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 MORE THAN RELEVANT, REFLECTING TODAY’S MODERN WARFARE - CYBER WARFARE.

Hackers’ technics are constantly changing, using more advanced and sophisticated attack methods, raising the security challenge to new levels. 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 to gain access to 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 increasing at the speed of light, and more data and platforms imply more risks. Finally, the list of security threats is not getting any shorter, and each new attack reveals a deeper level of sophistication.

What were the main security risks your network environment faced in the last year? What are the risks it will be exposed to next year? These were the key questions that kept Check Point’s security research team busy in the past few months. While gathering answers to these questions, Check Point has conducted an intensive security analysis.

This report provides a peek into 2012 network security events that occurred in organizations worldwide. The report presents the security events found at these organizations, with examples of incidents published publically, explanations on how some of the attacks were conducted, followed with recommendations on how to protect against such security threats. 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 last 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 888 companies’ network security events was done using data collected from Check Point Security Gateways, which scanned the companies’ incoming and outgoing live network traffic. The traffic was inspected with Check Point’s multi-tier Software Blades technology to detect a variety of security threats such as high risk applications, intrusions attempts, viruses and bots, sensitive data loss etc. The network traffic was monitored in real time by implementing the Check Point Security Gateway inline or in monitor (tap) mode.

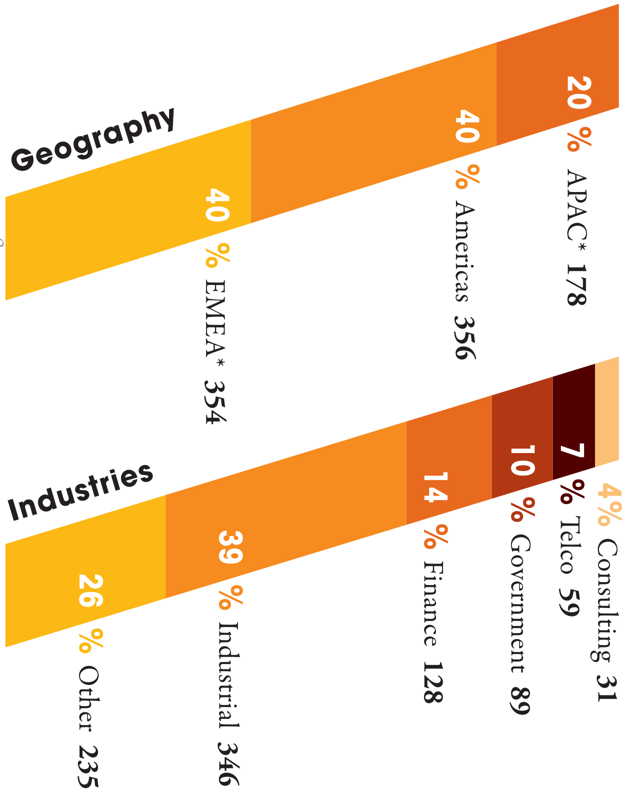
On average, each organization's network traffic was monitored for 134 hours. The companies in our research are from a wide range of industries and located worldwide as shown in chart 1-A and 1-B.

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 from a large network of global sensors, strategically placed around the globe, that gather information on threats and malware attacks. ThreatCloud enables identification of emerging global security trends and threats, creating a collaborative network to fight cybercrime. In our research we analyzed data from ThreatCloud that was gathered in a 3-month period between August and October, 2012.

Reference for threat data was gathered from Check Point's SensorNet™ sensor network for the period of July 1st through 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 build a real time view of security around the world.

Finally, meta-analysis of 628 endpoint security reports in a variety of organizations. The security analysis included scanning of each host validating data loss risks, intrusion risks and malware risks. The analysis was done with Check Point Endpoint Security report tool checking whether Anti-Virus is running on the host, Anti-Virus is up to date, software are running latest versions and more. The tool is free and 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 Cyber-Attack is Exposed

In 2012, cyber-attacks continued to proliferate and make headlines. Almost daily malicious software threats, attacks and botnets are front-page news, displaying the infamous success of hackers stealing data, paralyzing operations, and spying on corporations and governments. The following examples are only the tip of the iceberg of cyber-attacks that have occurred during 2012: Hackers attacking the White House network[6], Hactivist group Anonymous brought down the websites of trade groups U.S. Telecom Association and TechAmerica[7], Cyber-Attacks hits on Capital One Financial Corp., BB&T Corp., and HSBC Bank USA[8], and many others.

Advanced Persistent Threats

Cybercriminals are no longer isolated amateurs. In many cases cybercriminals belong to well-structured organizations that resemble terrorist cells - they are well-funded, have motivations and goals. Cybercriminals seem to dedicate considerable amount of time and resources to gather intelligence. Their criminal activities cause organizations severe damages, such as: loss of confidential data, business interruptions, reputation damages and of course financial loss. The most sophisticated and long-term attacks, working towards a very specific pre-determined goal, are referred to as Advanced Persistent Threats (APT). These attacks 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 huge increase in malicious activity in the last year can be attributed to hackers easily 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 - a widely-used, web-based software package. BlackHole includes a collection of tools that take advantage of security holes in web browsers to download viruses, bots, trojans and other forms of malicious software agents to computers of unsuspecting victims. Prices for these kits range from $50 for one day usage, up to $1,500 for a full year[9].

DATA-BREACH INCIDENTS IN 2012

Numerous data-breach incidents took place this year, exposing data stored on corporate servers related to payment cards, customer, student or patient data. These malicious activities share the common goal of acquiring confidential information. The following list presents a few examples:

Global Payments Inc.
A global payments 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 the names, Social Security numbers, and other personal data of about 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 in the U.S., resulted in an information breach of 123,000 federal employees' information.

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

U.S. Utah Dept. of Technology Services
In March 2012, 780,000 patient files related to Medicaid health program claims were stolen from a server by hackers believed to be operating out of 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. Then attackers make an initial intrusion into the target's network to open a back-door and stay persistent in the network. This is usually accomplished by infecting a host with a bot, allowing 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 this step the attacker has reached his target, he can now exploit the infected hosts to collect data or cause the intended damage remotely while maintaining persistence and under the radar for the long term.

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

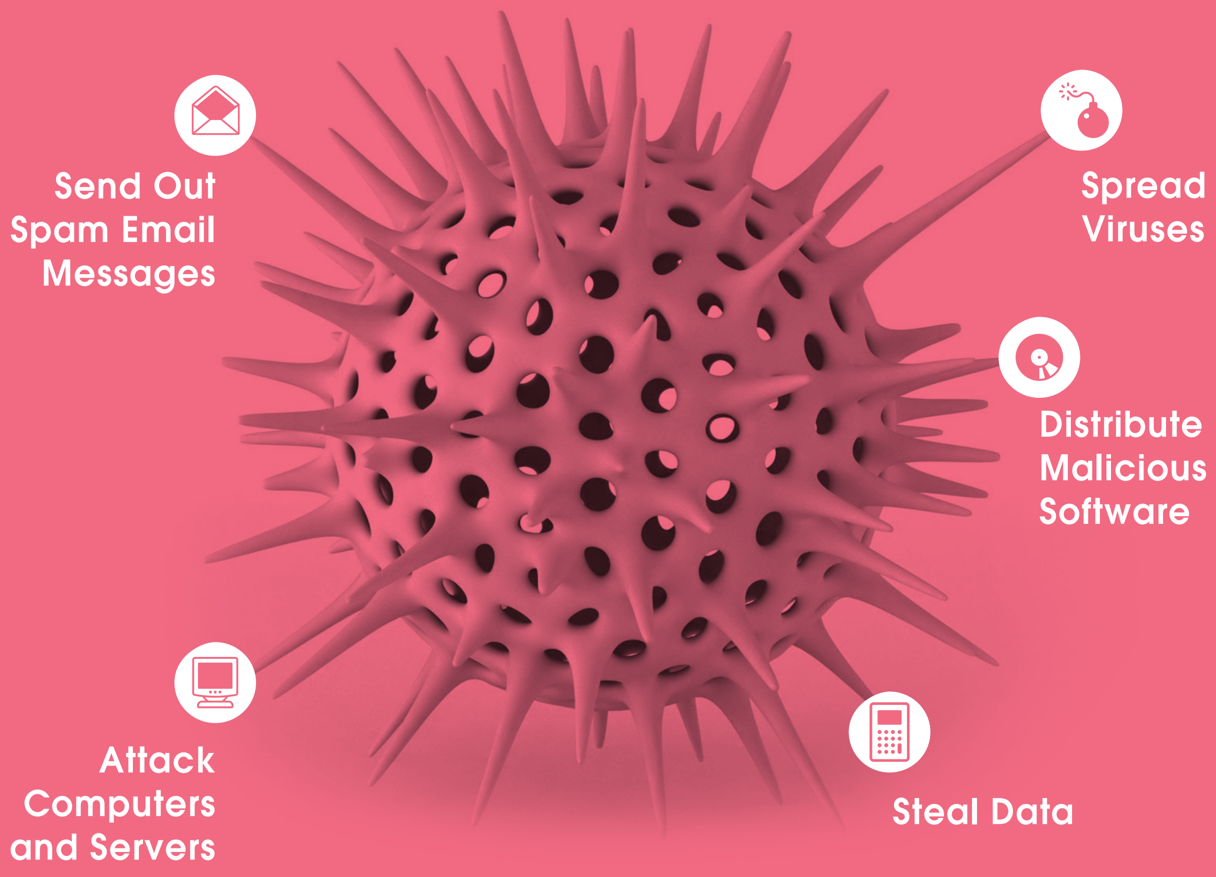
Botnets are Here to Stay

One of the most significant network security threats that organizations are facing today are botnets. A bot is a malicious software that invades and infects a computer to allow criminals to control it remotely. The infected computer 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 ignorant of these activities. Bots also play a key role in targeted APT attacks.

There are two major trends in today‘s threat landscape that are driven by bot attacks. The first trend is the growing profit-driven cybercrime industry - this industry includes cybercriminals, malware operators, tool providers, coders, and affiliate programs. Their “products“ can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and Denial of Service attacks) and organizations are finding it difficult to fight off these attacks. The second trend is ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Botnets are here to stay. As opposed to viruses and other traditional static malwares (which code and form remain the same), botnets by nature are dynamic and can quickly change form and traffic patterns. Bot toolkits are sold

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 ARE INFECTED WITH BOTS

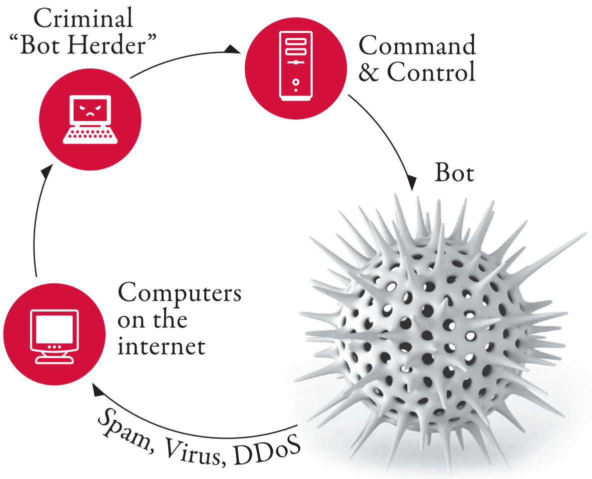
online for as low as $500, and their attacks cost businesses millions of dollars. The bot problem has become a big issue.

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 recent research shows that in 63% of the organizations at least one bot has been detected. Most organizations are infected by a variety of bots.

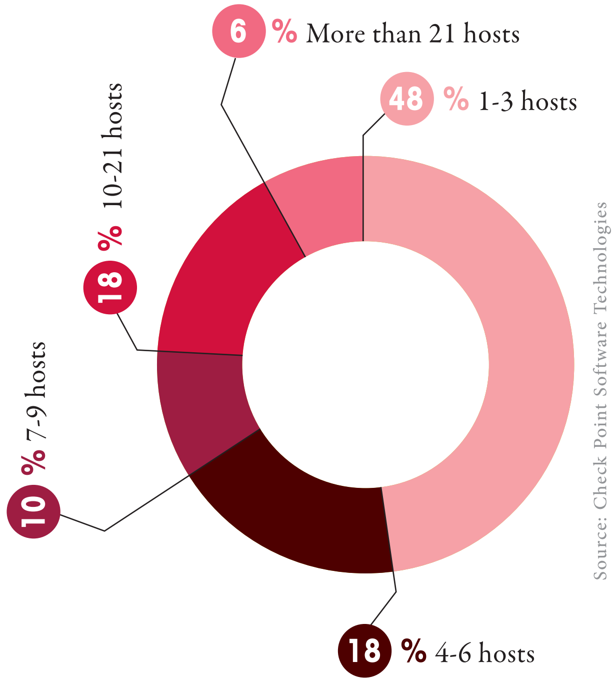
How Botnets Work

A botnet typically has a number of computers that have been infected with malicious software that establishes a network connection with a control system or systems, known as Command & Control 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 Command & Control (C&C) center for instructions from the cyber criminals. Many communication protocols are used for these connections,



Number of Hosts Infected with Bots

(% of Organizations)

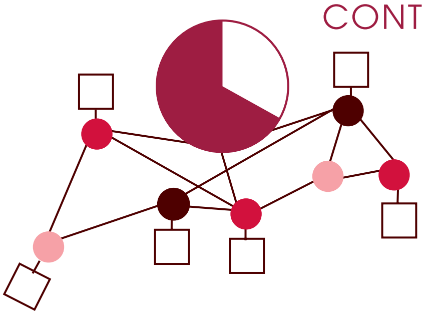


Source: Check Point Software Technologies

Chart 2-A

including Internet Relay Chat (IRC), HTTP, ICMP, DNS, SMTP, SSL, and in some cases custom protocols created by the botnet software creators.

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

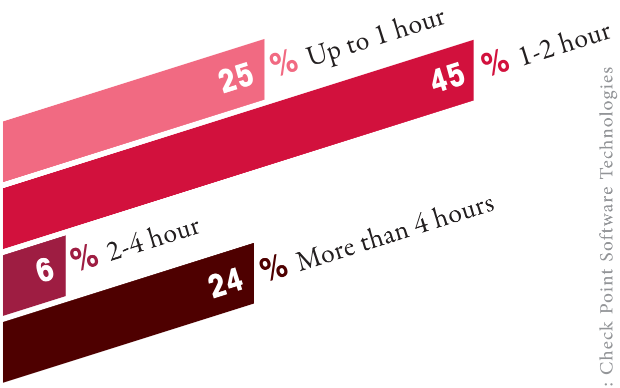


Command & Control Activity

Bots come in many different shapes and forms, and can execute a large 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 cyber criminals pinpoint individuals or organizations 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 2 hours. The majority of Command & Control activity is found in the USA, followed by Germany, Netherlands and France, as shown in chart 2-C.

The various types of bot communication to its Command & Control center include: reports of new hosts it has infected, keep-alive messages, and data collected from the host system. Our research shows that on average, a bot is communicating 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 wild today. The following table presents the top infamous and prominent botnets found during our research. To get a better understanding of these stealthy threats, more information on each threat has been compiled on Appendix A.

Botnet Family	Malicious Activity
Zeus	Steal online banking credentials
Zwangi	Present the user with unwanted advertising messages
Sality	Self-spread virus
Kuluoz	Remote execution of malicious files
Juasek	Remote malicious actions: open a command shell, search/create/delete files, and more
Papras	Steal financial information and gain remote access

See additional details in Appendix A

TOP COMMAND & CONTROL LOCATION COUNTRIES

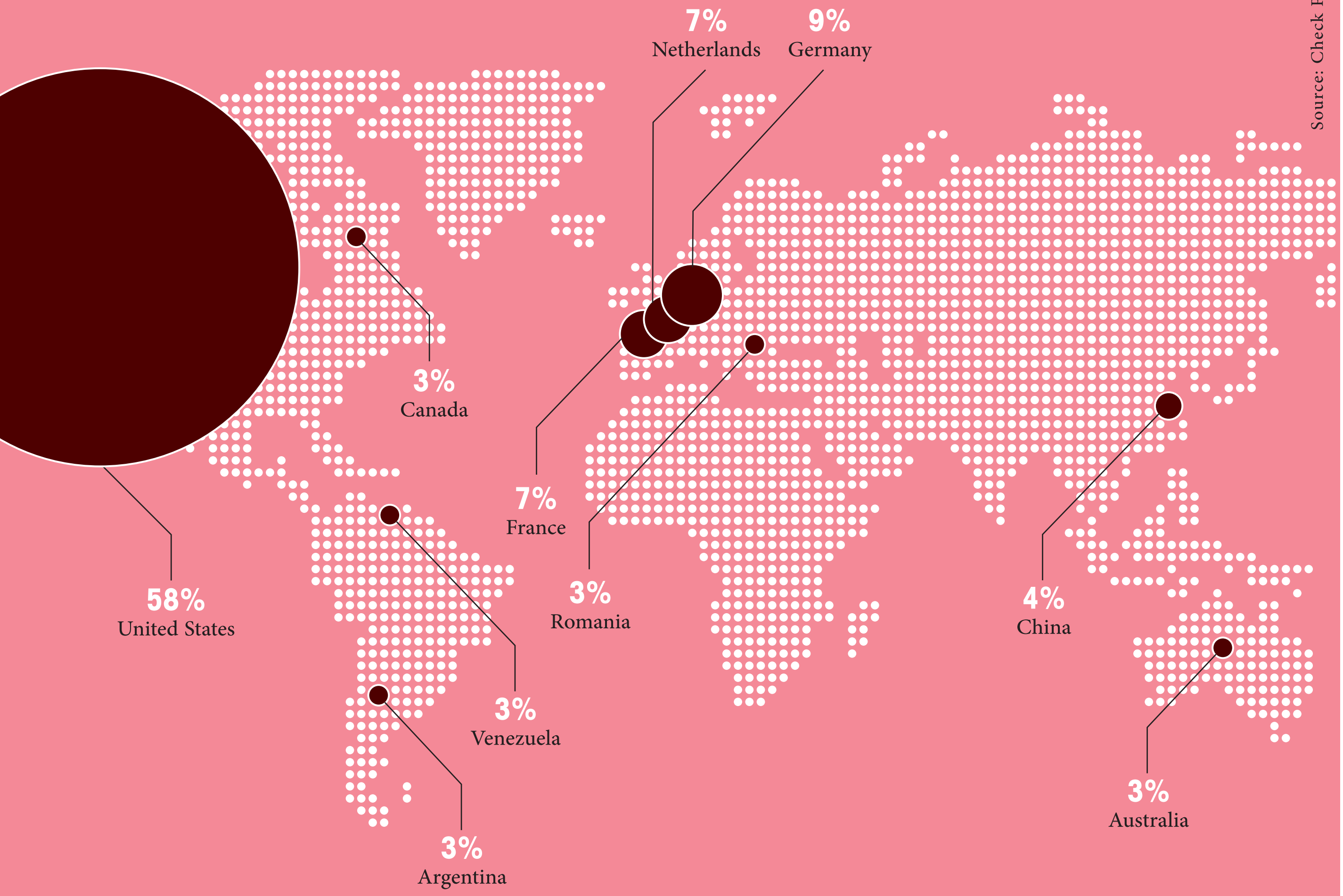


Chart 2-C

Source: Check Point Software Technologies

IN 75% OF ORGANIZATIONS, A HOST ACCESSES A MALICIOUS WEBSITE

EVERY 23 MINUTES A HOST ACCESSES A MALICIOUS WEBSITE

How Your Organization can be Infected with Malware

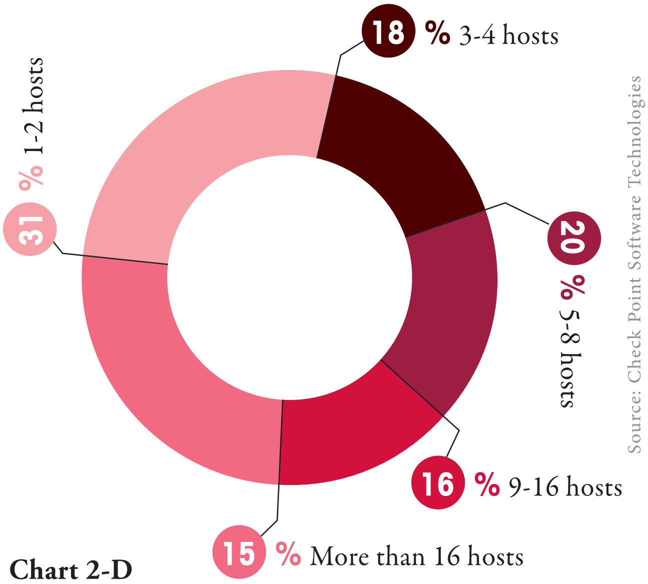
There are multiple entry points to breach an organization's defenses: browser-based vulnerabilities, mobile phones, malicious attachments and removable media, to name a few. In addition, the explosion of Web 2.0 applications and social networks used as business tools are giving hackers a huge opportunity to lure victims to click on malicious links or on "malvertisement" – malicious advertisements running on legitimate websites.

Although botnets are considered to be one of the most prominent network security threats today, organizations are facing additional security threats from the world of malware: viruses, worms, spyware, adware, trojans and so on. Our research shows that in 75% of organizations a host accesses a malicious website.

The following pie presents number of hosts that accessed a malicious website by the percentage of organizations. In over 50% of the organizations at least five hosts accessed a malicious website.

Access to Malicious Sites by Number of Hosts

(% of Organizations)



Source: Check Point Software Technologies

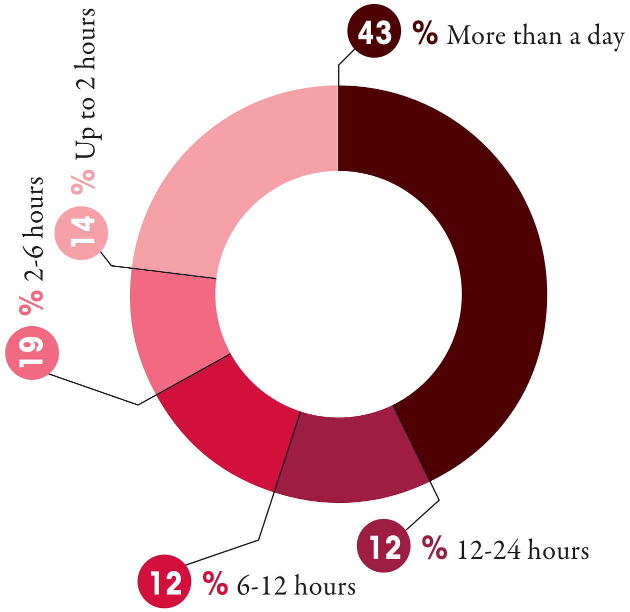
Chart 2-D

A malware can be downloaded by a user or by a bot that has already infected the host. We have found that in 53% of the organizations a malware was downloaded from the corporate network. In over 50% of these organizations, we have found that more than four hosts have downloaded malware.

The following pie presents the average frequency of malware downloads in the organizations under our research.

Malware Downloads Frequency

(% of Organizations)



Source: Check Point Software Technologies

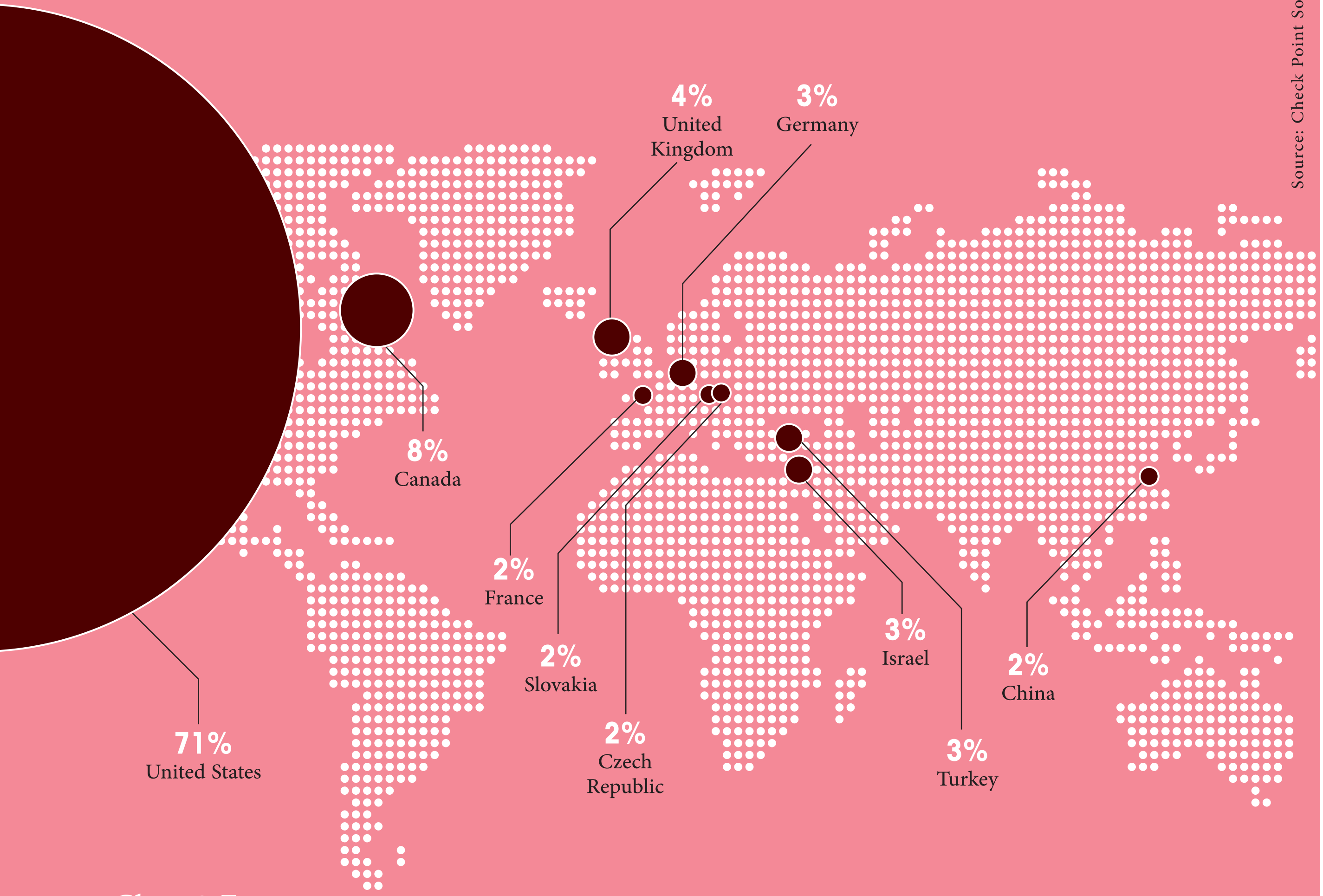
Chart 2-E

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

In our research, the majority of malware is found in the USA, followed by Canada and United Kingdom as shown in chart 2-F.

Anti-Virus protection is one of the methods to protect against malware infections, however our research shows that 23% of hosts in organizations do not update their Anti-Virus on a daily basis. A host that is not running an up to date Antivirus is exposed to the latest viruses. We have also found that 14% of hosts in organizations do not even run an Anti-Virus on host computers. Hosts that are not running an Anti-Virus is in high potential to get infected with a malware.

TOP MALWARE LOCATION COUNTRIES

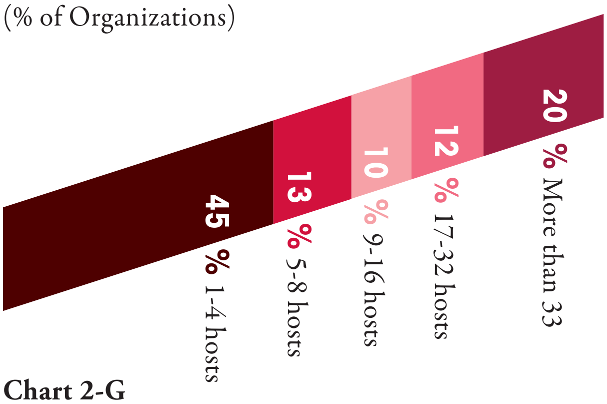


Source: Check Point Software Technologies

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 seems like the Flame malware that was discovered earlier this year was just the beginning. This year a related program was uncovered, named "miniFlame", which carries out more precise attacks on targets in the Middle East. miniFlame includes a "back door" allowing 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

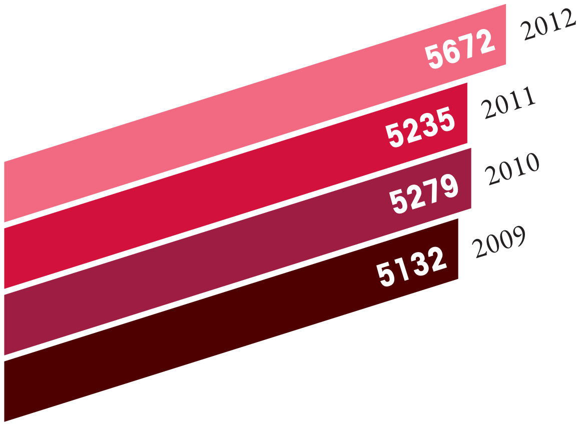
During 2012, a sophisticated multi-dimensional attack took place steeling an estimated 36+ million Euros from more than 30,000 bank customers from multiple banks across Europe. Entirely transparent, the online banking customers had no idea they were infected with trojans, that their online banking sessions were being compromised or that funds were being stolen directly out of their accounts. This attack campaign was discovered and named "Eurograbber" by Versafe and Check Point Software Technologies. The Eurograbber attack employs 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 as well. The multi-staged attack infected the computers and mobile devices of online banking customers and once the Eurograbber trojans were installed on both devices, the bank customer's online banking sessions were completely monitored and manipulated by the attackers. Even the two-factor authentication mechanism used by the banks to ensure the security of online banking transactions was circumvented in the attack and actually used by the attackers to authenticate their illicit financial transfer. Further, the trojans used to attack mobile devices was developed for both the Blackberry and Android platforms in order to facilitate a wide "target market" and as such was able to infect both corporate and private banking users and illicitly transfer funds out of customers' accounts in amounts ranging from 500 to 250,000 Euros each. Additional information on the Eurograbber attack, including a detailed walkthrough of the attack, can be found in the Eurograbber attack case study white paper[12] at Check Point website.

More Vulnerabilities More Exploits

Well known vulnerabilities are key targets for hackers who rely on the simple fact that many organizations do not update their software on a weekly basis. The bigger the organization, the harder it is for security administrators to keep all systems fully updated. Thus, in many cases, a year-old patched vulnerability can still be used to penetrate into systems of large and small organizations that haven't updated their systems with the latest software patches.

The sheer number of vulnerabilities disclosed every year is overwhelming, with more than 5,000[13] new ways for hackers to cause damage and access systems discovered in 2012. And there are still many more undiscovered vulnerabilities actively used by cyber criminals.

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 almost all organizations around the globe are also the most vulnerable – Oracle, Apple and Microsoft are the leading vulnerable vendors.

2012 Top Vulnerabilities and Exposures by Vendor

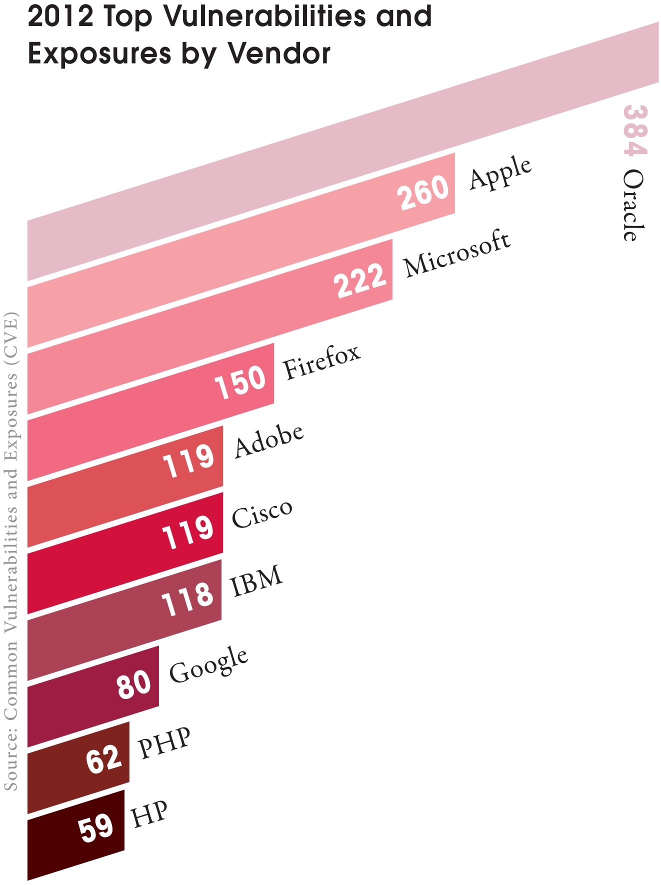


Chart 2-I

Our research shows that 75% of hosts in organizations are not using the latest software versions (for example: Acrobat Reader, Flash Player, Internet Explorer, Java Runtime Environment and more). The meaning is that these hosts are exposed to wide range of vulnerabilities that can be exploited by hackers. Our research also shows that 44% of hosts in organizations are not running the latest Microsoft Windows Service Packs. Service Packs usually include security updates for the operating system. Not running the latest Service Pack means a security risk.

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

Security Events by Software Vendor

% of Organizations

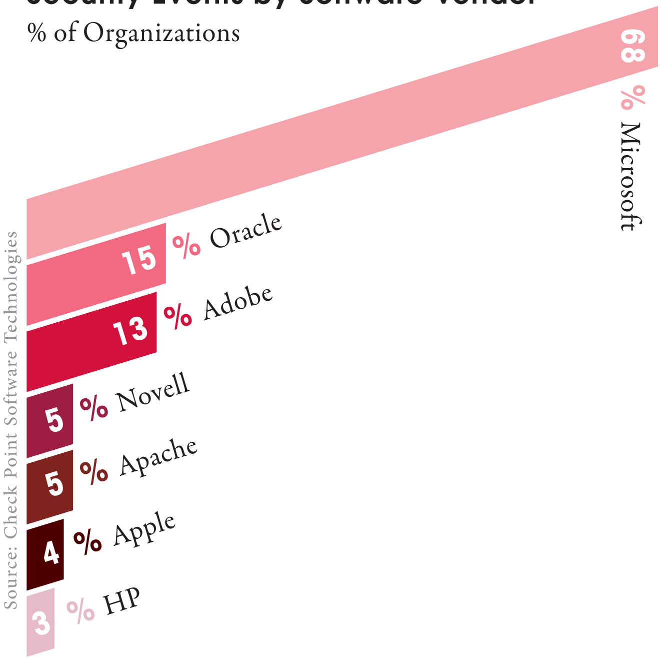
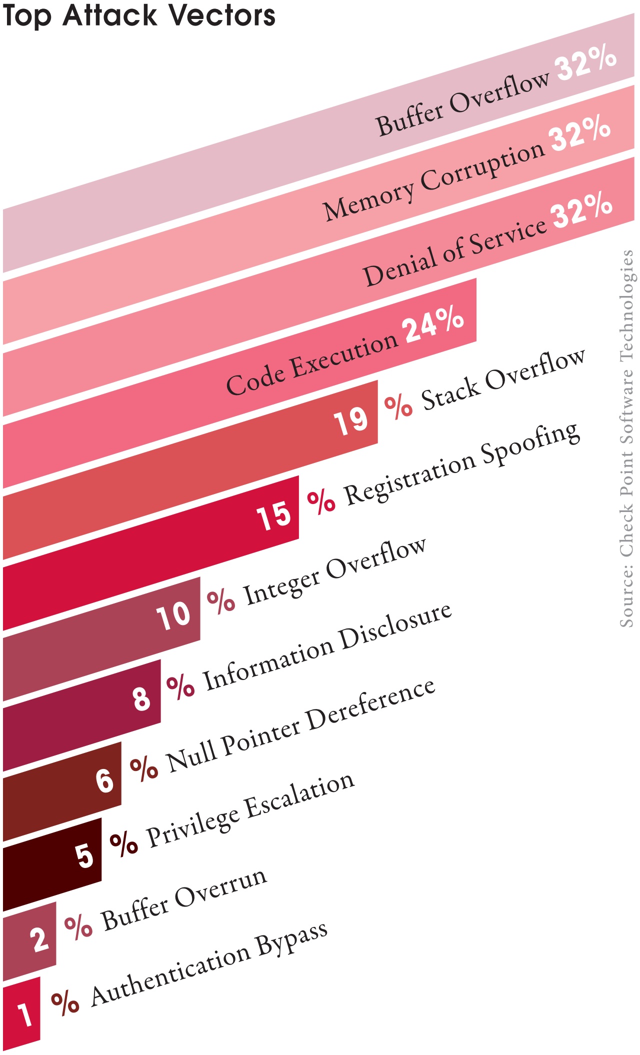


Chart 2-J

Hackers are using various techniques referred to as attack vectors. Chart 2-K lists some of these attack vectors, according to the percentage of organizations that suffered from them. Memory Corruption, Buffer Overflow and Denial of Service are the 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

This case shows a real example of a series of SQL Injection attacks that took place between July and October 2012 in a Check Point customer 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 how the attack looks. The marked text is the data the hacker tried to disclose with the SQL Injection (in this case, usernames and passwords). The SQL commands are: select, concat and from.
The attack occurred from 99 different IPs. Although the target organization is located in Europe, the attacks were originated from many different locations, as presented in the chart 2-M.

SQL Injection can be done manually (a hacker using a keyboard) or automated (scripted attack). In this case, as shown in the chart 2-L , the peak of the attack was a burst of 4,184 attack attempts (most likely automated) that were launched during two days, using the same injection pattern and originating from a single source IP.

SQL Injection Events Rate

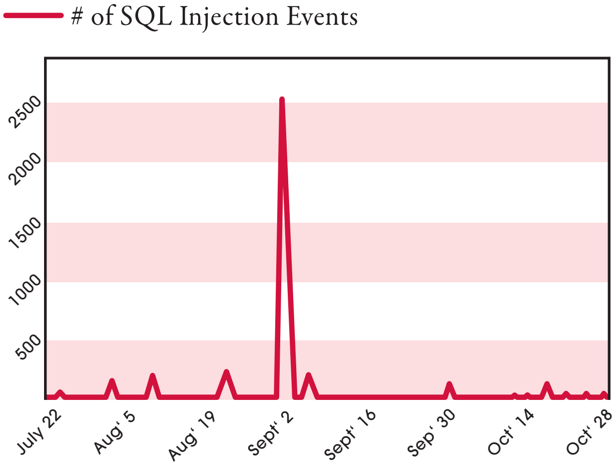
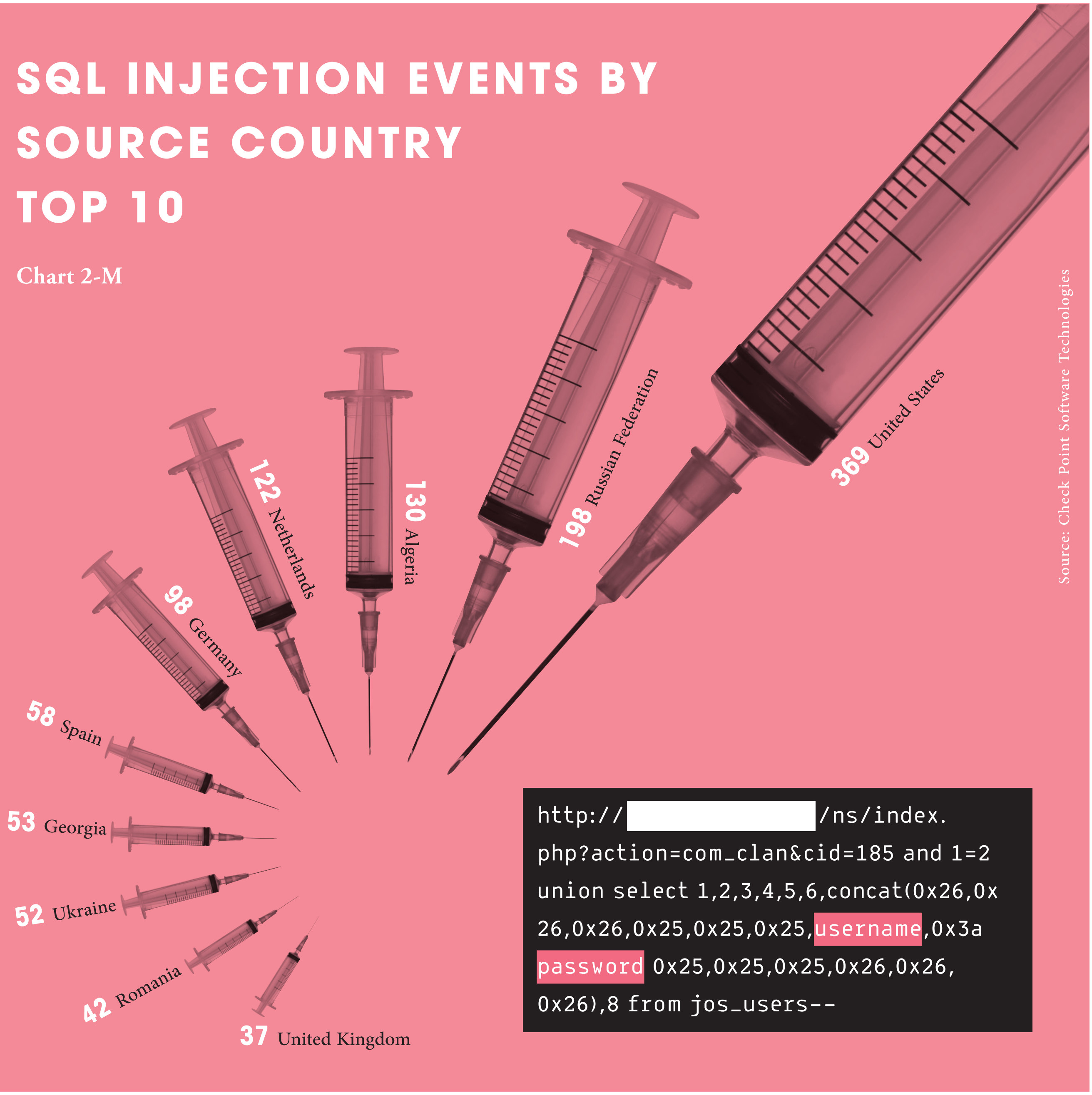


Chart 2-L

SQL INJECTION EVENTS BY SOURCE COUNTRY TOP 10

Chart 2-M



```
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--
```

Source: Check Point Software Technologies

SECURITY RECOMMENDATIONS MULTIPLE SECURITY LAYERS

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

- 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

An organization needs an Anti-malware solution that scans files coming into the network and can decide, in real time, if the files are infected by malware. This solution should prevent malicious files from infecting the internal

2012, A YEAR OF HACKTIVISM

In 2012 the global political arena turbulence that started in 2010 with the uprisings of many Arab countries continues with different civil protests in other countries. Not surprisingly, we are also seeing a wave of cyber-attacks based on ideological agendas.

Taiwan-based Apple supplier Foxconn was hacked by a group calling itself Swagg Security. This group was apparently protesting media reports about poor working conditions at the electronics manufacturer‘s factories in China[14].

Hacktivist group Anonymous claimed it hacked a U.S. Department of Justice website server for the 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 subject to a week-long attack by the Anonymous group. The group claimed its action was justified because the Vatican Radio System has powerful transmitters in the countryside outside Rome, which allegedly constituted a health risk. The group claimed that the transmitters supposedly caused “leukemia and cancer”, to people living nearby. The group also justified its attack and claimed that the Vatican allegedly helped the Nazis, destroyed books of historic value, and that its clergy sexually molested children[16].

In yet another cyber-attack, 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. This 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].

network and also prevent 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 blocking.

To maximize the ability to detect a bot in a network, a multi-tier bot discovery mechanism is needed to cover all aspects of a 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 phase neutralizes the threat and makes sure that the bot agents cannot send out sensitive information nor receive any further instructions for malicious activity. Thus, the bot related damage is immediately mitigated. This approach enables organizations to maintain work continuity - users can work normally, unaware that bot specific communication is being blocked, and the organization is protected with no impact on productivity.

Real-time Global Collaboration

The cyber-attack problem is too big for a single organization to manage. Organizations have a better chance to conquer 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 organizations to increase the likelihood of an attack's success. When enterprises fight these threats separately, many attacks are left undetected because there is no way for corporations to share threat information. To stay ahead of modern threats, businesses must collaborate and share threat data. Only jointly can they make security stronger and more effective.

Intrusion Prevention

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

- Protocol Validation and Anomaly Detection – Identify and prevent traffic that does not comply with protocol standards and can create device malfunction or 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

A clear view of security events and trends is another key component in the fight against cybercrime. The security administrator must have a constant and clear understanding of the network security status to be aware of threats and attacks targeting the organization. This understanding requires a security solution that can provide a high-level overview of the security protections and emphasize critical information and potential attacks. The solution should also enable the ability to conduct deep investigations on specific events. The ability to take immediate action based on this information is another essential capability that enables real-time prevention of attacks or for pro-actively blocking future threats. The security solution must have flexible and intuitive management to simplify threat analysis and reduce the operational overhead of changes.

Security Updates and support

In a constantly changing threat environment, defenses must evolve with or ahead of 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 based on:

- Vendor internal research and obtaining 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 specifics to the customer's 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 passtime activity; a means to see pictures from our friends' latest trips and to watch funny movies. Internet Web 2.0 applications have now become essential business tools in the modern enterprise. We communicate with colleagues, customers and partners, we share information with others, and we get the latest news, opinions and views. Internet based tools such as Facebook, Twitter, WebEx, LinkedIn, and YouTube to name a few, are becoming more and more prevalent in enterprises that acknowledge them as business enablers.

In this section of our research, we will discuss the general risks introduced by web 2.0 applications and their infrastructure, followed by a focus on specific applications found in use at the organizations in our research. Our findings will be illustrated with real reported incidents and examples.

Web Applications are Not a Game

As technology evolves so do the security challenges. Internet tools also introduce new security risks. A number of useful internet applications are used as attack tools against organizations, or may lead to a breach in network security. 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's a myriad of platforms and applications that could be used for personal or business reasons. Each organization needs to be aware of what employees are using, and for what purposes, and then define their own Internet policy.

In 91% of the organizations, users were found to be using applications with a potential to bypass security, hide identities, cause data leakage or even introduce a malware infection without their knowledge.

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 collector 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 alleged that the other organization, an auto dealer named Franklin's Budget Car Sales, Inc., exposed 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 is available on peer-to-peer (P2P) file-sharing networks. Any users of those networks could use the data to commit identity theft or fraud[19].

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

P2P Applications Open a Backdoor 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 backdoor 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 see a very high rate of P2P applications usage, more than half of the organizations (61%) were found to be using P2P applications. The most prominent P2P file sharing tools used are BitTorrent clients. From a regional perspective, the following chart shows that in Asia Pacific, P2P file sharing applications are more popular than in other regions.

Top P2P File Sharing Applications

(% of Organizations)

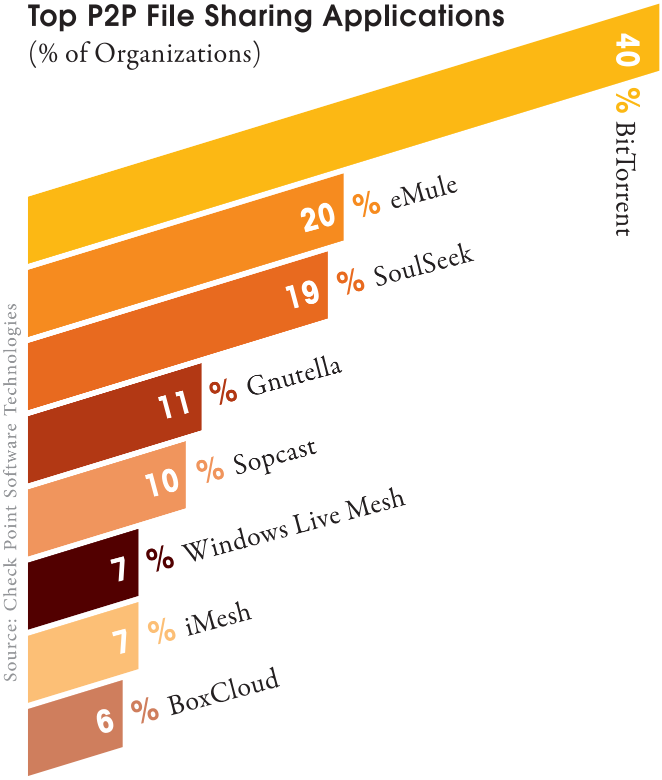


Chart 3-A

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

Usage of P2P File Sharing Applications Per Region

(% of Organizations)

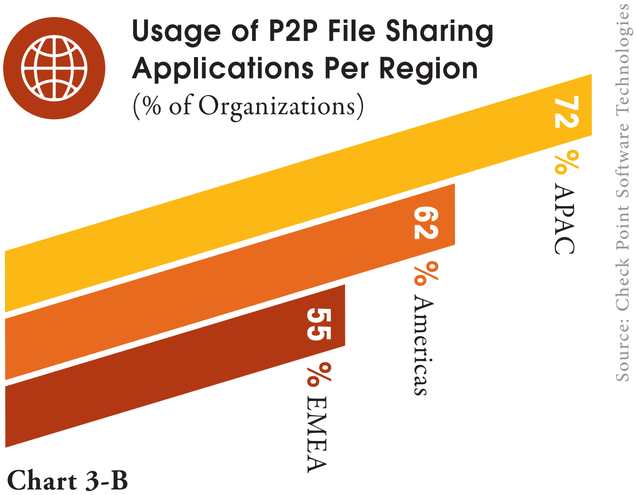


Chart 3-B

Anonymizer Applications Bypass Organization Security Policy

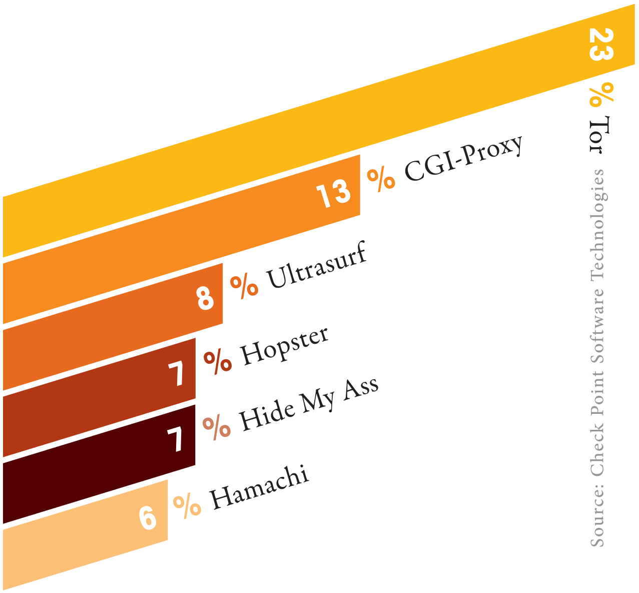
An Anonymizer (or an anonymous proxy) is a tool that attempts to make the user's activity on the Internet untraceable. The Anonymizer application utilizes a proxy server that acts as a privacy mask between a client computer and the rest of the Internet. It accesses the Internet on the user‘s behalf, 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 and trying to access different destinations, so the security policy may not be enforced for that user with the altered IP address and the altered destination address. In some cases, Anonymizers might also be used to hide criminal activity.

When looking at organizations in our study, 43% used at least one Anonymizer application by an employee, with Tor being the most prominent. 86% of the organizations where Anonymizer usage was found claimed that it was in a non-legitimate use conflicting with guidelines and security policy.

When we look at the usage of Anonymizer applications per region, we can see that they are more popular in the Americas and less in Asia Pacific.

Most Popular Anonymizer Applications

(% of Organizations)



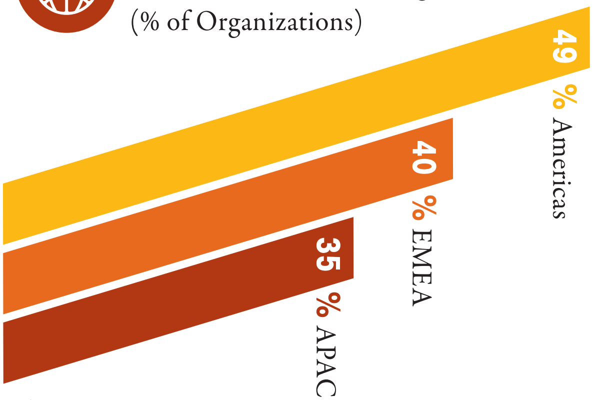
Source: Check Point Software Technologies

Chart 3-C

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

Usage of Anonymizer Applications Per Region

(% of Organizations)

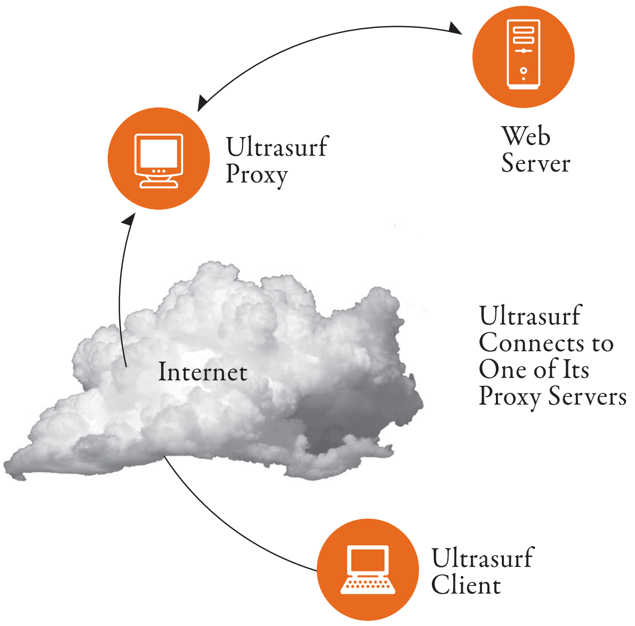


Source: Check Point Software Technologies

Chart 3-D

How does Ultrasurf Anonymizer Work?

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



IN 43% OF ORGANIZATIONS, ANONYMIZERS ARE USED

TOR ANONYMIZER COMPROMISES SECURITY

Recent security researches 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 very hard for surveillance systems that operate at the local network level or the ISP level to determine the intended destination of a user[20]. The Tor network's (also known as Onion Router) main goal is basically to provide anonymity while browsing the internet. Although it has wide support and enjoys great popularity, when used in an organizational environment it raises several security challenges. Tor can also be easily abused to bypass organizational 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.

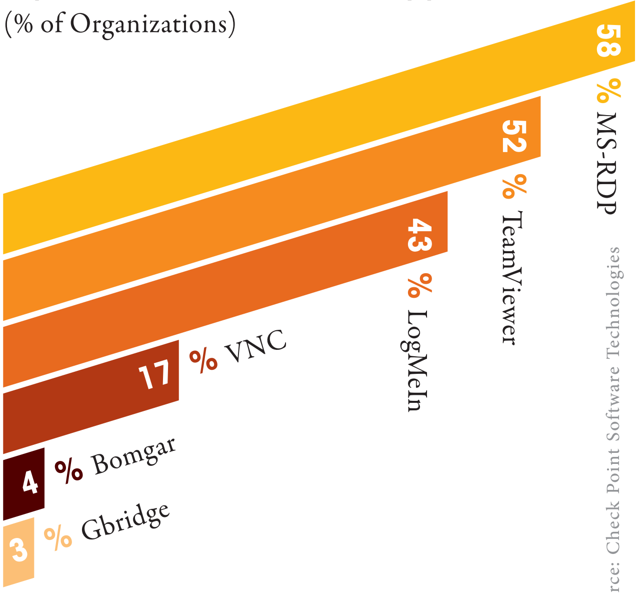
81% OF ORGANIZATIONS ARE USING **REMOTE ADMINISTRATION TOOLS**

Remote Administration Tools Used for Malicious Attacks

Remote Administration Tools (RAT) could be legitimate tools when used by admins and helpdesk. However, several attacks over the past years leveraged an off-the-shelf RAT to remotely control infected machines, further infiltrate networks, log keystrokes, or steal confidential information. Since Remote Administration Tools are usually essential business applications, they should not be blocked across the board; however, their usage should be monitored and controlled to prevent potential misuses.

When looking at the organizations in our research, 81% are using 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

From July to September 2011, an attack campaign tagged as :“Nitro” took place. Attackers used an off-the-shelf Remote Access Tool called Poison Ivy to sniff out secrets from nearly 50 companies, many of them in the chemical and defense industries. Poison Ivy was planted on Windows PCs whose owners were victims of a scam delivered via email. The emails touted meeting requests from reputable business partners, or in some cases, updates to antivirus software or Adobe Flash Player. When users opened the message attachment, they unknowingly installed Poison Ivy on their machines. From there the attackers were able to issue instructions to the compromised computers, troll for higher-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 that were successfully attacked were in the chemical and advanced materials trade - some of the latter with connections to military vehicles - while the other 19 were in a variety of fields, including the defense sector21. Nitro is not the only example of the misuse of RAT, other examples are the RSA breach, ShadyRAT and Operation Aurora. In all these cases Poison Ivy was utilized.

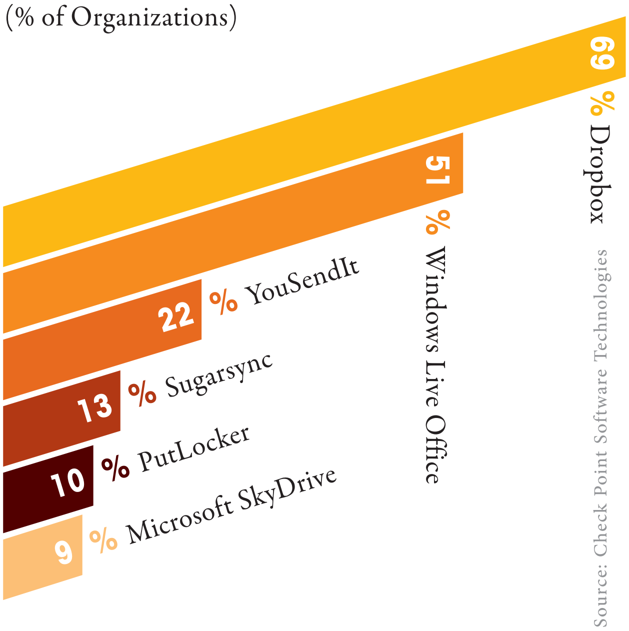
Sharing is Not Always Caring

The term ‘Sharing is caring’ usually means that if someone shares with others, they care about them. When sharing files using File Storage and Sharing Applications in workplace environments, this is not always the case. One of the prominent characteristics of Web 2.0 is the ability to generate content and share it, but this also presents a risk. Sensitive information can get into the wrong hands by sharing confidential files. Our research includes high risk File Storage and Sharing applications that may cause data leak or malware infection without user knowledge. Our research shows that 80% of organizations have at least one file storage or file sharing application running on their network. We found that 69% of events are a result of Dropbox usage. Windows Live Office is on the second place with 51%.

80% OF ORGANIZATIONS USE **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 per 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 are the most extensive users of high risk applications. There are cases where the use of some of these applications might be a legitimate use in an organization, for example the use of remote administration tools by help desk, therefore the horizontal bar in the chart indicates the probability level of legitimate usage in a business environment.

PERCENTAGE OF ORGANIZATIONS USING HIGH RISK APPLICATIONS PER INDUSTRY

(% of Organizations)

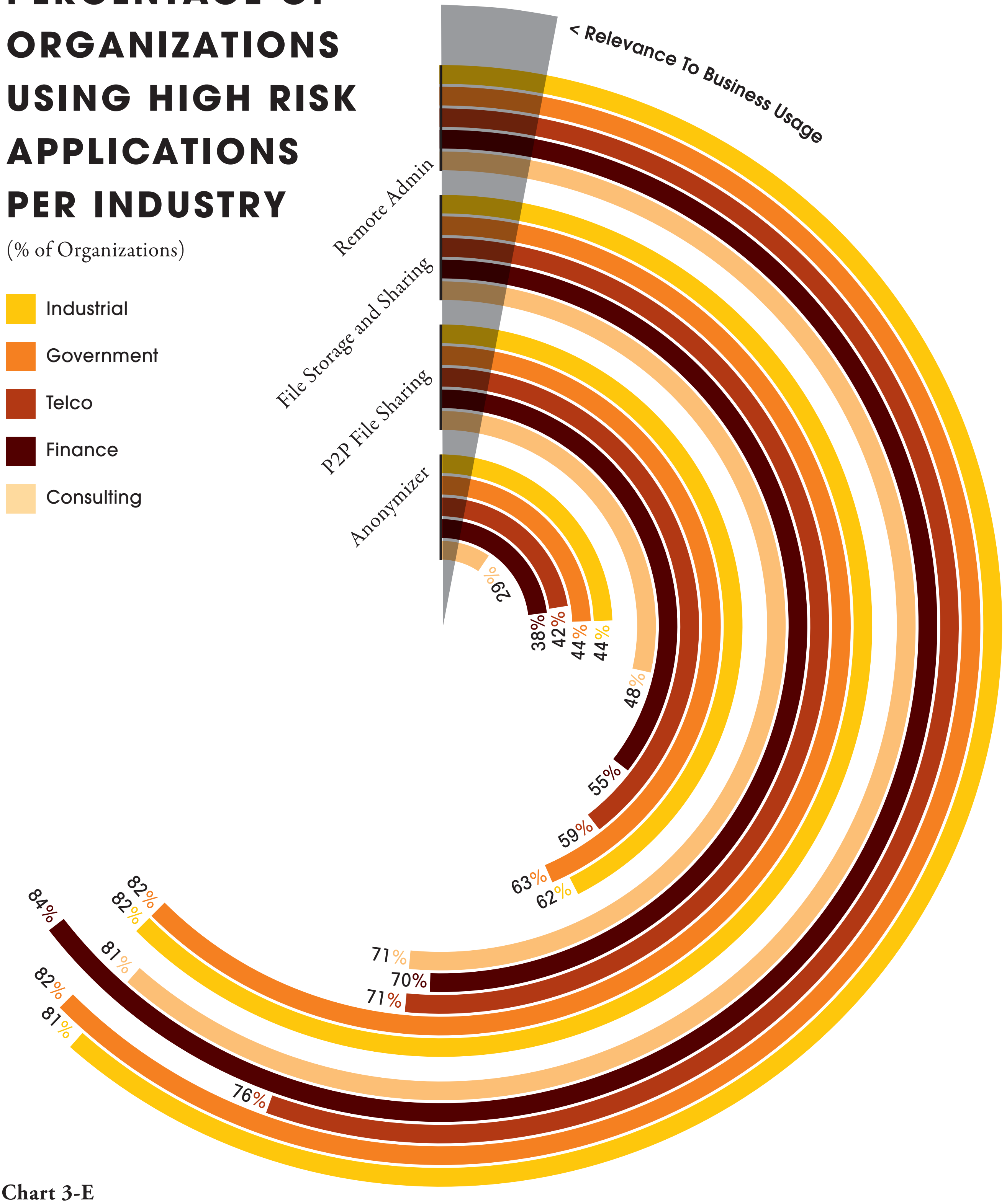


Chart 3-E

Source: Check Point Software Technologies

TWO MAJOR DROPBOX SECURITY INCIDENTS IN 2 YEARS

In July 2012, an attack on users of Dropbox took place. Dropbox user names and passwords exposed in breaches on another Web site 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' e-mail addresses. Spammers used those e-mail addresses to send spam[22].

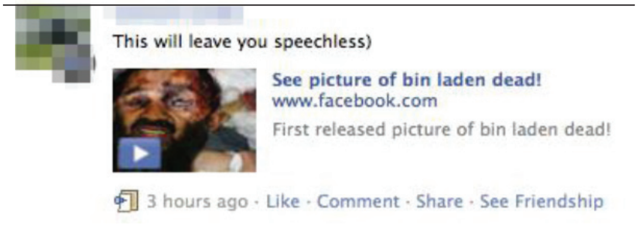
The incident illustrates a frequent tactic used by hackers. Hackers will often steal user names and passwords from sites which, at first glance, may not contain any valuable financial or personal information. Then, they will test those credentials across the Web sites of financial organizations, brokerage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

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

Legitimate Facebook Post or Virus?

With the increase in popularity of social networking on a constant rise, new challenges are 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 cause financial loss. Hackers are leveraging new socially-engineered hacking techniques to drive botnet activity. Embedded videos and links in social networking pages are becoming popular spots for hackers to embed malware. In addition to the security risks, social networking applications create a severe problem of network bandwidth hogging. Facebook is without a doubt the most accessed social network. Other social networks visited during a work day (but significantly less than Facebook) are Twitter and LinkedIn.

A Facebook link leading to a malicious site:



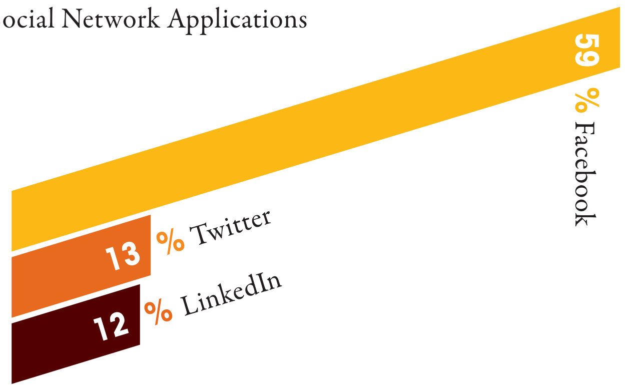
This will leave you speechless)

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

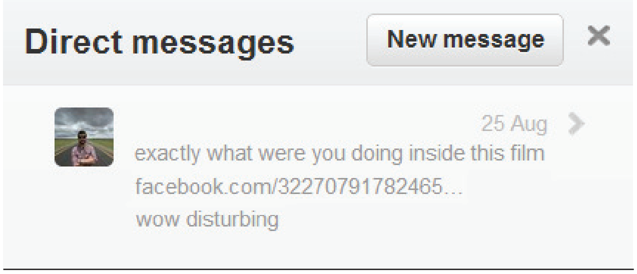


Source: Check Point Software Technologies

Chart 3-H

Social Engineering Attacks - Case Study

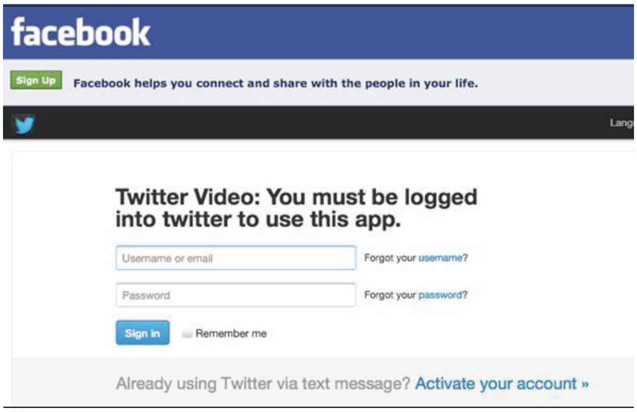
Recent attacks indicate that hackers are shifting the use of regular emails to social networks as a distribution channel. The following case is based on a real attack that took place in August 2012. Hackers used Twitter and Facebook social engineering technique to distribute malicious content. Using a compromised twitter account, the hacker sent direct messages to all the followers of the owner of the hacked account. The message reads: “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 points to a Facebook app which requires “Twitter Login”. The login screen is actually a web server owned by the hacker that is used to harvest the recipient’s twitter credentials.



Facebook helps you connect and share with the people in your life.

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

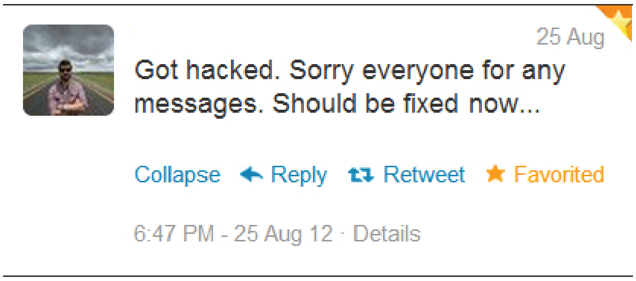
Username or email — Forgot your username?

Password — Forgot your password?

Already using Twitter via text message? Activate your account »

Using the twitter credentials, the hacker can now repeat the same process using the new hacked account to easily get even more passwords. The hacker can use these stolen credentials with other services such as Gmail, Facebook etc. but worse than that, it can be used to login to bank accounts or even to business related services such as SalesForce and others.

After the malicious message was redistributed (but this time to all the followers of the poor hacked user), the only effective thing that could be done in this situation 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

How do you Enable an 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 the more traditional URL-based aspect of the web – websites. As many sites (such as Facebook) enable running numerous applications based on their URL, it is essential to have granularity beyond the URL level – for example Facebook chat or gaming applications. Once this is achieved organizations should be able to easily block applications that can endanger their corporate security.

Enable Social Media for Business

There are cases where organizations choose to block Facebook entirely, but Facebook is an essential business tool for many businesses. Companies often publish information about upcoming webinars, events, information about latest releases and products, links to interesting articles and videos.

How can we enable use of Social Media in the organization while not compromising its security? By controlling features and widgets within apps and platforms. By being able to allow Facebook while blocking the less business relevant parts of it, it is possible to make Social Media usable while minimizing its security risks.

Different Users have Different Needs

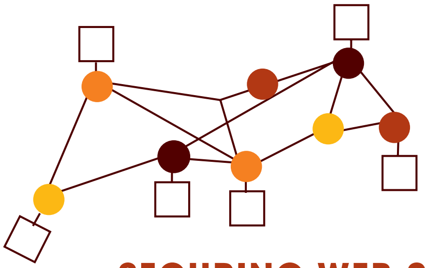
Different users in the organization have different needs, and the security policy should support the business, not interfere with it. For example, a sales person may use Facebook to stay in touch with customers and partners, whereas an IT staff member may use Facebook to get the latest industry news. So how do we make sure users get the access they need? Is it practical to expect the security manager to know what each user or group should or shouldn't be accessing?

A practical solution needs to have granular user-, group- and machine-awareness to easily distinguish between employees and others (i.e., guests and contractors).

Another important aspect is the capability to educate and engage end-users real-time when they use applications. When a user goes to a questionable site or starts a questionable application, a pop up message can ask the user to justify the business case for doing so, his or her response is logged and monitored, while the message can also educate the user on business use policy, and make him or her aware that usage of such applications are being audited.

'Understanding' is a Critical Component of Web Control

Administrators must have an overall view of web security events to ensure web control. A security solution that can provide clear and broad visibility into all Web Security events is needed. The solution should provide visibility and monitoring capabilities such as a timeline of events and a comprehensive list of these events that can be filtered, grouped and sorted by user, application, category, risk level, bandwidth usage, time and more. It is also important to be able to generate offline reports to show top categories, apps, sites and users to allow 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 CONTROL 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. It is not just stopping an application from running. Securing Web 2.0 requires an integrated approach of multi-layer protection: URL filtering, application control, malware protection and bot protection - all incorporating user awareness, user education, sophisticated monitoring and event analysis tools for keeping administrators in 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, and the vast majority of the corporate data is sensitive at various levels. Some are confidential simply because it includes internal corporate data and was not meant to be publicly available. Other types of data might be sensitive because of corporate requirements, national laws, and international regulations. But in many cases the value of data is dependent upon its confidentiality - consider intellectual property and competitive information.

To make the matter even more complex, along with the severity of data leakage, we now have tools and practices which make an irreversible mistake that much easier to happen: cloud servers, Google docs, and simple unintentional abuse of company procedures - such as an employee taking work home. In fact, most cases of data leakage occur because of unintentional leaks.

Data Leakage Can Happen to Any of Us

Data leakage can occur not only at the hands of a cybercriminal, but also unintentionally at those of 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. Any of these scenarios may inadvertently happen to any of us, 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 needs to define which data should not be sent outside the organization, many variables need to be taken into account. What type of data is it? Who owns it? Who is sending it? Who is the intended receiver? When is it being sent? What is the cost if

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 data loss incidents caused unintentionally by employees during 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. Eleven emails intended for a lawyer working on a case ended up being sent to another email address due to a typing mistake.

Japan's newspaper **Yomiuri Shimbun** fired one of its reporters during October 2012, for accidentally sending sensitive investigative information to the wrong people. The reporter meant to send some of his research findings to colleagues via email, but instead 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. An email was sent to the president of the graduating class containing an attached spreadsheet revealing the grade point average of every senior. Unaware of the additional attachment, the president then forwarded the message to another 258 students. The original intention was to email only a single spreadsheet that contained names and residences so students could confirm their mailing addresses[25].

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].

business processes are disrupted because the security policy is stricter than needed?

In our research, we analyzed traffic being sent from inside the organizations to the outside. We examined both HTTP and SMTP traffic. For example, in the case of emails sent to an external recipient, a Check Point device inspected the email body, email recipients and email attachments (even if zipped). We also inspected web browsing activities, such as web posts and web mails. As a security policy on these devices, we configured out-of-the-box pre-defined data types to detect sensitive data, forms and templates (such as credit card numbers, source code, financial data and more) that might indicate a potential data leakage if falling into the wrong hands. A detailed list of data types can be found in Appendix D.

Potential Data Loss in Your Organization

In our research, we found that 54% of organizations had at least one event which might indicate a potential

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

(% of Organizations)

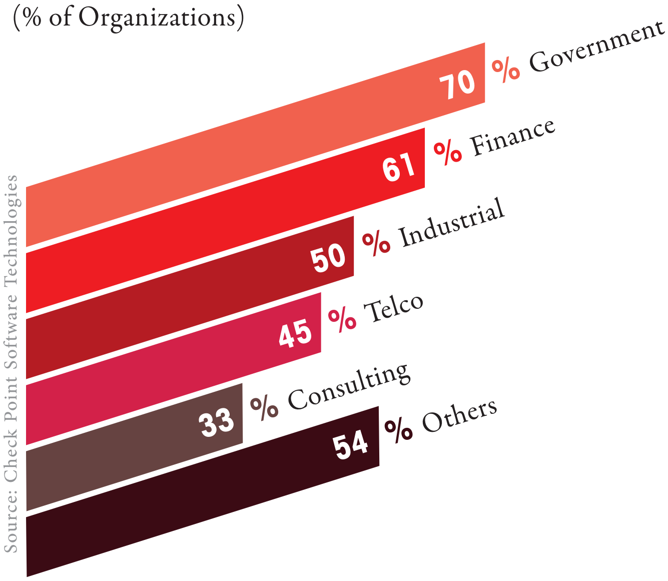
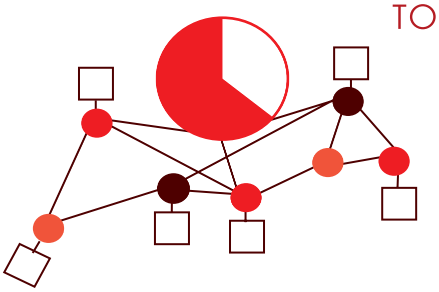


Chart 4-A

data loss event in an average time of 6 days. We took into account events that included internal information (see list of data types in Appendix D) which was sent to external resources, either by sending to an external email recipient or posting online.

Our research indicates that Governmental and Financial organizations are in high risk of potential data loss (see chart 4-A).

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



Internal Emails Sent Outside the Organization

In many cases, data loss events occur unintentionally through an employee sending email to the wrong recipient. In our research we looked at two types of emails that might indicate such cases. The first type consists of emails that are sent with internal visible recipients (To and CC) and external recipients in the BCC field. Such emails, in most cases, seem to be internal but are actually leaving the company. The second type consists of emails sent to several internal recipients and a single external one. Such emails are usually sent unintentionally to a wrong external recipient. One or both of these types of events were found in 28% of organizations examined.

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

Chart 4-C shows the top data types sent to parties outside the organization.Credit card information is leading the list, while source code and password protected files follow.

Is your Organization PCI Compliant?

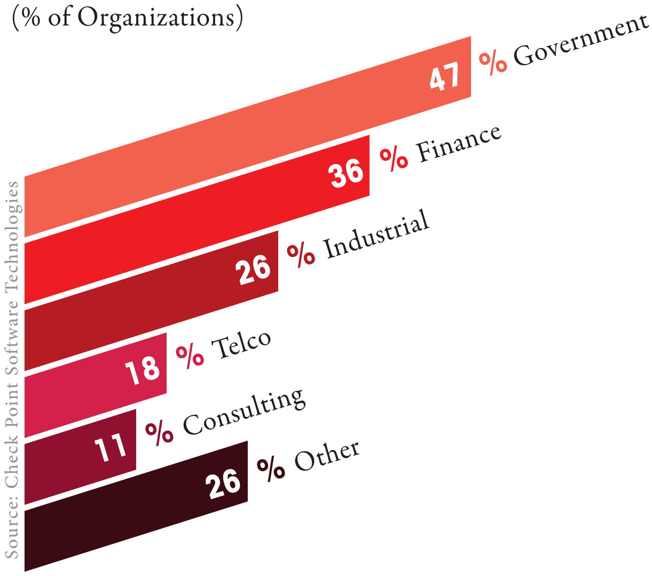
Employees send credit card numbers over the Internet, their own and customers' numbers. They send customer payment receipts that contain a credit card number in an email attachment. They reply to a customer email that originally contained his credit card number in the email's body. Sometimes employees even send spreadsheets with customer data to private email accounts or to a business partner. Often, credit card number-related incidents are a result of a broken business process or lack of employees' 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 resources.

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

In our research, we inspected outgoing traffic from organizations and scanned the content in all message parts, including attachments and archives, searching for emails containing credit card numbers or cardholder data. The inspections are based on regular expressions, validation of check digits, and PCI DSS compliance regulations.

Percentage of Organizations per Industry in which Credit Card Information was Sent to External Resources

(% of Organizations)



Source: Check Point Software Technologies

Chart 4-B

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

DATA SENT OUTSIDE THE ORGANIZATION BY EMPLOYEES

(% of Organizations)

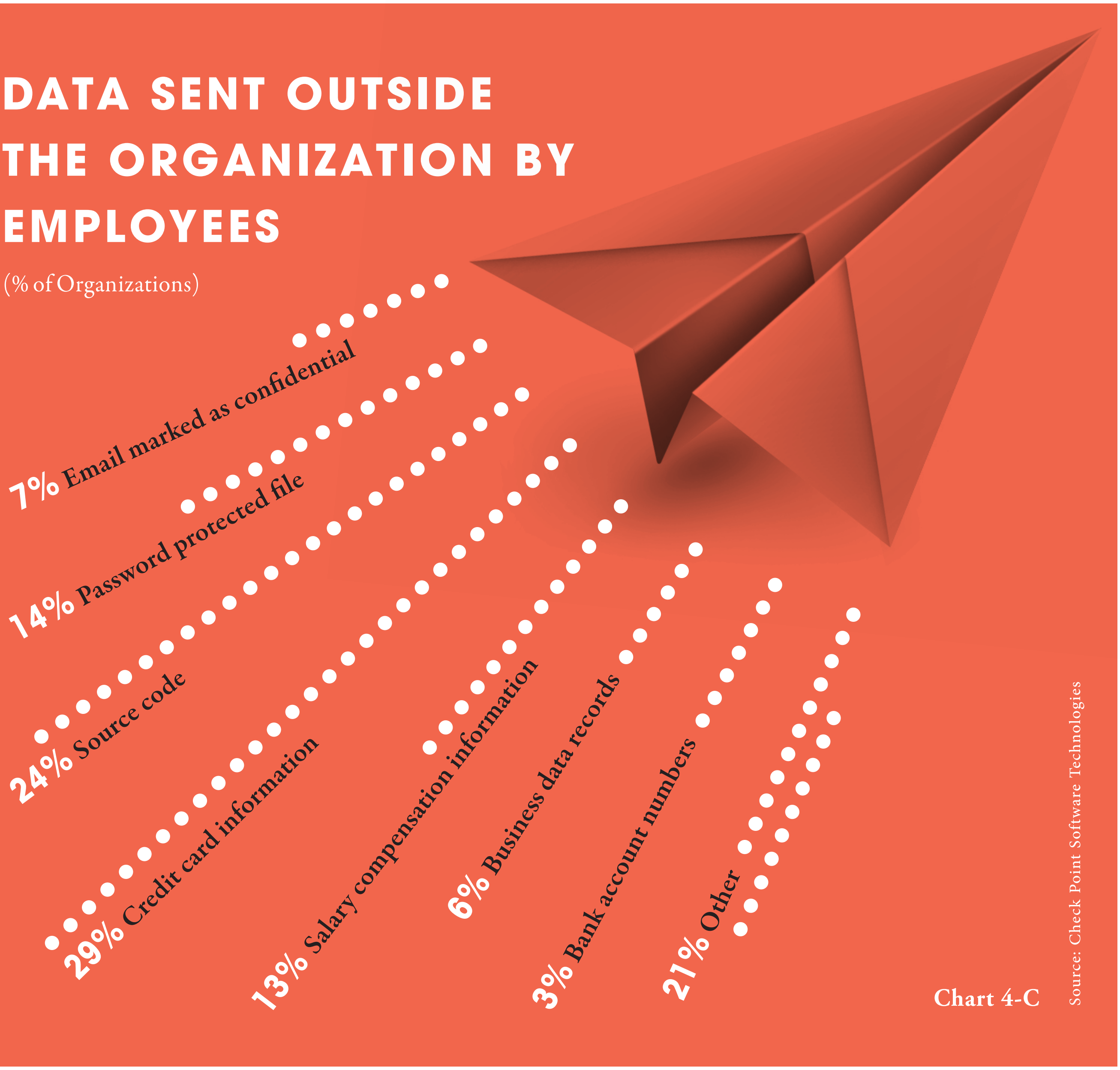


Chart 4-C

Source: Check Point Software Technologies

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

HIPAA

The HIPAA Privacy Rule provides federal protections for personal health information and gives patients 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 patient care and other important purposes.[27]

The HIPAA Privacy Rule permits health care providers to use email to discuss health issues with their patients, provided they apply reasonable safeguards. Encryption is not mandated; however, other safeguards should be applied to reasonably protect privacy. How do you keep email communication channels open with patients and partners while safeguarding privacy and keeping organizations compliant with HIPAA?

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 identifying personal information (such as Social Security Number) and related medical terms (CPT, ICD-9, LOINC, DME, NDC terms, etc.). We found that in 16% of Healthcare and Insurance organizations, HIPAA - Protected Health Information was sent outside the organization, to an external email recipient or posted online.

SECURITY RECOMMENDATIONS

In today's world of increasing data losses, organizations have little choice but to take action to protect sensitive data. The best solution to prevent unintentional data leaks is to implement an automated corporate policy that will catch protected data before it leaves the organization. Such a solution is known as Data Loss Prevention (DLP). Content-aware DLP products have a broad set of capabilities, and organizations have multiple options for approaching deployments. Before deploying the DLP solution, organizations need to develop clear DLP strategies with concrete requirements such as what is considered to be confidential information, who can send it, and so on.

IN 16%

OF HEALTHCARE AND INSURANCE ORGANIZATIONS, HIPAA - PROTECTED HEALTH INFORMATION WAS SENT OUTSIDE THE ORGANIZATION

Data Classification Engine

High accuracy in identifying sensitive data is a critical component of a DLP solution. The DLP solution must be able to detect personally identifiable information (PII), compliance-related data (HIPAA, SOX, PCI data, etc.), and confidential business data. It should be inspecting content flows and enforcing policies in the most widely used TCP protocols, including SMTP, FTP, HTTP, HTTPS and webmail. The DLP solution should also be able to inspect by pattern matching and file classification, in order to identify content types regardless of the extension applied to the file or compression.

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 not enough, because it cannot identify this intention and respond to it. Hence, a good DLP solution must engage the users in order to get optimal results. One such way is to empower users to remediate incidents in real time – the DLP solution should inform the user that his action might result in a potential data leak incident, and empower the user to decide to discard the message or to send it anyway. This improves security with raised awareness of data usage policies by alerting users of potential mistakes and allowing for instant remediation, while it allows for quick authorization of legitimate communications. This also makes management easier. While the administrator can track DLP events for analysis, there is no need to personally attend in real time to every request to send data outside the company.

Protection Against Internal Data Breaches

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

Data Protection for Endpoint Hard Drives

Companies must secure data on their laptops as part of a comprehensive security policy. Without securing data, outsiders can obtain valuable data through lost or stolen laptops which 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 ending up in the wrong hands via USB storage devices and other removable media, encryption and prevention of unauthorized access are required for these devices. Employees are often mixing personal files such as music, pictures, and documents with business files such as finance or human resource files on portable media which makes it even more challenging to maintain control over corporate data. By encrypting removable storage devices, security breaches can be minimized in case devices are compromised.

Document Protection

Business documents are uploaded to the web by file-storage applications, sent to personal smartphones, copied to removable media devices and shared externally with business partners on a regular basis. Each of these operations put sensitive data at risk of being lost or used improperly or accessed by non-authorized individuals. In order to keep corporate documents secured and protected, a security solution must be able to enforce a document encryption policy and grant access only to authorized individuals.

Event Management

Defining DLP rules to meet the organization's data usage policies should go with good 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 visibility into the information being sent outside, their sources and the ability to act in real time when needed.

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 fits today's fight against cyber warfare - the best network security is realized when all the different layers of protection are harmonized together to fight against all the 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 are a constant and real threat to organizations' security. The report presented that some web applications used by employees can compromise network security. Finally, the report disclosed that employees engage 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 achieve the level of security needed to protect an organization acknowledges that technology alone is not enough. Security needs to grow from a collection of disparate technologies and practices, to an effective business process. Check Point recommends that organizations look at three dimensions when deploying a security strategy and solution: Policies, People, and Enforcement.

Policies

Security starts with a widely understood and well-defined policy—closely aligned to business needs rather than a collection of system-level checks and disparate technologies. Policies should take into account that the priority is the business and should suggest ways to conduct business in a secure manner, as part of the corporate policy. For example, during the analysis we found that employees are using web applications that are necessary for the business flow but might also compromise security. If we deploy only technologies that block usage of such web applications, it would result in people flooding the security administrator with complaints, or even worse, finding ways to overcome the policy and creating security issues. Instead, Check Point recommends that you create a policy that acknowledges cases where the use of such applications may be needed and define the procedure to enforce usage in a secure manner. Users should be advised automatically of the policy when needed.

People

Users of computer systems are a critical part of the security process. It is often users who make mistakes that result in malware infections and information leakage. Organizations should ensure users are involved in the security process. Employees need to be informed and educated on the security policy and what is expected of them when browsing the Internet or sharing sensitive data. At the same time, security should be as seamless and transparent as possible and should not change the way users work.

Implementation of a security program should include:

- An education program – ensuring that all users are aware that systems are potentially vulnerable to attacks and that their own actions may allow or help prevent them.
- Technology - advising people in real time as to why certain operations are risky and how they could conduct them 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 is entering or leaving the network. This validation should be done in 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), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to develop new innovations 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 for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point‘s award-winning ZoneAlarm solutions protect millions of consumers 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 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 effective business process. With 3D Security, organizations can now implement a blueprint for security that goes beyond technology to ensure the integrity of all information security.

Check Point 3D Security enables organizations to redefine security by integrating these dimensions into a 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- network, data, application, content and user

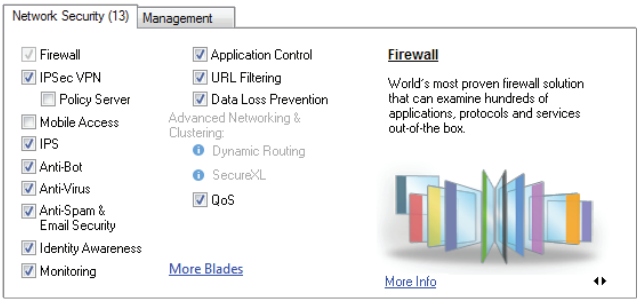
Check Point Software Blade Architecture

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. The Software Blade architecture is the first and only security architecture that delivers total, flexible and manageable security to companies of any size. What's more, as new threats and needs emerge, Check Point Software Blade Architecture quickly and flexibly extends security services on-demand—without the addition of new hardware or management complexity. Solutions are centrally managed through a single console that reduces complexity and operational overhead. Multilayered protection is critical today to combat dynamic threats such as bots, Trojans and Advanced Persistent Threats (APTs). Firewalls today are more like multi-function gateways but not all companies want the same security everywhere. Companies are looking for flexibility and control of their security resources.

Software Blades are security applications or modules such as a firewall, Virtual Private Network (VPN), Intrusion Prevention System (IPS), or Application Control to name a few, 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 a simple click of a mouse—no hardware, firmware or driver upgrades required. And as needs evolve, additional Software Blades can be easily activated to extend security to an existing configuration on the same security hardware.

Check Point offers a centralized event management for all Check Point products as well as third-party devices. Providing security events real-time views to help quickly grasp the security situation and take immediate actions, all 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



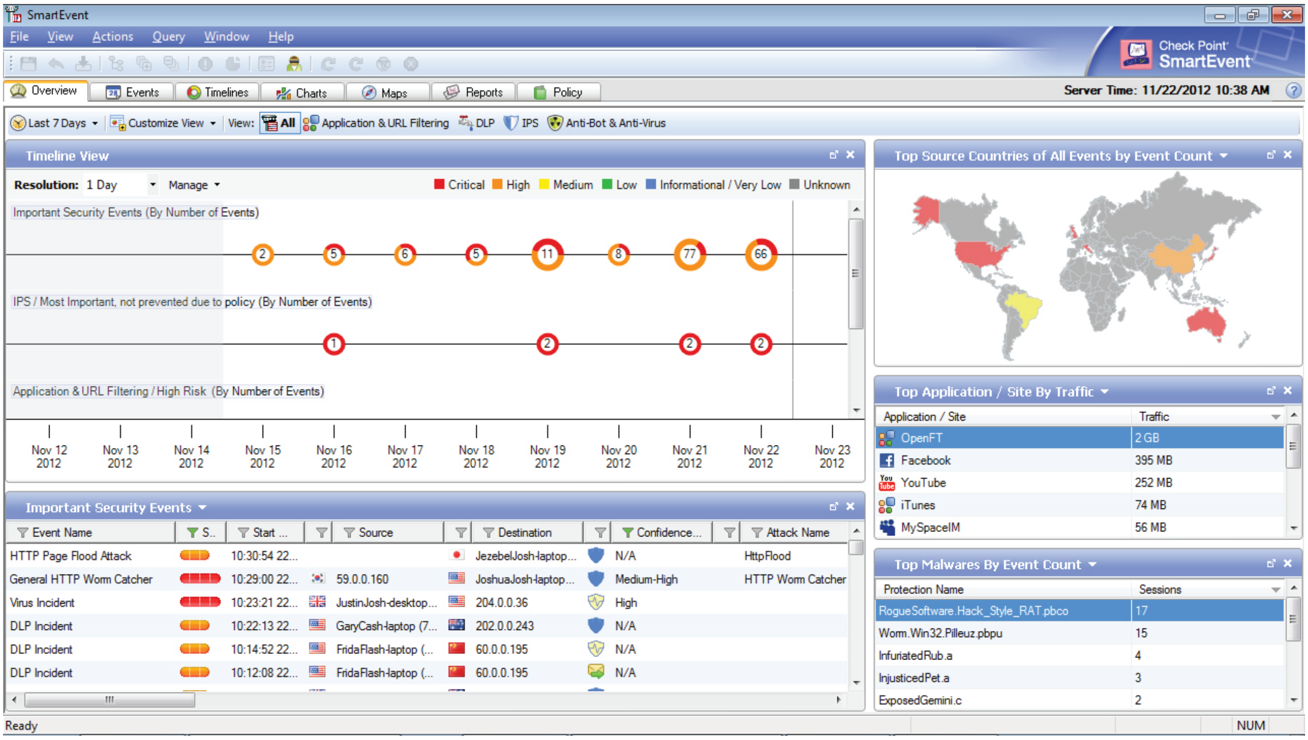
☑ Firewall
☑ IPSec VPN
□ Policy Server
□ Mobile Access
☑ IPS
☑ Anti-Bot
☑ Anti-Virus
☑ Anti-Spam & Email Security
☑ Identity Awareness
☑ Monitoring

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

Firewall

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

Check Point SmartEvent security events management. Real-time overview.



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 knowledge base 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 allowing gateways to investigate always-changing IP, URL and DNS addresses where Command and Control Centers are known. 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—they are devices presented with an ever-increasing number of sophisticated threats. They must use multiple technologies to control network access, detect sophisticated attacks and provide additional security capabilities like data loss prevention, protection from web-based threats and securing the increasing number of mobile devices such as the iPhone and Tablets in enterprise networks. These increased threats and security capabilities demand greater performance and versatility from security appliances.

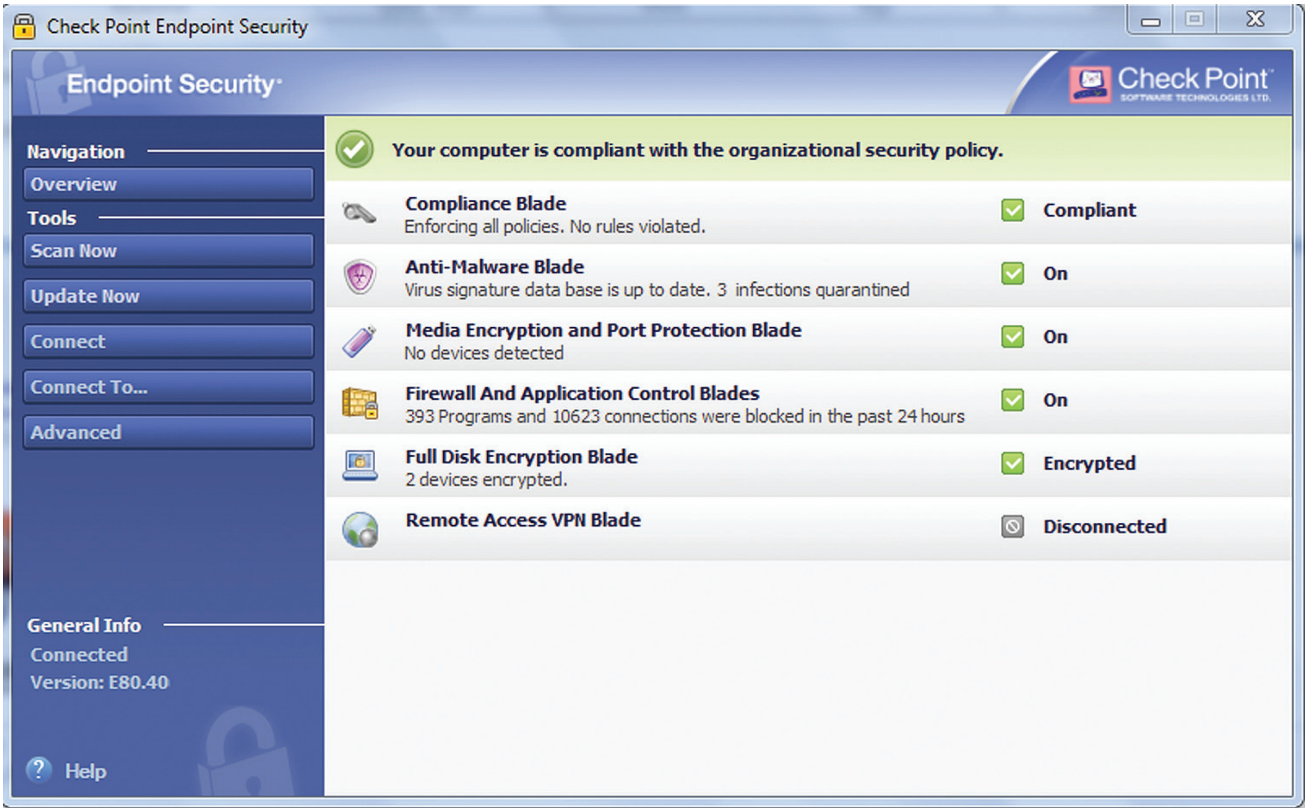
Empowered by Check Point GAiA, the next-generation security operating system, Check Point appliances combine high performance multi-core capabilities with fast networking technologies-providing the highest level of security for data, network and employees. Optimized for the extensible Software Blades 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-providing the 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 all of an organization business security needs. Introduced in August 2011, SecurityPower™ is a metric that measures the capacity of an appliance to perform multiple advanced functions in a specific traffic volume. It provides a revolutionary benchmark that enables customers 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 to deploy only the protection needed, with the freedom to increase security at any time. **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 traveling or 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** proactive protection for inbound and outbound traffic prevent malware from infecting endpoint systems, block targeted attacks and stop unwanted traffic. The Security Compliance Verification assures that your endpoints will always meet the organizational security policy required. **WebCheck Secure Browsing Software Blade** protects against the latest web-based threats including drive-by downloads, phishing sites and zero-day attacks. Browser sessions run in a secure virtual environment.

Check Point Endpoint Security client



Connected
Version: E80.40

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

Zwangi is an adware that targets Microsoft Windows platform. 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 platform. This bot, reportedly, 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 get started after system reboot.

Juasek is a backdoor bot that targets Microsoft Windows platform. This malware allows a remote un-authenticated attacker to perform malicious actions such as open a command shell, download or upload files, create new processes, list/terminate processes, search/create/delete files, and retrieve 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 hooks network functions and monitors a user's Internet activities to steal critical financial information. In addition, it has Backdoor functionality to provide remote attackers with unauthorized access on infected computers. The accepted control commands include download of other malicious files, collecting cookies and certificates information, reboot and shutdown of the system, sending out log information, taking screen snapshots, setup of socket connection to a remote host for other activities, etc. Moreover, the malware injects itself into processes and may inject other malicious files into target processes as well.

B APPENDIX B: TOP HIGH RISK APPLICATIONS

This appendix provides provide further information related to the top 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, including „visits to Web sites, 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 tocircumvent 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 pieces 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 saving.

Soulseek is a peer-to-peer file sharing application. It is used mostly to exchange music, although users are able to share a variety of 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 are designed for 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. VNC also runs of the Java platform and on the Apple iPhone, iPod touch or iPad.

File Storage and Sharing Applications

Dropbox is an application that allows users to share files. Dropbox is a file hosting service operated by Dropbox, Inc. that offers cloud storage, file synchronization, and client software. In brief, Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of the computer it is viewed on. Files placed in this folder are also accessible through a web site and mobile phone applications.

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

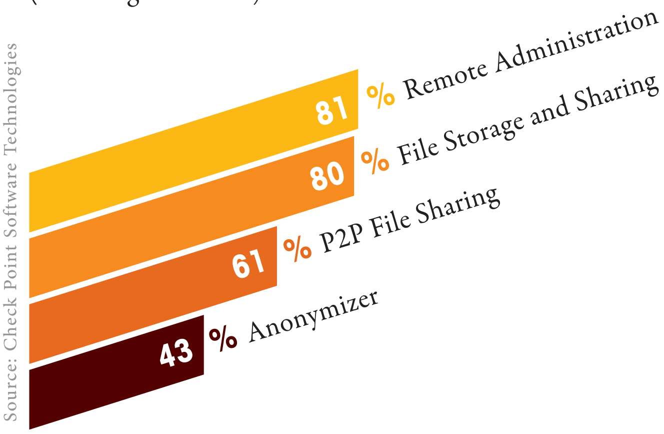
YouSendIt is a digital file delivery service. The service allows users to send, receive and track files on demand.

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 per category and per region.

Applicaiton Usage per Category

(% of Organizations)

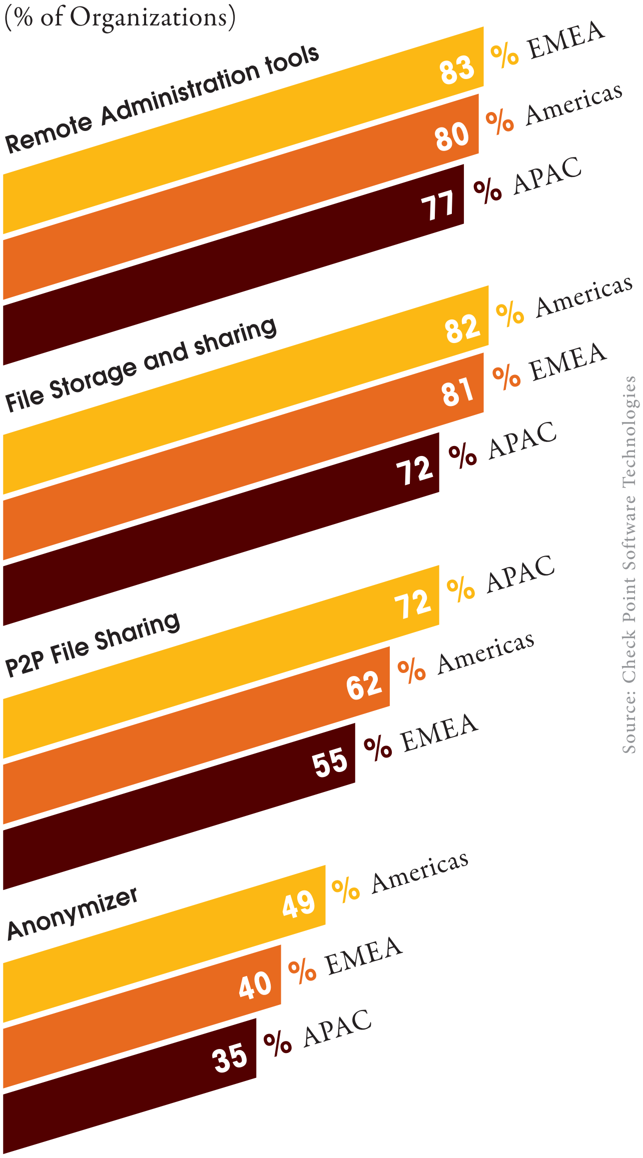


Source: Check Point Software Technologies

Chart C-A

Application Usage per 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 dozens of various data types 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 Cart 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 its storage. 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 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