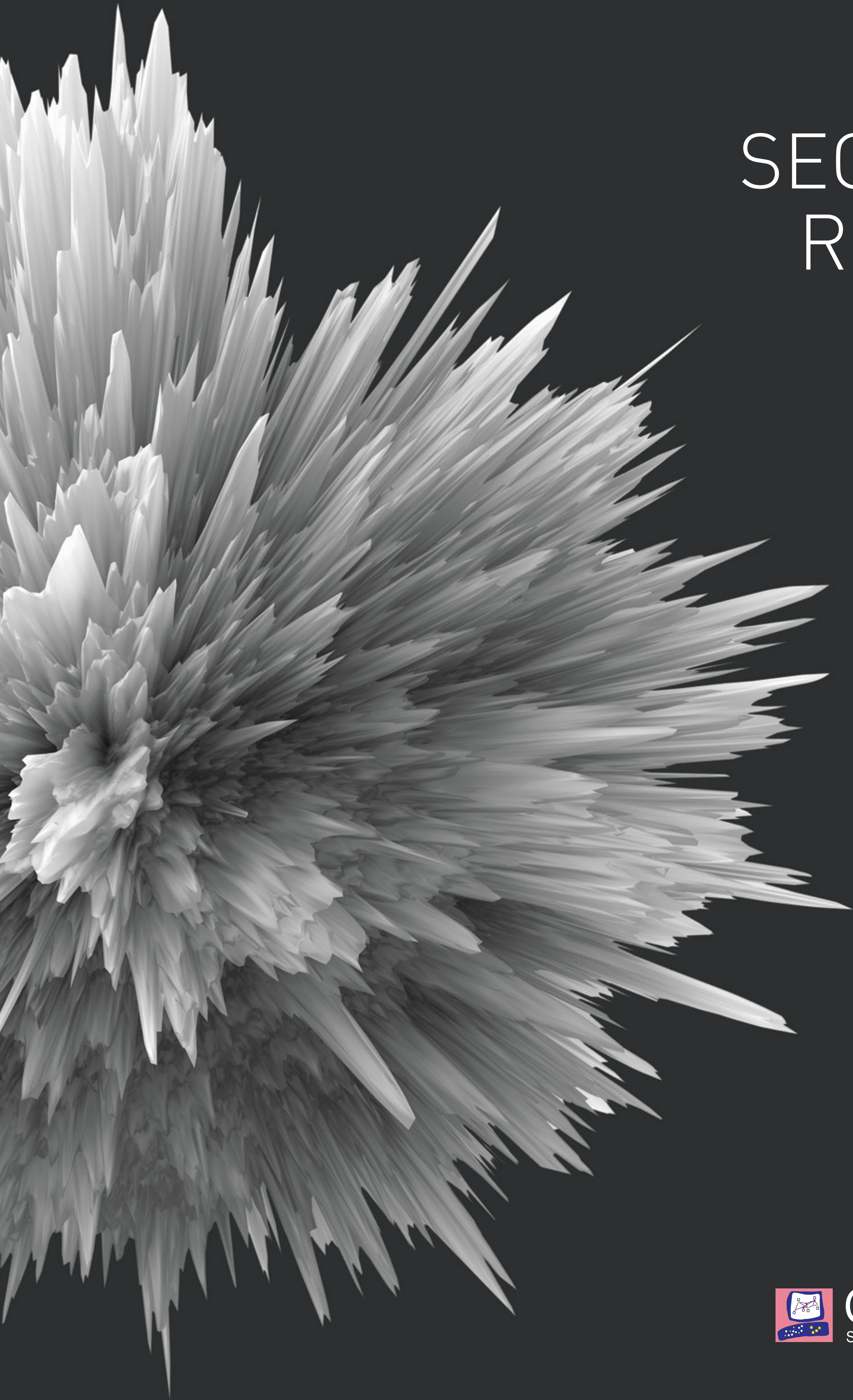


2015 SECURITY REPORT

Check Point®
SOFTWARE TECHNOLOGIES LTD

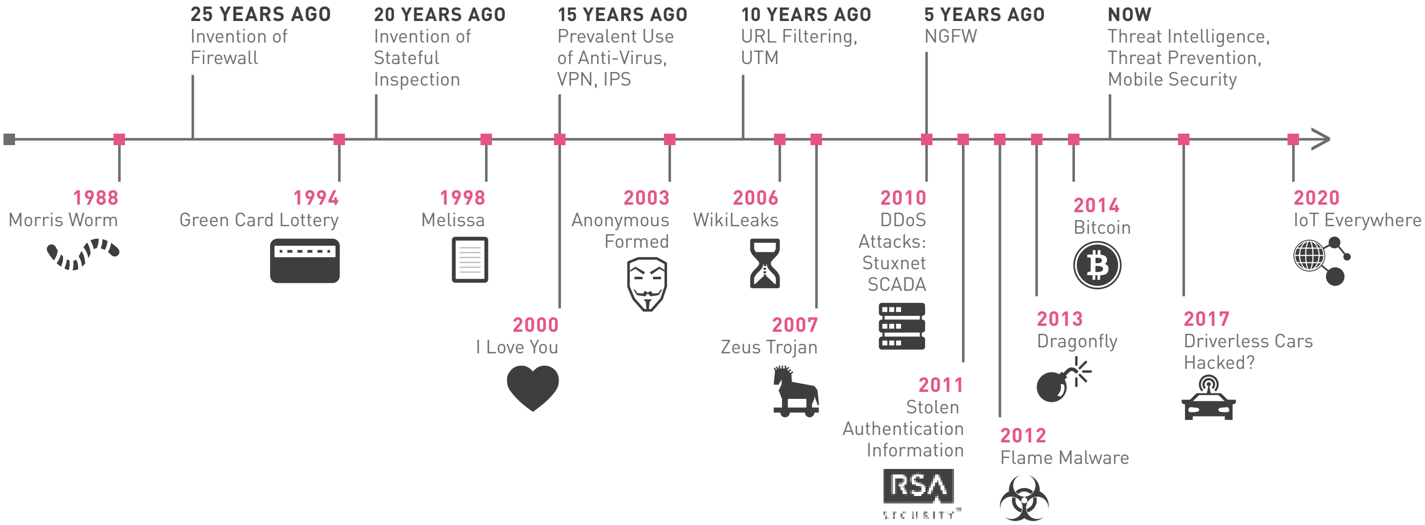
CHECK POINT
2015 SECURITY REPORT

01 INTRODUCTION AND METHODOLOGY

“The first time you do something, it’s science. The second time you do something, it’s engineering.”[1]

–Clifford Stoll, astronomer, author, digital forensics pioneer

THE EVOLUTION OF MALWARE



In science, it's all about discovery—studying cause and effect. Once something is understood and can be predicted, it then becomes a process of engineering, to replicate. In the world of cyber threats, it's the same. Cyber criminals are studying structures and thinking through how certain factors can spur desired outcomes. Once they have a predictive model, they set about engineering how to unleash what they've designed, for the greatest effect.

What are their tools?

1. **Malware**—malicious software code that hackers develop to either create disruption or to steal data. When malware becomes known, signatures are created to help identify, filter, and block it in subsequent deployment attempts. And that's when they turn to tampering with the code to create fresh unknown malware.
2. **Vulnerabilities**—defects in software or operating systems that hackers seek to exploit, which exist in almost all applications.
3. **Mobile Devices**—smartphones, Fitbits, iPads, and other mobile devices might not be tools, per se, but they can be hijacked to give hackers the ability to penetrate corporate networks.

During 2014, Check Point saw significant exploits of vulnerabilities in open source software, as well as in common applications by Adobe and Microsoft.

Known malware remained steady, continuing to be pervasive and inflicting damage. But with the creation of signatures to help identify, filter, and block subsequent deployment attempts of known malware, the focus among hackers changed. They looked to something easier and more rewarding: launching new attacks with unknown malware by slightly modifying what already existed—enabling it to evade detection. It's this area—unknown malware—that exploded and caught most people's attention during 2014. Launching at unprecedented rates, new malware seemed to have a singular purpose: stealing data.

AN AVERAGE DAY
AT AN ENTERPRISE ORGANIZATION

EVERY 24 SECONDS
a host accesses a malicious website

EVERY 34 SECONDS
an unknown malware is downloaded

EVERY 1 MINUTE
a bot communicates with its command and control center

EVERY 5 MINUTES
a high-risk application is used

EVERY 6 MINUTES
a known malware is downloaded

EVERY 36 MINUTES
sensitive data are sent outside the organization

1.1 SOURCE: Check Point Software Technologies

"The first computer viruses hit computers in the early 1980s, and essentially we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them....We've got to be just as fast and flexible and nimble in constantly evolving our defenses."[2]

-President Barack Obama

Contributing to the problem: cultural shifts. Mobility, virtualization and other new technologies have changed the way we work. And in the process, businesses have rushed to adopt these tools to boost productivity and efficiency. But they've done so without considering the security implications. While they are quite focused on stability and uptime, they don't realize that better-secured environments have higher uptimes.

Between the frequency of the breaches and the high profiles of the businesses targeted, 2014 sent all organizations a clear message: **Everyone is at risk.**

And when world leaders choose to focus on cyber security as they address their nations, it seems clear that cybercrime has reached a critical point.

METHODOLOGY

During 2014, Check Point collected event data from three different sources around the world to shine a light on security trends, and identify issues that are on the rise or, in some cases, in decline.

Sources of Check Point Research:

1. From security events found during more than 1,300 organizations' Security Checkups.[3] This information hailed from businesses from all industries around the globe.

2. From events discovered through Check Point ThreatCloud®, which is connected to security gateways of more than 16,000 organizations.

3. From more than 3,000 gateways connected to our ThreatCloud Emulation Services.

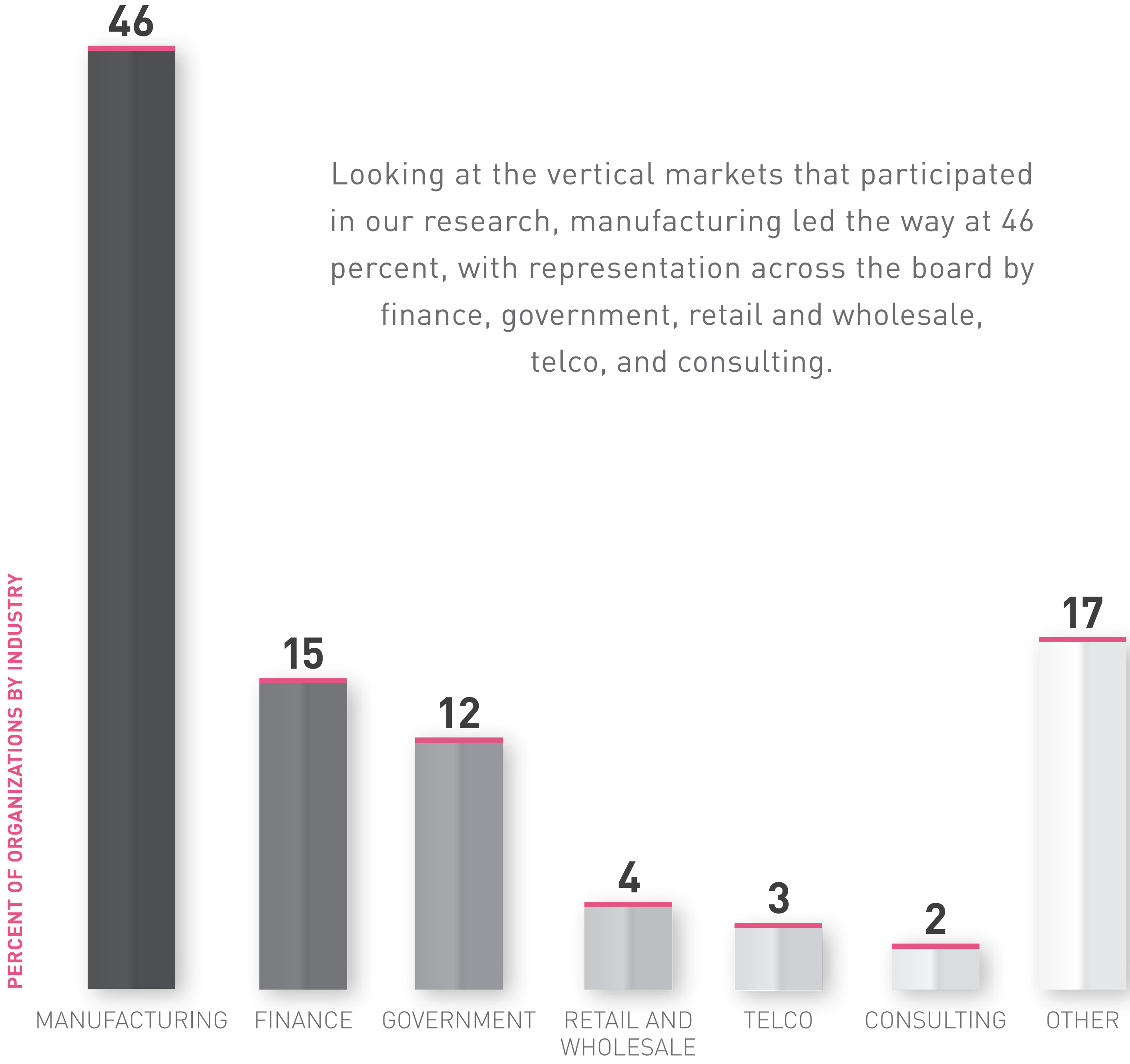
What did we look at?

Unknown Malware
Known Malware
Intrusion Prevention
High-Risk Applications
Data Loss Incidents

Almost every organization that was studied **experienced attacks due to high-risk applications**

81%
of the organizations sampled had suffered a data loss incident

CHECK POINT RESEARCH CROSSED ALL INDUSTRIES

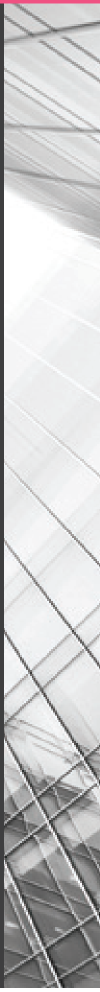


Looking at the vertical markets that participated in our research, manufacturing led the way at 46 percent, with representation across the board by finance, government, retail and wholesale, telco, and consulting.

1.2 SOURCE: Check Point Software Technologies

Security Statistics in 2014

- New malware increased 71%.[4]
- 106 downloads of unknown malware occurred per hour.
- 86% of organizations accessed a malicious site.
- 83% of organizations had existing bot infections.
- 42% of businesses suffered mobile security incidents costing more than $250,000 to remediate.
- 96% of organizations used at least one high-risk application.
- 81% of organizations suffered a data loss incident.
- Loss of proprietary information increased 71% over the past three years.



In the following pages, Check Point reveals the findings of our in-depth analysis of security threats and trends uncovered in 2014. Our aim is to help security and business leaders understand the threat landscape and how to create the strongest security posture possible.

> *"Hackers don't take realities of the world for granted; they seek to break and rebuild what they don't like. They seek to outsmart the world."*[5]
>
> -Sarah Lacy, journalist and author

02

UNKNOWN MALWARE: THE VAST UNKNOWN

"There's always the risk that there are unknown unknowns."[6]

–Nate Silver, statistician, journalist

106 unknown malware hit an organization every hour

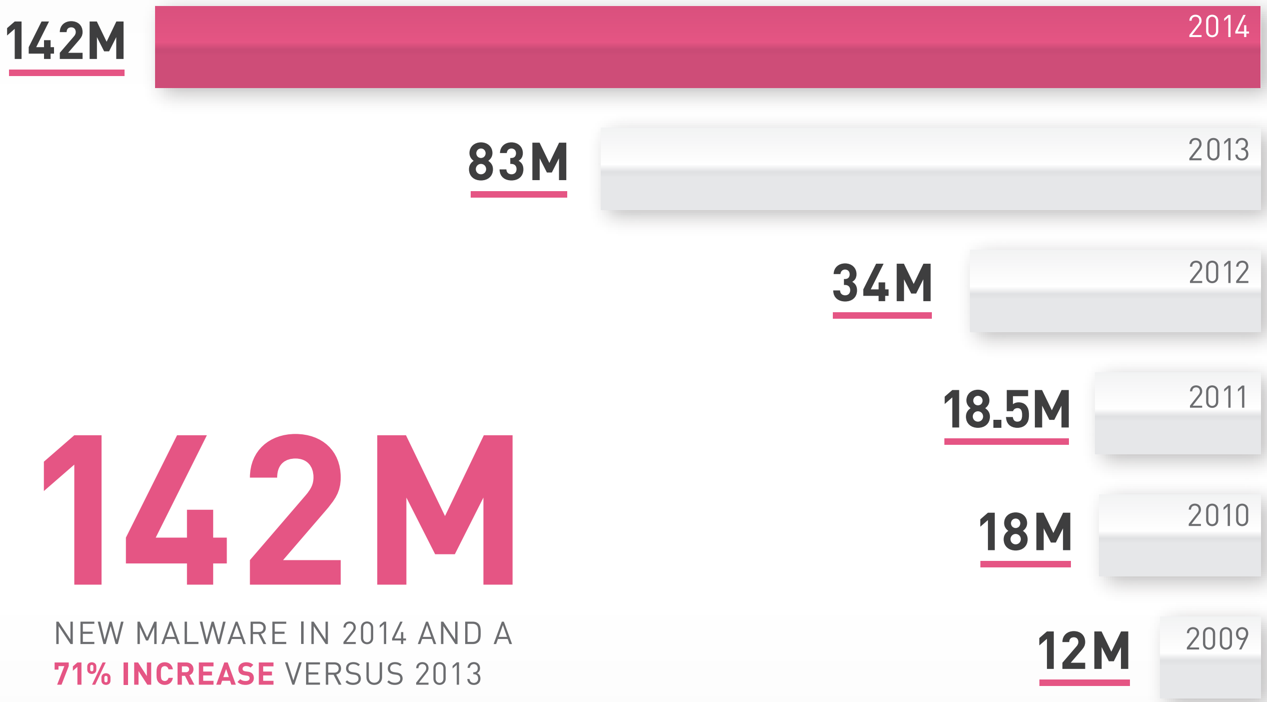
Unknown malware is malware typically not recognized or known by anti-virus systems. Each new unknown malware variant, even if it only has minor alterations, is potentially capable of bypassing the most current anti-virus and virtual sandbox protections.

While we saw an explosion of unknown malware last year, it was merely the tip of the iceberg, when viewed through today's lens. Now, the rate of zero-day and unknown malware is massive. **From 2013 to 2014, new malware jumped just over 71 percent** from 83M to 142M, according to AV-Test, an independent service provider of anti-virus research. And, more malware was found in the past two years than in the previous 10 years combined.

During 2014, **Check Point analyzed more than 3,000 gateways and found that 41 percent of organizations downloaded at least one infected file with unknown malware—almost a 25 percent increase from the previous year.**

Worse is the speed at which this is occurring. Check Point's research showed that on a daily basis, **106 unknown malware downloads were occurring per hour.** That staggering figure is 48 times bigger than last year's mere 2.2 downloads per hour.

Incredibly, only one percent of enterprises use technologies to prevent zero-day attacks. And, only one tenth of enterprises consume threat intelligence services. Looking at the volume of unknown malware that was downloaded, **52 percent of infected files were PDFs, while 3 percent were Office files.**



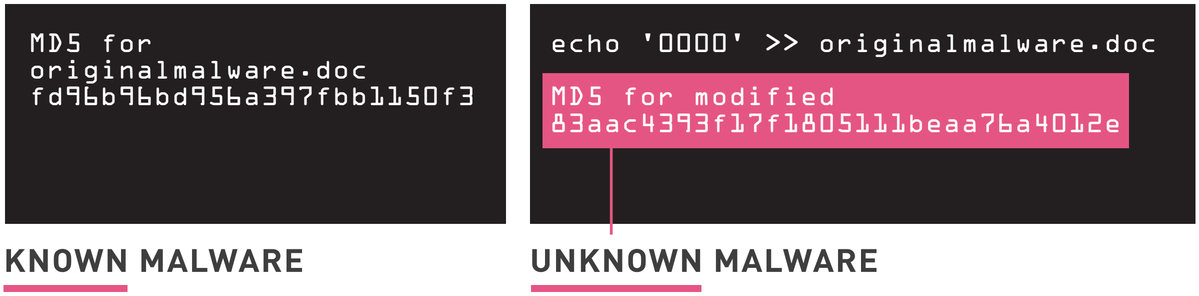
2.1 SOURCE: AV-Test

How Bad Is it, Really?

It's bad. Without a recognized malware signature to catch, the typical preventive tools can't do their job. The new face of malware is fast and stealthy thanks to obfuscation tools that help attacks slip past the most sophisticated anti-malware solutions. For hackers, working with unknown malware has become the go-to tool because it's easy and it's efficient to create variants from existing malware. In fact, it's so easy that even someone who is not technical could do it.

To illustrate, Check Point researchers took 300 known malware[7], downloaded from a sample set of well-known malicious PDF, DOC and executable files from Google's "VirusTotal" database. The goal: to test the speed and catch rate at which malware could be blocked. To turn the known into unknown malware, they simply added a null to the end of each PDF and DOC file (e.g. "echo'0000'>>1.doc). In addition, an unused header section was modified on each executable file. Next, they opened and ran each file to validate that the original behavior remained unchanged. In a nutshell, by taking existing malware and making slight modifications to it, you very quickly have something that won't be recognized.

With that simple technique, researchers were able to create new and unknown variants (hence the "Unknown 300") from existing malware.



```
MD5 for
originalmalware.doc
fd96b96bd956a397fbb1150f3
```

```
echo '0000' >> originalmalware.doc
MD5 for modified
83aac4393f17f1805111beaa76a4012e
```

These previously unseen files tested the ability of security systems to detect unknown malware.

From there, suspect files were downloaded to a host behind the security device, simulating the accidental downloading of malware from a malicious web page by an employee.

In the case of the Unknown 300, if the file behaved as expected, the data was allowed to enter the secure network. If it didn't, threat emulation technology created a signature for the type of file inspected and ensured that file was blocked. It then communicated the signature to all security gateways, making the unknown malware recognizable, or known.

Recently, Check Point discovered an attack campaign that originated in 2012, but has since been mutating into newer versions. Called Volatile Cedar, it uses a custom-made malware implant called "Explosive." Over the years this campaign has been active, it has penetrated targets across the globe, allowing hackers to monitor victims' actions and steal sensitive information.

In selecting targets, it tends to choose primarily defense contractors, telecommunications and media companies, as well as educational institutions. We believe this is because these servers are publicly exposed, easily accessible gateways to private and more secure internal networks. And, because they have a common business purpose, their security is often sacrificed for productivity, making them an easy target for attackers.

The campaign is able to fly under the radar because it limits its actions to achieving specific goals in order to minimize the risk of exposure. A typical Volatile Cedar attack starts with a scan of the target's server. Once it identifies an exploitable vulnerability, it injects a

41% **of organizations** downloaded at least one infected file with unknown malware

52% **of files** infected with unknown malware are PDFs

web shell code into the server. The web shell is then used as the means through which the Explosive Trojan is implanted into the victim server. Once inside, it lets the attackers send commands to all targets via an array of command and control (C&C) servers. The command list contains all the functionality required by the attacker to maintain control and extract information from the servers, such as keylogging, clipboard logging, screenshots, and run commands.

Then, once the attacker gains control over these servers, s/he can use them as a pivot point to explore, identify, and attack additional targets located deeper inside the internal network.

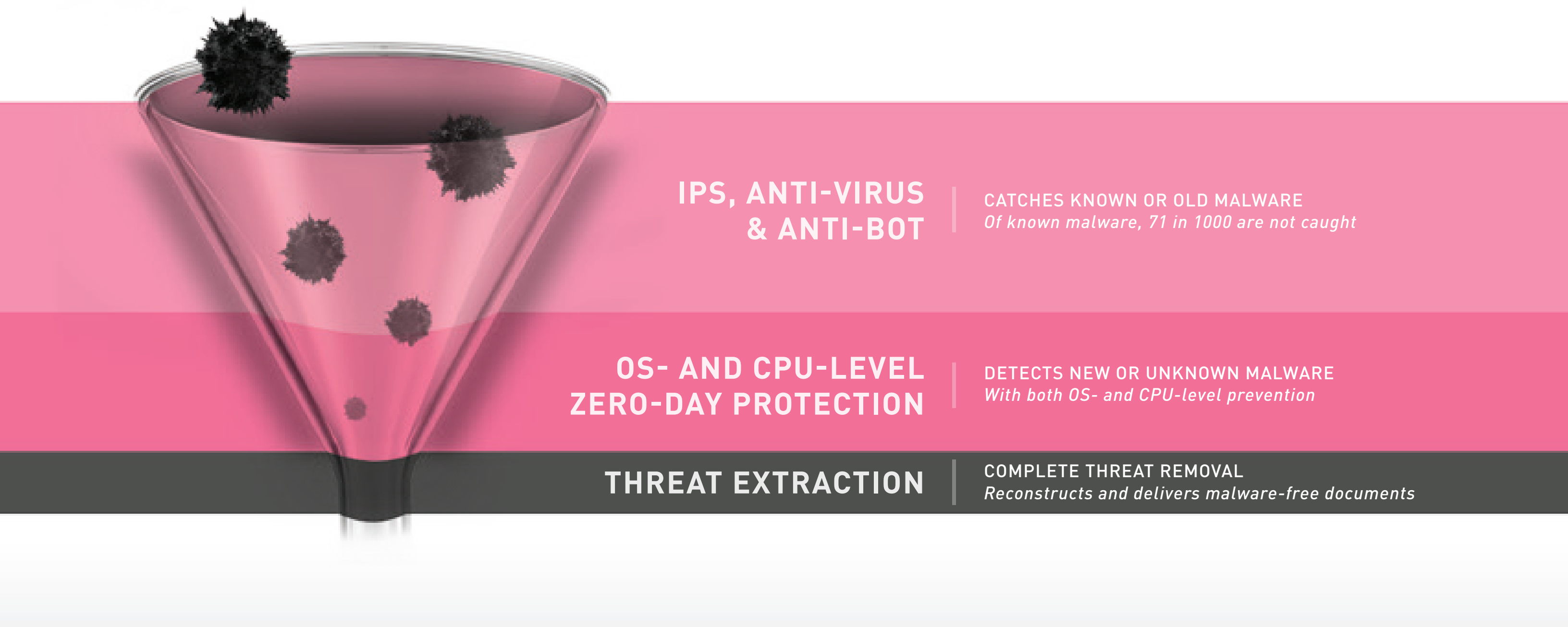
But even worse than unknown malware is zero-day malware. What's the difference? Unknown malware builds off of known malware; zero-day malware is effectively built from scratch, to exploit software vulnerabilities of which vendors aren't yet even aware. Compared with the cost of an unknown malware kit, hackers find that zero-day malware is much more expensive. This, alone, is probably why zero-day attacks tend to be selectively targeted.

One of the notable zero-day attacks of 2014 was called "Sandworm," a reference to creatures from the science fiction series, "Dune." In a targeted attack on NATO, the Ukrainian government, and some other political targets, Russian hackers exploited the CVE-2014-4114 vulnerability—the OLE package manager in Microsoft Windows and Windows Server. The vector: malicious PowerPoint files sent as email attachments. When a user clicked on the attachment, an exploit was activated and installed malicious code that opened a backdoor into the system. As a result, attackers could then execute commands.

YOU SAY YOU WANT AN EVOLUTION: EVOLVING MALWARE—EVOLVING TECHNOLOGY

The *first generation* approach to improving malware catch rates was to run suspect files in a sandbox outside the network; the point was to emulate a standard operating system (OS) in a restricted environment for safe observation. Then, using sandbox tools, you would activate files in various ways to simulate an actual user opening the file. Next, you would watch to see if it triggered anything beyond what was normally expected. The problem: Cybercriminals recognize these safeguards exist on some percentage of networks and are already implementing simple evasion techniques.

CHECK POINT CLOSES THE SECURITY GAPS



IPS, ANTI-VIRUS & ANTI-BOT | CATCHES KNOWN OR OLD MALWARE
Of known malware, 71 in 1000 are not caught

OS- AND CPU-LEVEL ZERO-DAY PROTECTION | DETECTS NEW OR UNKNOWN MALWARE
With both OS- and CPU-level prevention

THREAT EXTRACTION | COMPLETE THREAT REMOVAL
Reconstructs and delivers malware-free documents

2.2 SOURCE: Check Point Software Technologies

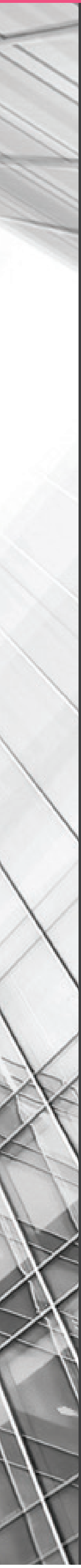
For instance, the malware might remain dormant until specific conditions are met, such as opening on a Tuesday, or when the user right clicks. This is why it's important to constantly focus on innovation and the latest in security technologies, to stay ahead of the hackers.

First-generation OS-level sandbox solutions help prevent some zero-day attacks and can detect malware once it is running. However, a lot of malware can still avoid detection. For that reason, a next-generation zero-day protection method is needed: CPU-level sandboxing.

While there are countless vulnerabilities, there are only a handful of exploitation methods that can be used to download the malware and execute it. CPU-level sandboxing lets you detect the use of exploitation methods by carefully examining CPU activity and the execution flow at the assembly code level while the exploit occurs. As a result, it preempts any possibility of hackers evading detection. The speed and accuracy of detection make CPU-level sandboxing the best technology in detecting zero-day and unknown attacks.

Taking that approach a step farther, when you combine deep OS- and CPU-level sandbox capabilities with threat extraction, such as Check Point's Next Generation Zero-Day Protection, you up the ante for threat elimination. At the OS level, you can detect attacks in both executable and data files alike. At the deep CPU level, you're able to detect an infection in data files at the exploit phase. Threat extraction, the third prong of this powerful combination, intercepts all documents, whether malicious or not, and removes dynamic objects to protect against any zero-day attack. Then, it flattens the file and delivers the document in an image-like format that is threat-free.

As evasion techniques evolve and get smarter, along with the types of attacks, so must the technology to keep your business secure. What has emerged as cutting edge in 2014 will simply be the standard for 2015.



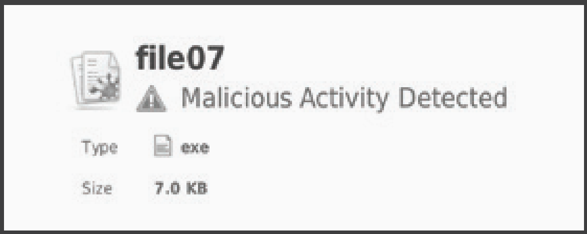
How Threat Emulation Could Have Prevented a Retail Breach

Black Friday, which follows the United States' Thanksgiving holiday, is one of the biggest shopping days of the year. On the Monday just before the 2014 holiday, Check Point Incident Response Team (CPIRT) was contacted by a retailer who had discovered unknown files on their systems. These files were not detected by major anti-virus vendors. The bits of available intelligence on each individual file may not have been enough to sound alarms, but the collective sum painted a much larger picture. The files appeared to be part of a kit designed to deliver malicious payload laterally, through a network.

Kit components consisted of tools used to:

- Extract, capture, and manipulate login credentials from Windows systems
- Capture keystrokes on Windows systems
- Transfer files

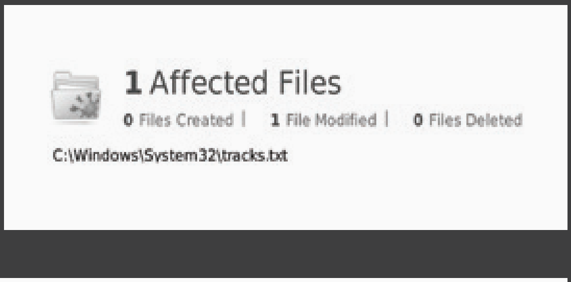
Still, details gleaned about other files in the kit were more ambiguous. Continuing with the investigation, the response team sought to confirm some suspicions by running the files through Check Point's online ThreatCloud Emulation Services. Many of those files were flagged as suspicious and showed downright malicious activity. One was particularly interesting to this situation: The file was caught writing a text file in a Windows system directory.



file07

⚠ Malicious Activity Detected

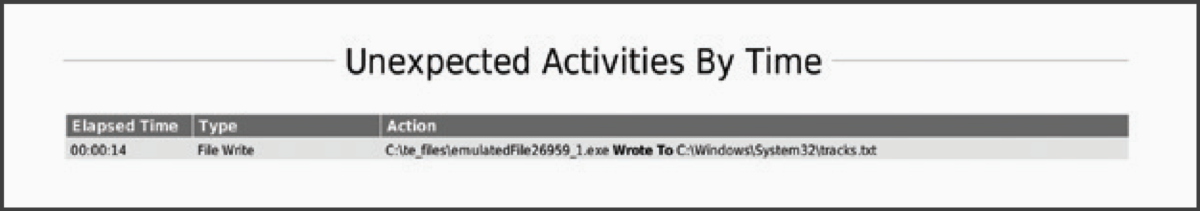
Type	exe
Size	7.0 KB



1 Affected Files

0 Files Created | 1 File Modified | 0 Files Deleted

C:\Windows\System32\tracks.txt



Unexpected Activities By Time

Elapsed Time	Type	Action
00:00:14	File Write	C:\te_files\emulatedFile26959_1.exe **Wrote To** C:\Windows\System32\tracks.txt

Seeing the file write tracks.txt in the C:\Windows\System32\ directory upheld the belief that this file was PoS malware, designed to harvest card track data. With that knowledge, it became evident that this malware was part of a kit that could capture credentials; use them to install malware; move around inside; and exfiltrate data out of the network. Had Threat Emulation been deployed, this malware—and other components in the malicious kit—could have been blocked.

RECOMMENDATIONS

To address unknown malware and zero-day threats, you need to be able to identify them within and beyond the operating system. The goal: to not only spot the threats, but also address evasion techniques. Check Point recommends utilizing a three-pronged approach: a combination of OS- and CPU-level sandbox capabilities with threat extraction.

Key factors to consider in selecting a good sandbox include:

- Ability to block attacks, not just detect them
- Ability to avoid evasions
- Fast and accurate detection
- Ability to decrypt SSL
- Ability to support common file types
- Ability to support web objects such as Flash

"Only the unknown frightens men.
But once a man has faced the unknown,
that terror becomes the known."[8]

-Antoine de Saint-Exupery, writer and poet

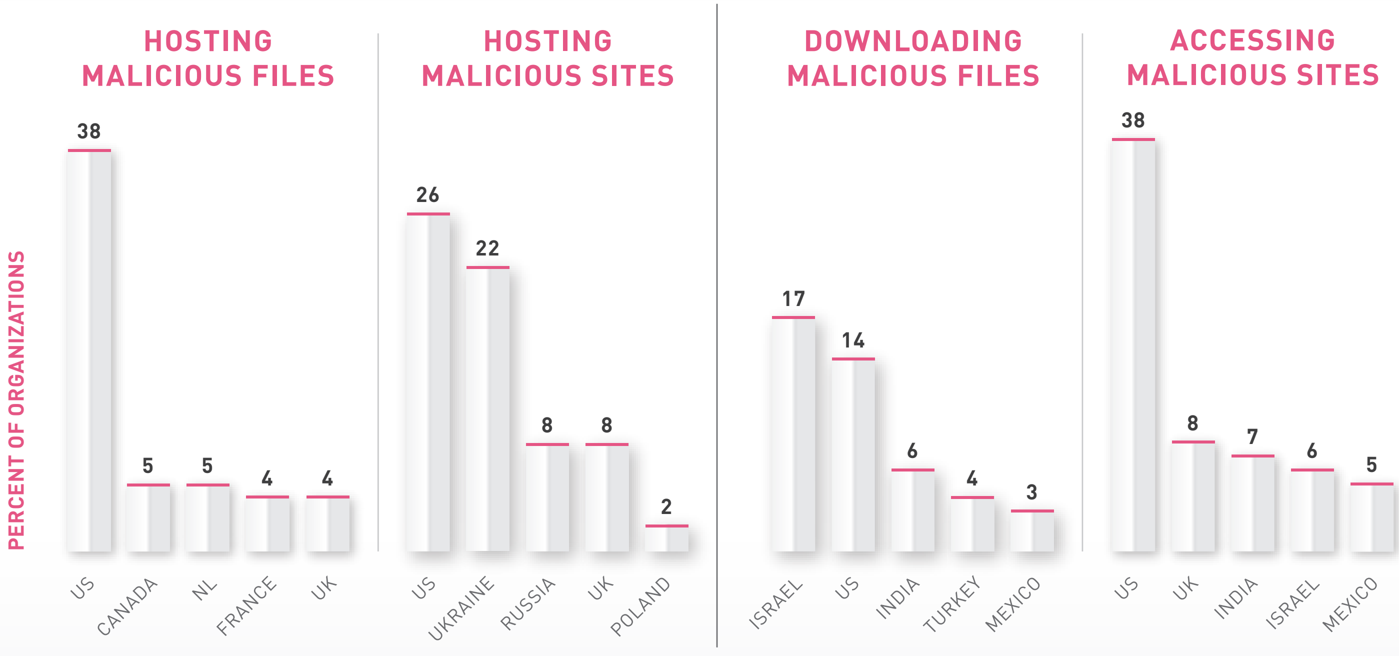
03

KNOWN MALWARE: KNOWN AND DANGEROUS

"We're all digital, we're all vulnerable and everything's instant—so instant. Instant success and instant failure."[9]

–Madonna, pop star, on the digital theft and leaking of her unfinished album, "Rebel Heart," before it was released.

TOP 5 COUNTRIES



3.1 SOURCE: Check Point Software Technologies

Given how easy and powerful unknown malware is to create and launch, you would think we would start seeing a decline in known malware. The reality, however, is that hackers continue to keep this method of attack in their arsenal.

In 2014, Check Point researchers discovered that roughly 86 percent of organizations accessed a malicious site. What's more, close to 63 percent of organizations downloaded a malicious file. Looking at speed and frequency, hosts accessed a malicious website every 24 seconds (compared to every minute in the previous year), and downloaded malware every six minutes (compared to every 10 minutes in the previous year). When you consider how quickly viruses can spread and wreak havoc, this goes way beyond alarming.

In 2014 hosts
downloaded malware
every 6 minutes

In 2014 hosts
accessed a malicious site
every 24 seconds

THERE WILL BE BOTS

One of the more efficient ways to amplify and accelerate the spread of malware is through bots—when a computer has been infected with a Trojan or virus, it can allow third-party control over some or all of the machine's functions. A botnet is a network of botted or zombie computers under the command of an individual or organization that uses them to forward spam email, attack other computers, or launch DDoS attacks.

Almost 83 percent of organizations had existing bot infections in 2014. And 47 percent of those were active for more than four weeks—a disturbing length of time given that a bot communicates with its command and control (C&C) center every minute. What's more, that speed and frequency represents a 66.7 percent jump from the previous year, and a 95 percent increase from 2012.

When looking at bots, what kind of damage are we talking about? Stealing banking credentials and other sensitive information; disabling system security services; installing malware; performing click-fraud; gaining remote access; and opening a backdoor for attacks comprised the majority of bot activity in 2014.

One of the more notable bot infections took advantage of a vulnerability in Apple's Mac computers in concert with the social, entertainment, and news site *Reddit*. A backdoor entry called

83% **of the organizations** studied were infected with bots. And, a bot communicates with its C&C every minute

FAMILY	ATTACK COUNT	DAMAGE
ZEUS	51,848,194	Steals banking credentials
GRAFTOR	21,673,764	Downloads malicious files
RAMNIT	12,978,788	Steals banking credentials
CONFICKER	12,357,794	Disables system security services, gains attacker remote access
SALITY	11,791,594	Steals sensitive information
SMOKELOADER	9,417,333	Installs malware
RAMDO	5,771,478	Performs click-fraud
GAMARUE	3,329,930	Opens a backdoor for attacks
TORPIG	3,290,148	Steals sensitive information

3.2 SOURCE: Check Point Software Technologies

"Mac.BackDoor.iWorm" gained access to Macs. From there, it used *Reddit* to connect the hacked computer with a command server. After infecting the computers, hackers would post to *Reddit* and then take advantage of the site's search function to identify those posts. Using the iWorm, they were able to capture server addresses from the posts and use them as a guide to connect to the botnet.

The bot that had the most action for 2014, however, was also the reigning champ the year before: ZeuS. It seems that this year, hackers followed the principle that if it isn't broken, don't fix it. According to the Spamhaus Botnet Summary Report for 2014, ZeuS led the list of bots with 2,246 command and controls, practically twice as many as Citadel, the next leading bot.[10]

So with the reach and power of bots at their disposal, what are cybercriminals most focused on? Essentially, critical elements that significantly hamper an organization's productivity.

Whirlwinds of Credential Harvesting

Tool automation and botnet distribution make credential harvesting through brute force easier every day. For instance, prior to 2014, only one computer at a time could crack a password. This past year, however, a popular password hash-cracking tool called Hashcat modified its source code to allow for distributed cracking—so more than one computer could help to crack the password—making operations much faster for attackers.

So how does it work? Criminals capture large amounts of data from attacks. Sometimes it's hashed or coded, and not easy to use right away. That's where the tools come in—they automate the cracking of the passwords and may already be part of a botnet that allows for easier distribution. Once the hashes are cracked, brute force attacks try to exploit password reuse; they also test to see if one person's password works for someone else's login. In fact, Check Point has observed constant brute force attacks lasting weeks, where the attempts per second/minute/hour/day are tuned by the attacker to evade detection. What's more, this can lead to dumps on open text sharing sites like Pastebin, where the information can then be sold.

To safeguard password storage, generate a cryptographic one-way hash of a password. In other words, if a password is "bluesky," a cryptograph will turn it into something like "fna84K." This prevents keeping plain-text passwords around and permits verification of user-supplied passwords by repeating the one-way hashing system. Adding a randomly generated value to a password before creating their cryptographic hash can also increase the difficulty of a password-cracking operation.

Since tools already exist to crawl the internet for hashes and passwords—and automate distributed password cracking—fortifying the way you store this data is critical. To keep this information safe, take extra precautions and use dual-factor verification, out-of-band user authentication, or even biometric authentication. Remember, the fact that people reuse similar passwords means that every breach of thousands of names creates the seeds for, potentially, hundreds of additional breaches.

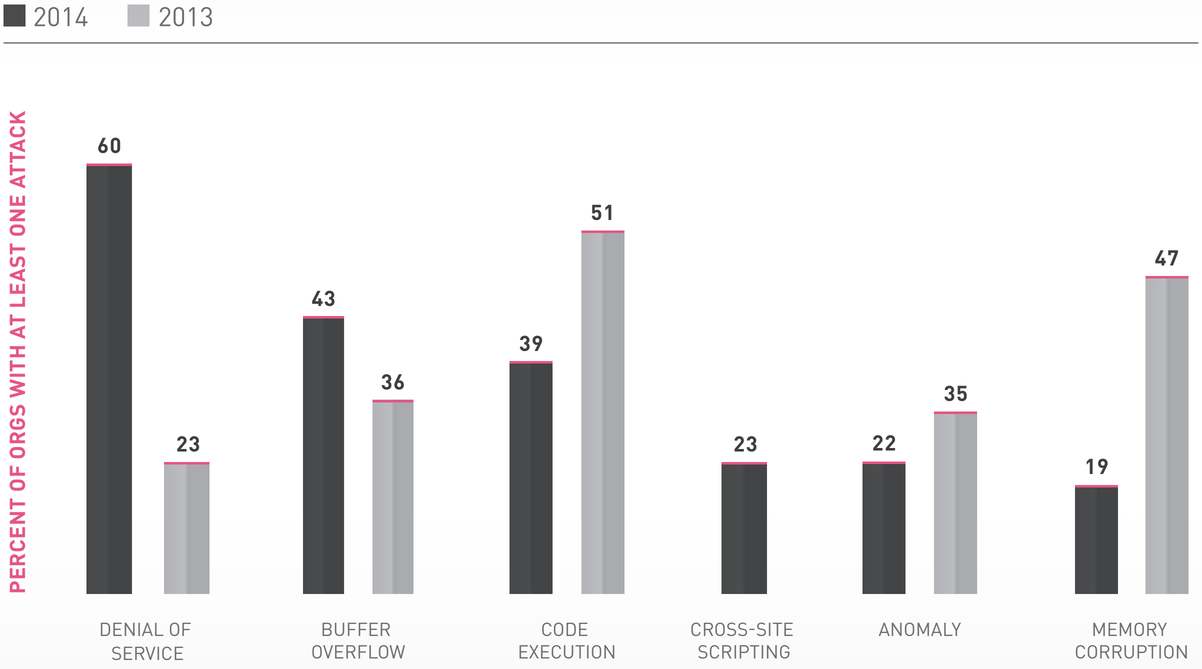
DDOS: THE NEW PICKET LINE

In the past, if you wanted to contest a company's policies, you'd gather some people, make some signs, and stand outside their place of business for a very public display of protest. Now? You just go online and buy an inexpensive DDoS toolkit, enter the URL for the company you're protesting, and you're done—the company's website is defaced. It's easy, convenient, and cheap.

In 2014, Distributed Denial of Service (DDoS) was the top attack vector, accounting for 60 percent of all attacks, almost double from the previous year. DDoS attacks, which temporarily knock a server or other network resource out of service, were occurring 48 times per day in 2014—up from eight times per day in 2013. That represents a 500 percent increase! Last year, the majority of DDoS attacks was found largely in the consulting sector. This year, it spans almost two thirds of businesses across all industries. After DDoS, the next biggest attack vectors for the year were Buffer Overflow, an attack that can corrupt data, and Code Execution, which allows a hacker to inject arbitrary code. Both increased significantly from the previous year.

48 DDoS attacks occurred every day in 2014

TOP ATTACK VECTORS



3.3 SOURCE: Check Point Software Technologies

HACKTIVISM:
When Protestors Take Their Ideology Online

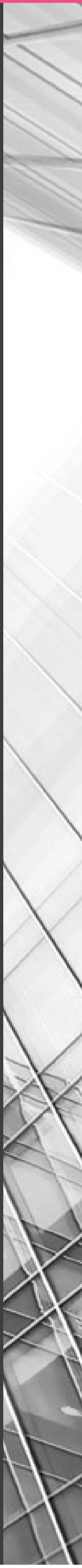
The past year saw an upswing in DDoS against educational facilities, service providers, US state governments and city governments. Regardless of politics, the effects of hacktivism through DDoS attacks are felt by innocent bystanders as much, if not more than, the intended targets. In countries where the government provides the majority of connectivity for educational services, an attack on a small school can impact every school in the network. A DDoS targeting one city's website can cause (and has caused) a loss of VPN connectivity with law enforcement field units and emergency services—and not just during a major protest.

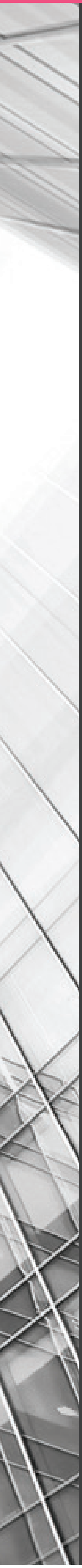
While the order of steps may vary, there are four main techniques used by hacktivists:

1. A multi-wave volumetric attack that uses millions of user datagram protocol (UDP) packets on port 80. As a stateless protocol, UDP is very easy to fake, making the source appear as if it was sent from a different internet protocol (IP) address. This floods the connection before organizations' premise security devices can detect and react.
2. A domain name system (DNS) 'reflection' attack in which attackers send millions of DNS queries to legitimate DNS servers, using a spoofed source IP address to appear as if they originated from a server on the victim's network. The legitimate DNS servers react by flooding DNS responses to the victim, causing another wave of volumetric attacks.
3. A SYN flood attack targets a specific host. Spoofing the source address in high volume, it consumes enough resources so that the host is unresponsive to legitimate traffic.
4. Slow attacks open as many connections as possible to a server and keep those connections open as long as possible by sending bits of data right before the transmission control protocol (TCP) sessions time out. The traffic is low, but the volume of slow connections congests inbound network ports.

Here's what you can do to secure your organization:

1. Understand and monitor traffic volume such as connections per second, packets per second, and throughput per second. If baseline thresholds are exceeded, tools like Check Point DDoS Protector™ can be deployed in front of security gateways to mitigate DDoS traffic before reaching the gateway. When volumetric attack traffic exceeds the internet circuit speed, it will saturate the network connection before it reaches DDoS Protector or the security gateway, thereby denying service. To prevent that from happening, DDoS Protector diverts traffic through DefensePipe to internet scrubbing centers, where malicious traffic is removed and clean traffic is diverted back.
2. Implement tight controls on networks with guest access or unknown users' bases such as educational facilities, cloud providers, and service hosting companies.
3. Deploy source IP spoofing rules to prevent users on targeted networks from launching reflection attacks. Dynamic, variant, and multi-wave styles of attacks can make it challenging to stop every form of DDoS. But, Check Point's Firewall Software Blade and IPS Software Blade have mitigation tools and protections built into them—such as Rate Limiting, SYN Defender and IPS SYN Attack, and IPS DNS—to help prevent DDoS attacks.





CRITICAL INFRASTRUCTURE DOOMSDAY: Not “If,” but “When”

James Arbuthnot, former chairman of the UK Defense Select Committee, said it best: “Our national grid is coming under cyberattack not just day by day, but minute by minute.”[11] **In fact, nearly 70 percent of critical infrastructure (CI) companies suffered a security breach over the last year.**[12] One attack during 2014, by a group of Russian hackers called Energetic Bear, launched a campaign that targeted oil and gas companies. Through infection of industrial control software that those companies relied on, attackers embedded malware that automatically downloaded and installed when the victim organizations updated their software. This gave attackers visibility into—and potential control of—the targeted networks.

In a separate incident, a German steel mill was targeted, causing major damage to a blast furnace. According to the German Federal office of Information Security, BSI, attackers deployed a socially engineered spear phishing campaign to trick specific individuals into opening messages. From there, the cybercriminals were able to capture login names and passwords, which helped them access the mill’s production network. Once in, they went after the control systems, causing elements to fail, which prevented the furnace from shutting down normally. As a result, the whole system was impaired.

Why is this happening?

When we look at the causes of CI incidents, we see a few things going on. To begin with, the supervisory control and data acquisition (SCADA) system, commonly used by CI, was not designed for security. Not only are its devices vulnerable, its networks are old and outdated. Plus, SCADA systems embed Windows and Linux operating systems, which are also vulnerable. A second cause is that, too often, the view of security is short-sighted, with an emphasis only on the electronic perimeter. This falls short because it leaves the production systems at risk. Finally, a third problem that we see is the mistaken belief that good physical security means good network security. Not recognizing the difference can lead to severe consequences.

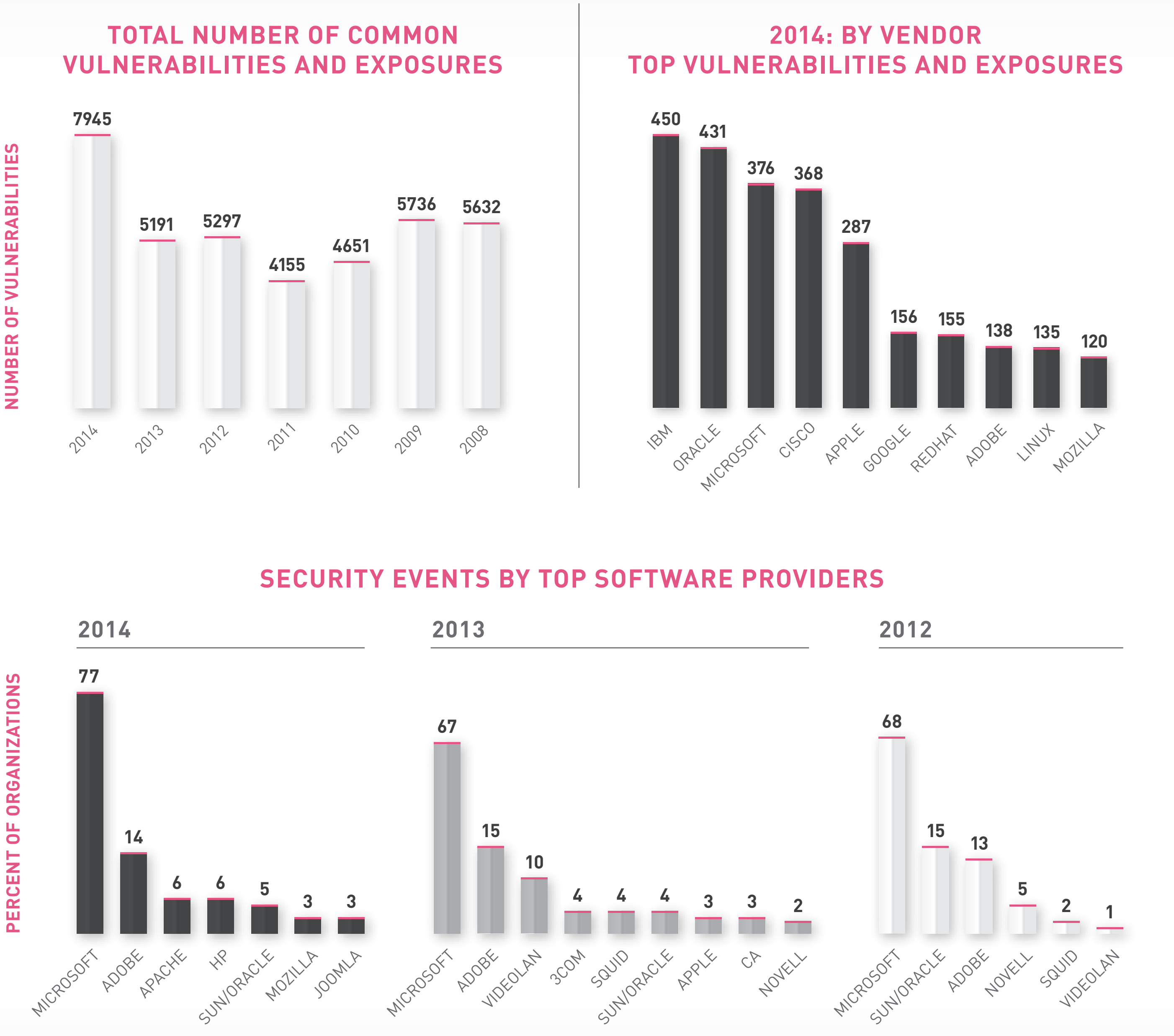
Securing critical infrastructure: What to do

Just as we see three causes of CI incidents, we also see three key paths to preventing such occurrences. Below are steps to safeguard critical infrastructures.

1. Security Architecture: First and foremost, protect the corporate network to block infiltration of the production network. Then, segment and protect your production network with specialized security. For perimeter security, use proper tools such as firewall, intrusion prevention, anti-virus, anti-bot, and threat emulation.

2. Security Products with Granular SCADA Support: Always use products specifically designed for SCADA systems. Remember, CI industries rely on dedicated systems on specialized networks with unique protocols. Solutions like Check Point SCADA security solutions include SCADA logging, firewall, app control, intrusion prevention, and SCADA workstation endpoint security.

3. Threat Intelligence: Be sure to independently log all SCADA activity by using in-depth SCADA traffic monitoring and analysis for threats.


TOTAL NUMBER OF COMMON VULNERABILITIES AND EXPOSURES

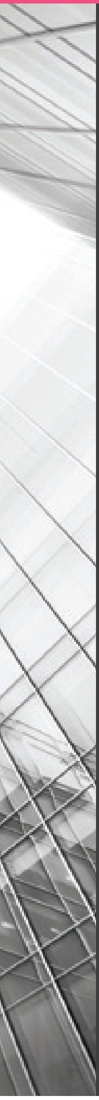
2014: BY VENDOR TOP VULNERABILITIES AND EXPOSURES

SECURITY EVENTS BY TOP SOFTWARE PROVIDERS

3.4 SOURCE: Common Vulnerabilities and Exposures (CVE) Database (top charts), Check Point Software Technologies (bottom chart)

FEELING VULNERABLE

One of the big issues that organizations need to address to help shore up their security is to patch and update software. When this is overlooked, it creates a serious business vulnerability that can needlessly interrupt performance—of man and machine. Looking at the total number of common vulnerabilities and exposures over the past three years, we saw little increase between 2012 to 2013. However, from 2013 to 2014, we saw a jump of just over 53 percent.[13] So while the good news is that awareness is increasing around these potential exposures, the bad news is that they still exist and are growing.



SHELLSHOCK: Hitting Networks at Their Core

Hackers understand the most impactful way to strike targets is to attack their foundations. For most operating systems, that foundation is a series of fundamental commands, often executed in Unix. At the core of the command line shell used commonly in Apple MAC OS X and Linux/UNIX operating systems is a command processor called Bash, or Bourne Again Shell.

In September 2014, a major security vulnerability was discovered in Bash that let attackers remotely execute shell commands. It worked by attaching malicious code in environmental variables used by the operating system.

From a hacker perspective, it does not get much better. Within days of the vulnerability announcement, additional design flaws were also discovered and a series of patches were created. The race was on to strike networks before the patches were inserted. Within hours, attackers exploited Shellshock by creating botnets on compromised computers, to perform distributed denial-of-service attacks and vulnerability scanning. While Check Point IPS-protected networks were patched the same day, Shellshock compromised millions of unpatched servers and networks.

Check Point customers supported by IPS protection saw blocked attempts as the attacks prominently targeted HTTP, Mail (SMTP/POP3/IMAP), FTP and DHCP protocols. Research findings showed that the US was both the top target and the top attacker by a significant margin.

EXPLOITS' NEW TARGET: OPEN-SOURCE SOFTWARE AND OS

Community sharing isn't always a good thing. Take open-source software (OSS), for instance. Unlike typical proprietary software that is closed, open-source software is written so that its source code is freely available to the public and can be modified by anyone. Worse, OSS is not managed as closely because it's not always part of the IT procurement process. And, because it's freeware, it's not as closely maintained as other software. Cybercriminals know this, so they redeploy attacks toward less-maintained, less-visible applications and systems. As a result, OSS has become an attractive target in order to steal data, intellectual property, and other sensitive information. Thus, it becomes an open door to the network for hackers to exploit.

For instance, OpenDaylight, a multi-vendor open-source software project, was forced to focus on security when a software-defined networking (SDN) flaw came to light. In August of 2014, a critical vulnerability was found in its platform, but it took about four months to get patched. The person who found the vulnerability had initially tried to report it privately, but since OpenDaylight did not have a security team, his efforts went nowhere. Instead, he ended up posting the vulnerability on a popular mailing list for security flaws. At issue was the potential for an SDN controller to be compromised, which would enable attackers to take control of the network.[14]

One open-source vulnerability discovered during 2014 was with the MediaWiki platform, which is used to run Wikipedia and thousands of other wiki sites worldwide. Check Point researchers discovered that a defect in the code could allow attackers to inject malicious code into every page in Wikipedia.org, as well as into other internal or web-facing wiki sites running on MediaWiki. With more than 94 million unique visitors per month to Wikipedia alone, and almost 2 million sites linking to it, it's easy to see the potential for widespread damage.

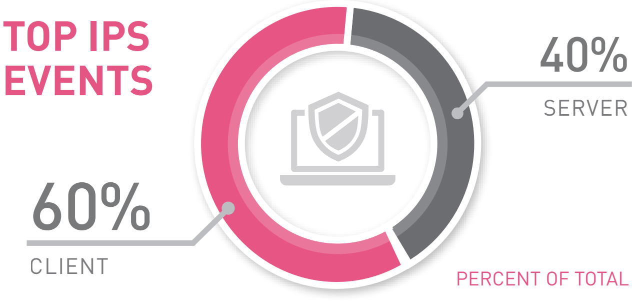
The biggest open-source exploits of the year were Heartbleed, Shellshock, and Poodle. In the past year, it seemed that businesses were hit with new, devastating malware that was the worst ever—until months later, the next worst-ever new malware arrived on the scene. Heartbleed was uncovered in April 2014, a vulnerability in OpenSSL software. What it does is allow hackers access to the memory of data servers—up to 64 kilobytes worth. This access then gives them the ability to steal critical information like user identities, passwords and other sensitive information that is contained in the servers.

Then, along came Shellshock. The staggering shame of this is that it stems from a quarter-century-old security flaw that allows malicious code execution within the Bash shell. This lets a hacker take over an operating system and access confidential information. Adding to that, many programs run Bash shell in the background. When extra code is added within the lines of existing code, the bug is let loose.[15]

Following up Shellshock was Poodle, a cute acronym that stands for Padding Oracle On Downgraded Legacy Encryption. Its focus: an 18-year-old encryption technology, SSL 3.0. If a website uses that protocol to encrypt traffic, attackers could prompt your computer to downgrade its encryption to that same antiquated standard, creating security issues with communications to servers.[16]

Open-source vulnerabilities like Heartbleed, Poodle and Shellshock affected nearly every IT operation in the world. Organizations may not be able to anticipate the next massive vulnerability, but they should understand that hackers love finding and exploiting flaws in open-source and commonly used platforms (such as Windows, Linux, and iOS) because of the rich opportunities they offer.

NO ONE TO BLAME BUT OURSELVES



3.5 SOURCE: Check Point Software Technologies

In 2013, servers were the preferred target. Last year this all changed: Clients are now the weakest link.

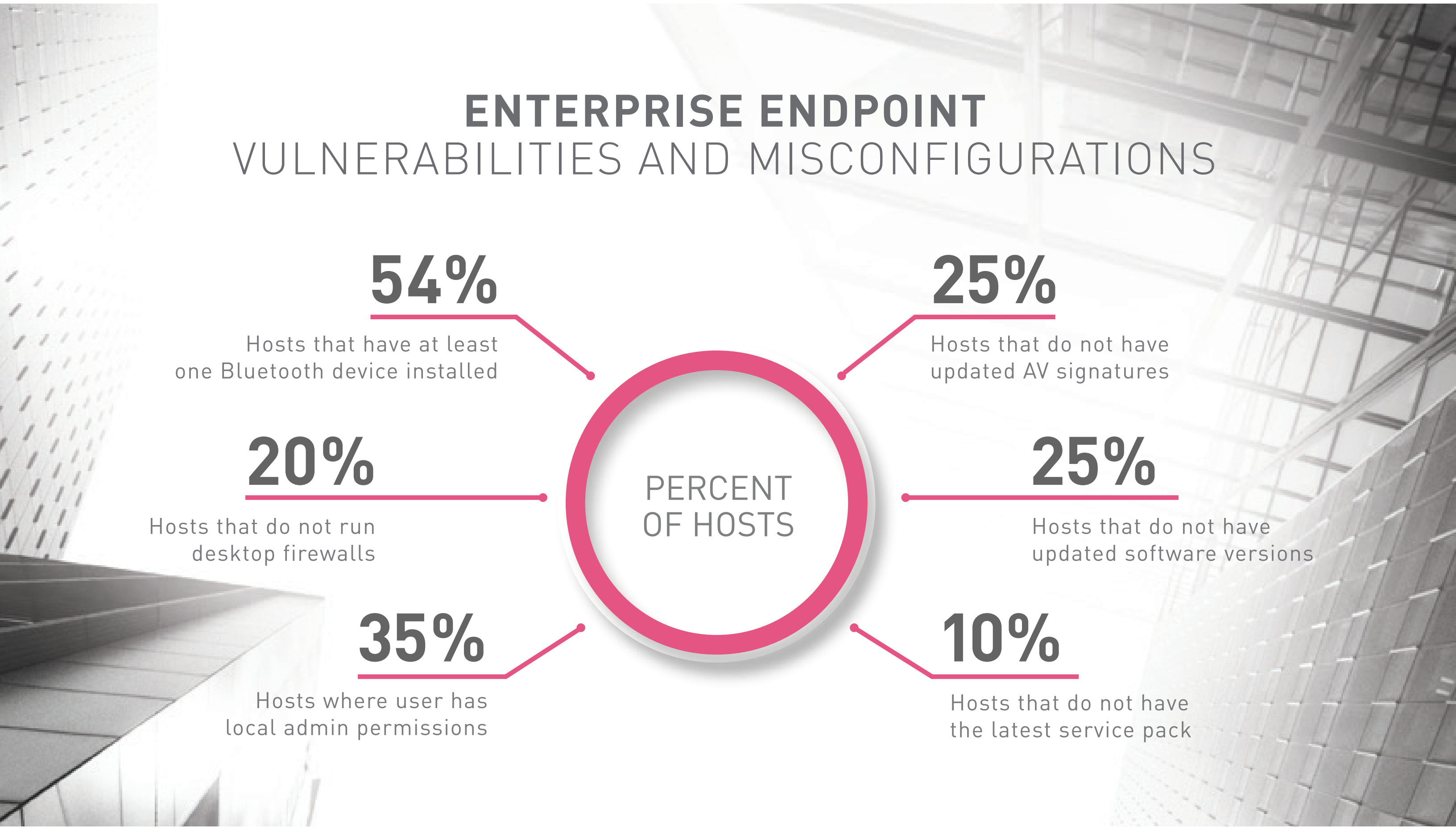
When we look at the change in the distribution of top IPS events between Client and Server, we see that the Client side jumped dramatically—to 60 from 32 percent. Meanwhile, the server side dropped from 68 percent to 40 percent. Why? Hackers show a preference for targeting clients because they can use social engineering and phishing tactics to trick people. In other words, humans are much easier to dupe than machines.

So what's contributing to the problem? Negligence around basic protections. In addition, organizations are using legacy security tools that fall short in addressing the evolving threats of today. If you want to keep your endpoints safe, you start with fundamental actions like ensuring your computers are running desktop firewall; have updated service packs and software; and have the latest anti-virus software installed.

Yet according to our findings, 20 percent of enterprise hosts are not running a desktop firewall; 10 percent of enterprise hosts don't have updated service packs; 25 percent don't have updated versions of their software; and 17 percent don't have anti-virus installed at all. In addition, 35 percent of enterprise hosts are configured such that users have local administrator permissions, putting their operating systems at greater risk for malware exploitation.

While those numbers might not seem huge, it's still an important flag that there are some enterprises that are not getting the security message: It only takes one vulnerable host to infect an entire network. And think about the number of businesses with whom those enterprises interact and exchange information. Part of managing the threat of cybercrime means being a responsible cyber citizen when it comes to basic protections—and sharing important security information with others.

ENTERPRISE ENDPOINT VULNERABILITIES AND MISCONFIGURATIONS

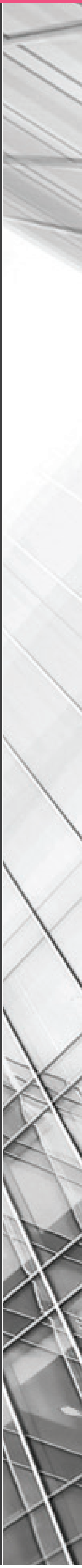


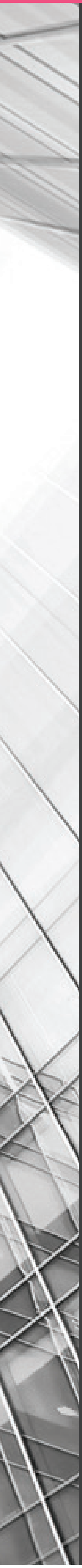
3.6 SOURCE: Check Point Software Technologies

Compliant Without Complaint

While most businesses understand their responsibilities around compliance and meeting industry regulations when it comes to security, it's still a very complex issue. You could be fully compliant one day, and then make a business-related change to your network and suddenly find yourself out of compliance. Knowing what to watch for is critical. But don't fall into the trap of thinking that just because your organization is compliant it is completely secure. Meeting regulatory requirements is typically tied to specific threats, making it less comprehensive than a security posture could and should be. It should not be the basis of your security policy. Below is what Check Point discovered in its 2014 research.

CHECK POINT FINDING	CHECK POINT ISSUE ANALYSIS	REGULATION	COUNTRIES IMPACTED BY THIS REGULATION
Anti-Spoofing not being activated for 75% of the respondents	Anti-spoofing verifies that packets are coming from, and going to, the correct interfaces on the gateway. It confirms that packets claiming to be from an internal network are actually coming from the internal network interface. It also verifies that, once a packet is routed, it is going through the proper interface.	PCI DSS 3.0	Global—any company processing or storing credit card data
		NIST 800:41	Mainly relevant to US Federal, but equally applicable to any US company adopting a robust firewall standard
		ISO 27001	Global—any company being certified to this standard or adopting it as a best practice
Discovering Any Any Accept rule in 27% of respondents	The fundamental concept of the firewall rule base is "That which is not explicitly permitted is prohibited." To discover that 27% of respondents had an Any Any Accept rule in their rule base was a major surprise. This is firewall 101, the basic of basics.	PCI DSS 3.0	Global—any company processing or storing credit card data
		NIST 800:41	Mainly relevant to US Federal, but equally applicable to any US company adopting a robust firewall standard
		ISO 27001	Global—any company following this standard
Out-of-State TCP packets not being dropped in 19% of respondents	TCP session timeout is the length of time an idle connection will remain in the security gateway connections table. This idle session is the delay in which an attacker can try to steal and use existing user session package transportation. Packets that are out of state should be dropped. We found that 1 out of 5 companies are not dropping out of state packets.	PCI DSS 3.0	Global—any company processing or storing credit card data
		ISO 27001	Global—any company being certified to this standard or adopting it as a best practice





Keep History from Repeating Itself

'Those who do not learn from history are doomed to repeat it.'

This rings true in security, as well.

Keeping current with the issues and employing best security practices can keep businesses of all sizes safe from the doom of replaying past mistakes. Below is a roundup of best practices that can help you avoid some of the security pitfalls of large and small customers.

Protections in Detect vs Prevent

With network protections, 'Detect' mode is used for low-risk threats, while 'Prevent' mode is used for critical severity and high-risk threats. We often hear from customers that an attack was 'detected' but not 'prevented' because it was miscategorized. Be sure to review threat policies regularly to understand how to properly categorize them.

Patches Out of Date

Despite the fact that patches are available for years-old vulnerabilities on platforms, they are often not installed. Attackers zoom in on this weakness; the older the vulnerability, the more likely an open-source exploit is available. To avoid being an easy target, we recommend patching early and often.

Poor Password Policy or Password Reuse

Most of the credentials harvested in brute force attacks are taken because an account password is weak. Other times, accounts are harvested because a password for one site was used on another site that was compromised. By mandating stronger password policies and educating users about password reuse, businesses can minimize account breaches. Moreover, good password policies make stronger networks.

Inter-Department Compartmentalization

In large organizations, we often observe a common theme of information compartmentalization and, sometimes, finger pointing between departments. In its most innocent form, some companies lack internal information-sharing mechanisms or consistent IT policies; this results in one group having a much more modern network than another. Unfortunately, many are not segmented internally so a breach for one can result in a breach for all.

RECOMMENDATIONS

You would think that if something is known, it would be easier to keep in check. As you've read about known malware in this chapter, it's clear that notion is misguided.

Combatting known malware requires a multi-pronged approach. The core principle: Automate and coordinate multiple layers of defense.

- Detect and Defend. Be sure to utilize gateway and endpoint anti-virus software blades along with URL filtering. This helps prevent connections with known distributors of malware.
- Block the Bot. Use an anti-bot software blade to spot malware and blunt botnet communications.
- Cover the Critical. Extend your IPS protection to make sure you're able to defend against critical severity attacks. Cover your network server and IT infrastructure systems, regardless of the vendor or platform.
- Manage and Maintain. Keep on top of vulnerabilities with patching processes for all systems and applications.
- Regulate and Restrict. When it comes to client and server configuration, restrict the use of administrator privileges; disable Java and other scripting; and regulate what applications can be installed on endpoints.

"There is no such thing as perfect security, only varying levels of insecurity." [17]

–Salman Rushdie, author

04
MOBILE SECURITY: DON'T FENCE ME IN

"Apart from the known and the unknown, what else is there?"[18]

–Harold Pinter, Nobel Prize-winning playwright, screenwriter, director, actor

42% **suffered mobile security incidents** costing more than $250,000

When mobility came along, so came the promise of untethered productivity. But for many, mobile security was an afterthought. The goal for all should be to identify solutions that enable productivity, regardless of whether you're on or off premises. And this becomes especially important as we see a rise in the usage of smartphones and tablets—along with their associated apps—to make our lives easier. Because with that rise has come a desire to do business with those same devices, putting corporate data at risk.

Predictably, the rising trend of Bring Your Own Device (BYOD) has spawned a host of mobile security problems. As an attack vector, mobile devices provide easier direct access to valuable organizational assets than any other network intrusion point, making them the weakest link in the security chain.

In a Check Point-sponsored global survey of more than 700 businesses, 42 percent of the survey sample had suffered mobile security incidents costing more than $250,000 to remediate—and 82 percent expected incidents to rise during 2015.

CORPORATE DATA AT RISK

INTELLECTUAL PROPERTY

NETWORK CREDENTIALS

EMPLOYEE LOCATION

PRIVILEGED COMMUNICATION

CALLS

4.1 SOURCE: Check Point Software Technologies

When mobile security is weak, it can provide attackers with personal information, passwords, business and personal email, corporate documents, and access to company networks and applications. In the business setting, that concern becomes magnified. In fact, 87 percent of IT professionals say careless employees are a greater threat to security than cybercriminals. And, 92 percent say employee behaviors could have made a difference in preventing high-profile security breaches.

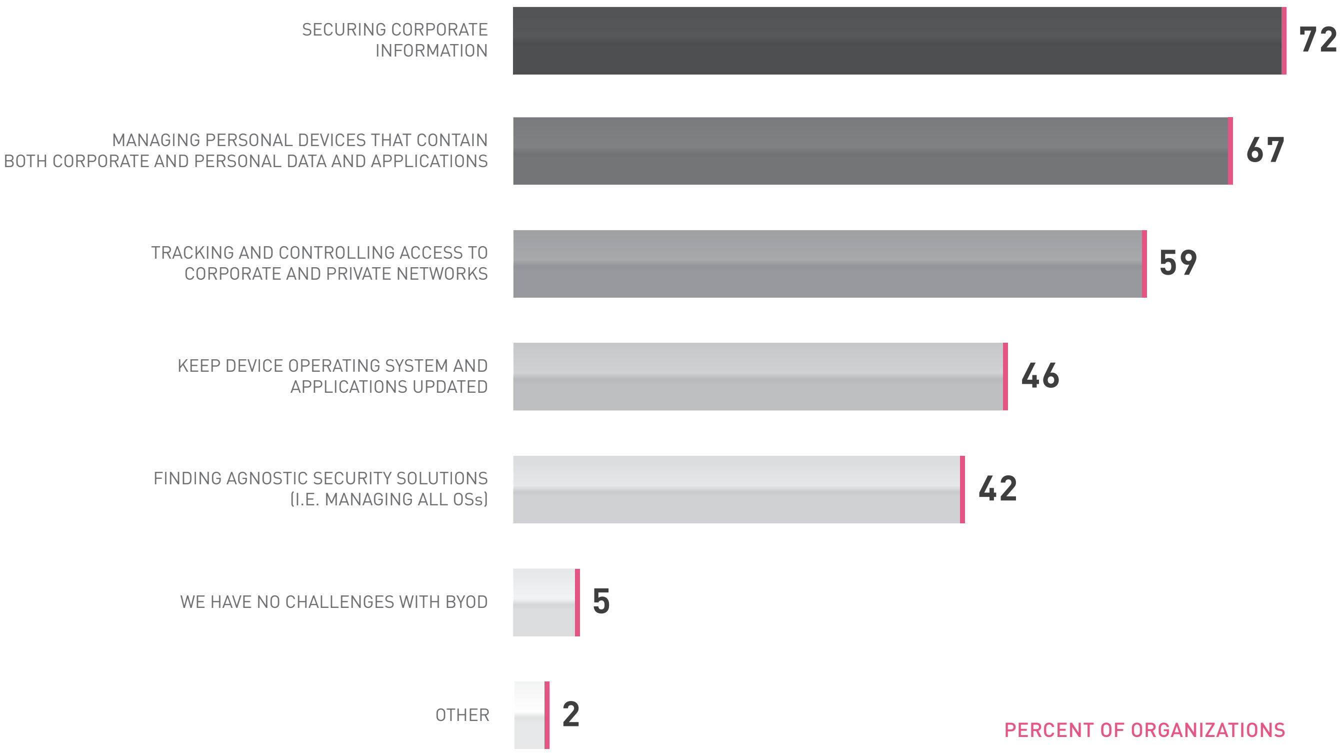
OUT OF CONTROL

Among those surveyed, 91 percent have seen an increase in the number of personal mobile devices connecting to corporate networks during the past two years. Alarmingly, 44 percent of organizations do not manage corporate data on employee-owned devices. Add to that, 33 percent of app developers do not test their apps for security.[21]

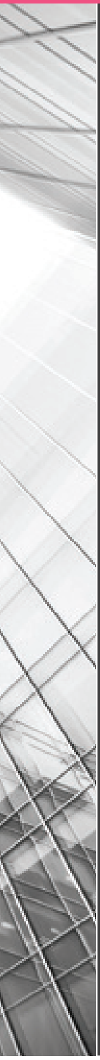
So it's no surprise that the top two BYOD security challenges faced by IT are securing corporate information—reported by 72 percent of our sample; and managing personal devices that contain both corporate and personal data and applications—cited by 67 percent of our respondents.

BYOD challenges become even more notable in the context of a separate global study we conducted. Commercial mobile surveillance kits, typically used for monitoring children—or in some cases spying—were put under the microscope. The reason: Such products are vulnerable to mobile remote-access Trojans (mRATs), which top the list of mobile malware. More than 500,000 Android and 400,000 iOS devices that connected to corporate Wi-Fi through Check Point firewalls in more than 100 countries were studied. If devices communicated with a command and control (C&C) server, they were considered infected. Researchers found that one out of every 1,000 devices was infected. And in fact, researchers determined that if there are 2,000 devices or more in an organization, there is a 50 percent chance that there are at least six infected or targeted mobile devices on their network. By platform, that breaks down to 60 percent Android and 40 percent iOS.

BYOD SECURITY CHALLENGES



4.2 SOURCE: Check Point Software Technologies



MOBILE THREAT RESEARCH:
Targeted Attacks on Enterprise Mobile Devices

Survey Sample

More than 500k Android and 400K iOS devices from more than 100 countries.

Infections

Approximately 1,000 devices infected: 60% Android, 40% iOS.

Malware

More than 20 variants and 18 different mRAT product families found.

Risk

Corporate data in the form of emails, messages, keystrokes, calls, employee location.

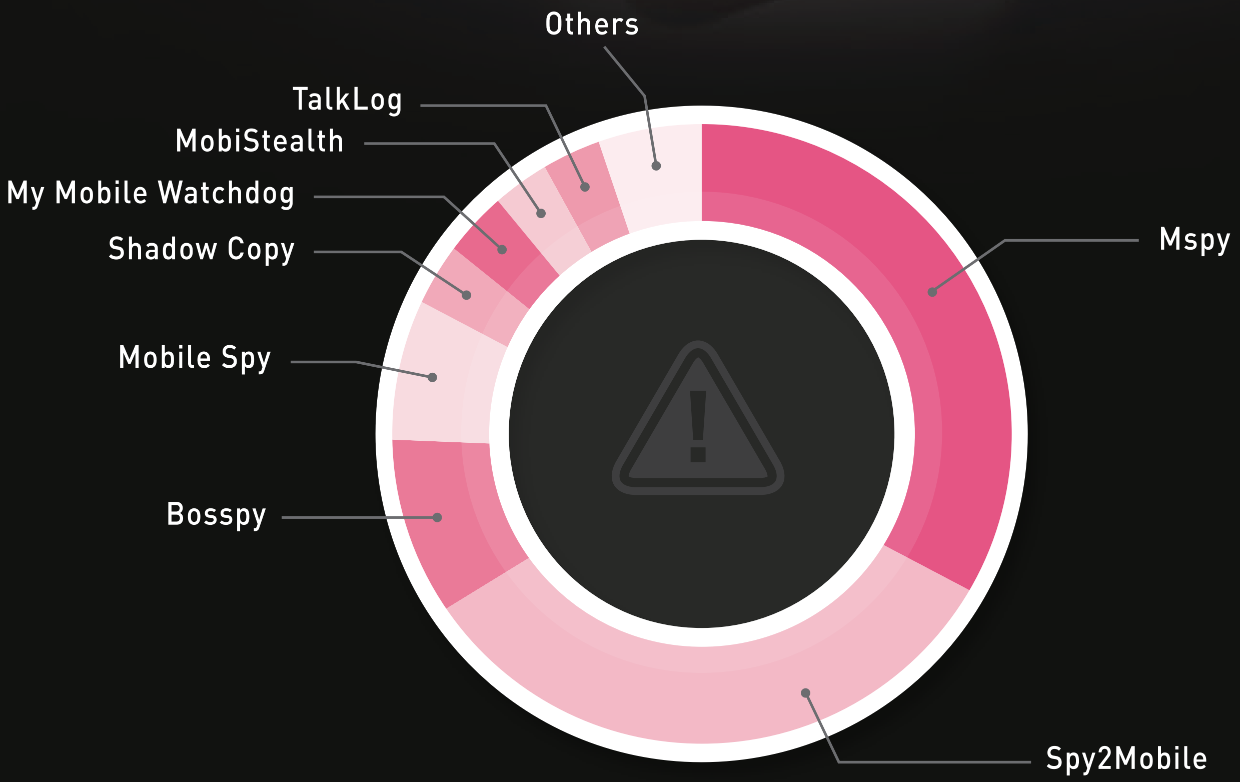
WHAT'S THE HARM?

Attackers can target an enterprise and extract sensitive information from its employees' mobile devices. Malicious mRATs can allow potential attackers to steal sensitive information from a device. They can take control of the different sensors to execute keylogging, steal messages, turn on video cameras, and more.

Interestingly, researchers discovered that employees of corporations are targeted by mRATs. More specifically, the study showed that attackers were choosing certain organizations and attacking multiple targets inside them—versus attacking corporate employees of random organizations and targeting them without relation to their organization.

In the earlier survey referenced, when asked which mobile device platform posed the most problems, 64 percent of IT professionals cited Android as the riskiest. Apple iOS and Windows Mobile followed, both at 16 percent. Only four percent cited BlackBerry.

18 MRAT FAMILIES FOUND



4.3 SOURCE: Check Point Software Technologies

BEWARE THE BINDER

The beauty of inter-process communication (IPC) is that it lets disparate specialized processes cross function within an operating system. Within Android, the message-passing mechanism of that system is Binder. In October 2014, Check Point's research team exposed a fundamental flaw associated with that system in a report entitled, "Man in the Binder: He Who Controls the IPC, Controls the Droid." In essence, our research team found it is possible to capture data communicated over the Binder protocol and intercept sensitive details.

Other key findings:

- Information sent and received through applications on a device, including those secured through two-factor authentication, encryption lines, and other security measures, can be intercepted.
- Man-in-the-middle commands can be inserted into the path of the intercepted command stream.
- Data intercepted via the Binder can include device keyboard input, in-application activities such as banking transactions, and SMS messages.

Learn more about Man in the Binder and other research findings from Check Point at **checkpoint.com/threatcloud-central.**

With Android's risk factor so much higher than the others, it's no surprise that hackers are having a field day with it. One recently discovered malware tricks Android users into believing they've powered down their devices, when in actuality, they haven't. The malware reportedly allows remote users to make calls, send and receive messages, and take photos.[22] Ultimately, this can enable a simpler path to stealing identities, as well as data.

Being aware of the risks associated with mobile technology is critical. In coming months we will need to consider the security implications of wearable tech and companion devices like Fitbit, Google Glass, smartwatches and others that connect to tablets and smartphones. As the Internet of Things (IoT) becomes commonplace in many homes and workplaces, the interconnectedness of technologies will make it possible to read everything going from one device to the other. This is why we need to get a grasp on mobile security now.

RECOMMENDATIONS

Don’t Rely on MDM as a Catch-All

Mobile Device Management (MDM) allows an IT department to control what the user can and cannot do with the device. But, there are two major shortfalls with MDM: First, from the user side, MDM policies can be very restrictive depending on the IT department; when employees feel restricted, they tend to find ways around the security protections. Second, from the organization side, MDM does not actually protect the device since MDM solutions do not include malware protection capabilities. So, you still need to identify solutions that can protect the device itself and control the data going in and out of it.

Protect on the Run

Document protection is an overlooked aspect of mobile security. Control your business documents, regardless of where they go. Encrypt files and ensure access by authorized users only. Solutions like Check Point Capsule provide document security and granular controls on who can access the data.

Shield the Space

Establish a secure business environment, segregating your business data and applications, including those on personally owned devices. If the device becomes compromised, protections can be activated to protect corporate information until the threat is removed.

Thwart Threats

Identify and prevent cyber threats to protect your entire mobile device. Be sure your mobile security solution helps you prevent suspicious file downloads, block malicious websites, and prevent threats before they do damage.

Connect to the Cloud

Protect your network traffic using cloud services that extend corporate policies to personal mobile devices (BYOD) to ensure you’re compliant. Look for a solution that enforces a single security policy to both on- and off-premises devices, and follows mobile users outside the enterprise security perimeter.

“What we are seeing with technologies like mobile devices and cloud computing is that they are enabling business models that simply didn’t exist before.... Giants everywhere are ripe for disruption by new businesses that understand how to use technology to create a brand new, never-before-possible value proposition for its customers.”[23]

-Eric Schmidt, chairman of Google

05

APPLICATIONS: GETTING YOU WHERE IT HURTS

"As our society tips toward one based on data, our collective decisions around how that data can be used will determine what kind of a culture we live in."[24]

–John Battelle, entrepreneur, author, journalist

96% **of organizations use at least** one high-risk application

It's clear that the digital landscape is a treacherous one. Threats can come by attack, by internal error, by sabotage. The one thing that poses as an especially vulnerable point of entry for businesses is that which is most relied upon for organizational productivity: applications.

Some applications, like file sharing, are obviously risky. But others don't as quickly come to mind because they're part of what's come to be known as shadow IT—applications that aren't sponsored or supported by the central IT organization. Instead, these technologies and applications are purchased and installed outside of IT as required tools to get the job done.

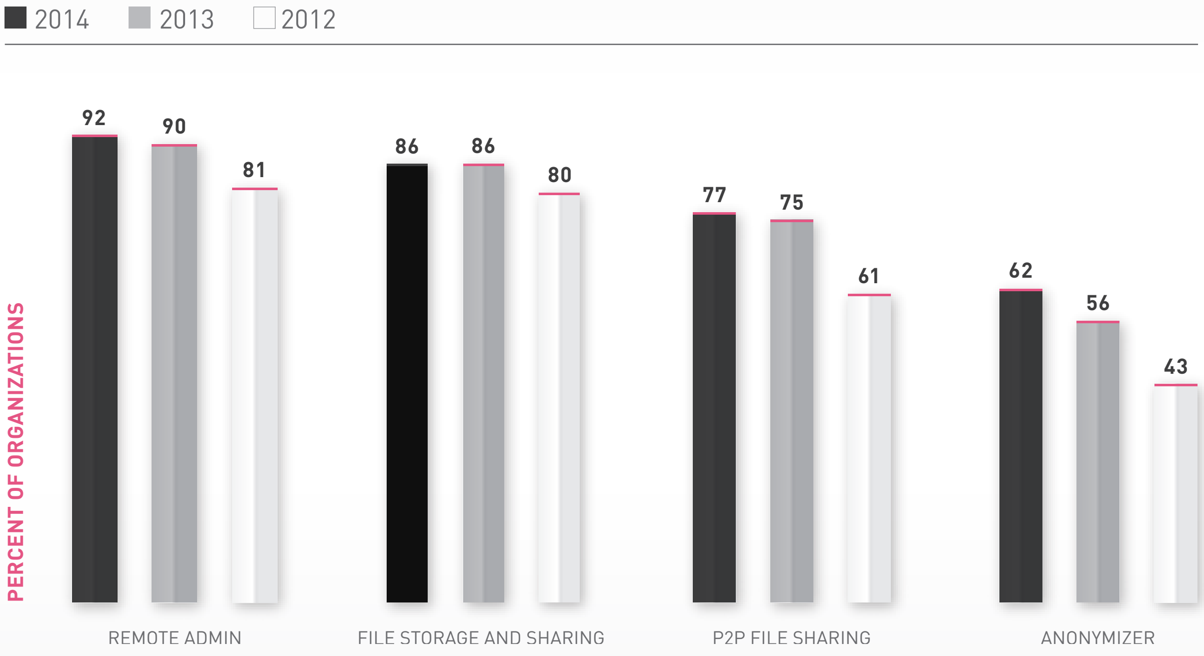
Given others' reliance on these applications, IT can't block usage of them. So, if they are allowed, threat prevention needs to be provided. The network must be protected while operating under the assumption that these high-risk applications ARE malicious, not that they MIGHT be.

To give you a sense of the pervasiveness of high-risk applications, Check Point researchers found evidence of them in 96 percent of the organizations studied—a 10-point jump from last year.

The main categories we look at include:

- Remote Admin Tools—applications like TeamViewer, RDP, and LogMeIn allow remote operators to work with your machine and its functions as though physically, in person. A handy tool for troubleshooting IT problems, it's also a handy tool that can give hackers a frightening amount of control and power over your network.
- File Storage and Sharing—applications like DropBox and others allow you to exchange and work with larger files than you could ordinarily email.
- P2P File Sharing—BitTorrent Protocol and SoulSeek are just two popular examples of what is typically used for media exchange like music, videos, or real-time communication.
- Anonymizers—browser plugins or web services such as Tor or OpenVPN allow users to interact

ORGANIZATIONS USING HIGH-RISK APPLICATIONS



5.1 SOURCE: Check Point Software Technologies

online, anonymously. These can be used legitimately, to minimize risk, but all too often, they are used for malicious purposes.

In 2014, remote admin tools (RATs) led the list of the biggest offenders in high-risk applications, with 92 percent of organizations studied affected. Of all the remote admin tools available, TeamViewer displaced RDP for first place for attack vectors in that category, with 78 percent of organizations reporting incidents.

Check Point found that the use of anonymizers increased across the board in every vertical.

And while the top three vectors of each major category of high-risk applications remained somewhat consistent from last year to this year, there was more shakeup in the anonymizer category. For instance, last year's top three included Tor, Ultrasurf, and Hide My Ass. This year: Tor slipped to third place; OpenVPN and Coralcdn were numbers one and two. Ultrasurf slid down the list and

Remote admin tools were found in 92% of organizations

Where’s Waldo?

Whether breaching for financial gain or hacking to make a point, attackers have several tools at their disposal to mask their location and identities. And contrary to what Hollywood may portray, tracing and identifying the criminals is very complex.

Cybercrime investigators admit that they are only catching ‘the bottom of the food chain’ when it comes to computer crime. That’s because criminal enterprises managed by informed and experienced attackers are likely to go undetected. Given that they are geographically distributed, well-structured and compartmented, affiliated hackers only know a small part of the larger organization—further minimizing the exposure to the criminal organization.

In operating under the radar, cybercriminals employ a host of tools to maintain their anonymity. It starts with erasing the internet trail back to their source location. The most basic tool for this is a web proxy. Also called anonymizers, a proxy server acts as an intermediary client computer, redirecting requests to the ultimately desired destination. In the early days of the internet, web proxies helped conceal a source’s IP address, but today are more easily countered and traced.

Hide Your Location

Use of VPN connections lets senders encrypt traffic between end points. The VPN server can be used to hide a sender’s identity, making the source IP untraceable (in real time). The connection between the attacker machine and the VPN server is encrypted so the traffic cannot be decoded. The VPN server itself is not masked, nor is the data once it is forwarded beyond the confines of the VPN connection.

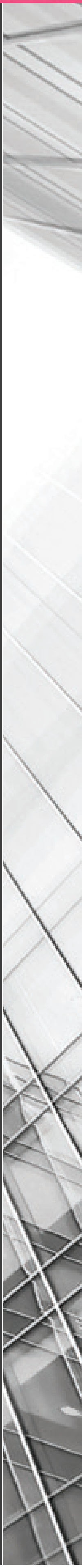
Hide Your Route

For more advanced anonymizing, some rely on tools like Tor networks. The “Tor project” uses free software that leverages a network of 5,000 volunteer relays around the world, designed to mask any individual user’s location and usage. Derived from the term ‘onion routing,’ the Tor network uses layers of encryption on addressing so each relay only sees the address for the next relay, not the source or ultimate destination.

Hide Your Computer ID

Each machine accessing the internet has a unique fingerprint: the machine’s internal MAC address, unique to every computer processor, combined with its operating system and web certificates. One of the most popular ways to mask a computer identity is “Tails,” a live operating system that can boot from a CD or USB stick. It offers a “one-time workstation” feature that transfers the machine identification signatures to the CD/USB operating system. Hackers use it once, then simply destroy the CD/USB. This allows an attacker to “switch” machine identities as many times as they want on the same computer.

In some cases, hackers use multiple cloaking layers, such as connection to a VPN behind the Tor network, sourced from a public Wi-Fi, obscuring both the source machine and internet routing locations.



TOP HIGH-RISK APPLICATIONS BY REGION

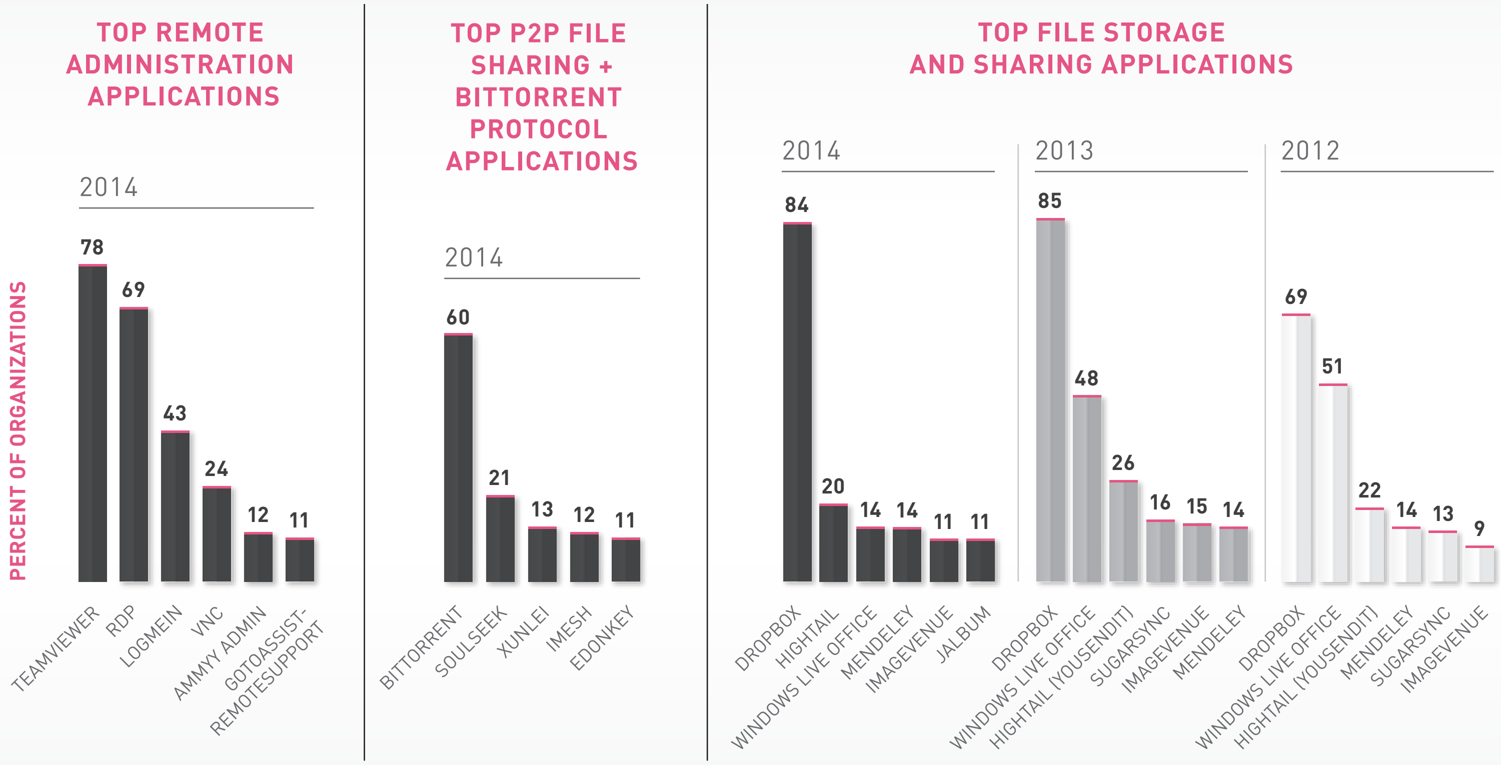
2014	AMERICAS	EMEA	APAC
ANONYMIZER	Hola • Tor • Coralcdn	OpenVPN • Coralcdn Proxy Suppliers	OpenVPN • Coralcdn • Tor
P2P FILE SHARING	BitTorrent Protocol • SoulSeek BoxCloud	BitTorrent Protocol • SoulSeek iMesh	BitTorrent Protocol • Xunlei QQ Download
FILE STORAGE AND SHARING	Dropbox • Hightail Windows Live Office	Dropbox • Hightail • Jalbum	Dropbox • Hightail • Mendeley
REMOTE ADMIN	RDP • LogMeIn • TeamViewer	TeamViewer • RDP • LogMeIn	TeamViewer • RDP • LogMeIn
2013			
ANONYMIZER	Tor • Ultrasurf • Hotspot Shield	OpenVPN • Coralcdn Proxy Suppliers	Ultrasurf • Tor • Hide My Ass
P2P FILE SHARING	BitTorrent Protocol • SoulSeek BoxCloud	BitTorrent Protocol • SoulSeek eDonkey Protocol	BitTorrent Protocol • Xunlei SoulSeek
FILE STORAGE AND SHARING	Dropbox • Windows Live Office Hightail	Dropbox • Windows Live Office Hightail	Dropbox • Windows Live Office Hightail
REMOTE ADMIN	RDP • LogMeIn • TeamViewer	RDP • TeamViewer • LogMeIn	TeamViewer • RDP • LogMeIn

5.2 SOURCE: Check Point Software Technologies

Organizations experienced 12.7 high-risk application events per hour, 305 times per day

Hide My Ass was nowhere to be seen. Likely, OpenVPN gained popularity following the Edward Snowden revelations about NSA eavesdropping. The reason is that as an industry standard, OpenVPN uses crypto technology that cannot be broken if implemented correctly, thus keeping communications private. Meanwhile, other anonymizers have climbed tremendously in popularity, even if not yet one of the top three.

For instance, the Hola anonymizer app rose from three percent to 17 percent. Part of its claim to fame could be credited to being in the right place at the right time. Hola emerged from beta testing just before the 2014 Sochi Olympics. Because it allows internet access across borders, programming that would be otherwise only available to people in a specific geography is accessible for those using Hola to cloak their geolocations.



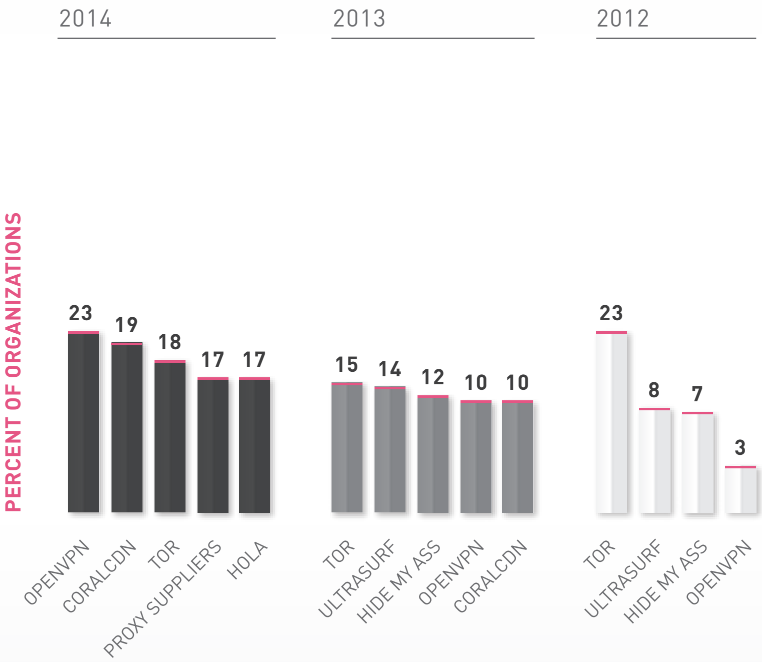
TOP REMOTE ADMINISTRATION APPLICATIONS

TOP P2P FILE SHARING + BITTORRENT PROTOCOL APPLICATIONS

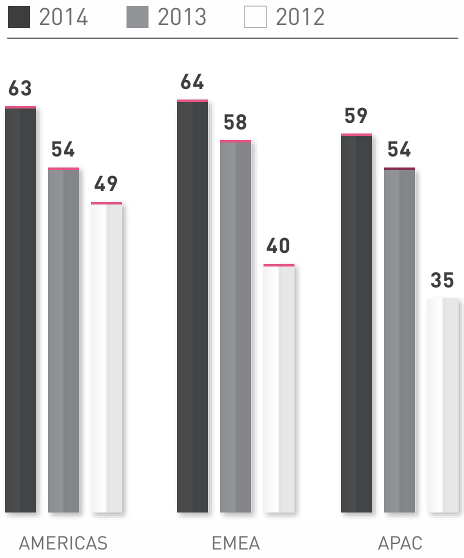
TOP FILE STORAGE AND SHARING APPLICATIONS

5.3 SOURCE: Check Point Software Technologies

MOST POPULAR ANONYMIZER APPLICATIONS



USAGE OF ANONYMIZER APPLICATIONS BY REGION



5.4 SOURCE: Check Point Software Technologies

For file storage and sharing, as well as peer to peer (P2P) sharing, the top applications noted last year were more or less the same. The good news: fewer occurrences of these in organizations. With the major media coverage in the past year of leaked photos and private emails, no doubt this helped to make many more aware and precautious.

But the big news in high-risk applications can be seen in the average number of events per hour and per day. Check Point researchers studied 4,049,111 events. **Organizations experienced 12.7 high-risk application events per hour, 305 times per day.** Compare that to last year's rate of 162 times per day and you have an 88 percent increase.

RECOMMENDATIONS

While malware—both known and unknown—can sometimes seem beyond control, use of high-risk applications at least offers some semblance of regulation.

Here are four steps you can take to minimize the dangers of these applications:

1. Educate your employees. Help people in your organization understand the risks associated with specific applications. Don't assume they know. Moreover, point them to more secure, IT-supported tools that can address their business and productivity needs.

2. Standardize on trusted, enterprise-grade applications. Identify the specific applications needed to ensure productivity and innovation. Then, map out the individuals who should have access to those programs. Monitor your network to ensure there are no rogue applications present.

3. Encrypt documents to prevent data loss. If a file is forwarded to someone who should not see it, encryption helps block the recipient from seeing or opening the document.

4. Define and practice category-based application control. Help your administrators to help you. Empower them with the ability to block entire categories of applications as needed. This simplifies administration by extending policy control to new applications as they are adopted.

> *"We live in a world where there are many risks, and it's high time we start taking seriously which ones we should be worried about."*[25]
>
> -Lisa Randall, physicist

06
DATA LOSS:
LIKE SAND THROUGH THE HOUR GLASS

"Mistakes are a fact of life. It is the response to the error that counts."[26]

–Nikki Giovanni, poet, writer, educator, and activist

Organizations suffered a data loss at a rate of 1.7 times per hour, 41 times per day

Breaches aren't the only way that the bad guys get the job done. Sometimes they need accomplices, even if they're unwitting ones. And that's where social engineering and phishing come in. Cybercriminals have become so good at knowing the psychology around their targets that their emails come across as credible for even some who consider themselves savvy. For instance, an employee gets an email from someone who claims to be a recruiter and tells the individual about an open position. When the person expresses interest, the so-called recruiter asks for more information about the company and possibly other sensitive information. In other instances, employees receive emails from people posing as co-workers and asking for sensitive information, knowing exactly the right phrasing to elicit a response. In fact, some employers have started to create phishing tests. Because internal error can be a major source of data leakage, companies are sending spoof phishing emails to employees. If they fall for it, it becomes a teachable moment.

While the internal issue might not capture as much media attention, it's definitely something that should be on the radar of any security-minded business. In 2014, **81 percent of organizations experienced at least one potential data loss incident.** Drilling down, an organization experiences 1.7 data loss events per hour, 41 times per day—a 41 percent increase over last year.

DATA SENT OUTSIDE THE ORGANIZATION BY EMPLOYEES

PERCENT OF ORGANIZATIONS

	2014	2013	2012
PROPRIETARY INFORMATION	41%	35%	24%
CREDIT CARD DATA	30%	29%	29%
BUSINESS DATA RECORDS	20%	21%	6%
SENSITIVE PERSONAL INFORMATION	25%	22%	
SALARY INFORMATION	13%	14%	13%
NETWORK INFORMATION	13%	14%	
PASSWORD-PROTECTED FILES	10%	10%	14%
CONFIDENTIAL OUTLOOK MESSAGE	5%	5%	7%
BANK ACCOUNT NUMBERS	5%	4%	3%
OTHER	27%	31%	21%

6.1 SOURCE: Check Point Software Technologies

Looking at the types of data that are stolen, proprietary information leads the way, at 41 percent. What's remarkable is that it just keeps climbing. Since 2012, we've seen almost a 71 percent increase. Credit card data was the second leading type of information leaked, though it's remaining steady year to year. The biggest leap looking at the past three years of data, regarding type of data lost, was with business data records, which was six percent in 2012 and is now 20 percent. How does it happen? In some cases, an employee might accidentally include someone from outside the organization in a confidential email. For instance, how many of us have started to type the name of someone in the 'To' field, only to realize that the email client autocompletes with a different recipient with a similar name? In other cases, an ill-intentioned employee might include external recipients in the BCC field of a confidential email. Interestingly, the percentage of companies that see this happening declined between 2012 and 2013, but started to creep up again in 2014. On average, companies experienced four data loss events per day as a result of an email going to several internal recipients and a single external one; when we looked at emails being sent with internal visible recipients (To and CC) and more than one external recipient in BCC field, we saw 15 data loss events per day.

But data also seeps out for other reasons: An employee inadvertently makes private information available online or a third-party vendor—perhaps a temp or contractor—steals the data.

Loss of proprietary information has increased 71 percent over the past three years

Every 36 minutes **sensitive data is sent outside the organization**

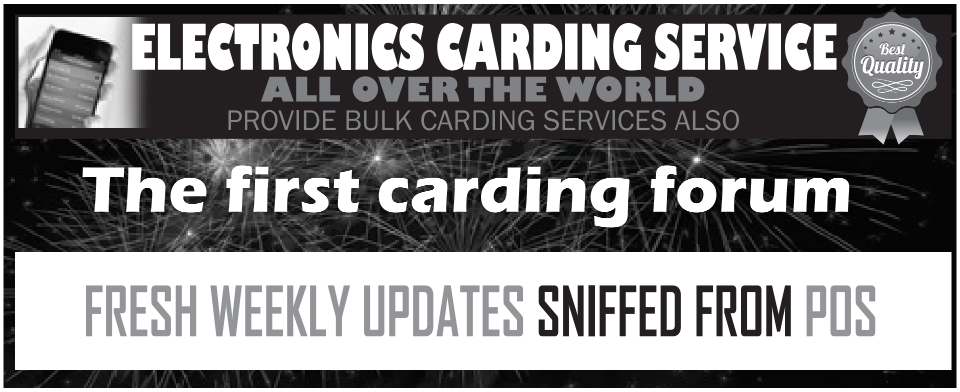
WHERE IS ALL THIS LEADING?

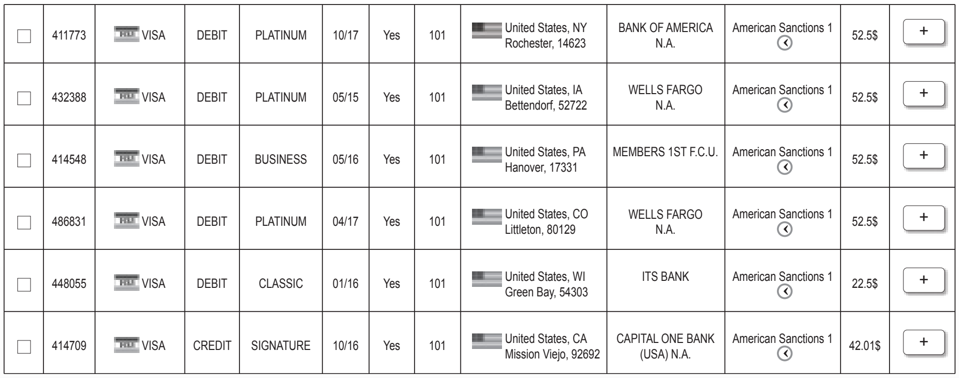
Regardless of whether the data is getting out due to external or internal engineering, the appetite for that information is fed by one thing: financial gain. Cybercrime has not only become profitable; it has become a big business. On the other side of the mirror, the data swiped is not just being sold on the black market, it's being marketed. Websites post the credit cards that are available for purchase with relevant criteria—issuing bank, how "fresh" it is. It's not just quietly passed to one or two people in a dark alley. It's broadcast, in broad daylight.

And it is happening faster than you might imagine. Within 30 minutes of leaving a department store, your credit card information could be "on sale" on the black market.

The fresher the theft of the data, the more money it fetches.

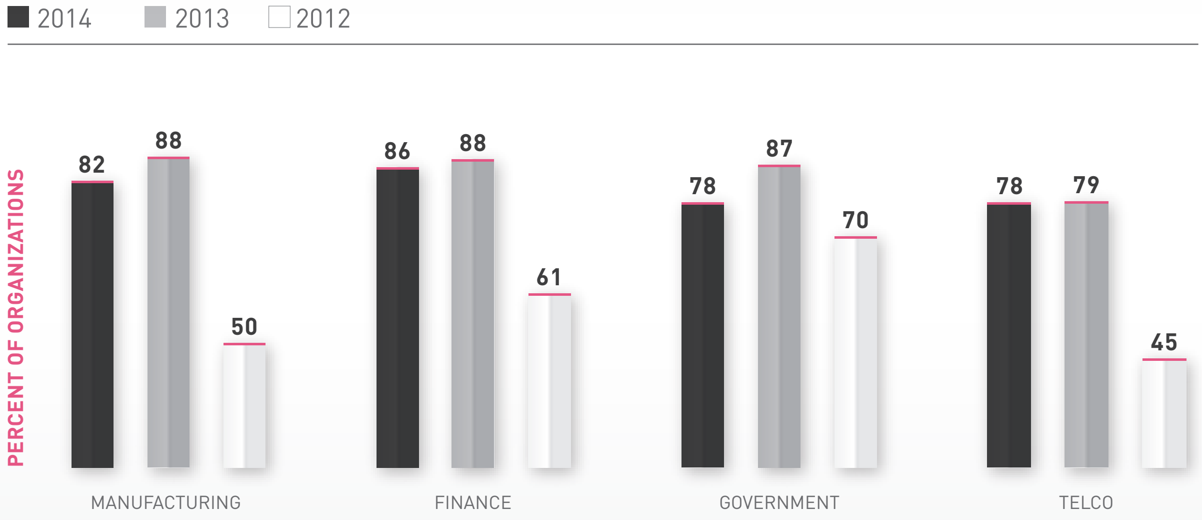
So who pays? In the United States, because of poor retail security practices, judges have ruled that retailers can be sued, allowing banks to recoup their costs.


ELECTRONICS CARDING SERVICE
ALL OVER THE WORLD
PROVIDE BULK CARDING SERVICES ALSO
Best Quality
The first carding forum
FRESH WEEKLY UPDATES SNIFFED FROM POS



□	411773	VISA	DEBIT	PLATINUM	10/17	Yes	101	United States, NY Rochester, 14623	BANK OF AMERICA N.A.	American Sanctions 1	52.5$	+
□	432388	VISA	DEBIT	PLATINUM	05/15	Yes	101	United States, IA Bettendorf, 52722	WELLS FARGO N.A.	American Sanctions 1	52.5$	+
□	414548	VISA	DEBIT	BUSINESS	05/16	Yes	101	United States, PA Hanover, 17331	MEMBERS 1ST F.C.U.	American Sanctions 1	52.5$	+
□	486831	VISA	DEBIT	PLATINUM	04/17	Yes	101	United States, CO Littleton, 80129	WELLS FARGO N.A.	American Sanctions 1	52.5$	+
□	448055	VISA	DEBIT	CLASSIC	01/16	Yes	101	United States, WI Green Bay, 54303	ITS BANK	American Sanctions 1	22.5$	+
□	414709	VISA	CREDIT	SIGNATURE	10/16	Yes	101	United States, CA Mission Viejo, 92692	CAPITAL ONE BANK (USA) N.A.	American Sanctions 1	42.01$	+

ORGANIZATIONS WITH AT LEAST ONE POTENTIAL DATA LOSS EVENT, BY INDUSTRY



6.2 SOURCE: Check Point Software Technologies

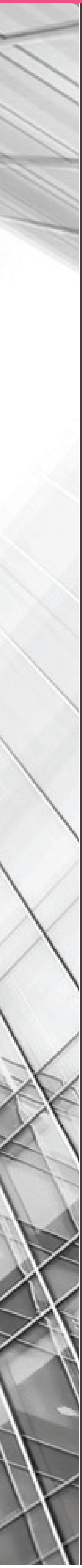
EASY MONEY

Like hunters looking for easy prey, cybercriminals have zeroed in on point of sale (PoS) as their hunting ground. The main reason: So many PoS terminals are running outdated operating systems like Windows XP, which end up going unpatched and unmanaged. If you were tuned into the media during the past year, it would have seemed like one major retailer after another was getting hit with security breaches.

The year started with a bang when Neiman Marcus was breached and lost 1.1 million account records, only to be outdone that same month by hobby store Michaels, which lost three million. As the year continued, taxis, beauty stores, Goodwill, UPS, and Dairy Queen followed. In September, Home Depot topped them all with 56 million. All of this adds up to 112,250,000 lost records within the United States, affecting one in three Americans.

PoS malware infections certainly occur throughout the world, but the United States leads the way with the most infections, in part because it is not yet on the chip and PIN credit card system being used in other countries. Chip and PIN is a global standard of payment that embeds an integrated circuit (IC) chip into the card and can only be authorized when used with a PIN. As part of this standard, retailers will need to update their PoS systems to ensure compatibility. But even with chip and PIN, retailers will still need to stay one step ahead. Infections like the "BackOff" malware, which impacted a large number of U.S. businesses, highlighted a large security vulnerability: The malware pre-installed tools in the supply lines of seven major manufacturers of PoS terminals before being shipped to merchants. Weak or unchanged admin passwords allowed hackers remote access into devices.

The Department of Homeland Security reports that more than 1,000 United States businesses were hit by PoS malware,[27] taking a huge toll on businesses and individuals. In fact, card replacement cost alone added up to $1.3 billion. A LexisNexis study called The True Cost of Fraud [28] says that the average merchant suffered 133 successful fraudulent transactions per month in 2014, up 46 percent from the previous year.



PoS: You Can’t Have Just One Chip

During 2013 and 2014, the retail industry experienced an alarming number of data and security breaches. These attacks resulted in the loss of millions of customer credit cards and personal information. The companies involved experienced negative financial effects from the event, with the largest retailer experiencing a 13% drop in its market valuation and a reduction in comparable-store sales. These breaches impact companies large and small. Between 2013 and 2014, notable names like Michaels, Neiman Marcus, PF Chang’s, Target and Home Depot have all suffered staggering losses from PoS-related data breaches.

Customer concerns over privacy and financial security are shaken, and corporate boards are actively looking for structural changes. The short-term effects are just now coming to light. The long-term impact will only be known in the coming years.

In responding to these types of incidents, companies often pursue knee-jerk reaction tactics. For example, they will focus on the most obvious weakness or choose a method that appears most prominently in the news.

In the case of the recent retail data breaches, much emphasis has been placed on a move to “chip and PIN” credit cards—a global standard of payment that employs two-factor authentication through a physical chip on a card that is tied to a user’s personal identification number (PIN). But, a cursory review of the attack methods associated with the retail breaches shows that chip and PIN would not have prevented these incidents.

The attackers targeting the retail stores used available remote connections to access store networks and installed multiple variants of malware and software tools to capture and export customer data. Shortcomings in store network design and point of sale (PoS) configuration further enabled the attacks by simplifying horizontal movement and malware infestation.

To secure against these types of attacks, take a broader view and implement a multi-layered approach that addresses the entire network—not just the parts believed to be most vulnerable.

RECOMMENDATIONS

Remember that security does not stand still. When you balance your body, there are lots of subtle movements at play that keep you standing. The same goes with how you need to think through your security. To stay ahead of the threats, you need to be constantly assessing and updating as you go. Don't stop with just making sure you're protected from outside attack; make sure you're covered internally, as well. Specifically, we recommend:

- Protecting your data by encrypting it—whether it's at rest or in transit. The goal is to provide a cloak of protection for the data, wherever it goes. When it's encrypted, only individuals who are authorized to view the information will be able to see it.
- Creating layers of protection with checks and balances.
- Helping everyone—from top down—understand the importance of mitigating cyber-related risks to protect intellectual property.
- Involving your workforce in improving your information security posture by educating them on how they can help. Create information security policies that employees can understand and help reinforce.

"It is better to look ahead and prepare than to look back and regret."[29]

-Jackie Joyner Kersee, athlete and olympic medalist

07

CONCLUSION AND RECOMMENDATIONS: THE PATH TO PROTECTION

"Status quo, you know, is Latin for 'the mess we're in'."[30]

–Ronald Reagan, actor and former President of the United States

"The Cold War didn't end in the 1990s. It simply moved online."[31]

-Jose Pagliery, journalist

It's clear that cybercriminals are not slowing down. In fact, based on how bad 2014 was, from a cyber security perspective, analysts expect the security industry to grow tenfold.

Threats can come from any direction and it has become impossible to say that any one organization is safe from attack. In fact, the biggest mistake any organization can make is to believe it is protected, and neglect to revisit its security infrastructure regularly.

When thinking through your security posture, take the time to truly understand your threats and vulnerabilities. Look for contributing factors, and also look at the big picture of where you're trying to lead your organization. The most prepared businesses know that security policy needs to stem from strategic goals, business objectives, and corporate policy—and tie to procedures and requirements, performance measurements, and of course, people at all levels of the organization.

Map out your process and make sure it includes even the most basic steps, such as applying software patches and updates. Also think about your ecosystem of partners and how they tie to the security process.

When it comes to technology, your security program must unify multiple layers and controls.

Given that threats are coming from multiple places, single-layer security architectures and multi-vendor point solutions are no longer adequate.

Start with thinking about your architecture as three interconnected levels.

A software-defined protection architecture based on a three-layer security approach is the best defense against fast-evolving attacks.

Enforcement Layer

Create a gateway- and endpoint-based protection plan that scans, identifies and blocks malware, botnets and weaponized content that is designed to collect and exfiltrate customer information. Assign network- and application-access authentication rules to prohibit unauthorized users and systems from accessing sensitive areas of the network.

Control Layer

Establish administrator-determined security policies and automated protections. Create rules that specifically define access control and data security policies with enforcement points. Restrict applications and system behavior according to 'least privilege' guidelines.

As you look to specific solutions, consider those that allow you to (1) investigate any incoming file types, including secure and encrypted files; (2) identify zero-day threats both within and beyond the operating system; and (3) deliver safe documents with zero malware in zero seconds. The best protection is a combination of the fastest operating solution that offers the top catch rate and protects your business from attack.

Check Point recommends threat prevention that includes:

- Deep OS- and CPU-level sandbox capabilities to detect and block malware
- Threat extraction to reconstruct incoming documents with zero malware in zero seconds

This approach looks for malicious activities at the OS level and exploits at the CPU level, preventing attacks before they occur. Detecting exploit attempts during the pre-infection stage helps you avoid evasion techniques.

When you combine OS- and CPU-level sandboxing with threat extraction, you have a next-generation technology that delivers the best possible catch rate for threats.

Management Layer

Monitor all business-aligned administrator privileges and create comprehensive reporting. Implement intelligence-based threat prevention that updates independently and proactively distributes new protections to enforcement points. Not keeping up to date is one of the huge vulnerabilities in most networks. Implement event management, logging and reporting tools that identify events in real-time and include filtering and analysis tools to ensure administrators have visibility into attacks without getting lost in less critical noise.

WHAT NEXT?

As mobile devices become, increasingly, primary devices, we expect hackers to look to them as their new attack vectors. What's more, according to the Ponemon Institute, 40 percent of mobile app developers do not scan their apps for vulnerabilities before releasing them.[32] Given this reality, and after reviewing what has come from the past year, we see 2015 as the year to define your mobile security and take a more aggressive stance with your security posture. That becomes especially important as the growth of mobile payment systems starts to accelerate.

While some solutions like Apple Pay, Google Wallet and PayPal offer multiple layers of security involving tokenization and encryption, not all of these systems have been thoroughly tested to withstand real-world threats. It's a safe bet that attackers will be searching out vulnerabilities to exploit.

Add to that, ABI Research estimates that the number of wearable computing device shipments will reach 485 million units by 2018.[33] Analyst firm Gartner believes that 4.9 billion things will be in use in 2015, up 30 percent from last year. Of that, the firm expects manufacturing, utilities and transportation industries will see the most use from the Internet of Things (IoT)— with 736 million combined connected things. By 2020, it expects to see 25 billion connected things.[34]

Ultimately, with all that connectivity, we can expect more vulnerabilities, more threats. At Check Point, our mission is clear: We secure the future. Similarly, organizations must also be future-minded. Being clear about long-term objectives and how to optimize the security infrastructure to support your vision is essential.

By understanding potential threats and vulnerabilities; creating a solid plan that aligns with your business; and ensuring protections are integrated into your IT infrastructure, you can turn security into an enabler. And in doing so, you're able to unlock innovation and foster an environment for high performance and productivity.

If you'd like to get a true assessment of your company's security, sign up for a free Check Point Security Check Up at www.checkpoint.com/resources/securitycheckup. Or, to learn more about Check Point and how we can help secure your business, please visit **www.checkpoint.com.**

"The riskiest thing we can do is just maintain the status quo."[35]

-Bob Iger, businessman, chairman/CEO of Walt Disney Company

REFERENCES

1 Stoll, Cliff. "The Call to Learn." TED Talk. February 2006.

2 Obama, Barack. The Cybersecurity and Consumer Protection Summit. February 13, 2015.

3 Check Point Software Technologies. http://www.checkpoint.com/resources/securitycheckup/

4 AV-Test. http://www.av-test.org/en/statistics/malware/

5 Lacy, Sarah. "The Irony of the Social Media Era: It Was Created By the World's Least Social People." Huffington Post, July 15, 2012. http://www.huffingtonpost.com/sarah-lacy/social-media-entrepreneurs-mark-zuckerberg_b_1518471.html

6 Amira, Dan. "Q&A With Nate Silver on His New Book, Whether Romney Has a Shot, and Why He Doesn't Play Fantasy Baseball Anymore." New York Magazine, September 28, 2012. http://nymag.com/daily/intelligencer/2012/09/nate-silver-book-signal-noise-interview.html

7 Check Point Software Technologies. "The Unknown 300 Test Report," 2014. https://www.checkpoint.com/downloads/300TestReport.pdf

8 Saint-Exupery, Antoine de. Wind, Sand and Stars, 1939.

9 Pareles, Jon. "Madonna on 'Rebel Heart,' Her Fall and More." The New York Times, March 5, 2015. http://nyti.ms/1A29332

10 Spamhaus. "The Spamhaus Project." http://www.spamhaus.org/news/article/720/spamhaus-botnet-summary-2014

11 Ward, Jillian. "Power Network Under Cyber-Attack Sees U.K. Increase Defenses," Bloomberg Business, January 8, 2015. http://www.bloomberg.com/news/articles/2015-01-09/power-grid-under-cyber-attack-every-minute-sees-u-k-up-defenses

12 Prince, Brian. "Almost 70 Percent of Critical Infrastructure Companies Breached in Last 12 Months: Survey," SecurityWeek, July 14, 2014. http://www.securityweek.com/almost-70-percent-critical-infrastructure-companies-breached-last-12-months-survey

13 CVE Details. http://www.cvedetails.com/browse-by-date.php; http://www.cvedetails.com/top-50-vendors.php?year=2014

14 Kirk, Jeremy. "An SDN vulnerability forced OpenDaylight to focus on security," CSO, March 25, 2015. http://www.csoonline.com/article/2902902/vulnerabilities/an-sdn-vulnerability-forced-opendaylight-to-focus-on-security.html

15 Reilly, Claire and Musil, Steven. CNET, September 24, 2014. http://www.cnet.com/news/bigger-than-heartbleed-bash-bug-could-leave-it-systems-shellshocked/

16 Gilbert, David. "What is POODLE? The Latest Online Security Threat After Shellshock and Heartbleed," International Business Times, October 16, 2014. http://www.ibtimes.co.uk/what-poodle-latest-online-security-threat-after-shellshock-heartbleed-1470300

17 Singh, Anita. "Hay Festival 2012: Salman Rushdie on security and The Satanic Verses," The Telegraph, June 3, 2012. http://www.telegraph.co.uk/culture/hay-festival/9309641/Hay-Festival-2012-Salman-Rushdie-on-security-and-The-Satanic-Verses.html

18 Pinter, Harold. The Homecoming, 1965.

19 Lunden, Ingrid. "Led By iPhone 6, Apple Passed Samsung In Q4 Smartphone Sales, 1.9B Mobiles Sold Overall In 2014" TechCrunch, March 3, 2015. http://techcrunch.com/2015/03/03/led-by-iphone-6-apple-passed-samsung-in-q4-smartphone-sales-1-9b-mobiles-sold-overall-in-2014/#.w6n4vv:a9vl

20 Gartner. January 5, 2015. http://www.gartner.com/newsroom/id/2954317

21 Taft, Darryl K. "IBM Study Shows Mobile App Developers Neglecting Security," eWeek, March 21, 2015. http://www.eweek.com/developer/ibm-study-shows-mobile-app-developers-neglecting-security.html

22 Schroeder, Stan. "Android Malware Spies on You Even After Phone Is Shut Down," Mashable, February 19, 2015. http://mashable.com/2015/02/19/android-malware-spies-shut-down/

23 Schawbel, Dan. "Eric Schmidt and Jonathan Rosenberg: What We Can Learn From Google," Forbes, September 23, 2014. http://www.forbes.com/sites/danschawbel/2014/09/23/eric-schmidt-and-jonathan-rosenberg-what-we-can-learn-from-google/

24 Battelle, John. "Thoughts on Ford's OpenXC: In the Future, Brands with Open Data Will Win," August 18, 2013. http://battellemedia.com/archives/2013/08/thoughts-on-fords-openxc-in-the-future-brands-with-open-data-will-win.php

25 Irion, Robert. "Opening Strange Portals in Physics," Smithsonian Magazine, December 2011. http://teachers.smithsonian.com/science-nature/opening-strange-portals-in-physics-92901090/?all

26 Giovanni, Nikki. Black Feeling, Black Talk, Black Judgment, 1970.

27 United States Computer Emergency Readiness Team. US-CERT, August 27, 2014. https://www.us-cert.gov/ncas/alerts/TA14-212A

28 LexisNexis. "2014 LexisNexis® True Cost of Fraud^{SM} Study." http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf

29 Schwartz, Larry. "Joyner Kersee Completes Huge Leap," ESPN.com. https://espn.go.com/sportscentury/features/00016055.html

30 Reagan, Ronald. "Address Before a Joint Session of the Tennessee State Legislature in Nashville," March 15, 1982. http://www.presidency.ucsb.edu/ws/?pid=42270

31 Pagliery, Jose. "Russia Attacks U.S. Oil and Gas Companies in Massive Hack,"CNN Money, July 2, 2014. http://money.cnn.com/2014/07/02/technology/security/russian-hackers/

32 Vijayan, Jai. "Rush To Release Resulting In Vulnerable Mobile Apps," Dark Reading, March 20, 2015. http://www.darkreading.com/attacks-breaches/rush-to-release-resulting-in-vulnerable-mobile-apps/d/d-id/1319566

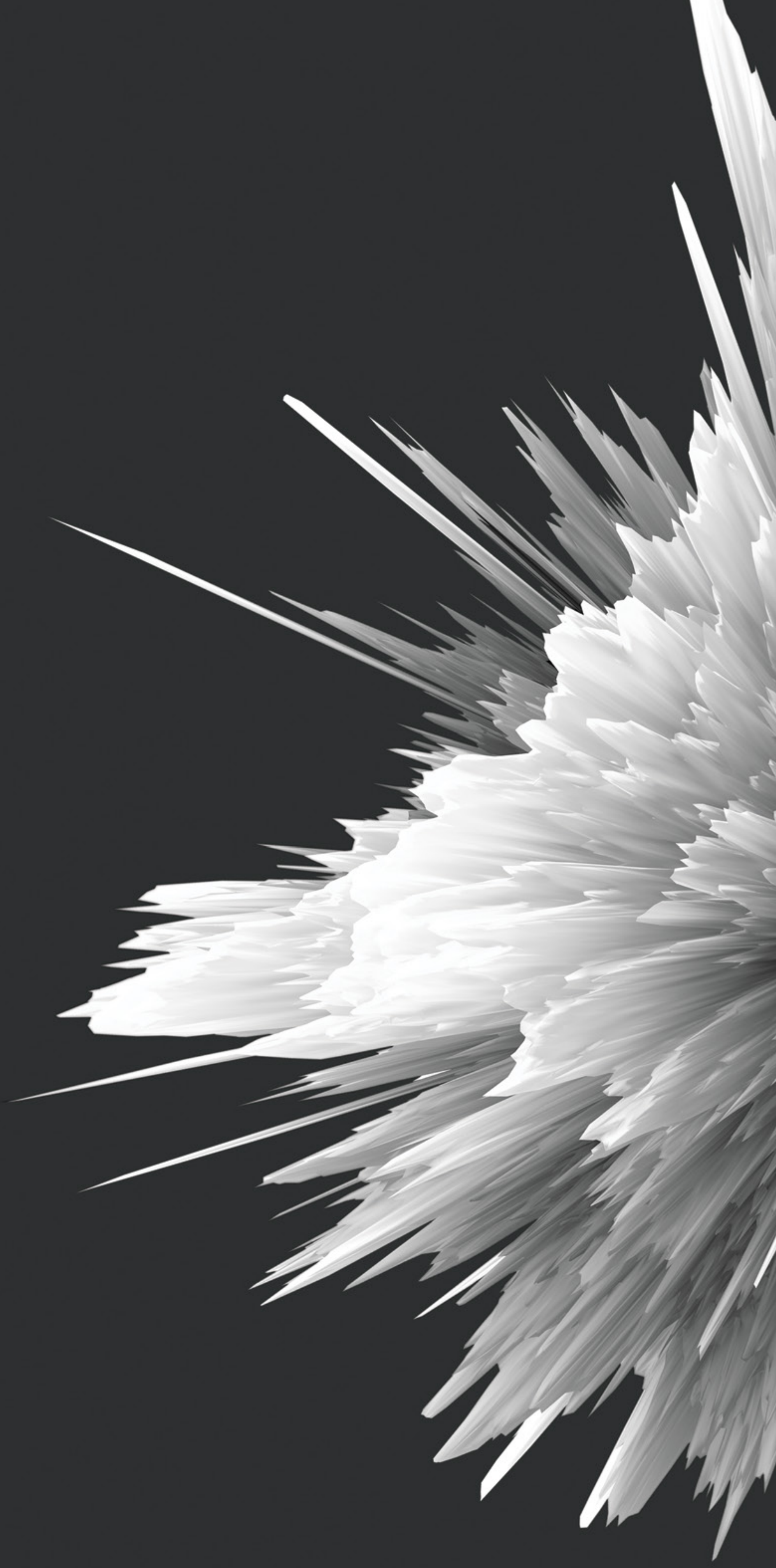
33 ABI Research. "Wearable Computing Devices, Like Apple's iWatch, Will Exceed 485 Million Annual Shipments by 2018," ABIResearch.com, February 21, 2013. https://www.abiresearch.com/press/wearable-computing-devices-like-apples-iwatch-will/

34 Moore, Michael. "Internet Of Things To Hit 4.9 Billion Things By 2015," TechWeekEurope, November 11, 2014. http://www.techweekeurope.co.uk/e-innovation/internet-of-things-4-9bn-gartner-155298

35 Iger, Bob. Disney Shareholder Meeting, Anaheim, NBC News, March 3, 2006. http://www.nbcnews.com/id/11767409/ns/business-us_business/t/pixars-star-disney-shareholders-meeting/#.VSRlovnF9Zt

Check Point
SOFTWARE TECHNOLOGIES LTD

WE SECURE THE FUTURE



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