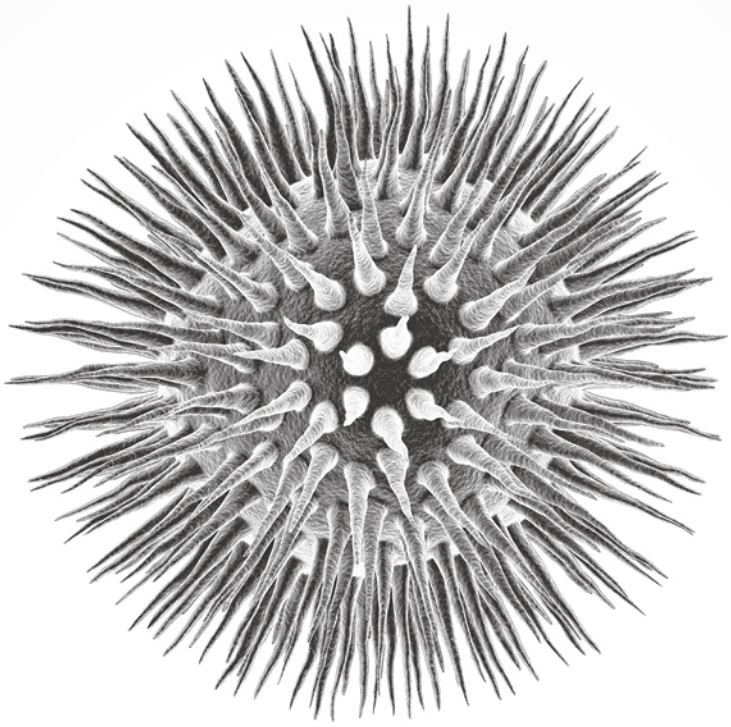
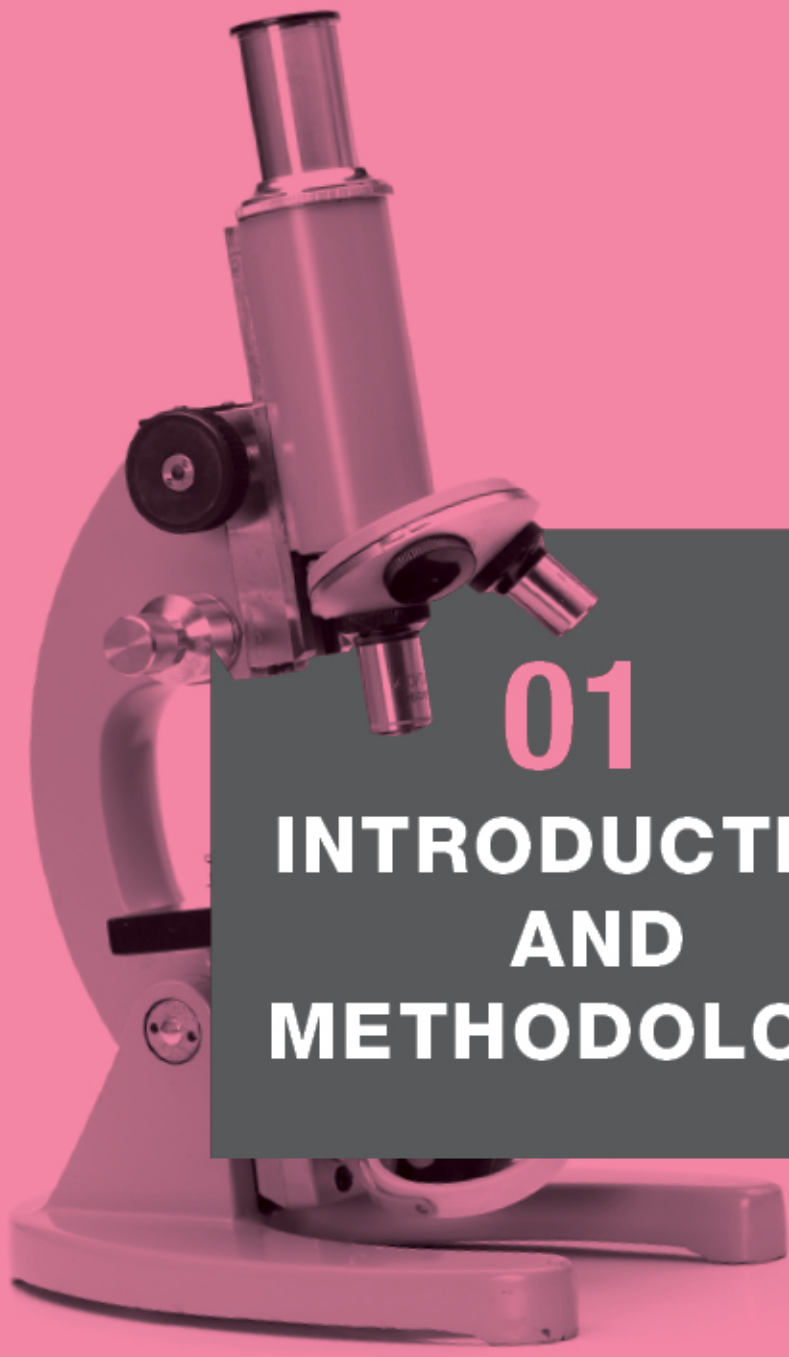
Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



CHECK POINT
SECURITY REPORT
2014

CHECK POINT 2014 SECURITY REPORT



01 INTRODUCTION AND METHODOLOGY

01 INTRODUCTION AND METHODOLOGY

SCANNING THE PRINTOUT, I COULD SEE THE HACKER GOING FISHING ON THE MILNET. ONE BY ONE, HE TRIED FIFTEEN AIR FORCE COMPUTERS, AT PLACES LIKE EGLIN, KIRTLAND, AND BOLLING AIR FORCE BASES. NO LUCK. HE'D CONNECT TO EACH COMPUTER, TWIST THE DOORKNOB ONCE OR TWICE, THEN GO ON TO THE NEXT SYSTEM. UNTIL HE TRIED THE AIR FORCE SYSTEMS COMMAND SPACE DIVISION. HE FIRST TWISTED ON THEIR DOORKNOB BY TRYING THEIR SYSTEM ACCOUNT, WITH THE PASSWORD OF "MANAGER." NO LUCK. THEN GUEST, PASSWORD OF "GUEST." NO EFFECT. THEN FIELD, PASSWORD "SERVICE." […] SHAZAM: THE DOOR HAD SWUNG WIDE OPEN. HE'D LOGGED IN AS FIELD SERVICE. NOT JUST AN ORDINARY USER. A COMPLETELY PRIVILEGED ACCOUNT. […] SOMEWHERE IN SOUTHERN CALIFORNIA, IN EL SEGUNDO, A BIG VAX COMPUTER WAS BEING INVADED BY A HACKER HALFWAY AROUND THE WORLD.

Clifford Stoll, *The Cuckoo's Egg*[1]

More than twenty-five years ago, a UNIX admin tracked a 75-cent billing error back to an Eastern Bloc spy ring that was attempting to steal secrets from the United States government and military. The story of how he traced a path from the initial red flags to the discovery of the larger infestation and his battle against the intruder was recounted in *The Cuckoo's Egg* and remains a model of the challenges of cyber defense. The technologies involved, the means of connection, and the methods of intrusion have evolved tremendously since the late 1980s, yet identifying compromised systems, incident responses, and securing systems and data against future attacks continue to define the core challenges of organizations worldwide, regardless of size and industry.

In 2013, information security gained its greatest prominence in the public consciousness, driven by high-profile data breaches. The theft and publication of U.S. intelligence information dominated the headlines for much of 2013 and shook diplomatic relationships across the globe. Large-scale breaches of payment card data erupted throughout the year and ruined the holiday season for major retailers and countless consumers alike. Cyber warfare and "hacktivism"[2] reshaped the nature of conflicts among people and nations, even as the emergence of the "Internet of Things"[3] brought more aspects of daily life onto the grid—and rendered them susceptible to threats.

Within the security community, an explosion of unknown malware—not just new threats, but new ways of creating and deploying undetectable threats on a massive scale—brought into question the viability of existing strategies and technologies. Even more familiar types of malware proved stubbornly resistant to the defenses in place, while mobility, consumerization and "shadow IT" vastly increased the complexity of the security challenge.

5 QUESTIONS THAT EVERY ENTERPRISE NEEDS TO ASK

1. HOW HAS TODAY'S RAPIDLY EVOLVING SECURITY LANDSCAPE AFFECTED YOUR ORGANIZATION?

2. WHAT THREATS HAVE YOU FACED, AND WHICH EMERGING RISKS MOST CONCERN YOU?

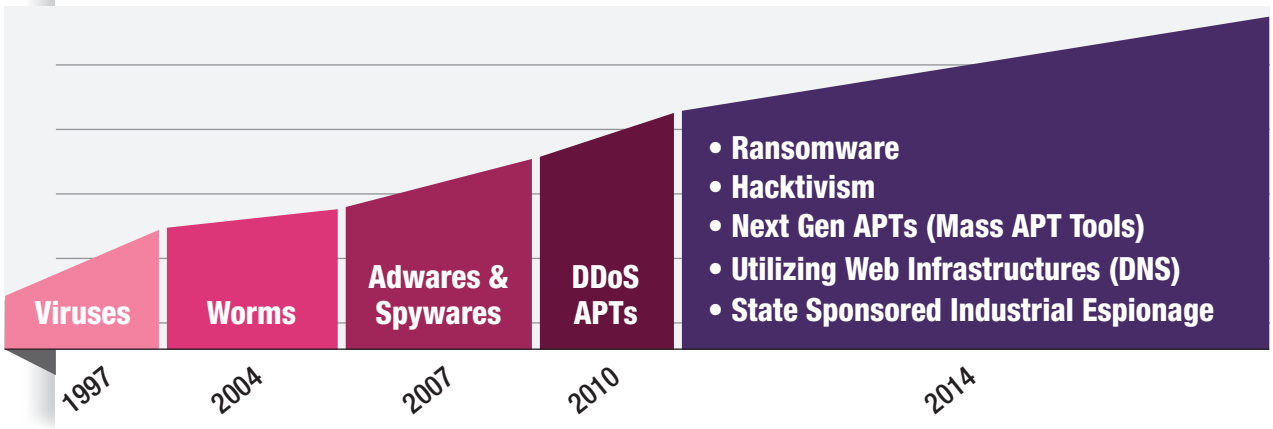
3. DO YOU FEEL THAT YOU HAVE THE RIGHT STRATEGY AND TOOLS TO RISE TO THE CHALLENGE—OR ARE YOU INCREASINGLY OVERWHELMED BY WAVE AFTER WAVE OF TROUBLING DEVELOPMENTS?

4. WHAT NEW MEASURES WILL YOU ADOPT IN THE YEAR TO COME?

5. HOW WILL YOU HELP YOUR ORGANIZATION AS A WHOLE TO MOVE TO A MORE SECURE FOOTING?

The Check Point security research team analyzed a year of event data from more than 10,000 organizations to identify the critical malware and information security trends in 2013 that organizations must address in 2014 and beyond. The Check Point *2014 Security Report* presents the results of our research. This in-depth analysis of security threats and trends in 2013 will help security and business decision-makers understand the range of threats facing their organizations. The report also includes recommendations on how to protect against these and future threats. The highlights of our research are:

Malware Trends



AN AVERAGE DAY IN AN ENTERPRISE ORGANIZATION

Every **1 min** a host accesses a malicious website

Every **3 mins** a bot is communicating with its command and control center

Every **9 mins** a High Risk application is being used

Every **10 mins** a known malware is being downloaded

Every **27 mins** an unknown malware is being downloaded

Every **49 mins** sensitive data is sent outside the organization

Every **24 h** a host is infected with a bot

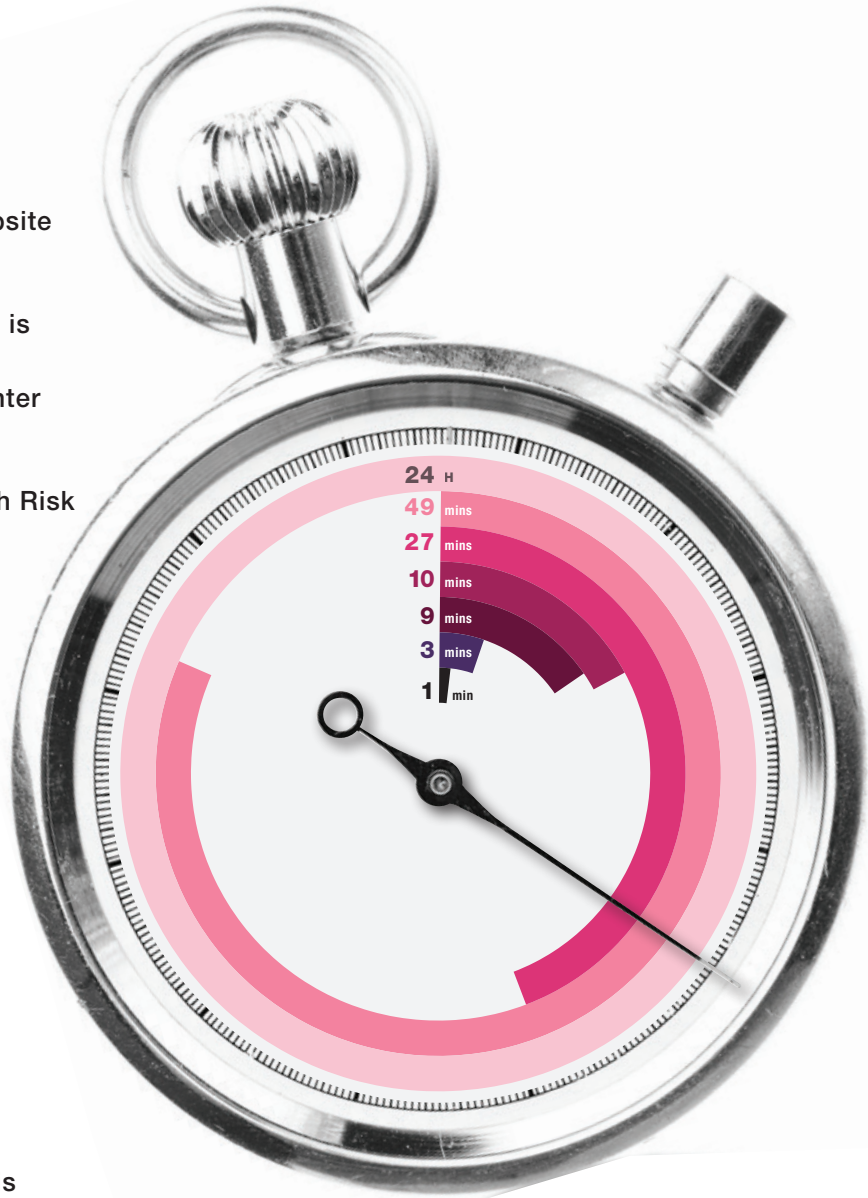
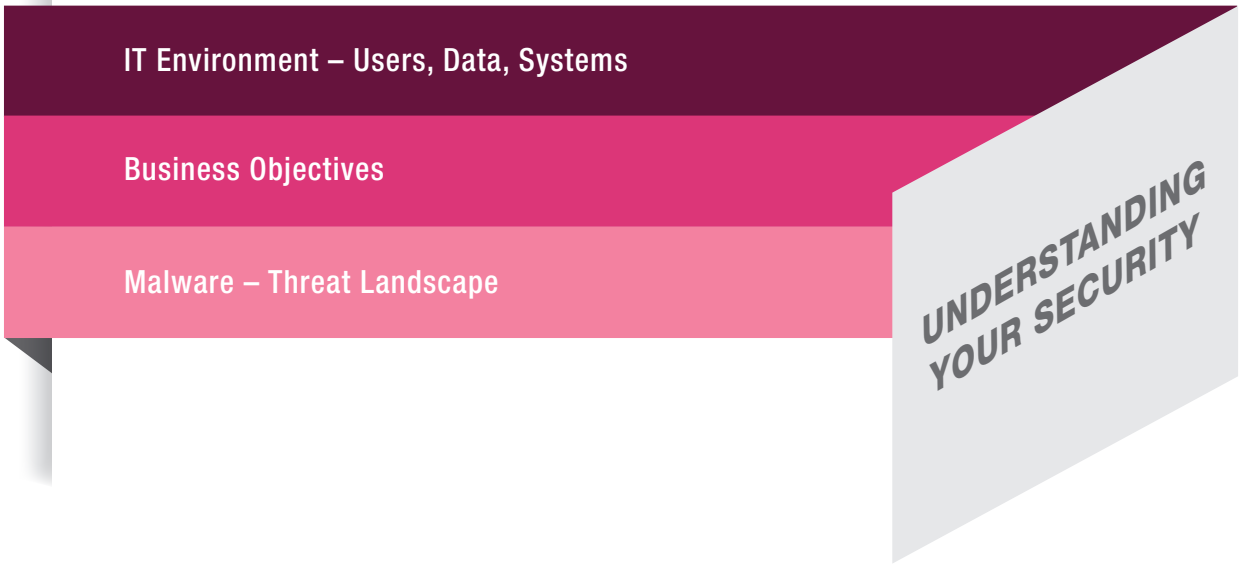


Chart 1-1

Source: Check Point Software Technologies

COMPLETE THREAT PICTURE



- The use of unknown malware exploded, driven by the trend of malware "mass customization"[4]—an average of 2.2 pieces of unknown malware (malware that hasn't been seen before) hit organizations every hour.
- Malware exposure and infections increased across the board, reflecting the increasing success of targeted malware campaigns—in 2013, 73% of organizations had at least one bot detected, compared with 63% in 2012.
- Every category of high-risk application increased their presence in enterprises worldwide—for example, 63% of organizations saw BitTorrent usage, compared with 40% in 2012.
- Data loss incidents increased across industries and data types—88% of organizations experienced at least one potential data loss incident, compared with 54% in 2012.

Data sources for this report

The Check Point *2014 Security Report* is based on a collaborative research and analysis of security events gathered from Check Point security gateway threat analysis reports (Security Checkup)[5], Check Point Threat Emulation[6] sensors, Check Point ThreatCloud™ [7], and Check Point Endpoint Security reports.[8]

A meta-analysis of network security events at 996 companies was conducted using data collected from Check Point Security Checkup assessments, which scanned the companies' incoming and outgoing live network traffic. This traffic was inspected by Check Point multi-tier Software Blades[9] technology to detect a variety of high-risk applications, intrusion attempts, viruses, bots, sensitive data loss and other security threats. The network traffic was monitored in real time by implementing the Check Point Security Gateway[10] inline or in monitor (tap) mode.

On average, each organization's network traffic was monitored for 216 hours. The companies in our research reflected a wide range of industries located globally as depicted in Chart 1-2.

In addition, events from 9,240 security gateways were analyzed using data generated by Check Point ThreatCloud. ThreatCloud is a massive security database updated in real time and populated with data collected from a large network of global sensors strategically placed around the globe. ThreatCloud gathers threat and malware attack information and enables identification of emerging global security trends and threats, creating a collaborative network to fight cyber crime. For our research, ThreatCloud data gathered over the full 12 months of 2013 was consolidated and analyzed.

Threat data for unknown malware was gathered from Check Point Threat Emulation sensors for the period between June and December 2013. Check Point Threat Emulation performs cloud-based sandboxing and dynamic analysis of suspicious files detected by Check Point gateways. Anonymized Threat Emulation data from 848 security gateways was relayed into ThreatCloud for aggregation, correlation and advanced analysis.

Finally, a meta-analysis of 1,036 Endpoint Security reports in a variety of organizations was conducted. This security analysis scanned each host to validate data loss risks, intrusion risks and malware risks. The analysis was performed with a Check Point Endpoint Security report tool which checks whether an antivirus solution was running on the host, if the solution was up-to-date, whether the software was running on the latest version, and more. This tool is free and is publicly available. It can be downloaded from the Check Point public website.

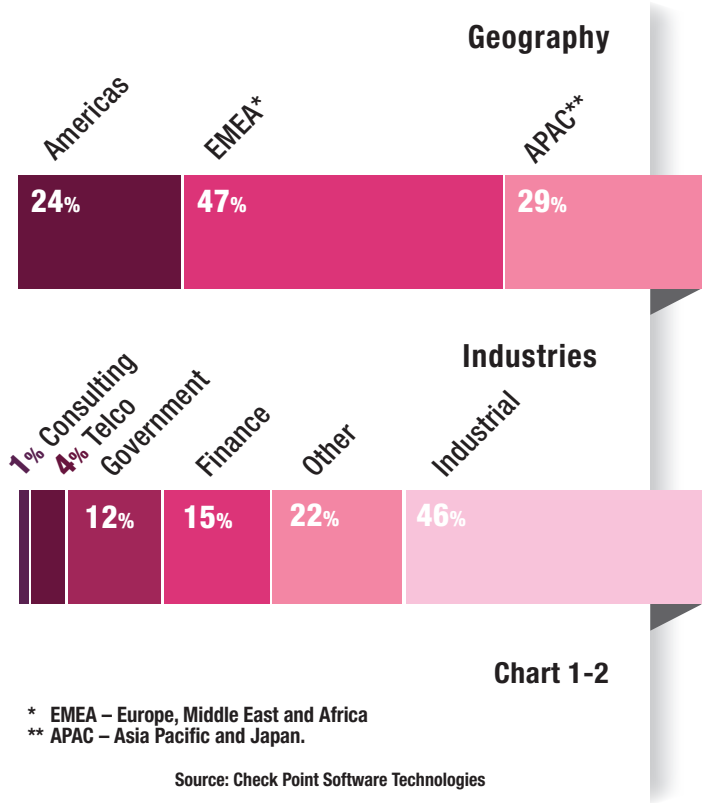


Chart 1-2

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

Source: Check Point Software Technologies

The Check Point *2014 Security Report* core data is complemented with examples of published incidents that illustrate the nature of today's threats, their impact on the affected organizations and their implications for the security community. Expert recommendations provide guidance for ensuring that your security strategy and solutions are relevant and effective for protecting against today's security risks. The report is divided into chapters addressing unknown malware, known malware, high-risk applications and data loss.

02

THE EXPLOSION OF UNKNOWN MALWARE

02 THE EXPLOSION OF UNKNOWN MALWARE

The threat of unknown malware

Traditional security technologies such as Anti-Virus and Intrusion Prevention systems are most effective in detecting attempts to exploit known software and configuration vulnerabilities and to some extent they are also preemptive in protecting against unknown exploits. Hackers understand this and have the luxury of testing their new malware and exploits against these technologies to check whether they are detected.

The arms race between security vendors and hackers leads to a fast-paced evolution in the techniques used by hackers, who are continuously trying to use both unknown vulnerabilities (also known as zero-day exploits, since it usually takes hours or days until they are detected and protections are provided for them) and unknown infection methods in order to circumvent security defenses.

THE KNOWN IS FINITE,
THE UNKNOWN INFINITE

Thomas Henry Huxley[11]

In late 2013, Check Point malware researchers working with our Threat Emulation service discovered and analyzed a new malware variation that employed a sophisticated combination of techniques to hide itself from proxies and anti-malware solutions. Referred to as "HIMAN"[12] by industry researchers, this malware exemplified the traits of the targeted attacks that are challenging enterprises and IT security professionals around the world.

A Security Gateway run by a Check Point customer subscribed to Threat Emulation service scanned a Microsoft Word document that was attached to an email

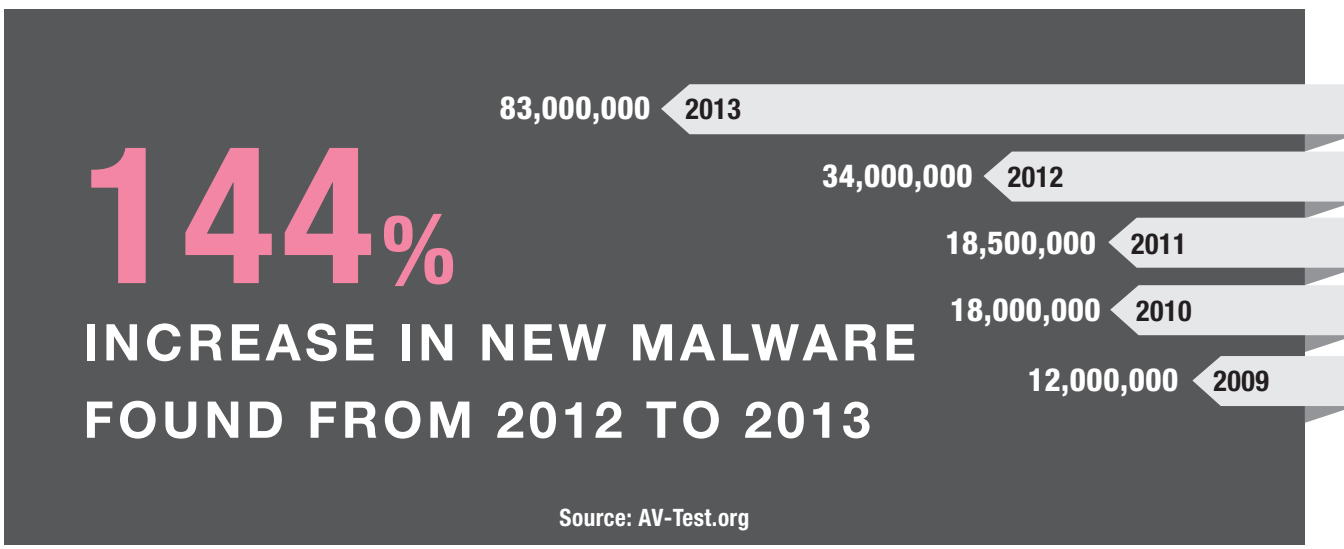


Chart 2-1

2.2

PIECES OF UNKNOWN MALWARE HIT AN ORGANIZATION EVERY HOUR

from the address "boca_juniors@aol.com" with the Subject line "Reception Invitation." When opened in a sandbox environment, it exploited a known vulnerability (CVE-2012-0158) in order to drop a file named "kav.exe" in the user's Local Settings\Temp folder of the target computer. The name of the dropper file seems to be a decoy initial name intended to resemble the Kaspersky antivirus executable[13], and the malware itself appears to be related to previous malware campaigns which researchers attributed to one or more Chinese APT groups. Analysis revealed that the file is a two-stage dropper that renames itself in the process of installing itself on the target system, and then hooks the explorer.exe process to load a malicious DLL.

Check Point security researchers conducted a search of databases of known malware and found that no antivirus vendor was able to detect this malware at the time it was discovered.

The malware injected a malicious library (mswins64.dll), using a series of Windows function calls and mutual exclusion checking to install the malware in the client system in a manner designed to avoid detection by existing anti-malware solutions. Once installed, the malware wrote an entry in the registry using a registry path other than the well-known ones that are commonly employed by the malware process—and which are therefore more closely monitored by anti-malware software. This combination of lesser-used API calls and registry paths enables the malware to increase its chances of evading detection.

HIMAN shows how malware writers are leveraging expertise in Windows API calls, OS behavior and the operation of anti-malware tools to avoid detection, without having to go to the expense of developing or purchasing a true zero-day vulnerability. This sophistication extends to the command and control (C&C) communications and exfiltration processes as well: HIMAN can brute-force outbound proxies using stored credentials, encrypt collected data using AES[14], and employ obfuscation techniques during exfiltration to evade outbound filtering.

Once successfully installed, and having established a verified connection to a functioning C&C server, HIMAN dynamically composes and runs a script that collects data about running services, local accounts with Administrator rights, and other information about system configuration and any parts of the local network that are visible to the infected machine. Armed with this information, an attacker has a map of the local network and a launch pad into their target organization for further reconnaissance, lateral movement, exfiltration and execution of attacks on servers, systems and business processes.

Using a combination of known and rare techniques to establish a foothold in the network of a targeted organization and steal sensitive information, the HIMAN malware highlights both the flexibility of malware writers and attackers, and the challenges facing security professionals in 2013.

LESS THAN 10% OF ANTIVIRUS ENGINES DETECTED UNKNOWN MALWARE
WHEN IT WAS FIRST CAUGHT IN THE WILD

CREATING UNKNOWN

IS SO EASY A CHILD COULD DO IT

How did we get here?
The evolution of unknown malware

For several years, the dangers of targeted attacks and advanced persistent threats (APT) have garnered much of the attention in the information security world. APTs burst onto the scene in 2010 with the Stuxnet[15] targeted attack, in which a highly specialized, purpose-built piece of malware destabilized the control system of an Iranian nuclear centrifuge as part of a state-sponsored combined kinetic attack and cyber attack.

This new breed of malware challenged many of the conventional malware defenses in three main ways. First, Stuxnet was very specialized, having been researched and designed for a specific system, in a specific environment, and with a specific objective in mind. Second, it was very rare, which meant that it had never been exposed to the collection and analysis networks that antivirus vendors had developed to keep up with the "mass market" viruses and bots that had defined the malware landscape for a decade, and it had stayed quiet, operating undetected for an unknown period of time—potentially years. Finally, the motive behind Stuxnet differed sharply from the high-profile points-scoring that characterized viruses and the majorityof the worms, such as Code Red[16] and Sasser[17], that followed them. Because of this motive, it was clear that whoever was behind Stuxnet would be persistent.

In short, Stuxnet represented a new kind of malware that existing antivirus and intrusion prevention technologies were ill-equipped to fight—targeted, rare and motivated. In this sense, it was the vanguard of a wave of custom malware that would demand a new set of tools and strategies. The emergence of HIMAN highlights the continuing evolution of this trend and the threat it poses.

33%

OF ORGANIZATIONS DOWNLOADED AT LEAST ONE INFECTED FILE WITH UNKNOWN MALWARE

TARGETED ATTACK, GLOBAL CAMPAIGN

On October 22, 2013, a media company received six suspicious emails which were subsequently analyzed by the Check Point Threat Emulation service.

- From: No-Replay@UPS.COM
- Subject: UPS Delivery Notification
- Attachment: invoiceBQW8OY.doc (MD5 ad0ef249b1524f4293e6c76a9d2ac10d)

During automated simulation in a virtual sandbox of a user opening a potentially malicious file, multiple abnormal behaviors were detected:

- Microsoft Word crashed and reloaded with an empty document
- A registry key was set
- A new process was initiated on the end device

As a result, Check Point Threat Emulation determined that this file was malicious.

Further analysis by Check Point security researchers discovered that the documents from all six emails were identical and exploited the CVE-2012-0158 vulnerability affecting Microsoft Word. This vulnerability, also known as the MSCOMCTL.OCX RCE[18], allows remote code execution on the end device.

Analysis identified the malicious payload as a customized variant of the Zbot Trojan[19], which steals information by man-in-the-browser attacks, keystroke logging, form grabbing and other methods. Registering these samples at VirusTotal[20] revealed a low (<10 percent) detection rate for both the malicious attachment and the Zbot variant at the time of submission.

Check Point security researchers analyzed the different URLs from which the malicious document was downloaded and determined that a list of unique parameters passed to the infecting servers was in fact a Base64 encoded target designator containing the targeted email address. These unique URLs represented email addresses of users in large international organizations—including financial institutions, international car manufacturers, telcos, government agencies, and North American education and municipal organizations—that were targeted by this attack. These targets indicate that the attacks are part of a targeted campaign designed to capture user credentials, banking information and other information that could be used to gain access to the targeted organizations' most sensitive data.

35%

OF FILES INFECTED WITH UNKNOWN MALWARE ARE PDFs

2013: Promising start, disappointing finish

Security administrators are becoming more and more acquainted not only with targeted attacks, but also with the new tools required to fight them. Automated, network-based malware sandboxing technologies were well-known tools to security teams at large companies and public agencies, who deployed them as add-on layers to their existing security infrastructure to help detect targeted malware that might otherwise evade their existing signature- and reputation-based defenses at the gateway and endpoint.

However, 2013 saw a dramatic increase in the frequency of "unknown malware"—attacks that applied the obfuscation and evasion techniques of APTs to known malware in targeted campaigns with a global reach (see inset: *Targeted Attack, Global Campaign*). While laser-focused, targeted attacks with highly specialized malware remain a challenge, now "mass customization" means that the heightened effectiveness of targeted malware is also available to broader-reaching campaigns that are motivated by financial gain.

"Unknown" or "zero-day"

It is important to distinguish between unknown malware and what are often referred to as "zero-day" exploits. Zero-day malware exploits a previously unknown and unreported vulnerability for which there is no patch. Unknown malware refers to malicious code that exploits a known vulnerability or weakness, but cannot be detected at the time of its discovery even by up-to-date antivirus, anti-bot or Intrusion Prevention System (IPS) solutions. The window of effectiveness for an unknown malware is often only 2–3 days, because its existence in the wild gives antivirus vendors time to detect it on their global networks and build signatures for it.

This is a crucial distinction because it enables us to understand the true nature of the kinds of malware that exploded on the scene in 2013.

Making the unknown known

In 2013, Check Point emulation engines, an advanced form of automated malware sandboxing, deployed around the world, detected that 2.2 pieces of unknown malware struck organizations every hour, a rate of 53 every day.

Check Point research found that two main factors drove this sudden increase in frequency:

1. Attackers were employing automated mechanisms for creating evasive, unknown malware on a large scale, and then targeting organizations around the world through coordinated campaigns in order to maximize their effectiveness.
2. The manual investigation and response processes that had been employed to mitigate targeted attacks would be unable to keep up with this new high volume of incidents.

How Sandboxing Works

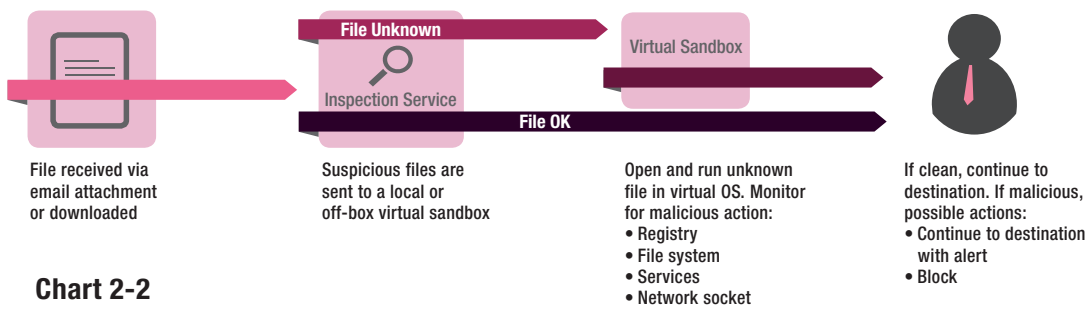


Chart 2-2

Analysis of detections in 2013 showed that the majority of unknown malware was delivered to targeted customers via email, most often embedded in attachments. In 2013, PDF was the most popular format, accounting for almost 35 percent of the files detected by emulation to contain unknown malware, designed to exploit unpatched versions of Adobe Reader (Chart 2-3). Ongoing research shows that that the EXE and archive formats are also popular, accounting for 33% and 27% of malicious files analyzed, respectively.

Of the Microsoft Office file formats, the most popular was Word (.doc), though our analysis of malware sandboxing data found that attackers spread their attacks around other formats as well. In all, we detected unknown malware in 15 different Office file types, including template files for Word and PowerPoint, and multiple Excel formats. Although the majority of malicious archive files were in the ZIP format—presumably because all Windows systems have the ability to open ZIP archives—Check Point analysis nonetheless detected malware in all of the other major archive file types, such as tar, RAR, 7z and CAB.

A flood of new malware

Analysis of Check Point 2013 malware data highlights the high frequency with which unknown malware was detected at gateways around the world. Data from external sources confirmed these findings. AV-TEST[21], an independent IT security and anti-virus research institute, registers over 220,000 new malicious programs every day. AV-TEST recorded over 80 million new malware in 2013, more than double compared with 2012.

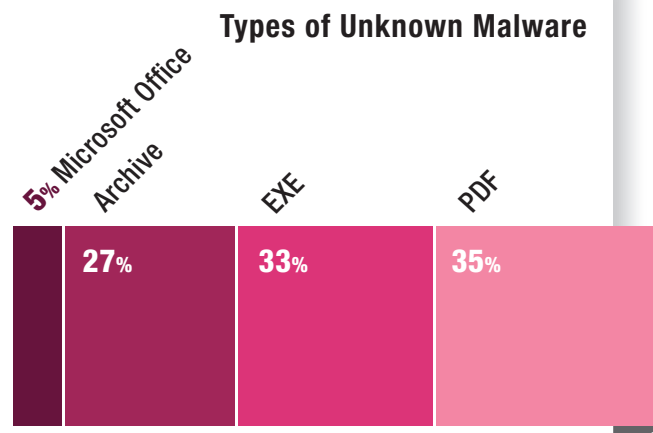


Chart 2-3

Source: Check Point Software Technologies

2.2 PIECES OF UNKNOWN MALWARE STRUCK ORGANIZATIONS EVERY HOUR, A RATE OF **53 EVERY DAY**

Our research into 2013 malware data sheds much greater light on this trend and its widespread impact. Across our entire sample, one-third of organizations downloaded at least one infected file with unknown malware.

TALES FROM THE CRYPTER

In order to bypass detection by anti-malware software, modern malware authors maintain and use specialized obfuscation tools called "crypters." To verify that their variants are undetected, malware authors avoid online antivirus scanning platforms such as VirusTotal and others which share samples with anti-malware vendors, and instead utilize private services such as RazorScanner, Vscan (aka NoVirusThanks) and chk4me. Crypters are classified by hacker communities as UD (UnDetectable) or FUD (Fully UnDetectable) according to their success at evading antivirus detection.

In 2013, Check Point Threat Emulation detected a crypted and previously unknown malware variant designed to deliver the DarkComet remote administration tool (RAT)[23]. In the case of our detected sample, an embedded PDB string revealed it to be a product of the iJuan Crypter, which is available online both as a free (UD) version as well as a premium (FUD) purchase option. Technically classified as a Portable Executable (PE)[24] Packer, and not to be confused with encrypting ransomware such as CryptoLocker[25], crypters like this sample disguise executables through the use of various encryption and encoding schemes, cleverly combined and recombined, often more than once.

This detected sample, which was able to evade most antivirus solutions, was compared with a similar detection from a different country, which was determined to be a differently obfuscated version of the same DarkComet payload, and to be communicating to the same C&C server. Together, these factors indicate that these two distinct detections—one in Europe and the other in Latin America—are in fact part of the same campaign.

These detections highlight the inner workings of the family of advanced attacks that are changing both the threat landscape and the range of solutions that security managers need in order to defend their networks and their data.

This explosion of unknown malware has been driven in part by the accessibility of obfuscation techniques that had in the past required specialized skills, tools or both (see inset: *Tales from the Crypter*)[22]. The cases we have studied in this chapter illustrate the ways in which the malware now being delivered has achieved a higher degree of sophistication than often associated with mere variants. This sophistication compounds the challenges they pose because it requires more subtle, intelligent detection and analysis capabilities to be deployed on a scale beyond the management, monitoring and incident response resources available in many organizations.

Recommendations

The explosion in 2013 of unknown malware means that organizations must revisit tools and processes deployed primarily to detect and respond to low-volume targeted attacks. Detection-only capabilities that require manual mitigation and lack automatic blocking leave security teams overwhelmed as they attempt to keep up with the wave of unknown malware striking their networks.

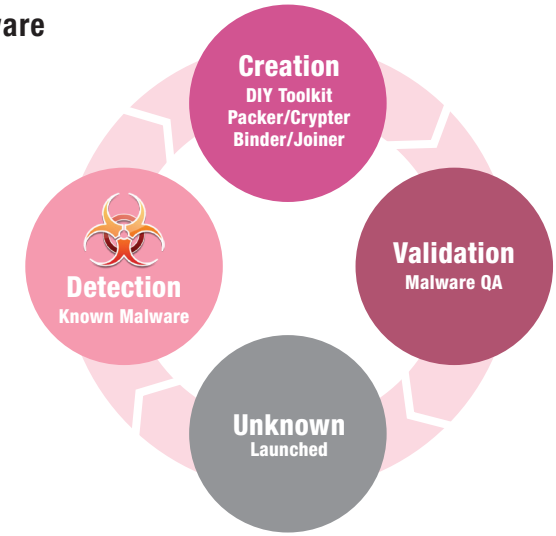
Emulation, or advanced automated malware sandboxing, is now a must-have solution for any organization. Even the most responsive antivirus, anti-bot and IPS solutions will face a 2–3 day window during which unknown malware remains undetected—an interval more than sufficient for attackers to gain a foothold within an organization.

Life Cycle of a Malware

DIY Kit/Malware Tookit
SpyEye
Zeus Builder
Citadel Builder

Crypter/Packer
UPX GUI
PFE CX
Indectables.net

Joiner/Binder
File Joiner
EXEBundle



Malware QA
Multi-AV Scan
NoVirusThanks

Critically, these solutions must be an integral part of an organization's security infrastructure rather than an additional layer that runs on top of it. Organizations should look for emulation solutions that can provide:

- **Integration**—Seamless integration with existing gateways, mail and endpoint infrastructure is the only way to scale and deploy without increasing complexity and cost. Mail integration is especially critical as email is the primary attack vector against clients both on and off the network.
- **Prevention**—Detection-only approaches are no longer sufficient for high-volume unknown malware. Organizations must look for prevention-based solutions that provide the ability to detect and automatically block unknown malware before it can reach its destination.
- **Automation**—Reducing manual processes for analysis and mitigation enables organizations to keep up with these attacks while also addressing other security and business objectives. Automated prevention is critical, but so are reporting and workflow integration for efficient notification and response.

The rapid rise of unknown malware clearly changes the game in security, calling for new strategies and technologies as well as an approach to security that can provide effective protection without overwhelming the organization's resources. Adapting to these new requirements should be seen as a top priority—and one of considerable urgency—for every organization. At the same time, more familiar and long-established types of attacks continue to pose a serious threat, and require continued vigilance and proactive countermeasures. The latest trends on known malware are explored in the next chapter.

EMULATION, OR ADVANCED AUTOMATED MALWARE SANDBOXING, IS NOW A **MUST-HAVE SOLUTION** FOR ANY ORGANIZATION

03

THE DEVIL YOU KNOW

Malware in the Enterprise

03 THE DEVIL YOU KNOW: MALWARE IN THE ENTERPRISE

Information security dominated the news in 2013, from revelations about state-sponsored cyber surveillance programs and hacks on organizations such as the *Washington Post* and Yahoo, to high-profile malware outbreaks like CryptoLocker and breaches of retail customer data on a scale that dwarfed anything previously reported.

The past year made 2012 seem calm by comparison—and 2012 was not a quiet time for cyber attacks by any stretch. That year was itself notable for the quantity and scale of its cyber attacks, including surging hacktivism, state-sponsored hacks on media and businesses, and data breaches at financial institutions around the world. The top 2012 malware trends noted in the Check Point *2013 Security Report*[27] were:

- Democratization of advanced persistent threats
- Pervasiveness of botnets
- Increase in vulnerabilities expanding the attack surface

> WE WORRIED FOR DECADES ABOUT WMDs—WEAPONS OF MASS DESTRUCTION. NOW IT IS TIME TO WORRY ABOUT A NEW KIND OF WMDs—WEAPONS OF MASS DISRUPTION.
>
> **John Mariotti**[26]

In our research, we found that these trends not only continued in 2013, but accelerated in almost every regard, from the frequency with which malware enters organizations to the extent and severity of bot infections.

Faster is not always better

If there is a single statistic from Check Point security research in 2013 that best captures the malware challenges now confronting security administrators, it is the rising frequency with which malware was downloaded by the organizations we studied (Chart 3-1). In 2012, almost half (43 percent) of the organizations we analyzed experienced a user downloading malware at a rate of less than one per day, and another 57 percent experienced a malware download every 2 to 24 hours.

84%

OF ORGANIZATIONS DOWNLOADED A MALICIOUS FILE

In 2013, by contrast, almost two-thirds (58 percent) of organizations experienced a user downloading malware every two hours or less. This acceleration in the pace of cyber attacks on organizations is reflected across all of the statistics from our latest security research. In this chapter, we explore the specifics of this shift and its implications for security and managers, with a look first at the changes in the vulnerabilities that create the attack surface for malware writers and hackers.

58 PERCENT OF ORGANIZATIONS EXPERIENCED A USER DOWNLOADING MALWARE **EVERY TWO HOURS OR LESS**

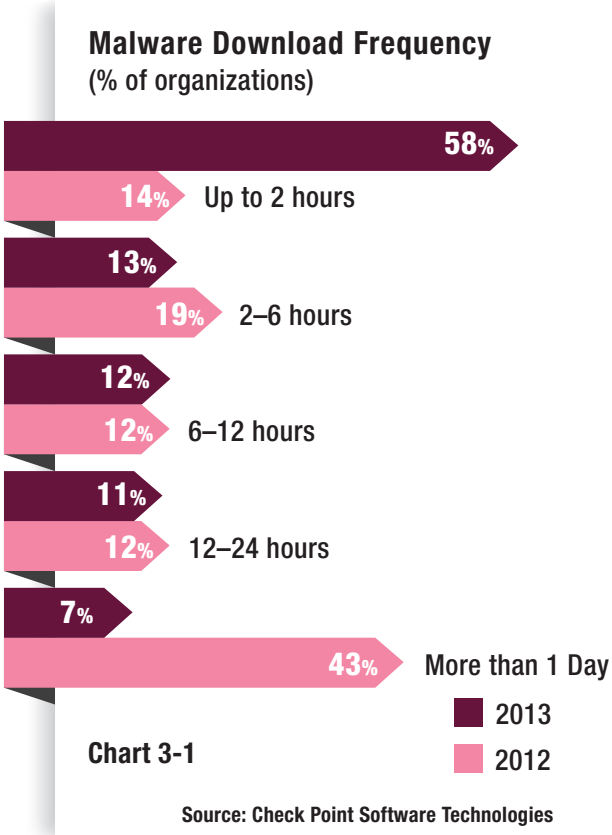


Chart 3-1

Source: Check Point Software Technologies

Fewer vulnerabilities, or a false hope?

The only risk factor in the information security landscape that did not increase in 2013 was the number of reported vulnerabilities. At first glance, this would seem to offer some relief after 2012 data that suggested that the recent downward trend in reported vulnerabilities had reversed, as their numbers surged 27 percent over the 2011 count to 5,297, as tracked by the Common Vulnerabilities and Exposures (CVE) database (Chart 3-2). Indeed, 2012 saw a vulnerability landscape that expanded the target opportunities for attackers, and also increased the area that security administrators—already struggling with the introduction of mobile devices and consumer services into the enterprise network—needed to defend.

But did 2013 truly represent a positive trend? In some respects, yes. Vulnerability defense typically involves two main approaches:

- Applying available vendor patches to vulnerabilities in order to correct the issue. For client systems, this is now often done automatically, with little or no testing; for servers, additional testing is often required in order to verify that patches carry no adverse effects.
- Deploying intrusion prevention systems (IPS) to detect and, if desired, block attempts to exploit known vulnerabilities. This is sometimes done as a stopgap measure until an update can be applied as part of the normal patching cycle. In other cases, IPS is the primary, long-term means of defense for systems that cannot be patched for a variety of reasons.

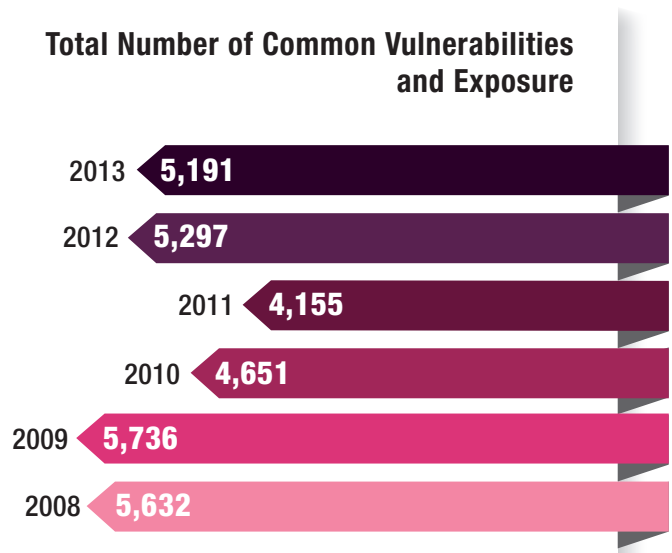


Chart 3-2

Source: Common Vulnerabilities and Exposures (CVE) database

EVERY 60 SECONDS A HOST ACCESSES A MALICIOUS WEBSITE

The number of newly reported vulnerabilities tends to have a direct positive correlation on the workload of security and IT organizations. In this light, 2013 certainly seems to have brought good news for overworked security managers. The CVE database showed a decrease in the number of reported vulnerabilities to 5,191 for the year, a modest 2 percent year-over-year decrease from 2012, and included a 9 percent decrease in the number of "critical" vulnerabilities reported.

But the story isn't as black-and-white as it may appear. While fewer vulnerabilities were reported, industry experts agree that an increasing number of critical vulnerabilities are being siphoned off by the gray and black markets—a potentially more dire development (see inset: *Zero-days, big dollars*).

ZERO-DAYS, BIG DOLLARS

Despite an increase in bounty programs by vendors for vulnerabilities detected by researchers, the high market-value of true zero-day vulnerabilities is causing researchers to sell them to "gray-hat"[28] government agencies—those working with hackers to expand their cyber defense capabilities—and professional penetration testing organizations. An even more lucrative underground malware market serves black-hat hackers; here, prices for previously unreported vulnerabilities vary by target platform, ranging from $5,000 for Adobe Reader to up to $250,000 for Apple iOS. The availability of zero-day exploits to buyers puts advanced cyber attacks within reach of any organization, regardless of their technical skills.

TARGET PLATFORM	PRICE
Adobe Reader	$5,000-$30,000
Mac OS X	$20,000-$50,000
Android	$30,000-$60,000
Flash or Java browser plug-ins	$40,000-$100,000
Microsoft Word	$50,000-$100,000
Microsoft Windows	$60,000-$120,000
Firefox or Safari browsers	$60,000-$150,000
Chrome or Internet Explorer browsers	$80,000-$200,000
Apple iOS	$100,000-$250,000

Source: Forbes

EVERY 10 MINUTES
A HOST DOWNLOADS MALWARE

Even as more new vulnerabilities drift "off the map" and potentially into the hands of malware writers, the distribution of reported vulnerabilities highlights another challenge facing security and IT managers (Chart 3-3). Oracle remained the top platform for reported vulnerabilities in 2013, many of which were found in the Java products that are used widely in both server and client applications, thus presenting a large target opportunity for attackers. Microsoft, meanwhile, moved further down the list to fourth, with more reported vulnerabilities in Cisco and IBM products, including large-scale server and network infrastructure components that are not always covered by IPS protection policies and monitoring.

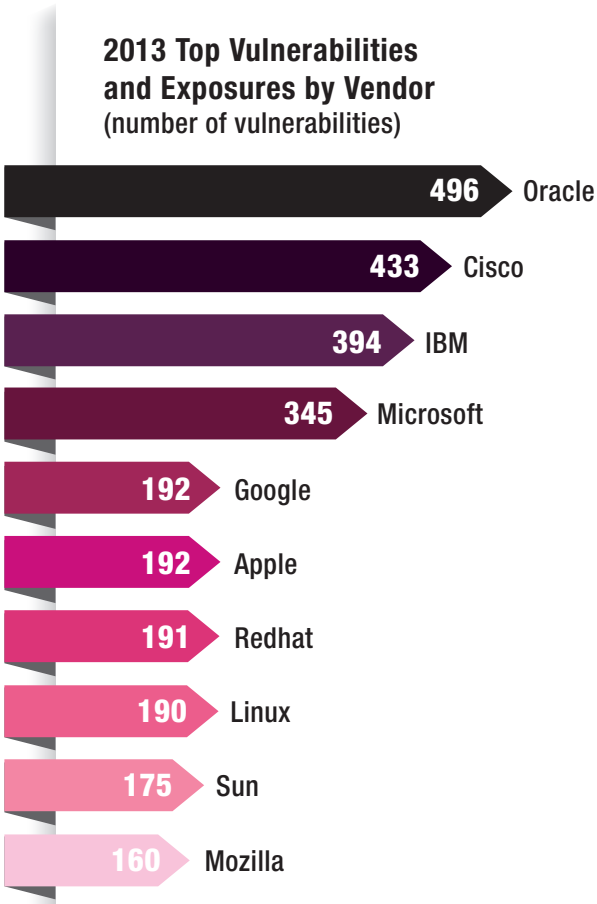


Chart 3-3

Source: Common Vulnerabilities and Exposures (CVE) database

Most organizations have well-defined processes for timely deployment of Microsoft patches. The same does not apply to client applications such as Java and Adobe Reader, and this gap leaves them exposed to browser-based attacks through spear phishing (targeted phishing emails) and "watering hole" attacks, in which an attacker compromises a popular website and embeds malware in it that can infect any vulnerable client that views that particular page.

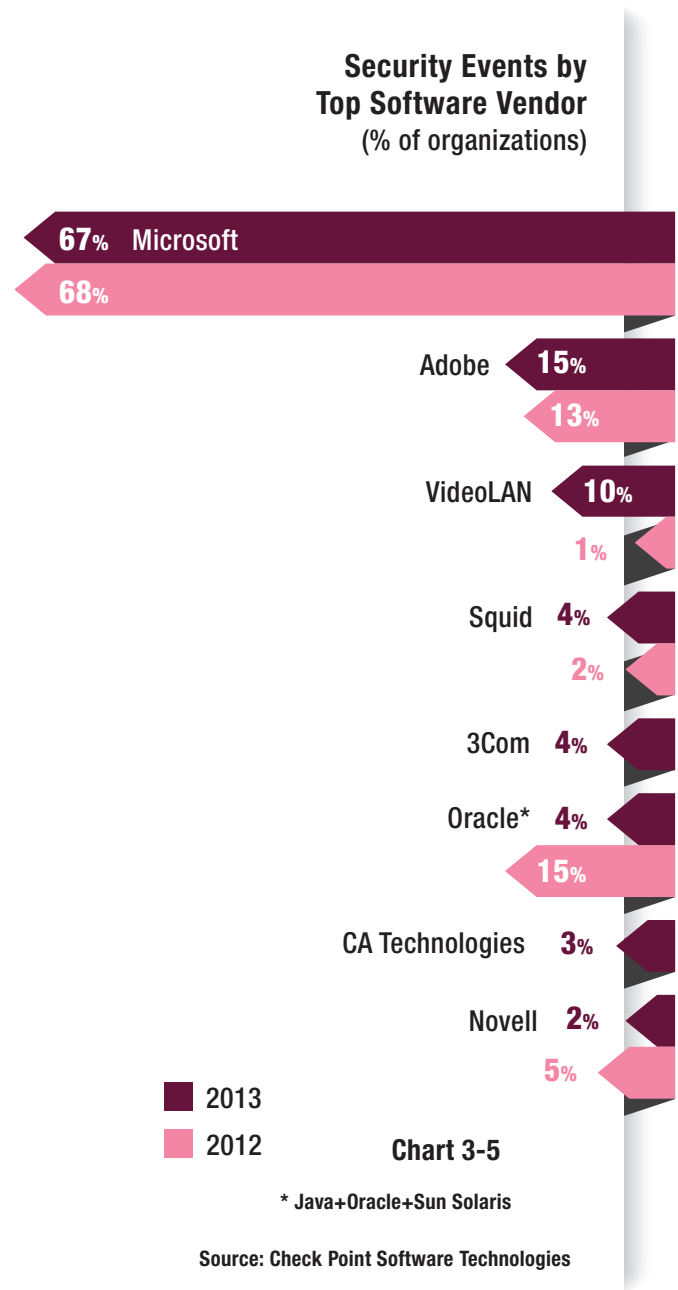
Endpoints: Unpatched, unrestricted, and unprepared

Endpoint Security statistics from our 2013 research confirm that keeping up with these patches remains a major challenge, particularly for client systems (Chart 3-4). Despite the widespread adoption of regular processes for applying Microsoft patches, 14 percent of the endpoints analyzed did not have the latest Microsoft Windows service packs, which roll up all previously released patches and updates. More importantly, 33 percent of enterprise endpoints did not have the current versions for client software such as Adobe Reader, Adobe Flash Player, Java and Internet Explorer, leaving gaps that render these clients vulnerable to many attacks.

The vulnerability of these systems is compounded by the fact that almost one-fifth (18 percent) of hosts studied did not have the latest signatures for their antivirus solution. The consequences of this lapse can be considerable; an attacker who succeeds in gaining a toehold on a vulnerable client can gain a solid platform for exploring the rest of the target organization's network. Of the enterprise endpoints analyzed, fully 38 percent configured the users with local Administrator permissions, enabling malware to run in the system (root) context when it executes, rather than being limited to the user context.

Far from offering hope to beleaguered security and IT managers, then, the environment in 2013 turns out to have been highly favorable for attackers:

- More vulnerabilities on the black market, where they remain unreported and unpatched
- Widespread unprotected clients
- A shift in the number of vulnerabilities towards applications and platforms that are less regularly patched



Attackers look beyond Windows

Attack data from our 2013 research show how attackers are adapting to these target opportunities in enterprise networks (Chart 3-5). While Microsoft still remained the most attacked platform in 2013, targeted by at least one attack in 67 percent of organizations analyzed, this represented a slight decrease from 2012. The increases in attacks for Adobe (Reader and Flash Player) and VideoLAN (VLC media player) reflects the increased targeting of end-user applications, while the heightened attention on infrastructure devices and platforms is evident in the greater incidence of attacks on systems from Squid (proxy and web caching), 3Com (switching and routing) and CA (analytics and identity). In fact, the distribution of attacks across platforms reflects the "long tail" described by author Chris Anderson[29] in 2006 (Chart 3-6). The trail of targeted platforms is a line of "niche markets to infinity" and attests to the economically motivated, market-driven business model of modern cyber attacks.

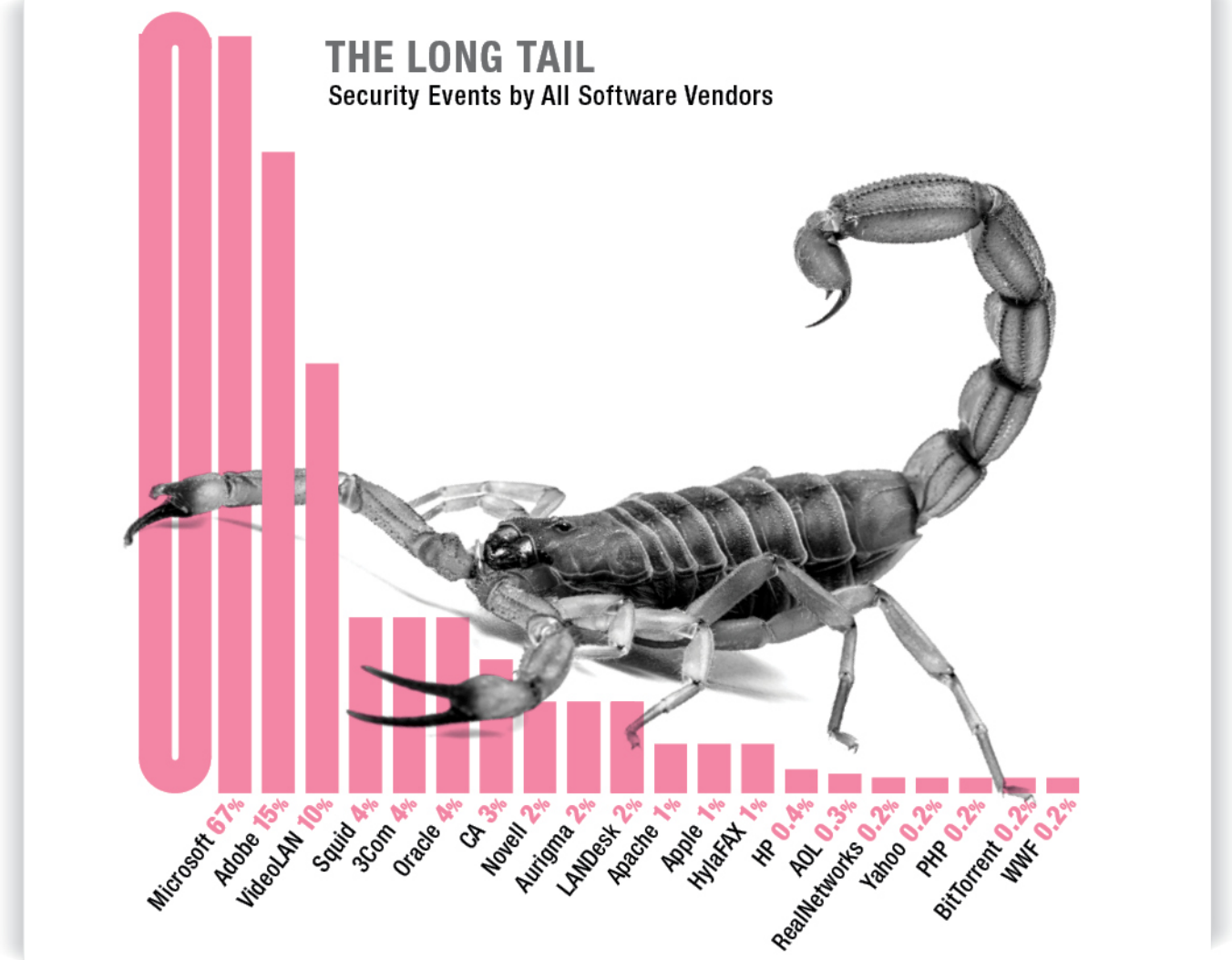


Chart 3-6 **Source: Check Point Software Technologies**

33%

OF HOSTS DO NOT HAVE UPDATED SOFTWARE VERSIONS

Servers are where the money is

In 2013, Check Point research found that servers remain a primary target of attacks detected by network-based intrusion prevention systems (IPS) by almost 2-to-1 (Chart 3-7). Considering the weak state of client systems described above, one wonders: Why attack servers when they are more likely to be patched and closely guarded? For much the same reason that Willie Sutton robbed banks, as he purportedly put it: "Because that's where the money is."[30] Application servers are network-facing and sometimes even Internet-facing in a DMZ, and automated attacks are well-suited to servers because they can exploit vulnerabilities in services or applications without end-user interaction. Servers can be port- and service-scanned from outside the network or from a compromised internal client, and then targeted with attacks specific to the version of the applications or OS they are running. Thus, there are many remote attacks that, if successful, will give an attacker remote control of the system.

Security Events by Platform
2013 % of total

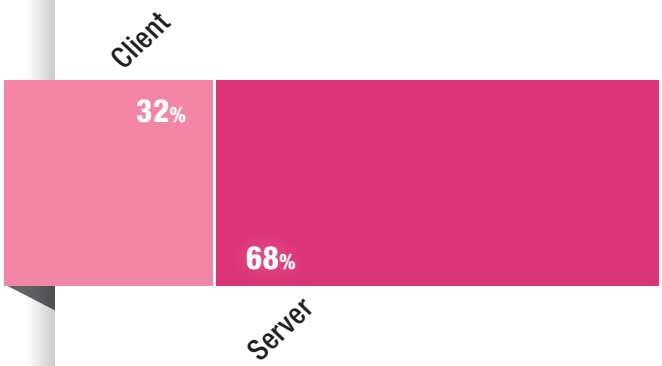


Chart 3-7

Source: Check Point Software Technologies

Top Attack Vectors
(% of Organizations)

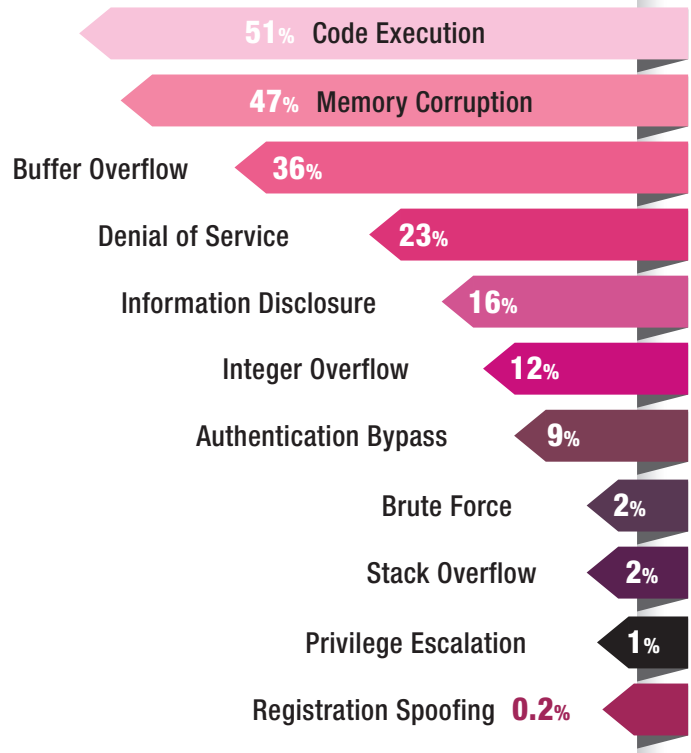


Chart 3-8

Source: Check Point Software Technologies

The top attack vectors observed in our 2013 research (Chart 3-8) lean heavily toward remote code execution (RCE)[31], with the top three by incidence being code execution, memory corruption and buffer overflows. Even Denial of Service (DoS) attacks can support a server attack by serving as a smokescreen to distract from the much lower-profile server attack as it is happening. By the time the smoke clears, the attack is complete and the target server has been compromised.

Clients: Unpatched, Unrestricted and Unprepared

Clients represent ready targets as well, especially for network-based attacks that attempt to propagate across an internal network or on an unprotected public network. In addition to missing patches and service packs that fix known and easily targeted services such as RPC[32], clients are often left vulnerable by important protection capabilities that have been disabled. For example, almost one quarter (23 percent) of enterprise endpoints analyzed by Check Point did not have a desktop firewall enabled, and more than half (53 percent) had enabled Bluetooth, exposing them to wireless attacks in public spaces.

Client systems also offer many other avenues for compromise, primarily by exploiting user behavior with email or web browsing. In these areas, the data from our 2013 analysis reflects both the acceleration in malware activity and the shift to mass customization.

JOKE OF THE DAY:
END USERS ARE STILL A WEAK LINK

Email remains the favored propagation vector for malware. An example from 2013 shows that even today, end users remain unwary of simple attacks, creating a ready distribution mechanism for malware among many organizations.

In October 2013, a user working at a large manufacturer in France received an email message with the subject line "Blagounette du jour," or "Joke of the day."[33] Attached to the email message was a 6MB Microsoft Excel file.

Automated analysis of suspicious incoming documents within a virtual sandbox revealed that the Excel file extracted an image from the Excel application into the computer's file system, and changed the registry's wallpaper key to the new image. Because the image was often perceived as humorous, the unsuspecting end user would be likely to share this "joke" by forwarding the email message to friends and co-workers. Further analysis found that this was exactly what happened, as the document was forwarded to at least three additional large French organizations.

Fortunately for these organizations, this specific document did not carry a malicious payload and was not designed to cause any damage to the computers of the users who opened it. However, it included all the ingredients of a targeted malware campaign. Users who opened this document exposed their computers and their organizations to a significant risk, one compounded by those who forwarded it to co-workers and to friends working at other organizations, who became an additional vector in the spread of a joke of the day that was really no laughing matter.

Access to Malicious Sites by Number of Hosts
(% of organizations)

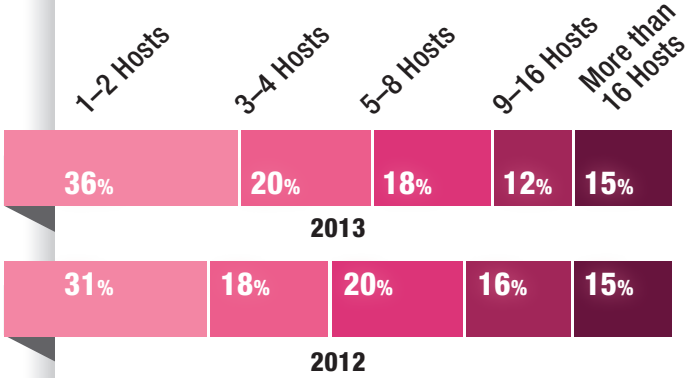


Chart 3-9

Source: Check Point Software Technologies

In 2013, the incidence of hosts accessing a malicious site continued to increase. Our research shows that on average, every 60 seconds a host accesses a malicious website. With the exception of the "1–2 hosts" range, Chart 3-9 shows that the distribution of the number of hosts accessing malicious sites remained relatively unchanged from 2012. This apparent good news belies a deeper problem, as it is an effect of spear-phishing campaigns that target a limited number of users within an organization and leverage social media profiling to create an email that is more likely to be opened by the recipients. Rather than blanketing the entire organization with an easily detected phishing email, these attacks target one or two users in an organization, a more effective approach that yielded a 20 percent increase in hosts accessing a malicious site compared to 2012.

This trend also explains the 2013 surge in incidences of hosts downloading a malware, as 76 percent of organizations analyzed had 1–4 hosts download malware, a 69 percent increase over 2012, while incidences remained the same or decreased for all other user counts (Chart 3-10).

A small number of hosts accessing malicious sites and downloading malware at a greater number of organizations drove an overall acceleration of malware activity in 2013. On average, a host accesses a malicious website every minute, and every ten minutes a malware is downloaded.

49% OF ORGANIZATIONS HAD
7 OR MORE BOT-INFECTED HOSTS

73%

OF ORGANIZATIONS HAD AT LEAST ONE BOT DETECTED, COMPARED WITH 63% IN 2012

CRYPTOLOCKER BLOCKER

CryptoLocker, a strain of malware known as "ransomware," was first identified at the beginning of September 2013. Like other forms of ransomware, CryptoLocker installs itself on the victim computer and runs in the background encrypting various user data files, unknown to the end user.

When the encryption phase is complete, CryptoLocker displays a prompt informing the user that their files have been "taken hostage" and demanding the payment of a ransom to the criminals to decrypt the files. The description states that if the user does not comply with this request within the payment window (often less than four days), the private key needed for decryption will be deleted from their servers, rendering the victim's data permanently unrecoverable.

There is no currently known alternative method for restoring access to encrypted files.

An important trait of CryptoLocker is that the malware agent needs to find and initiate communication with a command and control (C&C) server before it can begin the process of encrypting the files. The most effective way to defeat CryptoLocker is therefore to detect and block the initial communication attempt by the agent, before it can connect with the C&C server and start the encryption process.

CryptoLocker showed that bot detection, often regarded as a reactive measure, can also play a proactive, preventive role in advanced malware defense. During the CryptoLocker outbreak in late 2013, organizations that employed intelligent anti-bot solutions were able to mitigate the damage from CryptoLocker infections in their networks by not only identifying infected clients, but also blocking that critical initial C&C communication.

Number of Hosts that Downloaded a Malware
(% of organizations)

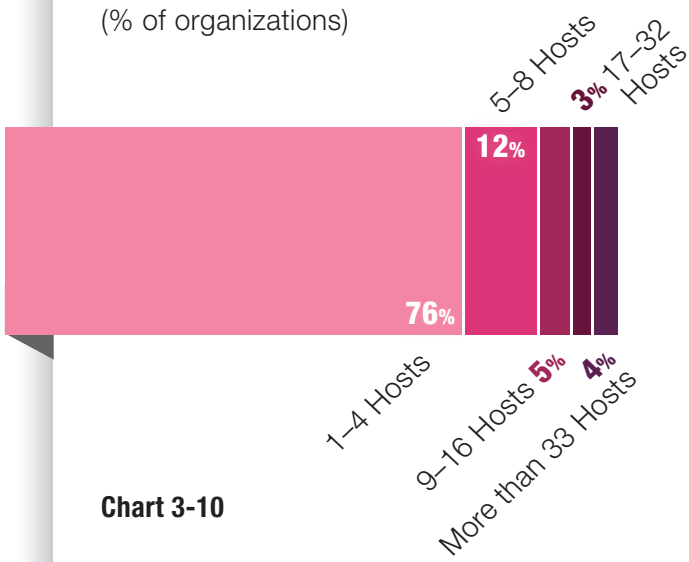


Chart 3-10

Source: Check Point Software Technologies

ON AVERAGE, A HOST ACCESSES A MALICIOUS WEBSITE **EVERY MINUTE**, AND **EVERY TEN MINUTES** A MALWARE IS DOWNLOADED

Bots extend their reach

As would be expected from this increase in infiltration activity, Check Point research found a corresponding increase in bot infections and activity in 2013. If for infiltration the theme was a lower volume of more targeted attacks, for bots the converse was true: high volume and high frequency. In 2013, organizations with 22 or more bot-infected hosts increased almost 400 percent (Chart 3-11), while smaller bot infestations actually decreased.

This should not be taken to mean that bot infections were decreasing overall, since more than one-third (38 percent) of organizations still had at least 1–3 bot-infected hosts.

Moreover, the stakes for bot infections are arguably getting higher with the advent of a new generation of ransomware, exemplified by the outbreak of CryptoLocker in late 2013 (see inset: *CryptoLocker Blocker*).

Not only are organizations struggling with more extensive bot infestations in their environments, but the bots are more active as well. Bot communication with C&C servers increased dramatically in frequency in 2013, with 47 percent of organizations detecting C&C communication attempts at a rate of more than one per hour, an 88 percent increase over 2012 (Chart 3-12). Averaged across our entire research sample, a bot is attempting to communicate with its C&C server every three minutes. Every one of these communication attempts is an occasion for the bot to receive instructions and potentially exfiltrate sensitive data outside the affected organization. This acceleration in C&C communication frequency represents a serious threat to organizations struggling to protect the security of their data and systems.

Number of Hosts Infected with Bots
(% of organizations)

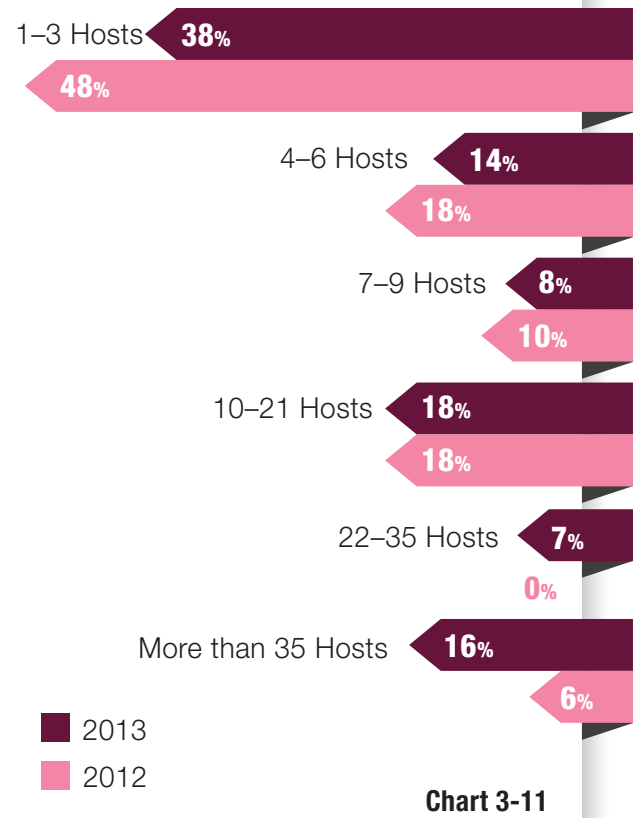


Chart 3-11

Source: Check Point Software Technologies

77%

OF BOTS ARE ACTIVE FOR MORE THAN 4 WEEKS

77% more than 4 weeks

less than 4 weeks **23%**

Source: Check Point Software Technologies

Frequency of Bots' Communication with Their Command and Control Center

(% of organizations)

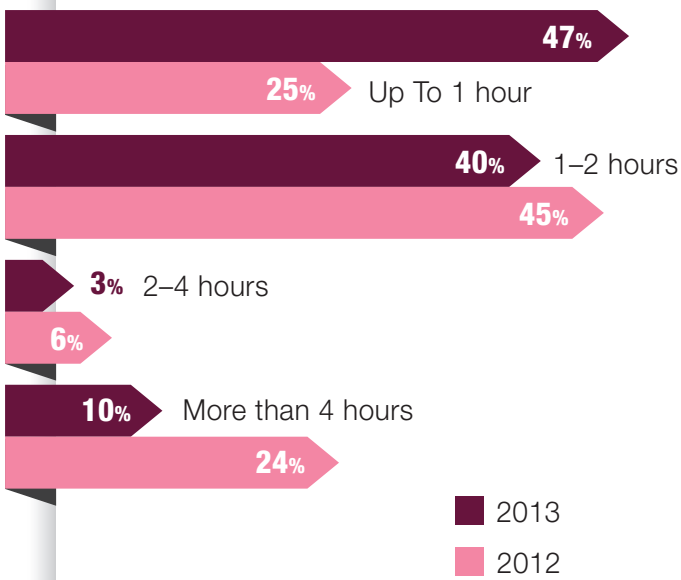


Chart 3-12

Source: Check Point Software Technologies

Bot defense becomes more vital, and more challenging

Increased frequency also presents an opportunity for security managers to detect, cut off and begin shutting down bot infections in their networks. Detecting bot communication is often the easier task; eradicating bots without re-imaging the infected system can present a bigger challenge. Effectively blocking bot communication is becoming the most difficult part of anti-bot warfare due to the newer, more sophisticated C&C channels employed by DGA-based botnets to evade traditional filtering and blocking tools (see inset: *Not Your Father's Phishing Campaign*)[34].

A BOT IS ATTEMPTING TO COMMUNICATE WITH ITS C&C SERVER **EVERY THREE MINUTES**

NOT YOUR FATHER'S PHISHING CAMPAIGN

In 2013, phishing campaigns analyzed by the Check Point Security and Malware Research Group highlighted the increasingly sophisticated techniques that today's phishing attacks employ to evade the blacklists that are the heart of most traditional defenses, including utilization of some form of dynamic URL scheme that evades detection by static blacklists. In the case of the phishing campaign around the Nuclear exploit kit, this scheme also resists analysis by malware researchers.

Analysis of CryptoLocker by our researchers revealed another aspect of this trend: as a Domain Generation Algorithm (DGA) based botnet[35], CryptoLocker employs dynamic, seemingly randomly generated domain names to establish communication between a bot and C&C server. The CryptoLocker bots generate 1,000 new domains every day, while on the other end CryptoLocker's managers register the same 1,000 new domains and then discard them after 24 hours. As a result, the malicious domains have little chance of being detected and registered by the industry resources that build and maintain blacklists of known malicious URLs and domains.

Viewed as a whole, these recent malware campaigns highlight the important role of dynamic URLs and domain names in these attacks, specifically in evading the static blacklists that have traditionally been used to detect and block phishing and bots. Dynamic URLs and DGA leverage the infrastructure of the Internet itself to generate obscure or single-use variants that confound a system of defenses based on looking for and blocking traffic from and to addresses that have been previously detected on a global network and classified as malicious.

These observations reflect a much larger trend in the malware industry. Attackers are exploiting weaknesses in the domain name system and traditional URL blacklisting methods to evade existing defenses and reach their targets. In their research findings for the second quarter of 2013, the Anti-Phishing Working Group (APWG)[36] found that while the .com top-level domain (TLD)[37] remained the most commonly used in phishing campaigns (44 percent of total phishing, up from 42 percent in Q1), some countries TLDs are more common in phishing attacks than are actually registered; for example, Brazil (.br) has only 1 percent of registered domains but accounts for 4 percent of phishing email TLDs. Phishers and malware writers are exploiting the sheer number of possible TLDs for countries alone to generate an immense number of unique domain names and URLs, and the controls that many assume are in place to prevent this kind of abuse are not working. APWG's "Global Phishing Survey 1H2013: Trends and Domain Name Use"[38] report explores the role of domain names in phishing attacks in greater detail and finds that the domain registrars are either asleep at the wheel or actively abetting the phishers.

This problem is only going to get worse. In 2013, Internet Corporation for Assigned Names and Numbers (ICANN)[39] announced plans to increase the number of top-level domains from the current 22 to 1,400, including TLDs in non-Latin characters such as Arabic, Chinese and Cyrillic, among others. While the APWG notes that non-Latin character TLDs have been available for years and have not shown signs of significant use among phishers, there is every reason to believe that attackers will look for ways to leverage them as security vendors become more sophisticated in stopping URLs and phishing domains that use Latin-based characters. These will test the limits of all blacklisting and URL filtering techniques that rely on lists—whether local or cloud-based—of known malicious or suspicious URLs and create a virtually infinite pool of single-use URLs that can be employed for phishing emails, and domain names that can be used for DGA-based botnets.

Recommendations

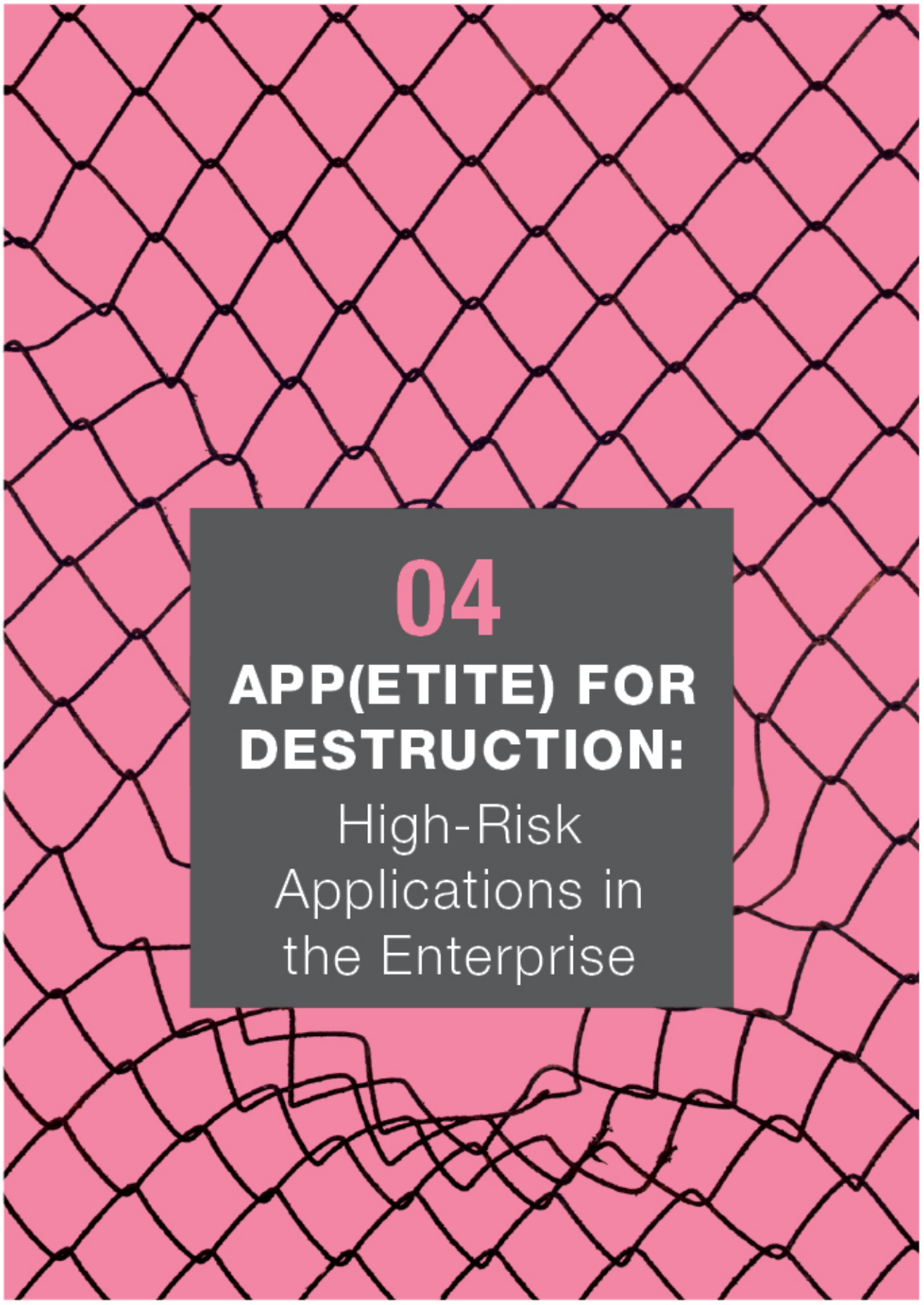
Check Point analysis of the security landscape in 2013 reveals that malware activity increased across all categories. This increase had three main aspects:

- Greater infiltration activity, in which users are exposed to malware through malicious websites, emails and downloads
- Increased post-infection threats in the form of larger bot infections with more frequent C&C communication
- More attacks on a wider range of platforms, targeting vulnerabilities not just on servers and Windows clients, but also network and server infrastructure and less-managed applications

As a whole, this acceleration in cyber attack activity represents a daunting challenge for enterprise business and security leaders who were already straining to meet the malware challenges described in the Check Point *2013 Security Report*. The only way for organizations to effectively manage this acceleration in malware activity, and to fight the accelerated pace of attacks, infection and exfiltration in their environment, is to automate and coordinate multiple layers of defense. Essential measures include:

- **Gateway and endpoint antivirus with URL filtering**—Organizations must be able to detect and block malware and attempts to connect sites that are known distributors of malware.
- **Gateway anti-bot**—In addition to detecting malware, these solutions should have the intelligence to mitigate DGA-based botnet communications.
- **Extended IPS protection**—Beyond monitoring, you should be able to enable blocking for critical severity attacks. The system should cover network, server and IT infrastructure systems from Cisco and other vendors and platforms, not just Microsoft Windows.
- **Comprehensive system and application maintenance**—Ensure that vulnerability management and patching processes are in place for all systems and applications, including Java and Adobe Reader, not just Microsoft Windows clients and servers.
- **Best practices for client and server configuration**—These include restricting use of Administrator privileges, disabling Java and other scripting, and limiting applications that end users can install on their endpoints.

In the next chapter, we will examine our 2013 research findings regarding applications and the risks they pose to enterprise data and end users.



04

APP(ETITE) FOR DESTRUCTION:

High-Risk Applications in the Enterprise

04 APP(ETITE) FOR DESTRUCTION: HIGH-RISK APPLICATIONS IN THE ENTERPRISE

Application control represents an internal challenge that complements and compounds the external challenges posed by cyber attacks. Applications are essential to productivity and the routine operation of every organization, but they also create degrees of vulnerability in its security posture. From a security perspective, they resemble the denizens of George Orwell's *Animal Farm*[41]: all applications are equal, but some are more equal than others.

BUT IF WE'RE ONLINE,
THE WHOLE WORLD IS LOCAL.

Neal Stephenson, *Cryptonomicon*[40]

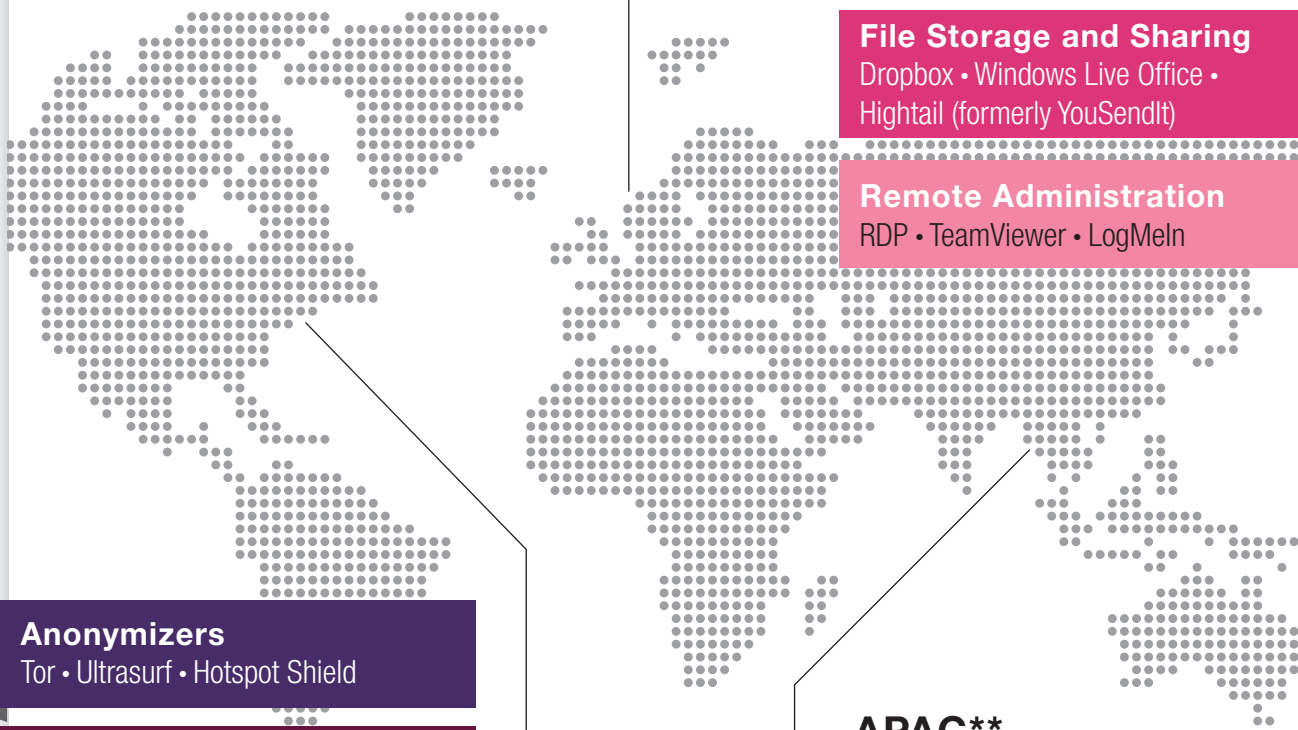
High-risk applications epitomize these challenges. Unlike productivity applications like Microsoft Office and increasingly accepted Web 2.0 social media applications such as Facebook, LinkedIn, Twitter, WebEx and YouTube, high-risk applications enable anonymous web surfing, cloud-based storage and sharing of files, remote use of desktop applications and data, and sharing of media and other files between users and computers. High-risk applications often run on the fringes of officially sanctioned IT and solutions, if not altogether outside them, and make up part of the growing shadow IT of end user-driven applications, devices and services that are operating within corporate networks with little or no oversight.

86%

OF ORGANIZATIONS HAVE AT LEAST ONE HIGH-RISK APPLICATION*

*** P2P File Sharing, Anonymizers and File Storage and Sharing**

TOP HIGH RISK APPLICATIONS PER REGION



EMEA*

Anonymizers
Tor • Hide My Ass! • OpenVPN

P2P File Sharing
BitTorrent Protocol • Soulseek • eDonkey Protocol

File Storage and Sharing
Dropbox • Windows Live Office • Hightail (formerly YouSendIt)

Remote Administration
RDP • TeamViewer • LogMeIn

APAC**

Anonymizers
Ultrasurf • Tor • Hide My Ass!

P2P File Sharing
BitTorrent Protocol • Xunlei • Soulseek

File Storage and Sharing
Dropbox • Windows Live Office • Hightail (formerly YouSendIt)

Remote Administration
TeamViewer • RDP • LogMeIn

Americas

Anonymizers
Tor • Ultrasurf • Hotspot Shield

P2P File Sharing
BitTorrent Protocol • Soulseek • Box Cloud

File Storage and Sharing
Dropbox • Windows Live Office • Hightail (formerly YouSendIt)

Remote Administration
RDP • LogMeIn • TeamViewer

Chart 4-1

*** EMEA – Europe, Middle East and Africa**

**** APAC – Asia Pacific and Japan**

Source: Check Point Software Technologies

Percentage of Organizations Using High-Risk Applications
(% of organizations)

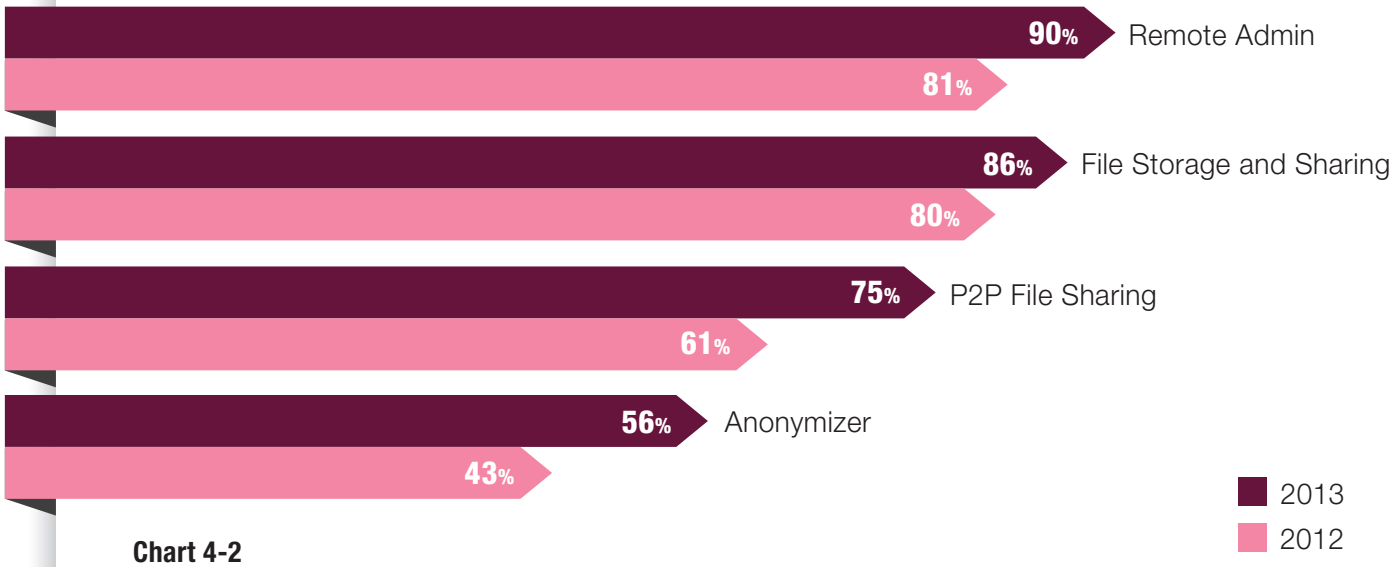


Chart 4-2

Source: Check Point Software Technologies

In 2012, Check Point security research found that high-risk Web 2.0 applications were pervasive throughout enterprise infrastructure and posed significant risks for compromise and data leakage. Our analysis of enterprise network security in 2013 found that despite their well-known risks, the incidence of high-risk applications increased across all categories (Chart 4-2). This chapter examines the findings for each category and shares recommendations for mitigating this challenge.

RESEARCH RECORDED AN OVERALL **INCREASE IN THE USE OF ANONYMIZERS** IN ENTERPRISE NETWORKS, WITH MORE THAN HALF (56 PERCENT) OF ANALYZED ORGANIZATIONS REGISTERING AT LEAST ONE INCIDENT OF ANONYMIZER

Danger in anonymity

Anonymizer applications are primarily associated with providing users a means to surf the Internet and view websites while preserving their anonymity. They typically rely on creating an encrypted tunnel to a set of HTTP proxy servers to allow users to bypass firewalls and content filtering restrictions. Some, such as Tor, employ additional routing obfuscation techniques and even special software or browser plug-ins to enable users to cover their tracks and evade employer, government or other controls.

In 2013, Check Point research recorded an overall increase in the use of anonymizers in enterprise networks, with more than half (56 percent) of analyzed organizations registering at least one incident of anonymizer, a 13 percent increase over 2012.

PORTAL TO THE DEEP WEB

Also known as The Onion Router, Tor[42] was again the most widely detected anonymizer application in our 2013 research. Tor was already well known for its uses as a vehicle for anonymous browsing that also easily bypasses organizational security policies, but in 2013 it earned new notoriety as a portal to the Deep Web, the shadowy underbelly of the open and searchable Internet, or "Surface Web"[43]. Characterized by inaccessibility from standard search tools, the Deep Web gained attention in 2013 in response to heightened concerns in the U.S. and abroad about surveillance and privacy, and to notoriety through the Silk Road arrests[44].

Other anonymizer applications pose a similar administrative challenge, but Tor's role as a gateway to Onionland and other areas of the Deep Web makes it a particular risk for security managers. While it provides anonymity and a marketplace for a vast underground, the Deep Web is also rife with malware and scams, and organizations are right to worry that employees who use Tor to escape from real or perceived surveillance will end up exposing their computers and the organization to a high degree of risk. More recently, investigators have determined that credit card data stolen from numerous retailers using the ChewBacca[45] remote access Trojan were exfiltrated to server drop-points using Tor.

Free speech and anonymity are essential freedoms and must be preserved for individuals. For security administrators in enterprise environments, however, detecting and blocking use of Tor and other anonymizers on company systems and within corporate networks must be a top priority in 2014 and beyond.

Most Popular Anonymizer Applications
(% of organizations)

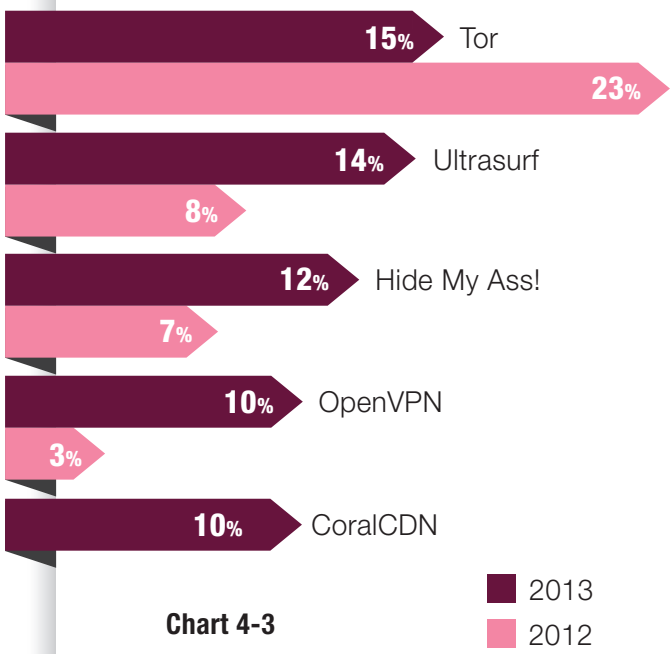


Chart 4-3

Source: Check Point Software Technologies

Individual anonymizer applications saw uneven gains, however, with Tor actually detected in fewer organizations than in 2012: 15 percent in 2013, compared to 23 percent in 2012 (Chart 4-3). This reflects increased attention to—and restriction of—Tor in enterprise security policies, and with good reason (see inset: *Portal to the Deep Web*). However, it could also result in part from employees engaging in anonymous browsing less frequently from corporate systems and networks, or from users switching to other anonymizer applications that are less well-known and therefore less likely to be blocked by corporate policies.

Touted by free-speech and privacy advocates, anonymizers have helped protect the secrecy—and even the lives—of dissenters in countries undergoing periods of unrest. More recently, 2013 revelations about state-sponsored surveillance have driven adoption by users in Europe and Asia as a refuge from real or perceived cyber snooping. The regional differences in detected incidences of anonymizer use in corporate networks attest to this factor, and also point to the relative success of security administrators in the Americas at constraining the use of this category of high-risk applications (Chart 4-4).

Like the mythical hydra[46], if administrators succeeded in cutting off Tor in 2013, it was only to see six more anonymizers sprout to take its place. The incidence of the remaining top ten anonymizer applications all increased compared to 2012.

Usage of Anonymizer Applications by Region
(% of organizations)

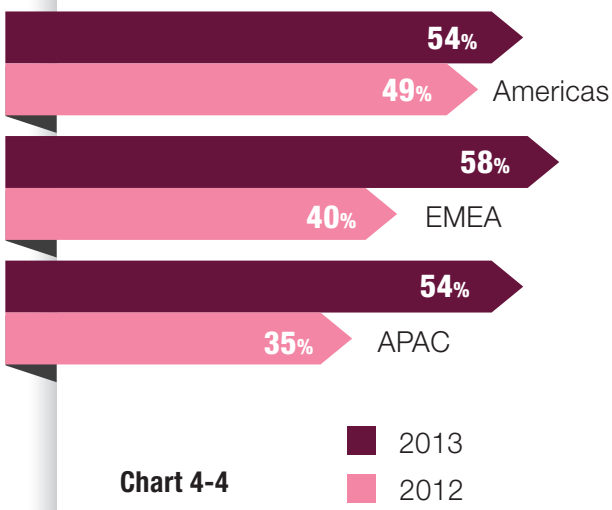


Chart 4-4

Source: Check Point Software Technologies

Top Remote Administration Applications
(% of organizations)

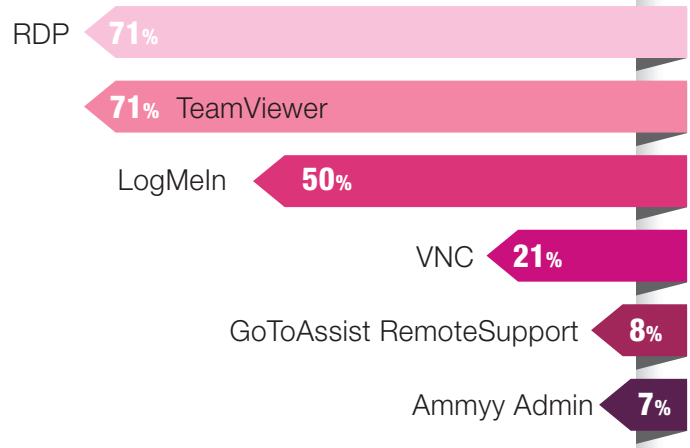


Chart 4-5

Source: Check Point Software Technologies

Who smells a RAT?

The most widely detected category of high-risk applications in our 2013 research was remote administration applications. The best known is Microsoft Remote Desktop (RDP)[47], but many others are in wide use around the world, with TeamViewer surging in popularity from 2012 (Chart 4-5). These applications do have legitimate uses, when they enable IT and corporate Helpdesk teams to service and manage employee desktops around the world (see inset: *Remote Admin Tools: The Good, the Bad and the Ugly*).

However, many organizations have adopted these tools haphazardly based on tactical needs, so that rather than standardizing on a single remote admin application, IT organizations instead employ three or more depending on the platform, connection and task. In 2013, remote admin applications were the only ones for which the highest incidence of use was found in the industrial vertical, with 90 percent of enterprises in this space recording at least one detected incidence of these apps.

REMOTE ADMIN TOOLS: THE GOOD, THE BAD AND THE UGLY

Remote administration tools are sometimes confused with remote access tools due to their common acronym, "RAT." In practice, while remote administration tools carry significant security and operational risks, these are different from those associated remote access tools such as ChewBacca, Poison Ivy[48], DarkComet and the famed Back Orifice[49]. Essentially Trojans in practice, remote access tools have no legitimate use in a corporate network, and as a major threat their detection should generate a rapid response for removal, remediation and forensic analysis of potential data exposure.

The most well-known remote administration tools, on the other hand, often proliferate in networks in response to the needs of IT and corporate helpdesk teams as they attempt to resolve issues and provide application and data access across an ever-expanding range of end-user devices and platforms. The remote administration tool TeamViewer is a good example of the trend in these tools. In 2013, TeamViewer's presence on surveyed networks surged in popularity, driven by the end to the free version of the popular LogMeIn and an expanding feature set that includes extensive support for non-Windows platforms, conferencing and collaboration features, and solid performance over a variety of connections without having to make the firewall changes required by RDP.

This comes at a price, because the features that make it a new favorite for IT teams also make it attractive to end users who want to remotely access their work computers from their smartphone, tablet or even home PC, thus opening holes in the corporate network and putting the security of the organization at risk. In these cases, even a well-intentioned employee can turn a good RAT into a dirty rat.

Top P2P File Sharing Applications
(% of organizations)

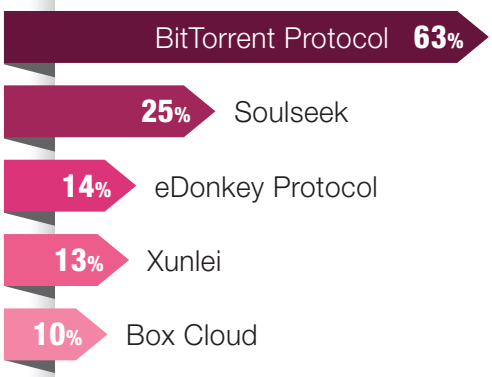


Chart 4-6

Source: Check Point Software Technologies

P2P file sharing: Not Safe for Work

Peer-to-peer (P2P) file sharing applications are used to share files between users. Often used for distributing copyrighted material, legal and pirated software, and other media, P2P file sharing is a favorite vehicle for spreading malware, which can be embedded within the shared files. In addition to distributing malware to unsuspecting or unprepared users, P2P applications can create a backdoor into corporate networks—one that can allow attackers into a network and to leak sensitive data outside the network.

Moreover, the frequent use of P2P applications such as BitTorrent for distributing copyrighted music and film files exposes organizations to liability for action from the Recording Industry Artists Association (RIAA), who have become aggressive in working with Internet Service Providers (ISPs) to identify and pursue the sources for distribution of pirated or unlicensed content (Chart 4-6). In 2013, BitTorrent remained the most popular P2P file sharing application, its detected

Top File Storage and Sharing Applications
(% of organizations)

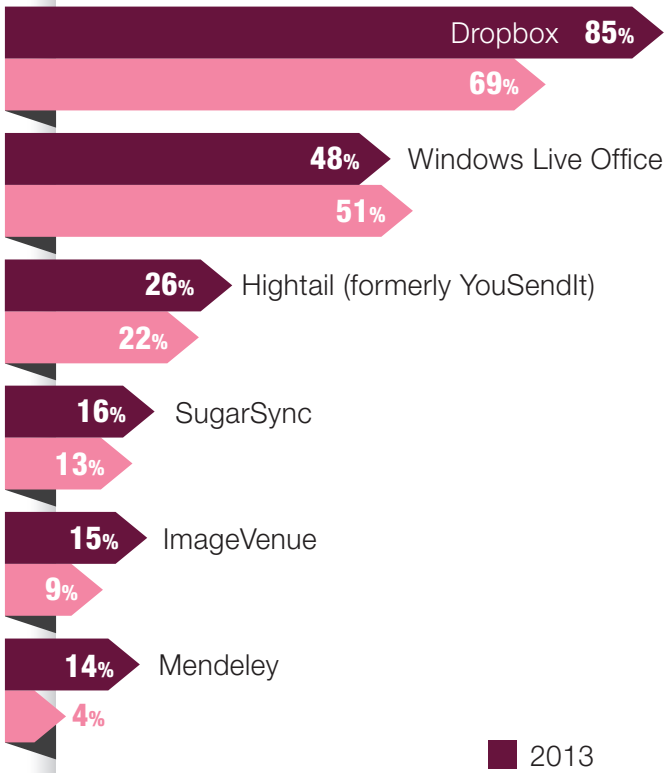


Chart 4-7

Source: Check Point Software Technologies

incidences increasing from 40 percent of organizations in 2012 to 63 percent in 2013. Incidences of detected P2P file sharing applications increased consistently in all regions.

File storage and oversharing

The ability to create and share content easily between devices and users is a defining trait of Web 2.0 applications. File storage and sharing applications play an important role in enabling this ability by making it easy for users to save content in a folder on one device and then have it automatically replicate to the cloud and synchronize across all of their other associated devices. Extending this by sharing with other users is often as easy as sending a link to the recipients, who can then access and even modify the shared files.

Obviously, this ease of sharing exposes an organization to significant risk of "oversharing," whether inadvertent or intentional, by users who synchronize sensitive corporate data from a protected system at work to other, unprotected devices and even to folders shared with other users.

In 2013, Dropbox extended its lead as the most popular file storage and sharing application, detected in 85 percent of analyzed networks, up from an incidence rate of 69 percent in 2012 (Chart 4-7). This was in contrast to almost all of the other top file storage & sharing applications, which fell in frequency compared to 2012, reflecting in part a consolidation by enterprises on a single, company-sanctioned application, but also the continued popularity of Dropbox among end users, who pull it into corporate environments as part of the "shadow IT"[50] infrastructure.

Social creatures

Social media platforms are an integral feature of Web 2.0 and have gained broad, if sometimes grudging acceptance in corporate IT environments. In the Check Point *2013 Security Report*, we described the ways in which Facebook exposed employees to hacking and social engineering, and recommended increased user education and defenses at the endpoint and network.

DROPBOX WAS FOUND IN

85% OF ORGANIZATIONS

DROPBOX SMACKED

2013 was notable as the year in which attackers and researchers realized the potential for file storage and sharing applications to serve as tools for infiltrating organizations and exfiltrating sensitive data. In March, it was revealed that hackers had developed a mechanism to use Evernote to support the command and control (C&C) and exfiltration communications for bot networks.

Soon afterwards, in April, a researcher detailed a mechanism for spreading malware into an organization using Dropbox's synchronization capabilities. Called DropSmack[51], the attack involves embedding macro commands in a file with a .doc extension and a legitimate header, and then placing this file in a Dropbox folder of a user from the targeted organization. It does not matter whether the computer is a company-managed device or one owned by the employee; once DropSmack is installed on one device, Dropbox's automatic synchronization routines replicate it to the Dropbox folder on every device associated with that account. DropSmack enables an attacker to bypass perimeter and even most device-level defenses for infiltration, C&C, lateral movement and exfiltration.

The introduction of new security features in Dropbox such as encryption and two-factor authentication was intended to address the concerns of security managers, but as DropSmack shows, these applications still have great potential for sharing malware and need to be monitored closely in corporate environments, if they are to be allowed at all.

In 2013 these risks remained, and were exacerbated by the increasing role of social media as an essential tool for hackers in planning and carrying out targeted attacks.

Social Media Profile

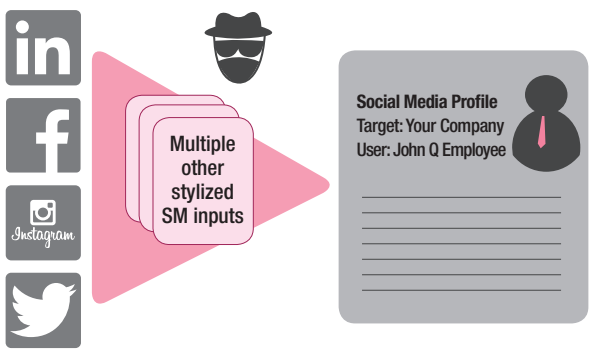


Chart 4-8

Once attackers have targeted an organization and identified individuals within it who have access to the desired data, the attacker builds a social media profile of each target employee (Chart 4-8). This profile tells the attacker valuable information such as websites and online shopping services commonly used by the employee, friends and associates from whom they might expect to receive email, and significant events that they have attended recently or will attend. Armed with this information, an attacker can create a very legitimate looking, spear-phishing email to the target employee with a high probability of success. We only need to look back to the findings of chapter 3 to see the effects of this profiling.

Among social media applications, Facebook remains the most popular, measured in terms of bandwidth consumption in the enterprise environments we analyzed for our 2013 research (Chart 4-9).

- Twitter and LinkedIn again rounded out the top three social media applications, but all saw a decrease in overall incidences compared to 2012. This likely has less to do with decreased use by employees than with a shift from work PCs and access through the corporate network to using mobiles and wireless data connections. While this shift may have the benefit of reducing the strain on corporate networks

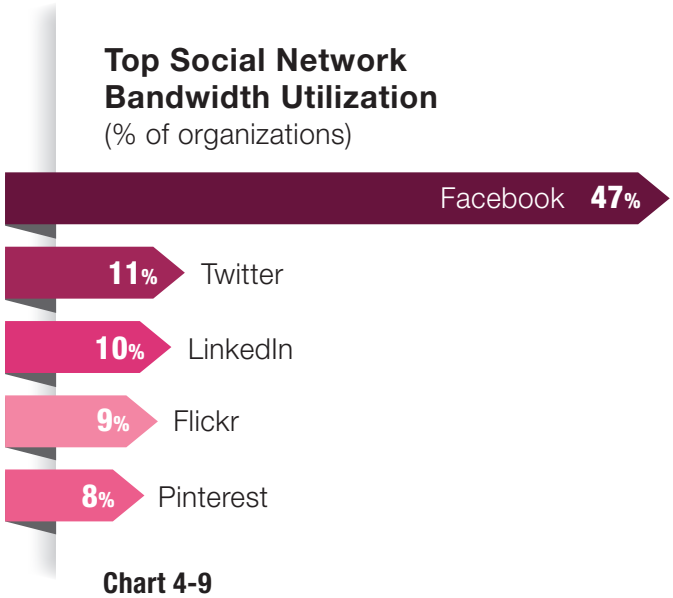


Chart 4-9

Source: Check Point Software Technologies

and decreasing the immediate malware threat to company-owned PCs, the widespread use of file storage and sharing applications such as Dropbox means that an infection on a user's personal MacBook or tablet can easily jump to their corporate system (see inset: *Dropbox Smacked*).

Recommendations

High-risk applications of all kinds continue to pose a rising threat in the enterprise, even as the specific tools favored by end users change over time. While some of these, especially anonymizers and P2P networks, have no legitimate business use and should be eradicated entirely, tools for remote administration and file sharing and storage can address legitimate needs for users and IT, posing a more complex challenge. Even commonly accepted social media platforms such as Facebook, LinkedIn and YouTube, which can play an important role in social media marketing and content marketing strategies, can present an attractive vector for spear-phishing attacks. While malware protection can focus on comprehensive detection, prevention and eradication as its guiding principles, applications call for a more nuanced approach. This should include:

Category-based application control—Administrators need to be able to block entire families of applications if they choose, rather than have to enable blocking for them one-by-one. This not only simplifies administration, but it enables policy controls to be applied to new applications as they are adopted by employees to replace applications that have been blocked or restricted.

Standardization on sanctioned applications—Organizations that need remote administration tools to support IT or business functions should standardize on a single application, and then monitor their networks for the presence of other remote admin tools. If blocking is not feasible, their presence should trigger a notification and investigation process to determine who is using them and how they are being used, and verify whether these are valid exceptions to policy or tactical digressions that should be brought in line with policy. Moreover, monitoring and enforcement should be tied to specific, authorized users or user groups, in order to ensure that only those employees with a valid business need are able to use them. A similar approach can be used for file storage and sharing tools; IT should implement a secure, enterprise-grade service or solution to meet this need. Otherwise, users will inevitably turn to shadow IT apps to enable the file sharing and cross-device synchronization their work requires.

End-user education—Given the impracticality or undesirability of entirely blocking certain categories of applications, IT and security managers should develop comprehensive ongoing programs to inform end users of the risks posed by high-risk applications. Employees need to understand the specific risks posed by different types of applications; how to avoid spear phishing, copyright violations and other threats; and how they can address legitimate business and productivity needs through more secure, IT-sanctioned tools and practices.

It doesn't always take malware or an inappropriately used application to expose your organization to risk. While malicious software does play a role in many data loss incidents, all too often a key factor comes down to simple human error. The next chapter will explore major incidents and trends in data loss in 2013.

05
DATA LOSS PREVENTION:
The Big Comeback

05 DATA LOSS PREVENTION: THE BIG COMEBACK

Data loss incidents gained new prominence in 2013 as Adobe Systems, Target, Neiman Marcus and other high-profile organizations suffered high-profile breaches involving millions of consumers.

Data has long been a prime target for hackers, including financial information, intellectual property, insider business information and authentication credentials. Now there are more ways than ever for data to fall into the wrong hands as mobile devices and shadow IT apps open new attack vectors and increase the risk of loss or exfiltration. The Internet of Things exacerbates the situation as devices communicate directly with each other to exchange information on home energy consumption, vehicle location and status, package tracking, personal health and more. As more data flows in more ways, it becomes ever more difficult to control and secure.

> SOCIAL SECURITY, BANK ACCOUNT, AND CREDIT CARD NUMBERS AREN'T JUST DATA. IN THE WRONG HANDS THEY CAN WIPE OUT SOMEONE'S LIFE SAVINGS, WRECK THEIR CREDIT AND CAUSE FINANCIAL RUIN.
>
> **Melissa Bean**[52]

Hackers are not the only threat to enterprise data. Many breaches occur inadvertently, as users email the wrong file to the right recipient, or the right file to the wrong recipient—or simply leave an unsecured laptop in the wrong place. Employee error played a key role in many of the past year's data loss incidents, but intentional or not, the result can be the same: sensitive data exposed to risk, angry customers, damaged reputations, fines for non-compliance and serious business disruptions.

IN 2013 88%

OF ORGANIZATIONS EXPERIENCED AT LEAST ONE POTENTIAL DATA LOSS INCIDENT

THINK YOU'RE NOT AT RISK OF DATA LOSS? GUESS AGAIN...

Many organizations continue to neglect implementing robust data protection policies and controls because they think that they are not at risk for data breaches. The painful reality is that hackers do not target only big banks and retailers, and that every organization has sensitive data that can be exposed by an errant email or a lost laptop. These are just a few of the examples from 2013:

Personal information, including Social Security numbers, for 3,500 patients was **stolen** from the Florida Department of Health by employees who passed the data on to a relative for use in filing fraudulent tax returns[53].

The council government of Islington (London) was fined BP70,000 after an internal team inadvertently **published** spreadsheets containing the **personal information** of 2,375 residents, including health history, on the public website of a housing agency[54].

Rotech Healthcare reported the **accidental exposure of personal and health information** for up to 3,500 employees by a former Human Resources employee who was permitted to keep her personal computer when she left the firm[55].

The UK Information Commissioner's office cited over sixty violations of the Data Protection Act by the Anglesey (Wales) council related to **improper access to personal data of residents**, including inadvertent posting on public websites and via email[56].

The retail sector may have been the highest profile industry to suffer data breaches in 2013, but according to Check Point research, organizations across all industries are losing control of sensitive data, and they are doing it at a faster rate than in 2012 (Chart 5-1).

It would be easy for a small organization to consider itself too small to have to worry about data loss, but nothing could be further from the truth (see inset: *Think you're not at risk of data loss? Guess again...*). One of the largest breaches in history targeted Heartland Payments[57], a 700-person company, when thieves stole the digital information encoded onto the magnetic stripe built into the backs of credit and debit cards. Every organization in the information supply chain is at risk of attack, and even a relatively small theft can yield worthwhile results for hackers.

Check Point research found that 88 percent of companies we analyzed experienced at least one potential data loss event, meaning a piece of sensitive data was sent outside the organization via email or uploaded via a web browser. This was a dramatic increase over the already-high figure of 54 percent that we observed in 2012, and highlights the ongoing struggle of organizations to secure sensitive data from accidental or intentional exposure.

EVERY DAY AN ORGANIZATION EXPERIENCES **29 EVENTS OF POTENTIAL EXPOSURE** OF SENSITIVE DATA

Percentage of Organizations with at Least One Potential Data Loss Event, by Industry (% of organizations)

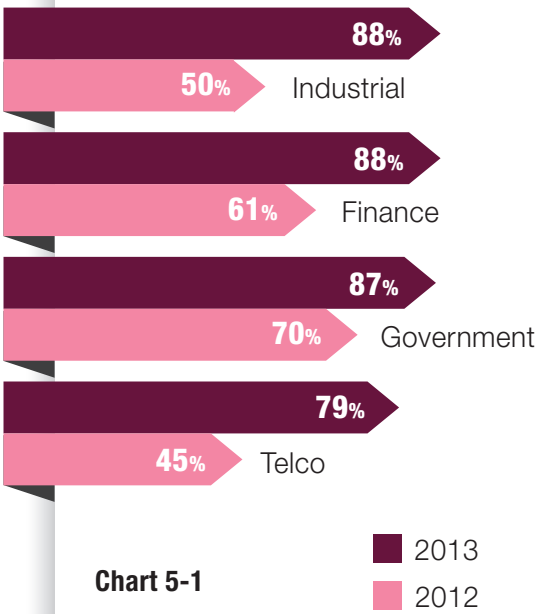


Chart 5-1

Source: Check Point Software Technologies

EVERY **49 MINUTES** SENSITIVE DATA IS SENT OUTSIDE THE ORGANIZATION

Put another way, every 49 minutes sensitive data is sent outside the organization. Every day, an organization experiences 29 events of potential exposure of sensitive data. This is a serious rate of data leakage for any organization in any industry, and it highlights the need for more aggressive controls around sensitive data.

By industry, the most dramatic increases were in the Industrial and Consulting sectors. These increases make more sense in the context of the data types that were attacked in 2013. (Chart 5-2) Our research found that source code was the most most popular data type sent outside the organization in 2013, jumping almost 50 percent from 2012.

Source code, business data records and other trade secrets are estimated to represent the majority of assets of American companies, and they are under constant attack. Economic espionage is estimated to cost American businesses alone as much as $250 –$500 billion every year. While banks and health care companies have long faced the pressure of external regulations for the protection of customer and patient data, companies in sectors such as manufacturing, energy infrastructure, shipping, extractive industries and even entertainment have not always taken a proactive approach to data security. These are the organizations that are increasingly targeted in campaigns that use mass-customized malware as well as more focused targeted attacks.

Regulations adapt as well

Despite the numerous high-profile credit card data breaches that took place in 2013, Check Point research found that the incidence of PCI data loss events in financial organizations slightly reduced to 33%, compared with 36% found in 2012. Within the healthcare and insurance organizations was under our research, there was an increase from 16% of organizations in 2012 to 25% in 2013 in events related to HIPAA regulation.

DATA SENT OUTSIDE THE ORGANIZATION BY EMPLOYEES

(% of organizations)

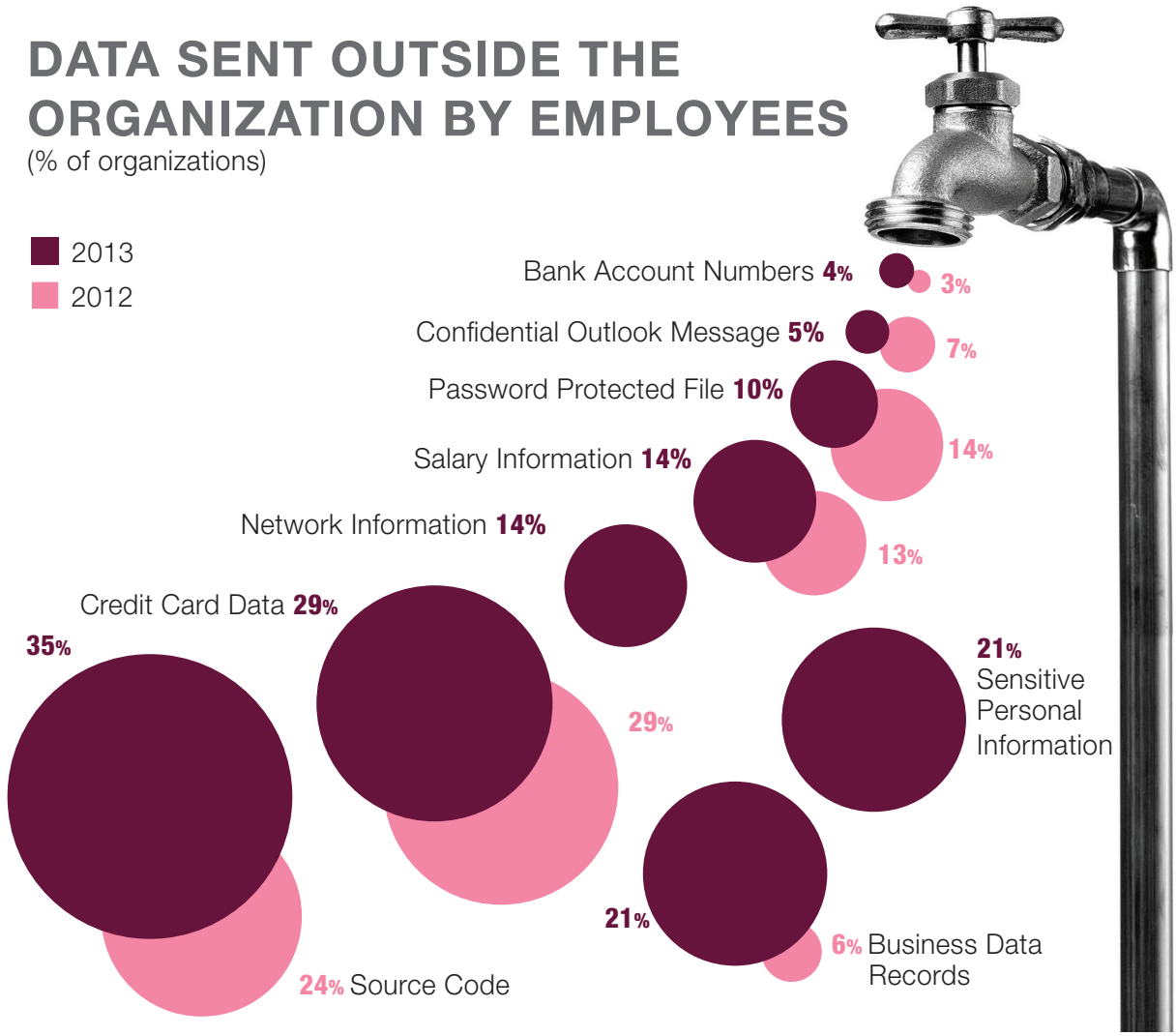


Chart 5-2

Source: Check Point Software Technologies

IN 33%

OF FINANCIAL INSTITUTIONS SCANNED, CREDIT CARD INFORMATION WAS SENT OUTSIDE OF THE ORGANIZATION

2013 saw the publication of Payment Card Industry Data Security Standards 3.0, (PCI-DSS 3.0)[58], which included numerous—and timely—new requirements regarding:

- Security practices for non-end user systems, such as point-of-sale (POS) and other terminals.
- Increased user education around potential attacks (phishing, USB, etc.) and responsible handling of sensitive data.
- Penetration testing of controls and protections that define segmentation between cardholder data and other parts of the network.
- Credentials used by service providers for remote access to the environments of customers who are subject to PCI-DSS.

Overall, the revised DSS requirements emphasize "education, awareness and security as a shared responsibility." The 3.0 standards took effect on January 1, 2014, and events of 2013 have created a new sense of urgency behind the adoption of these new requirements.

Looking ahead to 2014, organizations will have new compliance and data protection regulations and requirements to contend with, including PCI-DSS 3.0, with its expanded requirements around protection of POS systems as well as a new emphasis on user education.

In Europe, the European Union's new Data Privacy Directive, the General Data Protection Regulation (GDPR)[59], takes effect in 2014 as well, creating more stringent requirements for protection of citizen and customer data both within countries and across national and EU boundaries. Organizations will be required to continue evolving their security policies and practices to comply with the new regulations or risk significant financial sanctions.

Recommendations

The rash of large-scale, highly publicized data breaches throughout 2013—affecting some of the world's best-known brands as well as many smaller organizations—show that much work needs to be done to protect personal and business information. This challenge will only grow in scope as trends such as mobility and the Internet of Things expose data to theft or accidental exposure in new ways. Human error plays an especially central role in many data loss incidents, and it will take a truly comprehensive, holistic approach to ensure that data is not exposed to risk or left vulnerable to theft.

In today's world of increasing data losses, organizations must take action to protect sensitive data. The best way to prevent unintentional data loss is to implement an automated corporate policy that catches such incidents before the data leaves the organization. Such policies can best be enforced through a Data Loss Prevention (DLP) solution. Content-aware DLP products have a broad set of capabilities and present organizations with multiple deployment options.

Before deploying the DLP solution, organizations need to develop a clear DLP strategy based on clearly defined considerations such as: What is considered to be confidential information? Who can send it? Where, how and on what types of devices can it be used? With this policy framework in place, you can optimally implement and configure the solution to support your organization's unique business, security and user productivity requirements. For effective data loss prevention, your solution should encompass the following measures and capabilities.

DOES PCI COMPLIANCE CREATE A FALSE SENSE OF SECURITY?

The massive credit card data breaches of late 2013 re-energized a running debate about the relation between PCI-DSS and security, and specifically whether a company certified as "PCI compliant" is truly secure from hacking.

Some argue that PCI compliance certification fosters a false sense of security among retailers and the public. Data breaches at compliant companies and actions such as the retroactive revocation of PCI compliance status are bound to engender cynicism, while the continual evolution of the standard can create the sense that it is a moving target.

In the face of these concerns, the PCI organization and practitioners correctly point out that instances where PCI-compliant companies like Target which were known to follow sound security processes, yet nonetheless suffered a data breach, point to a core problem in the way that security is often practiced: namely, that it is not a product, but a process.

Bob Russo, Chairman of the PCI Security Standards Council, underscored that PCI compliance certification is a "snapshot in time" when he observed to Computerworld, "You can be in compliance today and totally out of compliance tomorrow."[60]

Standards are valuable tools for measuring and comparing security posture against common metrics. The danger of compliance certification is more in the risk that the organization will think that they are "done" with security, and not engage in the continual process of reassessment and adaptation as their environments and data practices change.

Data classification—High accuracy in identifying sensitive data is a critical component of a DLP solution. The DLP solution must be able to detect personally identifiable information (PII), compliance-related data (e.g., HIPAA, SOX, PCI data, etc.), and confidential business data, including both out-of-the-box data types and your own custom-defined data types. As data moves through the organization and beyond, the solution should inspect content flows and enforce policies in the most widely used TCP protocols, including SMTP, FTP, HTTP, HTTPS and webmail, using pattern matching and file classification to identify content types regardless of the file extension or compression format. The DLP solution must be able to recognize and protect sensitive forms based on predefined templates and file/form matching.

User-driven incident remediation—Traditional DLP solutions can detect, classify and even recognize specific documents and various file types, but they cannot capture the user's intent behind the sharing of sensitive information. Technology alone is inadequate because it cannot identify this intention and respond to it accordingly. Hence, a quality DLP solution must engage users in order to achieve optimal results. One approach is to empower users to remediate incidents in real-time. In other words, the DLP solution should inform the user that his/her action may result in a potential data leak incident, and then empower the user to decide whether to discard the message or to continue with sending it. This methodology improves security by elevating data storage policy awareness and alerting users of potential mistakes in real—

time, and reduces user impact by allowing for quick self-authorization of legitimate communications. As a result, security management is simplified because the administrator can track DLP events for analysis without having to personally attend to each external data send request as it happens.

Protection against internal data breaches—Another important DLP capability is the ability to not only control sensitive data from leaving the company, but also inspect and control sensitive emails sent between departments within the same company. Policies can be defined to prevent confidential data from accidental interdepartmental leakage—for example, compensation plans, confidential human resource documents, mergers and acquisitions documents or medical forms.

Data protection for endpoint hard drives—Companies must secure laptop data as part of a comprehensive security policy in order to prevent outsiders from obtaining valuable information through lost or stolen computers. You can prevent unauthorized users from accessing information by encrypting the data on all endpoint hard drives, including user data, operating system files, and temporary and erased files.

Data protection for removable media—Employees often mix personal files such as music, pictures and documents with business files such as finance or human resource files on USB storage devices and other removable media. This makes corporate data even more challenging to control. By encrypting removable storage and preventing unauthorized access for these devices, you can minimize security breaches in the event that they are lost or stolen.

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

IN 25%

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

LEARNING FROM POINT-OF-SALE ATTACKS

While hacking point-of-sale (POS) terminals in order to steal credit card data has long been technically possible, for many years attackers found the servers storing this data to be much easier targets. Improvements in the security of the servers storing credit card and customer data forced attackers to shift their focus to the source of the data, and 2013 marked a watershed year for POS hacking. While the scope and scale of these retail data breaches was shocking to many, equally interesting to security professionals was the variety in this category of malware.

POS malware itself ranges in sophistication from the memory scraping of the generic ChewBacca and Dexter[61], to the complex BlackPOS[62] and even more highly targeted POS malware discovered at Neiman Marcus[63]. However, they share several characteristics that enable the attackers to infiltrate POS systems and steal large amounts of credit card data:

- Reliance by POS systems on outdated operating systems that often remain unpatched for months even if a patch becomes available
- Gaining entry to the POS systems by way of an infected client or server in the targeted retailer
- Ability to circumvent application control and other system lockdown measures, for example by infecting an update server
- Use of encryption, common protocols and normal network traffic patterns to hide the data as it is being exfiltrated
- On many networks, direct Internet access from the POS device itself, often because this was how the actual billing is performed

Tackling these issues in isolation will not solve the problem because it does not solve the root cause: weak or non-existent segmentation of POS and production networks. Retail networks highlight the importance of developing and implementing a best-practices segmentation strategy that enables organizations to enforce containment policies for compromised hosts and define intra-segment interactions that can be monitored and enforced automatically. For example, monitoring enforcement of traffic direction and types for segments containing POS devices would restrict opportunities for malware to propagate and exfiltrate data. In this regard, retailers will find themselves on the vanguard of a shift by all organizations to define and implement logical segmentation and policy-driven enforcement across their IT environments.

Event management—In addition to defining DLP rules to meet your organization's data usage policies and implementing technologies to support and enforce them, a complete data loss prevention strategy must include robust monitoring and reporting capabilities. Your security solution should enable monitoring and analysis of both real-time and historical DLP events. This gives the security administrator a clear and broad view of the information being sent externally and their sources, and it also provides the organization with the ability to respond in real-time if necessary.

The next chapter presents a comprehensive high-level blueprint for effective security today.

06

THE SECURITY ARCHITECTURE FOR TOMORROW'S THREATS: Software-defined Protection

06 THE SECURITY ARCHITECTURE FOR TOMORROW'S THREATS: SOFTWARE-DEFINED PROTECTION

The Check Point *2014 Security Report* presents the results of our in-depth analysis of security threats and trends in 2013. This report can help security and business decision-makers understand the range of threats facing their organizations and consider new actions to improve the protection of their IT environment.

The highlights of our research are:

- The use of unknown malware exploded, driven by the trend of malware "mass customization."
- Malware exposure and infections increased across the board, reflecting the increasing success of targeted malware campaigns.
- Every category of high-risk application increased their presence in enterprises worldwide.
- Data loss incidents increased across industries and data types.

Facing the challenges

The findings of this report clearly indicate that the threat landscape continues to evolve while the security strategies and technologies employed at many organizations are inadequate in the face of increasingly sophisticated and damaging attacks. The explosion of unknown malware is quickly rendering detection-only solutions obsolete. Known malware is overwhelming existing defenses and striking a wider range of platforms. High-risk applications—as well as Web 2.0, file storage and sharing, and remote administration tools with legitimate business uses—continue to proliferate, opening new threat vectors as they spread. As both malicious and unintentional data loss incidents cause unprecedented damage to organizations of all sizes across sectors, and as mobility, consumerization and the Internet of Things compound the data protection challenge, organizations need a better control over the flow and usage of information.

A NEW PARADIGM IS NEEDED TO PROTECT ORGANIZATIONS PROACTIVELY

But facing the evolving threat landscape is not the only challenge in the IT environment. Businesses today are becoming more and more driven by free-flowing information, causing corporate networks to no longer have clear boundaries. Corporate data travels through the cloud and mobile devices and radiates through ideas and posts in social networks. Bring your own device (BYOD), mobility and cloud computing have revolutionized static IT environments, introducing the need for dynamic networks and infrastructures.

In our world of complex IT infrastructures and networks, where perimeters are no longer well defined, and where threats grow more intelligent every day, we need to define the right way to protect enterprises.

Today, there is a wide proliferation of point security products; however, these products tend to be reactive and tactical in nature rather than architecturally oriented. Today's corporations need a single architecture that combines high performance network security devices with real-time proactive protections.

A new paradigm is needed to protect organizations proactively.

Software-Defined Protection Security Architecture

In order to meet today's needs to protect against the evolving security threats while supporting complex IT infrastructures, Check Point introduces Software-Defined Protection.[64] It is a new, pragmatic security architecture and methodology that offers an infrastructure that is modular, agile and most importantly, SECURE.

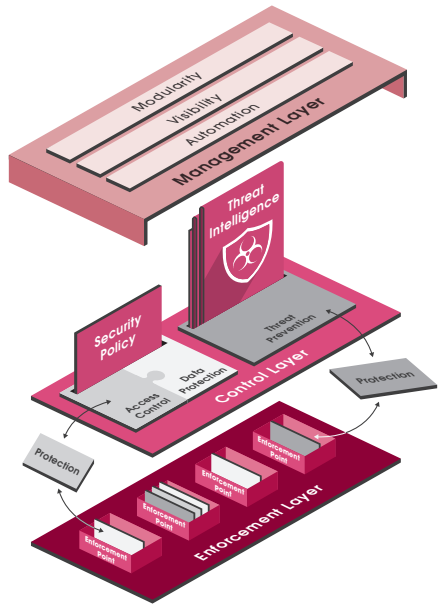
By implementing Software-Defined Protection architecture, organizations of all sizes and at any location are protected: headquarters networks, branch offices, roaming through smartphones or mobile devices, or when using cloud environments.

Based on Software-Defined Protection architecture, protections are automatically adapted to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections integrate seamlessly into the larger IT environment, and the architecture provides a defensive posture that collaboratively leverages both internal and external intelligent sources.

The Software-Defined Protection (SDP) architecture partitions the security infrastructure into three interconnected layers:

- An **Enforcement Layer** that is based on physical, virtual and host-based security enforcement points and that segments the network as well as executes the protection logic in high-demand environments.
- A **Control Layer** that analyzes different sources of threat information and generates protections and policies to be executed by the Enforcement Layer.
- A **Management Layer** that orchestrates the infrastructure and brings the highest degree of agility to the entire architecture.

By combining the high performance Enforcement Layer with the fast-evolving and dynamic software-based Control Layer, the SDP architecture provides not only operational resilience, but also proactive incident prevention for an ever-changing threat landscape.



Software-Defined Protection Layers

Implementing Security Blueprint in Your Organization

One of SDP's key benefits is that it offers a simple security blueprint implementation methodology. Check Point Software-Defined Protection—Enterprise Security Blueprint describes in detail the SDP architecture, its benefits and a clear implementation methodology. It is available online for free at checkpoint.com/sdp.

The following section describes in high level, layer by layer, how SDP can be integrated in your organization to protect against the threats presented in this report.

Enforcement Layer

Starting with the Enforcement Layer, designed to be reliable, fast and simple, it consists of both network security gateways and host-based software that function as the enterprise network enforcement points. These enforcement points can be implemented as either physical, virtual or as endpoint host components in the enterprise network or in the cloud.

Where to deploy these enforcement points in our network? When networks were simple, we could enforce protections on the perimeter alone. But when perimeters are not well defined, where should enforcement points be deployed?

Segmentation is the answer. It is the new perimeter. By dividing a complex environment into small segments based on security profiles, and deploying an enforcement point at the boundary of each segment, the environment is secure!

Control Layer

The next element of SDP architecture is the control layer. It is where protections are generated and security policies are pushed to the enforcement points. Using access control and data protection policies, administrators define rule-based policies to control interactions between users, assets, data and applications. This is basically a firewall and next generation firewall.

This is where policies are defined to control access to high-risk applications described in chapter 4 such as Anonymizers, P2P File Sharing, File Storage and even Remote Admin applications. These policies are also controlling the flow of data in motion and at rest and protect against data leakages such the ones described in chapter 5.

Access control and data protection policies are not enough; there is also a need to protect organizations against the bad guys and the evolving threats. In order to accomplish this goal as well, we need to implement protections that can identify known and unknown attacks such as the ones described in chapters 2 and 3.

It is being done by Threat Prevention, the second part of the control layer. Here, the threat protections are being updated in real-time, and automatically protected by the enforcement points so there is no need to define any specific policy here but rather only enable the Threat Prevention mechanism.

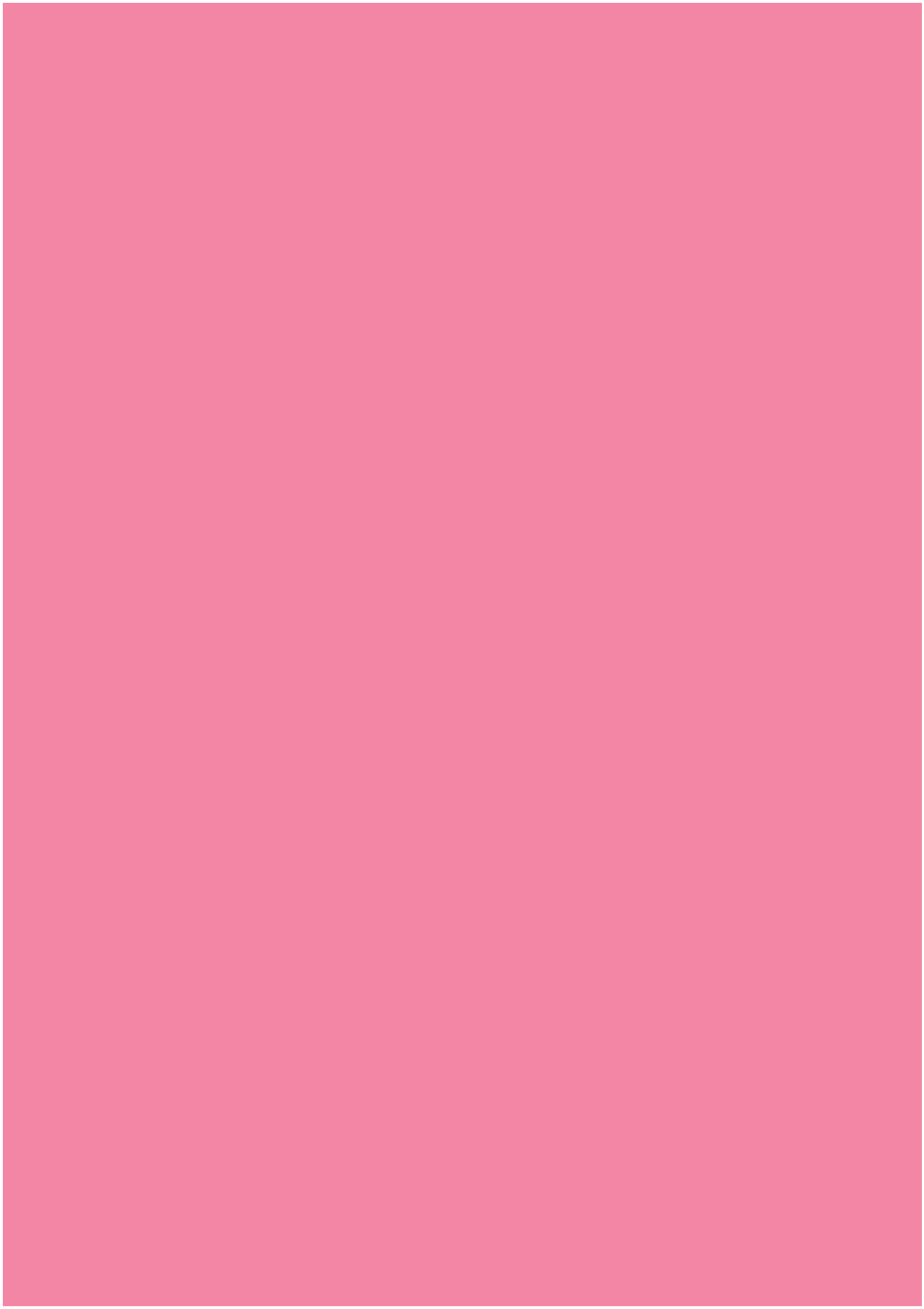
The key for effective threat prevention is intelligence. Threat intelligence should be built from as many resources as possible, processed and translated into new security protections, and fed to all enforcement points in real-time.

Management Layer

The third layer is the management layer, which brings the SDP architecture to life and is crucial for managing the entire architecture. The management layer has 3 key characteristics: modularity, automation and visibility.

Modularity provides a layered policy with the ability to segregate administrative duties for optimum management flexibility. Automation and openness allow integration with 3rd party systems creating policies and protection in real-time. And finally, visibility, the ability to collect security information from all enforcement points, providing a global view of the security posture of the organization.

Software-Defined Protection delivers a modular and dynamic infrastructure that adapts quickly to evolving threats and IT environments.



07
ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

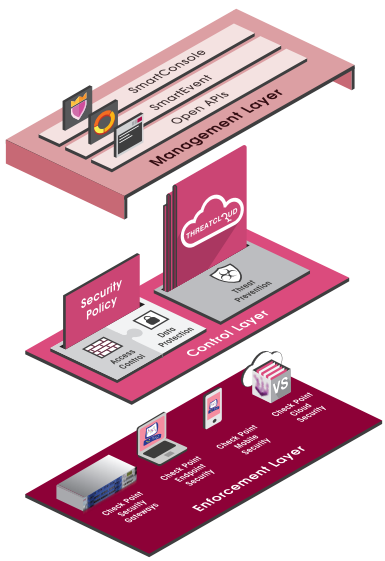
07 ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

For 20 years, the mission of Check Point has been to secure the Internet. From inventing the firewall to now leading the network security industry, Check Point focuses on developing the technologies needed to secure enterprises as the Internet continues to evolve.

Today the Internet is not only a legitimate platform for businesses; it's also a green field for cyber criminals. Given this environment, Check Point has developed an architecture to enable the deployment of multi-layer threat prevention that provides maximum protection against all threats including zero-day attacks.

Check Point SDP

Check Point defined and embraced the SDP architecture and provides the flexibility needed to cope with new threats and embrace new technologies.



Check Point SDP

Check Point offers a wide range of enforcement points, including: high-performance network security appliances, virtual gateways, endpoint host software and mobile device applications. It can be deployed at the enterprise network or in the cloud.

In terms of Control Layer, Check Point has the most advanced next generation firewall in the market and our ThreatCloud is the largest open big data, real-time threat knowledge that feeds our enforcement points in real-time.

And finally, Check Point architecture is managed from a unified security console that is modular, highly scalable and open for 3rd party systems.

Check Point provides the security architecture organizations need today to protect against tomorrow's threats.

For more information go to: www.checkpoint.com/sdp

Check Point combines this holistic approach to security with its innovative technology solutions to address today's threat challenges and to redefine security as a business enabler.

Consistently identified by analysts as a market leader in network security, Check Point Software has provided customers with innovative, enterprise-class security solutions and best practices for the past 20 years. Check Point customers include more than 100,000 organizations of all sizes, including all Fortune 100 and Global 100 companies.

REFERENCES

1 Stoll, Cliff. (2005). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York, NY: Pocket Books.

2 http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/

3 http://www.entrepreneur.com/article/231886

4 http://www.darkreading.com/advanced-threats/mass-customized-attacks-show-malware-mat/240154997

5 http://www.checkpoint.com/campaigns/securitycheckup/index.html

6 http://www.checkpoint.com/products/threat-emulation/

7 http://www.checkpoint.com/threatcloud-central/index.html

8 https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=20602

9 https://www.checkpoint.com/products/softwareblades/architecture/

10 http://www.checkpoint.com/products/index.html#gateways

11 Huxley, Thomas Henry (1887). *On the Reception of the Origin of Species*, http://www.todayinsci.com/H/Huxley_Thomas/HuxleyThomas-Quotations.htm

12 http://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

13 http://usa.kaspersky.com/

14 http://msdn.microsoft.com/en-us/magazine/cc164055.aspx

15 http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon

16 http://news.cnet.com/Code-Red-worm-claims-12,000-servers/2100-1001_3-270170.html

17 http://www.cnn.com/2004/TECH/internet/05/03/sasser.worm/

18 http://support.microsoft.com/kb/2664258

19 http://www.pcmag.com/article2/0,2817,2370016,00.asp

20 https://www.virustotal.com/

21 http://www.av-test.org/en/home/

22 http://www.checkpoint.com/threatcloud-central/downloads/10001-427-19-01-2014-ThreatCloud-TE-Thwarts-DarkComet.pdf

23 http://contextis.com/research/blog/malware-analysis-dark-comet-rat/

24 http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Portable_Executable.html

25 http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

26 Mariotti, John. (2010). *The Chinese Conspiracy.* Bloomington, IN: iUniverse.com

27 http://www.checkpoint.com/campaigns/security-report/download.html?source=google-ngfw-us-sitelink-report&gclid=ClfK-JuOhrwCFZFxQgodsBYA_w

28 https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-risk.html

29 Anderson, Chris. (2006). *The Long Tail: Why the Future of Business is Selling Less of More.* New York, NY: Hyperion.

30 http://www.fbi.gov/about-us/history/famous-cases/willie-sutton

31 http://searchwindowsserver.techtarget.com/definition/remote-code-execution-RCE

32 http://searchsoa.techtarget.com/definition/Remote-Procedure-Call

REFERENCES Cont.

[33] https://www.checkpoint.com/threatcloud-central/articles/2013-11-25-te-joke-of-the-day.html

[34] http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

[35] http://www.checkpoint.com/threatcloud-central/articles/2013-11-14-defeating-cryptocker.html

[36] http://www.apwg.org/

[37] http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

[38] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf

[39] http://newgtlds.icann.org/en/program-status/delegated-strings

[40] Stephenson, Neal. (2002). *Cryptonomicon.* New York, NY: Avon.

[41] Orwell, George. (1956). *Animal Farm.* New York, NY: Signet Books.

[42] https://www.torproject.org/

[43] http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html

[44] http://www.huffingtonpost.com/tag/silk-road-arrest

[45] http://www.pcworld.com/article/2093200/torenabled-malware-stole-credit-card-data-from-pos-systems-at-dozens-of-retailers.html

[46] http://www.britannica.com/EBchecked/topic/278114/Hydra

[47] http://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx

[48] http://www.securityweek.com/poison-ivy-kit-enables-easy-malware-customization-attackers

[49] http://www.checkpoint.com/defense/advisories/public/2005/cpai-20-Decf.html

[50] http://www.emea.symantec.com/web/ShadowIT-enduser/

[51] http://www.techrepublic.com/blog/it-security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/

[52] http://vote-il.org/politicianissue.aspx?state=il&id=ilbeanmelissa&issue=buscrime

[53] http://www.scmagazine.com/florida-health-department-employees-stole-data-committed-tax-fraud/article/318843/

[54] http://www.islingtongazette.co.uk/news/data_leak_lands_islington_council_with_70_000_fine_1_2369477

[55] http://healthitsecurity.com/2013/11/12/rotech-healthcare-reports-three-year-old-patient-data-breach/

[56] http://www.dailypost.co.uk/news/north-wales-news/anglesey-council-under-fire-over-6330304

[57] http://www.informationweek.com/attacks/heartland-payment-systems-hit-by-data-security-breach/d/d-id/1075770

[58] https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

[59] http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

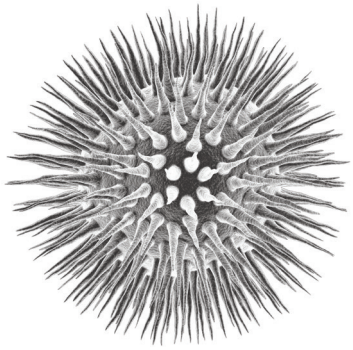
[60] http://www.computerworld.com/s/article/9245984/Despite_Target_data_breach_PCI_security_standard_remains_solid_chief_says

[61] http://www.csoonline.com/article/723630/dexter-malware-infects-point-of-sale-systems-worldwide-researchers-say

[62] http://www.darkreading.com/vulnerabilities---threats/securestate-releases-black-pos-malware-scanning-tool/d/d-id/1141216

[63] http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[64] http://www.checkpoint.com/sdp



Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

www.checkpoint.com

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