also educate the user on the company's usage policy, making him or her aware that the usage of such applications are constantly monitored and may be subject to future audits.

'Understanding' is a Critical Component of Web Control

Administrators must have a clear overview of web security events in order to ensure web control. As such, a security solution needs to provide clear and broad visibility into all web security events. The solution should provide visibility and monitoring capabilities such as comprehensive event timelines and lists. The list of events should be searchable to allow efficient filtering, grouping and sorting by user, application, category, risk level, bandwidth usage, time and other criteria. As well, off-line reports depicting top used categories, applications, websites and users should also be available to facilitate trend and capacity planning.



SECURING WEB 2.0 TAKES AN INTEGRATED APPROACH OF URL FILTERING, APPLICATION CONTROL, USER AWARENESS, USER EDUCATION AND A WAY OF HAVING ALL WEB CONTROLS VISIBLE TO THE ADMINISTRATOR

Summary

The rules of the game have changed. Securing Web 2.0 is no longer as simple as blocking an inappropriate URL or stopping a certain application from running. Securing Web 2.0 requires an integrated approach to achieve multi-layered protection. This system should incorporate technology (i.e. URL filtering, application control, malware protection and bot defense) with user awareness, user education and sophisticated monitoring and event analysis tools that enable administrators to maintain control at all times.

04 DATA LOSS INCIDENTS IN YOUR NETWORK

Corporate Data: Organizations' Most Valuable Asset

Corporate data is more accessible and transferable today than ever before; the vast majority of which is sensitive at various levels. Some are confidential because it contains internal corporate information which is not intended to be made public. Other confidential data might be sensitive due to corporate requirements, national laws, or international regulations. In many cases, the value of the data is dependent on its level of confidentiality - consider intellectual property and competitive information.

To further complicate the matter, there are numerous tools and practices which can lead to data leakage. Some of these include cloud servers, Google Docs and the simple unintentional abuse of company procedures such as an employee bringing work home.

Data Leakage Can Happen to Anybody

Data leakage is not always caused by cybercriminals. It can happen unintentionally by the actions of well-intentioned employees. A classified document maybe mistakenly sent to the wrong person, a sensitive document might be shared on a public site or a work file may be sent to an unauthorized home email account. These scenarios may inadvertently happen to anybody, with devastating results. Loss of sensitive data can lead to brand damage, compliance violations, lost revenue or even hefty fines.

Our Research

When an organization determines to define which data should not be sent externally, a number of variables must be considered: What type of data is it? Who owns it? Who is sending it? Who is the intended recipient? When is it being sent? What are the associated business disruption repercussions caused by a hyper-restrictive security policy?

54%

OF THE ORGANIZATIONS IN OUR RESEARCH HAD AT LEAST ONE POTENTIAL DATA LOSS INCIDENT

OOPS... I SENT THE EMAIL TO THE WRONG ADDRESS

Here are some examples of unintentional data loss incidents caused by employees in 2012.

In October 2012, **Stoke-on-Trent City Council** in the UK was fined £120,000 after a member of its legal department sent emails containing sensitive information to the wrong address. 11 emails intended for a lawyer working on a case were sent to another email address due to a typing mistake.

Japan's newspaper **Yomiuri Shimbun** fired one of its reporters in October 2012 for accidentally sending sensitive investigative information to the wrong recipients. The reporter meant to send some of his research findings to his colleagues via email, but instead, he sent the messages to several media outlets, disclosing the identities of his sources[24].

In April 2012, **Virginia Military Institute** in Lexington inadvertently sent out students' grade point averages via an email attachment. The original intention was to email a single spreadsheet that contained names and residences so that students can confirm their mailing addresses[25]. Instead, the school sent an email to the graduating class president containing that spreadsheet along with another confidential spreadsheet which listed the grade point averages of every senior student. Unaware of the second spreadsheet, the president forwarded the message to 258 students.

Texas A&M University accidentally sent an email with an attachment containing 4,000 former students' Social Security numbers, names and addresses to an individual who subsequently notified the university of the mistake. The incident took place in April 2012[26].

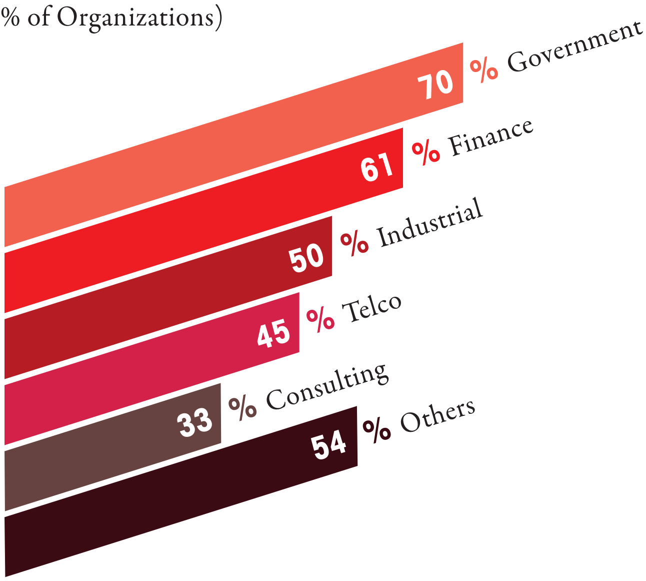
Our research analyzed traffic sent externally from organizations. We examined both HTTP and SMTP traffic. In other words, when emails were sent to an external recipient, a Check Point device inspected the email body, email recipients and attachments including zipped files. We also inspected web browsing activities such as web posts and web mails. As a security policy for these devices, we configured out-of-the-box pre-defined data types to detect sensitive data, forms and templates (e.g. credit card numbers, source code, financial data and others) that may indicate a potential data leak to illegitimate recipients. A detailed list of researched data types can be found in Appendix D.

Potential Data Loss in Your Organization

Our findings reveal that 54% of organizations in our research had at least one event which may indicate a potential data loss occurrence over a 6-day average period. We considered events that included internal information

Percentage of Organizations with at least One Potential Data Loss Event by Industry

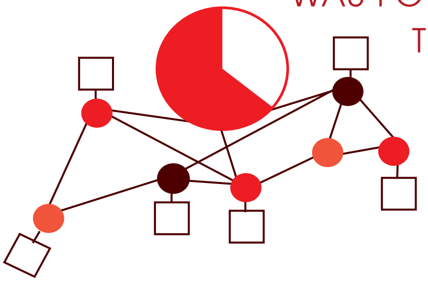
(% of Organizations)



Source: Check Point Software Technologies

Chart 4-A

IN 28% OF TEST ORGANIZATIONS AN INTERNAL EMAIL WAS FOUND TO BE SENT TO AN EXTERNAL RECIPIENT



(see list of data types in Appendix D) which were sent to external destinations either by email or other online posting means.

Our findings, as depicted on Chart 4-A, indicate that Government and Financial organizations were at the highest risk of potential data loss.

Internal Emails Sent Outside of the Organization

In many cases, data loss events occur unintentionally through employees sending email communications to the wrong recipients. Our research looked at two types of emails that may indicate such incidents. The first type consisted of emails that were sent with internal visible recipients (i.e. To and CC) and external recipients in the BCC field. Such emails, in most cases, seemed to be internal but actually left the company. The second type consisted of emails sent to several internal recipients and a single external party. Such emails were usually sent unintentionally to a wrong external recipient. One or both of these types of events were found in 28% of organizations examined.

What Types of Data Do Employees Send to External Recipients or Post Online?

Chart 4-C shows the top data types sent to parties outside of the organization. Credit card information led the list, while source code and password protected files registered second and third respectively.

Is your Organization PCI Compliant?

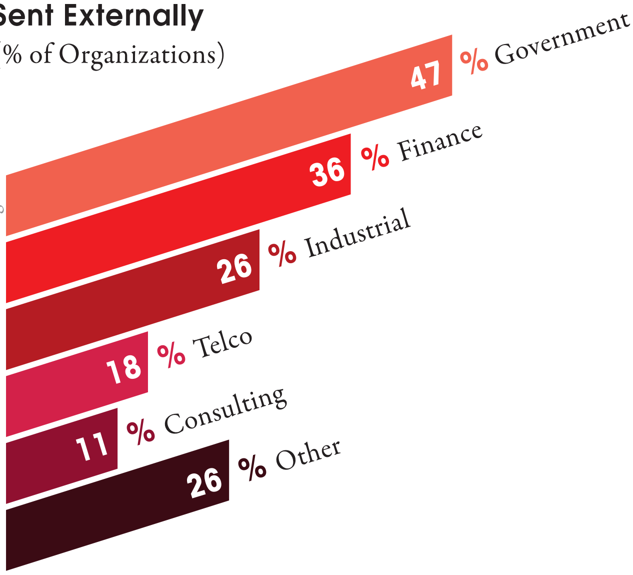
Staff members routinely send credit card numbers over the Internet - their own and their customers'. Employees send customer payment receipts that contain credit card information in email attachments. They reply to customer emails that contain credit card information in the original email body text. At times, employees even send spreadsheets with customer data to private email accounts or to email addresses of business partners. Often, credit card number-related incidents resulted due to broken business processes or employees' lack of attention and awareness. Such incidents may indicate that the corporate security policy does not meet the objective of promoting secure and careful use of corporate property.

Moreover, sending credit card numbers over the Internet is not compliant with PCI DSS requirement 4, which mandates that cardholder data must be encrypted during transmission across open public networks. Failing to comply with PCI DSS can result in a damaged corporate reputation, lawsuits, insurance claims, cancelled accounts, payment card issues, and government fines.

Our research inspected outgoing traffic from organizations and scanned the content of all message parts, including attachments and archives. We also searched for emails containing credit card numbers or cardholder data. The inspections were based on regular expressions, validation of check digits, and PCI DSS compliance regulations.

Percentage of Organizations by Industry in which Credit Card Information was Sent Externally

(% of Organizations)



Source: Check Point Software Technologies

Chart 4-B

IN 36% OF FINANCIAL ORGANIZATIONS WE SCANNED, CREDIT CARD INFORMATION WAS SENT OUTSIDE OF THE ORGANIZATION

DATA SENT OUTSIDE THE ORGANIZATION BY EMPLOYEES

(% of Organizations)

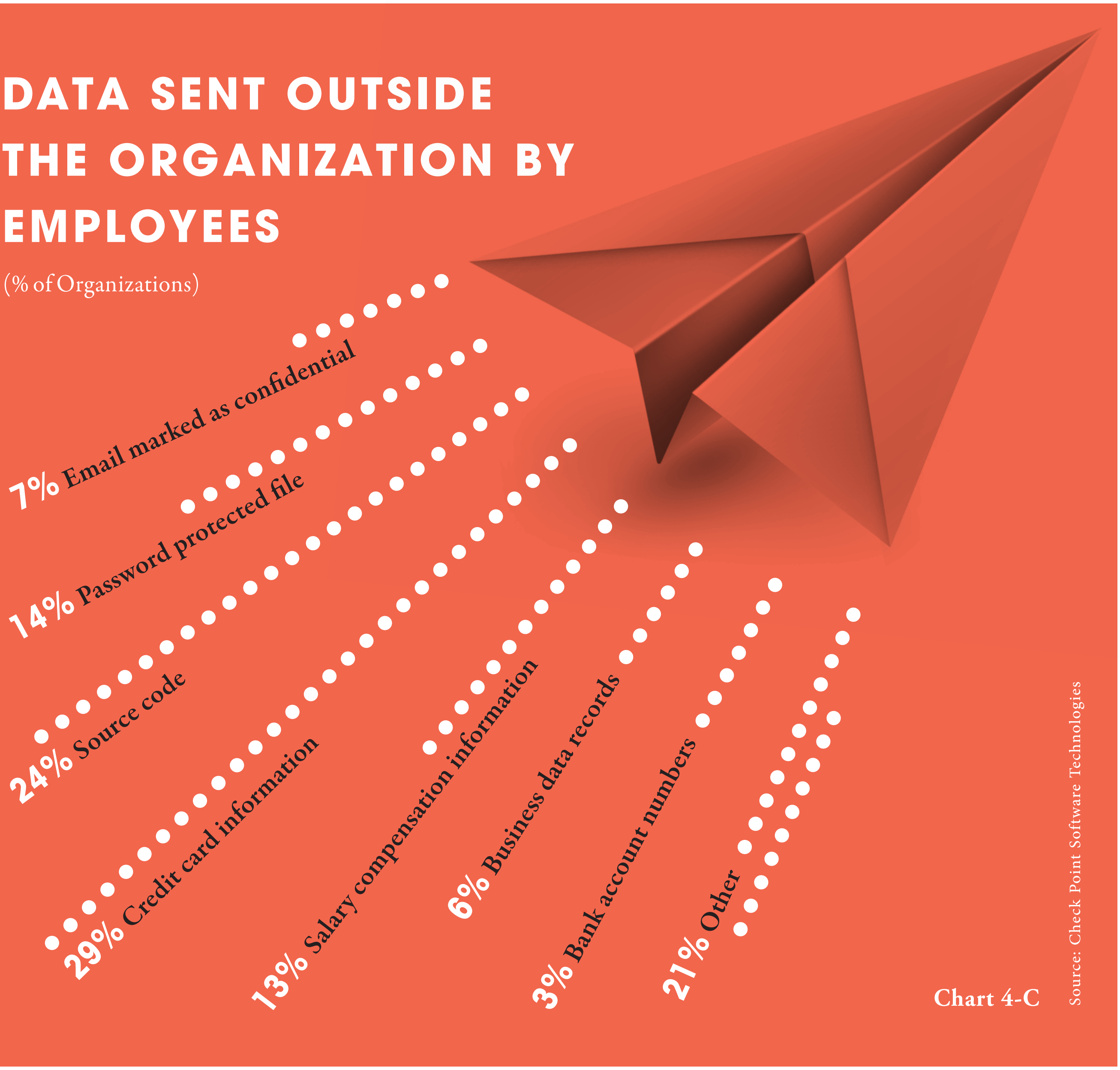


Chart 4-C

Source: Check Point Software Technologies

Our research shows that in 29% of examined organizations, at least one event was found during the analysis period which indicated that PCI-related information was sent outside of the organization. Our findings also indicate that within 36% of tested financial organizations, which are usually obligated to be compliant with PCI regulations, at least one PCI-related event had occurred.

HIPAA

The HIPAA Privacy Rule provides federal protection for personal health information and grants patients with an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for proper patient care and other important purposes.[27]

The HIPAA Privacy Rule permits healthcare providers to use email to discuss health issues with their patients, provided that reasonable safeguards are applied. Encryption is not mandated. However, other safeguards should be applied to reasonably protect privacy. How do healthcare providers keep email communication channels open with patients while safeguarding privacy and maintaining HIPPA compliance?

In our research, we monitored the outgoing traffic from organizations while scanning all parts of messages and attachments, searching for emails containing patient private information by keying on personal information identifiers (e.g. Social Security numbers) and related medical terms (e.g. CPT, ICD-9, LOINC, DME, NDC terms, etc.).

We found that in 16% of healthcare and insurance organizations, HIPAA - Protected Health Information was either sent outside of the organization to an external email recipient or was posted online.

SECURITY RECOMMENDATIONS

In today's world of increasing data losses, organizations must take action to protect sensitive data. The best solution to prevent unintentional data loss is to implement an automated corporate policy that catches such incidents before the data leaves the organization. Such solutions are known as Data Loss Prevention (DLP). Content-aware DLP products have a broad set of capabilities and present organizations with multiple deployment options. Before deploying the DLP solution, organizations need to develop a clear DLP strategy with concrete requirements such as: What is considered to be confidential information? Who can send it? and so forth.

Data Classification Engine

High accuracy in identifying sensitive data is a critical component of a DLP solution. The DLP solution must be

IN 16%

OF HEALTHCARE AND INSURANCE ORGANIZATIONS WE EXAMINED, HIPAA - PROTECTED HEALTH INFORMATION WAS SENT OUTSIDE OF THE ORGANIZATION able to detect personally identifiable information (PII), compliance-related data (e.g. HIPAA, SOX, PCI data, etc.), and confidential business data. It should inspect content flows and enforce policies in the most widely used TCP protocols, including SMTP, FTP, HTTP, HTTPS and webmail. The DLP solution should also be able to conduct inspections by pattern matching and file classification, so that it can identify content types regardless of the file extension or compression format.

In addition, the DLP solution must be able to recognize and protect sensitive forms, based on predefined templates and file/form matching. An important feature of a DLP solution is the ability to create custom data types for maximum flexibility, along with the vendor's out-of-the-box data types.

Empower Users to Remediate Incidents

Traditional DLP solutions can detect, classify and even recognize specific documents and various file types, but they cannot capture the user's intent behind the sharing of sensitive information. Technology alone is inadequate because it cannot identify this intention and respond to it accordingly. Hence, a quality DLP solution must engage users in order to achieve optimal results. One approach is to empower users to remediate incidents in real-time. In other words, the DLP solution should inform the user that his/her action may result in a potential data leak incident. It should then empower the user to decide whether to discard the message or to continue with sending it. This methodology improves security by elevating data storage policy awareness and alerting users of potential mistakes in real time. As well, it allows for quick self-authorization of legitimate communications. As a result, security management is simplified because the administrator can track DLP events for analysis without having to personally attend to each external data send request as it happens.

Protection Against Internal Data Breaches

Another important DLP capability is the ability to not only to control sensitive data from leaving the company, but also to inspect and control sensitive emails sent between departments within the same company. Policies can be defined to prevent confidential data from leaking to wrong departments. Examples of data that might need protecting from accidental interdepartmental leakage include: compensation plans, confidential human resource documents, mergers and acquisitions documents or medical forms.

Data Protection for Endpoint Hard Drives

Companies must secure laptop data as part of a comprehensive security policy. Without securing hard drive data, outsiders can obtain valuable information through lost or stolen computers; this can result in legal and financial repercussions. A proper solution should prevent unauthorized users from accessing information by encrypting the data on all endpoint hard drives, including user data, operating system files and temporary and erased files.

Data Protection for Removable Media

To stop incidences of corporate data compromises via USB storage devices and other removable media, encryption and prevention of unauthorized access for these devices are required. Employees often mix personal files such as music, pictures, and documents with business files such as finance or human resource files on their portable media. This makes corporate data even more challenging to control. By encrypting removable storage the devices, security breaches can be minimized in case the devices become lost or stolen.

Document Protection

Business documents are routinely uploaded to the web by file-storage applications, sent to personal smartphones, copied to removable media devices and/or shared externally with business partners. Each of these actions places sensitive data at risk of being lost or used inappropriately. In order to secure corporate documents, a security solution must be able to enforce a document encryption policy and grant access exclusively to authorized individuals.

Event Management

Defining DLP rules to meet the organization's data usage policies should accompany quality monitoring and reporting capabilities. To minimize the potential of data leakage in an organization, the security solution must include monitoring and analysis of real-time and historical DLP events. This gives the security administrator a clear and broad view of the information being sent externally, their sources, and it also provides the organization with the ability to respond in real time if necessary.

05 SUMMARY AND SECURITY STRATEGY

WE WILL CONCLUDE THE REPORT WITH ANOTHER SUN ZI QUOTE TAKEN FROM THE ART OF WAR: HERE IS AN ADVICE FOR A MILITARY GENERAL:

"HAVING COLLECTED AN ARMY AND CONCENTRATED HIS FORCES, HE MUST BLEND AND HARMONIZE THE DIFFERENT ELEMENTS THEREOF BEFORE PITCHING HIS CAMP."[28]

2,600 years later, the same approach perfectly describes today's fight against cyberwarfare as the best network security is realized when all the different layers of protection are harmonized to fight against all different angles of security threats.

This report covered multiple aspects of security risks that Check Point detected in a wide range of organizations. It showed that bots, viruses, breaches, and attacks posed a constant and real threat to corporate security. It indicated that some web applications used by employees can compromise network security. Finally, it revealed that employees routinely engaged in many practices that may cause unintentional leakage of sensitive data.

In your Security Strategy: Technology Alone is Not Enough

The Check Point approach to corporate security acknowledges that technology alone is not enough. Our view is that security needs to evolve from a collection of disparate technologies and practices to form an cohesive and effective business process. Check Point recommends organizations to consider three key dimensions when deploying a security solution strategy: Policies, People, and Enforcement.

Policies

Security starts with a widely understood and well-defined policy which is closely aligned to business needs rather than a collection of system-level checks and dissimilar technologies. Policies should place business as the top priority and suggest ways for business to be carried out in a secured manner. This aspect should be incorporated into the corporate policy.

For example, during our analysis we found that employees used web applications that were necessary for business flow, but these applications may also compromise security. If technologies that blocked the usage of such web applications were deployed, it would have resulted in employees flooding the security administrator with complaints. Or worse, employees may have found ways to bypass the technology themselves and in doing so, created new, and potentially more harmful security concerns. Instead, Check Point recommends a policy that acknowledges situations where the use of such applications may be necessary, and thus the procedure needs to be further defined in order to enable usage in a secure manner. Users should be automatically advised of the policy when necessary.

People

Computer system users are a critical part of the security management process as they often make mistakes that result in malware infections and information leakage.

Organizations should ensure that users are involved in the security process. Employees need to be informed and educated on the company's expectations of them when they browse the Internet or share sensitive data. At the same time, security should be seamless and transparent and should not change the way users perform their work. Implementation of a security program should include:

- Education programs: to ensure that all users are aware that corporate systems are potentially vulnerable to attacks and that their own actions may allow or help prevent these assaults.
- Technology: to advise people in real time as to why certain operations are risky and how these can be conducted in a secure manner.

Enforcement

Deployment of security technology solutions such as security gateways and endpoint software is critical for protecting organizations from security breaches and loss of data. Security gateways should be installed at all interconnects, ensuring that only relevant and authorized traffic enters and leaves the network. This validation should take place at all layers of security and on all communications, protocols, methods, queries, responses and payloads using firewall, application control, URL filtering, DLP, IPS, anti-virus and anti-bot security solutions.

06 ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies Ltd. (www.checkpoint.com) is the worldwide leader in securing the Internet. Check Point provides its customers with uncompromised protection against all types of threats. Its product offerings reduce security complexity and lower total cost of ownership. Check Point first pioneered the security industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to develop innovative products based on the Software Blade Architecture™, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement best practices to achieve a greater level of information asset protection. This unique approach enables organizations to implement an effective security policy blueprint that aligns with actual business needs. Check Point serves customers of all sizes, industries and geographies. Its client portfolio includes all Fortune and Global 100 companies. As well, Check Point's award-winning ZoneAlarm® security solutions protect millions of individuals and small businesses from hackers, spyware and identity theft.

Check Point 3D Security

Check Point 3D Security redefines security as a 3-dimensional business process that combines policies, people and enforcement for a stronger protection across all layers of security including network, data and endpoints. To achieve the level of protection needed in the 21st century, security needs to grow from a collection of disparate technologies to an integrated business process. With 3D Security, organizations can now implement a blueprint for security that goes beyond technology to ensure information security integrity.

Check Point 3D Security enables organizations to redefine security by integrating these dimensions into an effective business process:

Policies that support business needs and transform security into a business process

Security that involves **People** in policy definition, education and incident remediation

Enforce, consolidate and control all layers of security (i.e. network, data, application, content and user)

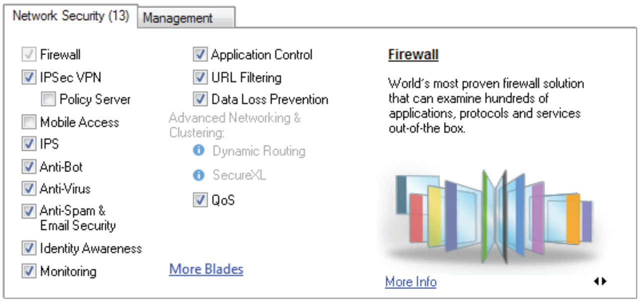
Check Point Software Blade Architecture™

As a key tool in creating true 3D Security, the Check Point Software Blade Architecture™ allows companies to enforce security policies while helping to educate users on those policies. This is the first and only security architecture that delivers total, flexible and manageable security to companies of any size. More importantly, as new threats and needs emerge, Check Point Software Blade Architecture™ quickly and flexibly extends security services on-demand and without the addition of new hardware or management complications. Solutions are centrally managed through a single console that reduces complexity and operational overhead. Multilayered protection is critical to combat dynamic threats such as bots, trojans and Advanced Persistent Threats (APTs). Current firewalls behave like multi-function gateways, but not all companies want the same level of security throughout their entire system. Companies seek flexibility and control of their security resources.

Software Blades are security applications or modules such as: firewalls, Virtual Private Networks (VPN), Intrusion Prevention Systems (IPS), or application controls, that are independent, modular and centrally managed. They allow organizations to customize a security configuration that targets the right mix of protection and investment. Software Blades can be quickly enabled and configured on any gateway or management system with no additional hardware, firmware or driver upgrades. As needs evolve, additional Software Blades can be easily activated to extend the security parameters of an existing configuration running on the same security hardware.

Check Point offers centralized event management features for all Check Point products and third-party devices. This provides real-time views of security events as they take place, enables quick analysis of the security situation, and allows for immediate mitigating actions, all conducted via a single console. The 'timeline view' enables the visualization of trends and propagation of attacks. The 'charts view' provides event statistics in either a pie chart or a bar graph format. The 'maps view' shows potential threats by country.

Check Point Security Gateway SmartDashboard. Software Blades Activation Screen



Network Security (13) | Management

- ☑ Firewall
- ☑ IPSec VPN
  - □ Policy Server
- □ Mobile Access
- ☑ IPS
- ☑ Anti-Bot
- ☑ Anti-Virus
- ☑ Anti-Spam & Email Security
- ☑ Identity Awareness
- ☑ Monitoring

- ☑ Application Control
- ☑ URL Filtering
- ☑ Data Loss Prevention
- Advanced Networking & Clustering:
  - Dynamic Routing
  - SecureXL
- ☑ QoS

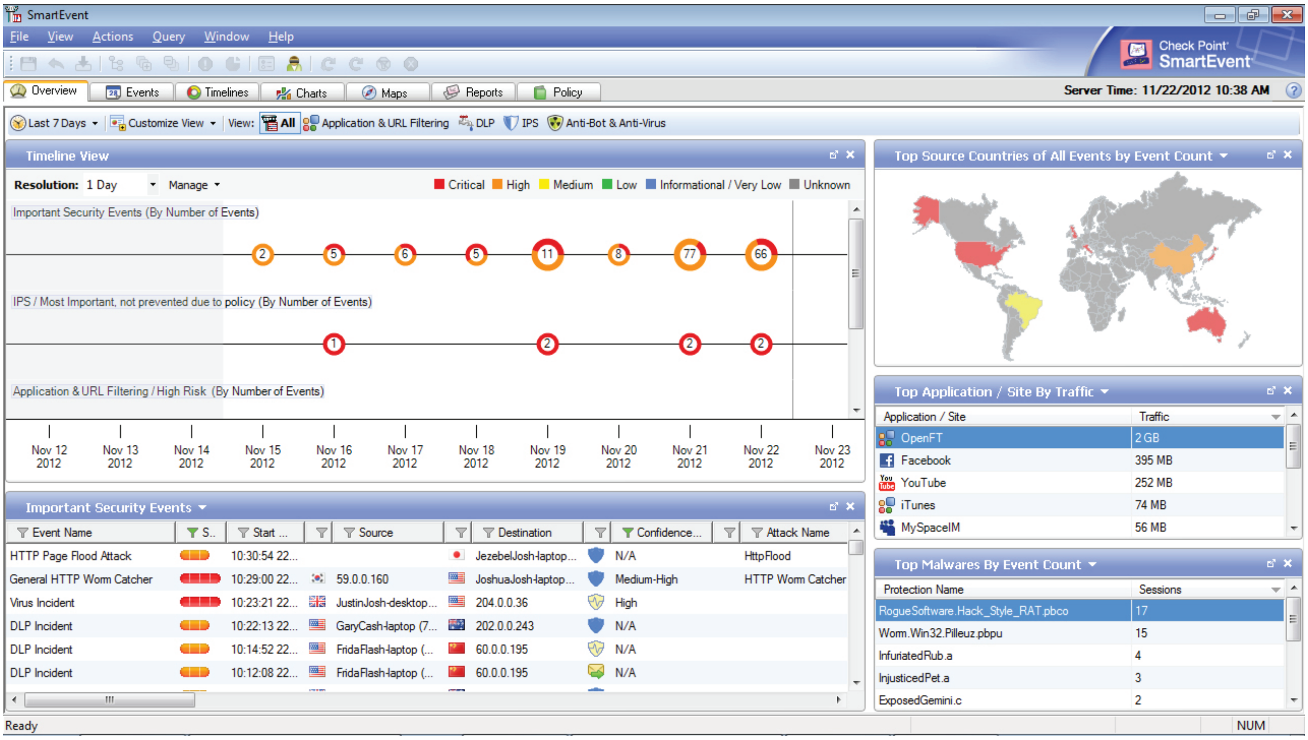
More Blades

Firewall

World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.

More Info

Check Point SmartEvent Security Events Management. Real-time Overview



SmartEvent
File View Actions Query Window Help
Check Point SmartEvent
Overview Events Timelines Charts Maps Reports Policy
Last 7 Days Customize View View: All Application & URL Filtering DLP IPS Anti-Bot & Anti-Virus
Timeline View
Manage
Critical High Medium Low Informational / Very Low Unknown
Important Security Events (By Number of Events)
2 5 6 5 11 8 77 66
IPS / Most Important, not prevented due to policy (By Number of Events)
1 2 2 2
Application & URL Filtering / High Risk (By Number of Events)
Nov 12 2012
Nov 13 2012
Nov 14 2012
Nov 15 2012
Nov 16 2012
Nov 17 2012
Nov 18 2012
Nov 19 2012
Nov 20 2012
Nov 21 2012
Nov 22 2012
Nov 23 2012
Top Source Countries of All Events by Event Count
Ready
NUM

Server Time: 11/22/2012 10:38 AM

Resolution: 1 Day

Important Security Events

Event Name	S..	Start ...	Source	Destination	Confidence...	Attack Name
HTTP Page Flood Attack		10:30:54 22...		JezebelJosh-laptop...	N/A	HttpFlood
General HTTP Worm Catcher		10:29:00 22...	59.0.0.160	JoshuaJosh-laptop...	Medium-High	HTTP Worm Catcher
Virus Incident		10:23:21 22...	JustinJosh-desktop...	204.0.0.36	High	
DLP Incident		10:22:13 22...	GaryCash-laptop (7...	202.0.0.243	N/A	
DLP Incident		10:14:52 22...	FridaFlash-laptop (...	60.0.0.195	N/A	
DLP Incident		10:12:08 22...	FridaFlash-laptop (...	60.0.0.195	N/A	

Top Application / Site By Traffic

Application / Site	Traffic
OpenFT	2 GB
Facebook	395 MB
YouTube	252 MB
iTunes	74 MB
MySpaceIM	56 MB

Top Malwares By Event Count

Protection Name	Sessions
RogueSoftware.Hack_Style_RAT.pbco	17
Worm.Win32.Pilleuz.pbpu	15
InfuriatedRub.a	4
InjusticedPet.a	3
ExposedGemini.c	2

ThreatCloud™ Real-time Security Intelligence Feeds

ThreatCloud™ is a collaborative network and cloud-driven knowledgebase that delivers real-time dynamic security intelligence to security gateways. That intelligence is used to identify emerging outbreaks and threat trends. ThreatCloud™ powers the Anti-Bot Software Blade which allows gateways to investigate dynamic IPs, URLs and DNS addresses where Command & Control centers are known to exist. Since processing is done in the cloud, millions of signatures and malware protection can be scanned in real time.

ThreatCloud™'s knowledgebase is dynamically updated using feeds from a network of global threat sensors, attack information from worldwide gateways, Check Point research labs and the industry's best malware feeds. Correlated security threat information is then shared among all gateways collectively.

THREATCLOUD

Check Point Security Appliances

In today's enterprise networks, security gateways are more than a firewall as they face an ever-increasing number of sophisticated threats. Today's security gateways must use multiple technologies to control network access, detect sophisticated attacks and provide additional security capabilities such as data loss prevention, protection from web-based threats and securing mobile devices such as the iPhones and tablets in enterprise networks. These increased threats and security capabilities demand greater performance and versatility from security appliances.

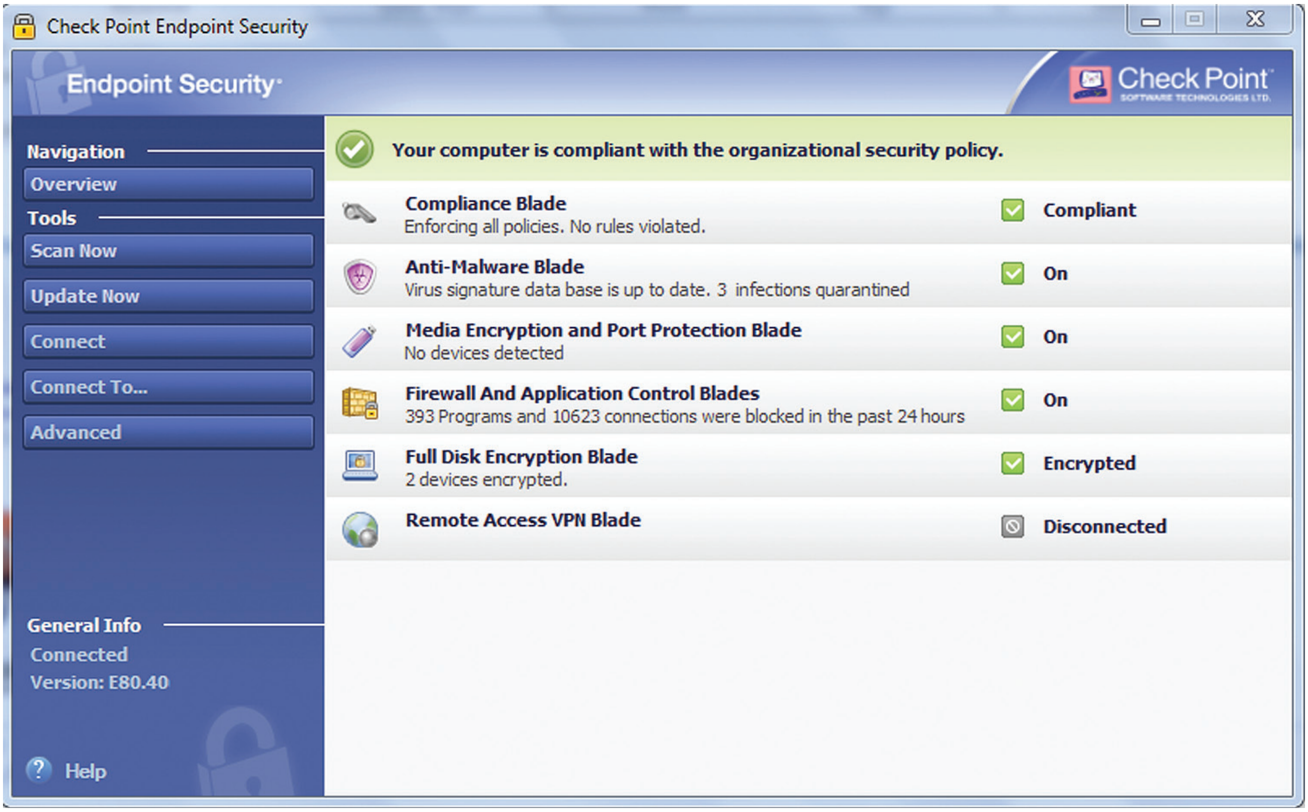
Empowered by Check Point GAiA, a next-generation security operating system, Check Point appliances combine high performance multi-core capabilities with fast networking technologies to provide the highest level of data, network and employee security. Optimized for the extensible Check Point Software Blades Architecture™, each appliance is capable of running any combination of Software Blades including: Firewall, IPsec VPN, IPS, Application Control, Mobile Access, DLP, URL Filtering, Anti-Bot, Antivirus, Anti-spam, Identity Awareness and Advanced Networking & Clustering. This provides the necessary flexibility and the precise level of security for any business at every network location. By consolidating multiple security technologies into a single security gateway, the appliances are designed to deliver advanced and integrated security solutions to meet an organization's full business security requirements. Introduced in August 2011, SecurityPower™ is a metric that measures the capacity of an appliance to perform multiple advanced functions in a specified traffic volume. This revolutionary benchmarking tool enables companies to select the appropriate security appliances for their specific deployment scenarios. The SecurityPower™ ratings are determined based on real-world customer traffic, multiple security functions and a typical security policy.

Check Point 61000 Appliance

Check Point Endpoint Security

Check Point Endpoint Security Software Blades bring unprecedented flexibility, control and efficiency to the management and deployment of endpoint security. IT managers can choose from six Endpoint Software Blades and deploy only what's necessary to fulfill their existing protection requirements. As needs evolve, the option to increase security at any time is always available. **Full Disk Encryption Software Blade** automatically and transparently secures all information on endpoint hard drives. Multi-factor pre-boot authentication ensures user identity. **Media Encryption Software Blade** provides centrally enforceable encryption of removable storage media, with the granularity to encrypt only business-related data while engaging and educating the end user. **Remote Access VPN Software Blade** provides users with secure, seamless access to corporate networks and resources when working remotely. **Anti-Malware and Program Control Software Blade** efficiently detects and removes malware from endpoints with a single scan. Program Control assures that only legitimate and approved programs run on endpoints. **Firewall and Security Compliance Verification Software Blade** proactively protects inbound and outbound traffic by preventing malware from infecting endpoint systems, blocking target attacks and stopping unwanted traffic. The Security Compliance Verification assures that corporate endpoints will always meet the organization's security policy requirements. **WebCheck Secure Browsing Software Blade** protects against the latest web-based threats including drive-by downloads, phishing sites and zero-day attacks. It also enables browser sessions to run in a secure virtual environment.

Check Point Endpoint Security Client



Your computer is compliant with the organizational security policy.

Compliance Blade Enforcing all policies. No rules violated.	✓	Compliant
Anti-Malware Blade Virus signature data base is up to date. 3 infections quarantined	✓	On
Media Encryption and Port Protection Blade No devices detected	✓	On
Firewall And Application Control Blades 393 Programs and 10623 connections were blocked in the past 24 hours	✓	On
Full Disk Encryption Blade 2 devices encrypted.	✓	Encrypted
Remote Access VPN Blade	⊘	Disconnected

A APPENDIX A: TOP MALWARE

This appendix provides further information related to the top malware found in our research. Check Point's full malware database is available at threatwiki.checkpoint.com

Zeus is a back door bot agent that targets Microsoft Windows platforms. A back door is a method of bypassing authentication procedures. Once a system has been compromised, one or more back doors may be installed in order to allow easier access in the future[29]. Our research detected Zeus bots generated from Zeus toolkit version 2.0.8.9. Zeus is a large family of banking Trojans with considerable numbers of versions and variants. The malware provides the attacker with remote access of the infected systems. Its primary purpose is to steal online banking credentials used by target users when accessing their accounts.

Zwangi is an adware that targets Microsoft Windows platforms. It is registered as a browser helper object on an infected system. It may create a custom tool bar within Internet Explorer and present the user with unwanted advertising messages. This malware infects systems through software bundles.

Sality is a virus that spreads itself through infecting and modifying executable files and copying itself to removable drives or share folders.

Kuluoz is a bot that targets Microsoft Windows platforms. This bot is sent in spam messages pretending to be from US Postal Service. It sends out system information and accepts instructions from a remote server to download and execute malicious files on the infected computer. Moreover, it creates a registry entry in order to self-initiate after system reboot.

Juasek is a back door bot that targets Microsoft Windows platforms. This malware allows a remote un-authenticated attacker to perform malicious actions such as opening a command shell, downloading or uploading files, creating new processes, listing/terminating processes, searching/creating/deleting files, and retrieving system information. In addition, it installs a service to survive system reboots.

Papras is a banker trojan that targets both 32bit and 64bit Microsoft Windows platforms. This malware sends out system information and requests configuration information from a remote host. It affects network functions and monitors users' Internet activities to steal critical financial information. In addition, it has back door functionalities to provide remote attackers with unauthorized access to infected computers. The accepted control commands include downloading of other malicious files, collecting cookies and certificates information, system rebooting and shutting down, sending out login information, taking screen shots, setting up socket connections to remote hosts for other activities, etc. Moreover, the malware injects itself into processes and may also inject other malicious files into target processes.

B APPENDIX B: TOP HIGH-RISK APPLICATIONS

This appendix provides further information related to the top high-risk applications found in our research. Check Point's full application database is available at appwiki.checkpoint.com

Anonymizers

Tor is an application intended to enable online anonymity. Tor client software directs internet traffic through a worldwide volunteer network of servers to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity such as website visits, online posts, instant messages and other communication forms, back to the user.

CGI-Proxy is a Common Gateway Interface software package. It appears to a user as a web page that allows access to a different site. Supported protocols include HTTP, FTP and SSL.

Hopster is an application for bypassing firewalls and proxy server, allowing anonymous browsing and chatting.

Hide My Ass is a free web proxy service that masks IP addresses enabling users to connect to websites anonymously.

Hamachi is a virtual private network (VPN) shareware application. It is used for establishing a connection over the internet that emulates the connection over a local area network (LAN).

Ultrasurf is a free proxy tool that enables users to circumvent firewalls and Internet content blocking software.

OpenVPN is a free open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

P2P file sharing

BitTorrent is a peer-to-peer file sharing P2P communication protocol. It is a method of distributing large amounts of data widely without the original distributor incurring the entire costs of hardware, hosting, and bandwidth resources. Instead, when data is distributed using the BitTorrent protocol, each recipient supplies portions of the data to newer recipients, reducing the cost and burden on any given individual source, providing redundancy against system problems, and reducing dependence on the original distributor. There are numerous compatible BitTorrent clients, written in a variety of programming languages, and running on a variety of computing platforms.

eMule is a peer-to-peer file sharing application that connects to the eDonkey network and the Kad network. The software provides direct exchange of sources between client nodes, recovery of corrupted downloads and the use of a credit system to reward frequent uploaders. eMule transmits data in zlib-compressed form for bandwidth efficiency.

Soulseek is a peer-to-peer file sharing application. It is used mostly to exchange music, although users are able to use it to share a variety of other files.

Gnutella is a popular file sharing network, and one of the most popular peer-to-peer protocols, used by applications such as BearShare, Shareaza, Morpheus and iMesh. It is commonly used to exchange MP3 music files, videos, applications, and documents.

Sopcast is a media streaming application which allows media streaming via P2P networks. Sopcast allows users to broadcast media to other users or watch streams broadcasted by other users.

Remote Administration Tools

Remote Desktop Protocol (RDP) is a proprietary application developed by Microsoft, which provides a user with a remote interface to another computer.

Team Viewer allows users to control remote computers using client software or by logging into a website.

LogMeIn is a suite of software services that provides remote access to computers over the Internet. The various product versions cater to both end users and professional help desk personnel. LogMeIn remote access products use a proprietary remote desktop protocol that is transmitted via SSL. Users access remote desktops using an Internet-based web portal, and optionally, the LogMeIn Ignition stand-alone application.

VNC is a software that consists of a server and client application for the Virtual Network Computing (VNC) protocol to control another computer remotely. The software runs on Windows, Mac OS X, Unix-like operating systems, Java platform and Apple iOS which operates the iPhone, iPod and iPad.

File Storage and Sharing Applications

Dropbox Dropbox is a file hosting/sharing service application. It offers cloud storage, file synchronization and client software. In brief, Dropbox users create a special folder on their computers. Dropbox then synchronizes the folder so that it appears the same and contains the same content regardless of which computer the user chooses to use. Files placed in this folder are also accessible through a website and mobile phone applications.

Windows Live Office is an online Microsoft Office document storage, editing, and sharing tool. With Office Web Apps, online users can create, view, edit, share, co-author and collaborate on documents, worksheets, presentations and notes from virtually anywhere with an Internet connection.

Curl is a command line tool that enables the user to transfer data with URL syntax. It supports FILE, FTP, HTTP, HTTPS, SSL certificates and other transfers protocols.

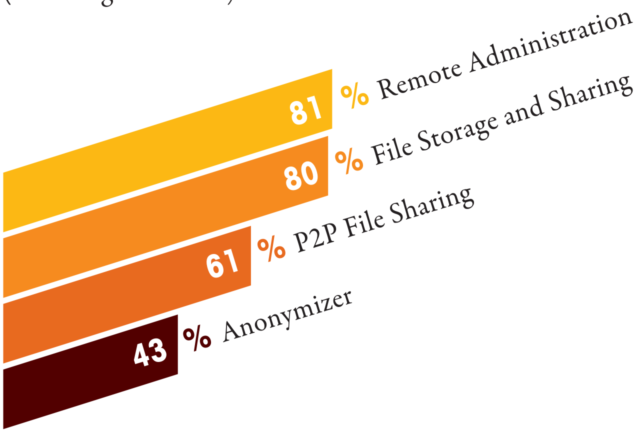
YouSendIt is a digital file delivery service. The service allows users to send, receive and track files on demand.

C APPENDIX C: ADDITIONAL FINDINGS WEB APPLICATIONS USAGE

The following data provides additional elaboration to the findings presented in the "Applications in The Enterprise Workspace" section.
Charts C-A and C-B summarize the usage of applications by category and by region.

Applicaiton Usage by Category

(% of Organizations)

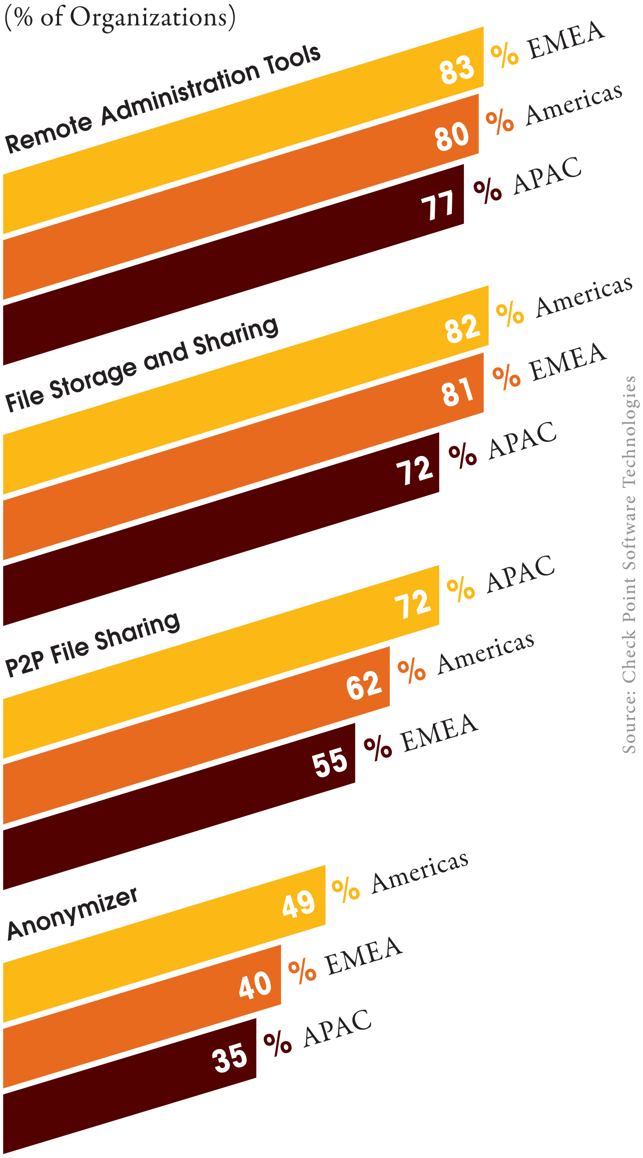


Source: Check Point Software Technologies

Chart C-A

Application Usage by Region

(% of Organizations)



Source: Check Point Software Technologies

Chart C-B

The following tables provide additional insight into the most popular BitTorrent and Gnutella clients

Top BitTorrent Clients	Number of Organizations
Vuze	108
Xunlei	74
uTorrent	55
BitComet	25
FlashGet	21
QQ Download	8
Pando	7
P2P Cache	7
Transmission	6
Other	242

Top Gnutella Clients	Number of Organizations
BearShare	52
LimeWire	23
FrostWire	16
Foxy	2
Other	31

The table below provides additional information on the top used applications per category by region

Application Category	Region	Application Name	% of Organizations
Anonymizer	Americas	Tor	24%
		CGI-Proxy	16%
		Hamachi	8%
		Hopster	8%
		Ultrasurf	7%
	EMEA	Tor	23%
		CGI-Proxy	12%
		Hamachi	4%
		Hopster	7%
		Hide My Ass	7%
	APAC	Tor	20%
		Hopster	6%
		CGI-Proxy	6%
		Hamachi	6%
		Hide My Ass	7%

Application Category	Region	Application Name	% of Organizations
P2P File Sharing	Americas	BitTorrent Clients	35%
		SoulSeek	23%
		eMule	21%
		Windows Live Mesh	8%
		Sopcast	8%
	EMEA	BitTorrent Clients	33%
		SoulSeek	19%
		eMule	15%
		Sopcast	12%
		iMesh	10%
	APAC	BitTorrent Clients	62%
		eMule	26%
		SoulSeek	11%
		Sopcast	10%
		BearShare	8%
File Storage and Sharing	Americas	Dropbox	73%
		Windows Live Office	52%
		Curl	28%
		YouSendIt	26%
		ZumoDrive	12%
	EMEA	Dropbox	71%
		Windows Live Office	51%
		Curl	22%
		YouSendIt	21%
		ImageVenue	18%
	APAC	Dropbox	57%
		Windows Live Office	50%
		Curl	26%
		YouSendIt	16%
		Hotfile	10%

Application Category	Region	Application Name	% of Organizations
Remote Administration	Americas	MS-RDP	59%
		LogMeIn	51%
		TeamViewer	45%
		VNC	14%
		Bomgar	8%
	EMEA	MS-RDP	60%
		TeamViewer	55%
		LogMeIn	44%
		VNC	20%
		pcAnywhere	3%
	APAC	TeamViewer	58%
		MS-RDP	51%
		LogMeIn	26%
		VNC	16%
		Gbridge	3%

D APPENDIX D: DLP DATA TYPES

Our research included inspection of various data types while searching for potential data loss events. The following list presents the top data types inspected and detected by Check Point DLP Software Blade.

Source code - Matches data containing programming language lines such as: C, C++, C#, JAVA and more; indicates leaks of intellectual property.

Credit card information - Includes two data types: credit card numbers and PCI-Sensitive Authentication Data.

- **Credit card numbers:**

  Match Criteria: Related to Payment Card Industry (PCI); matches data containing credit card numbers of MasterCard, Visa, JCB, American Express, Discover and Diners Club; match is based on both pattern (regular expression) and validation of check digits on the schema defined in Annex B of ISO/IEC 7812-1 and in JTC 1/ SC 17 (Luhn MOD-10 algorithm); indicates leaks of confidential information.

  Example: 4580-0000-0000-0000.

- **PCI - Sensitive Authentication Data:**

  Match Criteria: Related to Payment Card Industry (PCI); matches information that is classified as Sensitive Authentication Data according to PCI Data Security Standard (DSS). Such data, unlike Cardholder data, is extremely sensitive and PCI DSS does not permit storage of this data. Matches data containing a credit card magnetic stripe track data (track 1, 2 or 3), an encrypted or unencrypted PIN block and a Card Security Code (CSC).

Examples: %B4580000000000000^JAMES /L.^99011200000000000?, 2580.D0D6.B489.DD1B, 2827.

Password protected file - Matches files that are either password protected or encrypted. Such files may contain confidential information.

Pay slip file - Matches files containing a pay slip, also known as pay stub, pay advice and paycheck stub; indicates loss of personal information.

Confidential email - Matches Microsoft Outlook messages that were marked by the sender as <Confidential>; such emails usually contain sensitive information. Note: Microsoft Outlook allows the sender to mark sent emails with various sensitivity values; this Data Type matches emails that were marked as <Confidential> using Outlook's sensitivity option.

Salary compensation information - Matches documents containing words and phrases with employees compensation data such as: salary, bonus etc.

Other data types detected during the research - Hong Kong Identity Card, Financial Report Terms¸ Bank Account Numbers, Finland IBAN, Canada Social Insurance Number, FERPA - Confidential Educational Records, U.S. Zip Codes, UK VAT Registration Number, Mexico Social Security Number, U.S. Social Security Numbers, Student Grades – GPA, Hong Kong Identity Card, Bank Account Numbers, Salesforce Reports, Finland Personal Identity Code, ITAR - International Traffic in Arms Regulations, Sensitive personal records, CAD-CAM Designs or Graphic Design File, HIPAA - Protected Health Information, France Social Security Number, Employee Names, New Zealand Inland, PCI - Cardholder Data, U.S. Driver License Numbers, HIPAA - Medical Record Number, Canada Social Insurance Number, Finland IBAN, HIPAA - ICD-9, Denmark IBAN, Finland VAT Number, Finland Personal Identity Code, International Bank Account Number – IBAN, Hong Kong Identity Card and others.

REFERENCES

[1] The Art of War By Sun Tzu, http://suntzusaid.com/artofwar.pdf
[2] http://www.checkpoint.com/campaigns/3d-analysis-tool/index.html
[3] http://www.checkpoint.com/products/threatcloud/index.html
[4] http://supportcontent.checkpoint.com/file_download?id=20602
[5] http://www.nytimes.com/2012/03/05/technology/the-bright-side-of-being-hacked.html?pagewanted=2&ref=global-home
[6] http://edition.cnn.com/video/#/video/bestoftv/2012/10/01/exp-erin-cyberattack-nuclear-networks-leighton.cnn?iref=allsearch
[7] http://www.networkworld.com/news/2012/071312-security-snafus-260874.html?page=4
[8] http://www.businessweek.com/news/2012-10-18/bank-cyber-attacks-enter-fifth-week-as-hackers-adapt-to-defenses
[9] http://arstechnica.com/security/2012/09/blackhole-2-0-gives-hackers-stealthier-ways-to-pwn/
[10] http://www.networkworld.com/slideshow/52525/#slide1
[11] http://www.ihealthbeat.org/articles/2012/10/30/breaches-at-uks-nhs-exposed-nearly-18m-patient-health-records.aspx
[12] http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf
[13] http://cve.mitre.org/index.html
[14] http://www.networkworld.com/news/2012/020912-foxconn-said-to-have-been-255917.html
[15] http://news.cnet.com/8301-1009_3-57439718-83/anonymous-attacks-justice-dept-nabbing-1.7gb-of-data/
[16] http://news.cnet.com/8301-1009_3-57396114-83/vatican-anonymous-hacked-us-again/
[17] http://news.cnet.com/8301-1023_3-57411619-93/anonymous-hacks-into-tech-and-telecom-sites/
[18] http://www.ftc.gov/opa/2012/06/epn-franklin.shtm
[19] http://www.ftc.gov/opa/2010/02/p2palert.shtm
[20] http://www.networkworld.com/news/2012/091212-botnet-masters-hide-command-and-262402.html
[21] http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secres
[22] http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/
[23] http://news.cnet.com/8301-31921_3-20072755-281/dropbox-confirms-security-glitch-no-password-required/
[24] http://japandailypress.com/newspaper-reporter-fired-for-emailing-sensitive-info-to-wrong-people-159277
[25] http://www.roanoke.com/news/roanoke/wb/307564
[26] http://tamutimes.tamu.edu/2012/04/13/am-acting-on-email-message-that-inadvertently-included-some-alumni-ss-numbers/
[27] www.hhs.gov/ocr/privacy/hipaa/index.html
[28] The Art of War By Sun Tzu, http://suntzusaid.com/artofwar.pdf
[29] http://en.wikipedia.org/wiki/Malware#Backdoors

Design: RoniLevit.com

Check Point®
SOFTWARE TECHNOLOGIES LTD.

www.checkpoint.com

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

December 2012