An Excerpt from the iDefense 2011 Cyber Threats and Trends Report

Dec. 1, 2010

The Verisign® iDefense® Intelligence Operations Team

Contents

1 Technology Trends

1.1 Malicious Code Trends

1.1.1 Anti-analysis Tactics Become More Restrictive

In 2010, iDefense observed more malware samples that included anti-analysis tactics. Malware authors use anti-analysis techniques to frustrate individuals attempting to analyze their code. The tactics that iDefense observed during 2010 included virtual machine (VM) detection, sandbox detection and hardware-locking mechanisms.

"Malware authors use anti-analysis techniques to frustrate individuals attempting to analyze their code."

The VM and sandbox-detection anti-analysis techniques are by no means a new concept. Many malware families check the environment for artifacts of analysis systems, such as VM hard drive drivers and VM processes. In addition, iDefense observed an increase in malware families that incorporate VM-detection techniques. For example, when iDefense first analyzed the Mariposa Trojan (BFBot) in 2009,[1] it only checked for artifacts related to a sandbox environment and if the Trojan was operating within a debugger. In July 2010, iDefense analyzed a Mariposa sample that also checked for video card drivers related to virtual machines. The addition of new checks suggests that malware authors see the benefits of including VM detection in their code.

Even malware samples that are noisy and blatantly obvious to the victim have begun using VM detection. iDefense analyzed a dropper Trojan that installed a Trojan whose sole purpose was to perform click-fraud and display advertising pop-ups on the system. This type of Trojan does not attempt to be stealthy; however, iDefense noticed the following code within the dropper Trojan that detects a VMware environment based on VMware's ComChannel:

```
// Moves "VX" into EDX, then uses the VM ComChannel "IN" command
004012FB . BA 58560000 MOV EDX,5658
00401300 . ED IN EAX,DX
00401301 . 90 NOP
00401302 . 87D9 XCHG ECX,EBX
00401304 . 87CB XCHG EBX,ECX
// Checks to see if EBX has "VMXh" in it, if true it terminates
00401306 . 81FB 68584D56 CMP EBX,564D5868
```

In addition to an increase in the use of VM detection, iDefense observed malware that locks itself to a system to thwart analysis on another system. The notorious Zeus banking Trojan, specifically versions 2 and later, includes a hardware-locking mechanism that will modify the Trojan to only run on the infected system. The Trojan accomplishes this locking by obtaining unique information from the local system and writing the information to its binary stored on the system. Upon execution, the Trojan compares the information included in the binary with the same information located on the system and will terminate if there are any differences. This hardware-locking technique is very effective and drastically increases the amount of effort required to analyze the sample on an analysis system.

1 iDefense Malicious Code Summary Report (ID# 536506, Oct. 28, 2009).

The increase in the use of anti-analysis tactics suggests that malware developers have considered the pros and cons involved with such tactics. The main con that malware developers accept with anti-analysis techniques is that their code will run on fewer systems; however, malware developers seem to weigh the pro of avoiding execution on analysis systems over the negative side effect of fewer infections. Efforts to avoid analysis show that malware continues to shift from a goal of spreading quickly to malware with an emphasis on stealth. iDefense predicts that at least one major family will appear in 2011 that uses new, stricter anti-analysis tactics.

1.1.2 Mobile Malware

Users are increasingly using mobile devices to send e-mails, perform transactions for online banking and store personal information. Some of the new popular applications track personal health or fitness information, scan barcodes, and help with time management. The ability for new mobile devices to track such a wealth of information and provide detailed real-time information draws more users to mobile platforms. Modern mobile devices allow applications to track real-time global positions, facing direction and even gravitational forces. It is no surprise that users want to develop applications that access this type of information because it will increase those users' interaction with both the real world and the electronic world from their mobile devices. iDefense first identified mobile platforms as a disruptive technology for security in 2007.

Mobile operating system vendors and telecommunications companies still wish to control applications that users may run on their mobile phones. Their primary reasons might be to satisfy laws, limit bandwidth usage, limit abuse, reduce maintenance costs and capitalize on existing communications such as short message service (SMS). Mobile users, however, want to utilize mobile devices to install new applications without permission, and the community interested in jailbreaking devices has grown in the past year. Now that jailbreaking is officially legal, according to a press release by the Electronic Frontier Foundation (EFF),[2] community efforts to subvert these security controls are likely to continue to escalate.

In August 2010, one website, jailbreakme.com, released code to jailbreak the iPhone simply by visiting its website. Upon visiting, the code uses a zero-day exploit to execute code on visitors' phones to disable the security measures and enable non-official applications to run. The ease of jailbreaking the iPhone by visiting this website demonstrates that even novice users can jailbreak their mobile devices. If attackers had the information that jailbreakme.com uses, they could have written a mobile worm that after jailbreaking a phone attempts to spread to other phone contacts. A worm using this type of vulnerability has not happened, however, and the jailbreaking community's intent is largely not currently malicious, even though those who are part of that community are more active than attackers in developing exploits for mobile devices. As a side effect, jailbroken phones are less secure than their non-jailbroken counterparts, which could encourage more attackers to target jailbroken devices with malicious code.

"The ease of jailbreaking the iPhone by visiting this website demonstrates that even novice users can jailbreak their mobile devices."

2 Staff. "EFF Wins New Legal Protections for Video Artists, Cell Phone Jailbreakers, and Unlockers." July 26, 2010. EFF. http://www.eff.org/press/archives/2010/07/26.

Financially motivated attacks against mobile devices also exist. The most popular of financially motivated attacks installs applications that make phone calls to premium-rate phone numbers; however, there is also malicious mobile software that works with banking Trojans that affect computers running Microsoft Windows. On Sept. 27, 2010, iDefense received samples of a Zeus binary that has a secondary payload to target certain brands of mobile phones in the UK. Upon infecting a Microsoft Windows system, the Zeus binary injects HTML into banking websites to convince users to install an application on their mobile phones. Once installed, the application monitors SMS messages and relays those messages to an attacker's UK phone number to defeat one-time-password (OTP) challenges.

Mobile devices continue to be a segmented market with many choices including iPhone, Android, Symbian, BlackBerry and Windows Mobile. Users in the US have purchased more Android devices than iPhones in 2010 so far.[3] Android has a less controlled application store, which may be one of the reasons for its increase in popularity. In 2011, iDefense predicts that at least one malicious application in the Android store will receive 50,000 downloads.

"In 2011, iDefense predicts that at least one malicious application in the Android store will receive 50,000 downloads."

1.1.3 Malware and 64-bit Platforms

While rare to find on desktops just 5 years ago, 64-bit processors have become standard equipment for even the least expensive laptops on the market today. The primary advantage this architecture has over its 32-bit predecessor is a larger address space for memory. While the maximum number a computer can express with 32 bits is just greater than 4 billion, 64 bits can represent numbers more than 18 quintillion (that is 18 billion billion). To put more than 4 gigabytes (GB) of memory into a computer, that computer must be able to support these larger numbers so the processor can easily address each byte of memory. With processor support in place, the operating system (OS) must also support this architecture to allow users to make use of the extra space.

While 64-bit versions of Windows XP and Windows Vista both exist, their adoption rate is very low compared to Microsoft's latest OS, Windows 7. In July 2010, 46 percent of Windows 7 installations used the 64-bit version of the OS compared to just 11 percent for Windows Vista and less than 1 percent for Windows XP.[4] As more users begin using Windows 7 and dispose of their older Windows XP and Vista systems, 64-bit versions of Windows will make up a significant portion of the Windows ecosystem.

This change will force malware authors to adapt, as 64-bit versions of Windows contain additional security features not present in 32-bit distributions. Most importantly, 64-bit versions include Kernel Patch Protection (KPP), or PatchGuard. This feature prevents 64-bit versions of Windows from loading kernel drivers that developers have not signed with a legitimate Authenticode signing certificate. One category of malware that often requires access to the kernel to operate properly is that of rootkits. These types of

3 Tofel, Kevin C. "Android Sales Overtake iPhone in the U.S." Aug. 2, 2010. Gigaom. http://gigaom.com/2010/08/02/android-sales-overtake-iphone-in-the-u-s/.

4 LeBlanc, Brandon. "64-Bit Momentum Surges with Windows 7." July 8, 2010. Windows. http://windowsteamblog.com/windows/b/bloggingwindows/archive/2010/07/08/64-bit-momentum-surges-with-windows-7.aspx.

malware hook the OS at the lowest possible level to hide files and system modifications from users and security software.

To effectively create a rootkit that operates on these systems, malware authors are likely to use three possible tactics. First, they may sign their malware using legitimate code-signing certificates. In July 2010, security researchers discovered the Stuxnet worm, which used this tactic after its creators stole code-signing certificates that belonged to Realtek Semiconductor and JMicron. The disadvantage to this tactic for the malware author is that once administrators detect the rootkit, the certificate authority responsible for the code-signing certificate may revoke the certificate, effectively disabling the driver.

A second tactic that malware authors may use is disabling Windows' ability to prevent unsigned drivers from loading into the kernel. One malware family, TDL3, has already implemented this technique to properly infect 64-bit systems. The rootkit overwrites the system's master boot record (MBR) to take control of the system before the protection is in place, disabling KPP so the system will load the rootkit's driver once the system finishes booting.

The third tactic would be to only install user-mode rootkits that operate above the kernel. User-mode rootkits are still capable of hiding files and system modifications from the user, but they are much easier for rootkit-detection tools to find because those tools typically work at a lower level in the OS.

In 2011, it is likely that additional rootkits will begin targeting 64-bit versions of Windows by changing their code to match the tactics listed above. If attackers do not adapt, they will quickly find that their code does not operate on a large percent of the systems they want to infect.

1.1.4 Low-Distribution (APT) Malware Hiding in Plain Sight

Most modern malware uses a technique named "packing" to obfuscate the functionality of their programs to simultaneously evade detection by AV programs and thwart the efforts of malware analysts attempting to discover that functionality. While packing is often effective, malware uses some packers so commonly that AV engines detect the packer code itself rather than the malicious code it hides.

AV programs also use heuristics to detect suspicious activity on a system. For instance, when a program accesses the memory of other programs on a system and creates remote threads within them, an AV program may flag the program as malicious. Malware that attackers intend to distribute widely, by sending spam or stealing credentials for online banking websites, must contain a packing algorithm to hide its behavior. Without a packing algorithm, AV programs would quickly write signatures that detect and remove the malware.

On the other hand, AV programs are not likely to detect malware very quickly if attackers distribute it in very small numbers, such as that used in targeted attacks often characterized as APTs. The lack of detection is not a result of a

packing algorithm, instead analysts who write signatures for their engines have never seen the malware before.

Attackers who create APT malware often use no packing techniques and execute their malware using methods that make them appear to be legitimate programs. One example is the DNSCalc[5] malware on which iDefense reported in May 2010 related to targeted attacks. Malware in this family uses functionality that is not heavily obfuscated. The malware uses filenames such as "windfvsrv.exe" and installs itself as a Windows service. The program acts as a simple backdoor through which the attacker can execute commands; the program does not conduct any detectably malicious activities. By not using techniques that malware typically uses, these programs can hide in plain sight and evade detection for weeks or months.

"Attackers who create APT malware often use no packing techniques and execute their malware using methods that make them appear to be legitimate programs."

1.2 Vulnerability Trends

1.2.1 Increase in Out-of-Band Patches from Notable Software Vendors

In its 2010 Trends Report, iDefense discussed the burden of patch alignment stemming from the trend of software vendors that purposely chose the second Tuesday of the month to release security updates for their scheduled patch release, which coincides with Microsoft's monthly Security Bulletin release. Vendors did this in an effort to leverage existing processes and resources. This year, iDefense saw a trend of an unusual number of out-of-band (OOB) patch releases from three of the now five vendors (Microsoft, Oracle, Cisco, Adobe and SAP) that follow a scheduled patch release for some or all of their products. On paper, this indicates that vendors are quick to respond to vulnerabilities discovered in their products; however, data will show that the discovery of a previously unknown vulnerability released publicly for which a patch does not exist, otherwise known as a zero-day vulnerability, is what is forcing vendors to release these OOB patches. This signifies the common occurrence of zero-day vulnerabilities in a broader range of products, which has not been nearly as prevalent until this year.

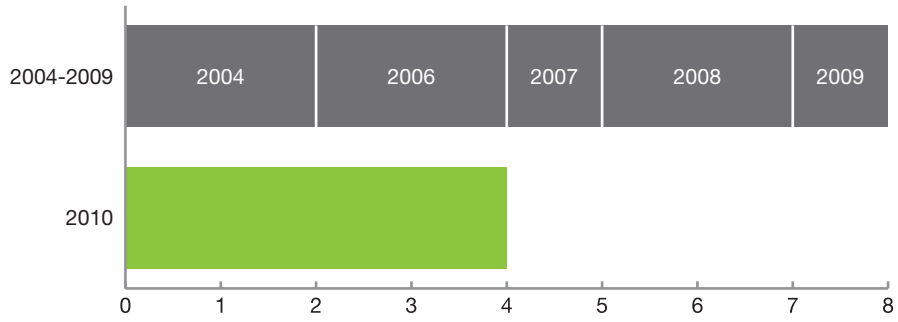


Exhibit 1-1: Microsoft OOB Patches Released in 2010 Compared to Patches Released between 2004 and 2009

In 2010, Microsoft has released four OOB security bulletins, which almost matches the six OOB security bulletins that Microsoft released in a 5-year span from 2004 to 2009 (see Exhibit 1-1). All but one of the four OOB Security Bulletins began as either exploits or malware that malicious actors

5 DNS-Calc APT Trojan Uses DNS Queries to Generate C&C Port Number (ID# 595094, May 13, 2010).

used in targeted attacks that could result in arbitrary code execution with the privileges of the current user.[6] The one exception was the last OOB Security Bulletin that Microsoft released to address an information disclosure vulnerability in ASP.NET, which security researchers Juliano Rizzo and Thai Duong publicly disclosed at the Ekoparty security conference in Buenos Aires. At the end of their presentation, they threw three USB flash drives containing documentation of the vulnerability and a working exploit into the audience.[7]

Oracle uses quarterly patching cycles through releases of Critical Patch Updates (CPUs). Oracle has historically released CPUs on the Tuesday closest to the 15th day of the quarterly month. In 2010, Oracle's OOB security advisories came in the form of out-of-cycle security alerts. Oracle has released two out-of-cycle security alerts to address a trivially exploited vulnerability affecting Oracle WebLogic Server; a malicious actor could use this vulnerability to gain unauthorized access to a vulnerable host to execute arbitrary commands without any user interaction.[8] The other out-of-cycle security alert was in response to publicity due to the public disclosure of two vulnerabilities in Sun Java; with these vulnerabilities, malicious actors could execute arbitrary code on a victim's system by social engineering the victim into viewing a malicious website.[9] Prior to 2010, the last out-of-cycle security alert was in July 2008 for a buffer overflow vulnerability in xine-lib, which affected multiple vendors.[10]

Cisco uses a semiannual scheduled patching cycle that occurs on the fourth Wednesday of March and September and only applies to the Cisco IOS, which is Cisco's operating system that powers Cisco's vast array of routers and network switches. Cisco released three IOS out-of-cycle security bulletins in 2009, even though there were no reports indicating that malicious users were exploiting the fixed vulnerabilities. On Jan. 20, 2010, Cisco released a single security advisory outside its semiannual scheduled release to fix a memory exhaustion vulnerability in IOS that could result in a denial of service (DoS) condition; however, Cisco would likely argue that this vulnerability does not classify as an OOB security release since the vulnerability did not fit any of Cisco's conditions for making an out-of-cycle release.[11]

A month after Adobe's first scheduled quarterly patch release for Acrobat and Reader on June 9, 2009, Adobe released its first out-of-cycle security bulletin during late July 2009, to address a PDF vulnerability that attackers were exploiting in the wild.[12] Much like the vulnerabilities that Microsoft fixed OOB, the four vulnerabilities that Adobe fixed OOB started as either exploits or malware that malicious actors used in targeted attacks, with the exception

6 Microsoft Internet Explorer Invalid Pointer Reference Code Execution Vulnerability (ID# 560358, Jan. 14, 2010); Microsoft Internet Explorer Invalid Pointer Reference Memory Corruption Vulnerability (ID# 578152, March 9, 2010); Microsoft Windows Shortcut .lnk Design Error Vulnerability (ID# 601740, July 16 2010).
7 Microsoft ASP.NET Ciphertext Padding Information Disclosure Vulnerability (ID# 617272, Sept. 18, 2010).
8 Oracle Weblogic Server Node Manager Command Execution Vulnerability (ID# 563044, Jan. 25, 2010).
9 Maurice, Eric. "Security Alert for CVE-2010-0886 and CVE-2010-0887 Released." April 15, 2010. Oracle Corp. http://blogs.oracle.com/security/2010/04/security_alert_for_cve-2010-08.html; Oracle Java SE and Java for Business Desktop Java Deployment Toolkit Unspecified Vulnerability (ID# 595164, May 18, 2010); Oracle Java SE and Java for Business Desktop Java New Java Plug-in Unspecified Vulnerability (ID# 595165, May 18, 2010).
10 Multiple Vendor xine-lib 1.1.10.1 sdpplin_parse() Function Buffer Overflow Vulnerability (ID# 468070, March 11, 2008).
11 "Products & Services Security Vulnerability Policy - Cisco Systems." Sept. 8, 2010. Cisco Systems Inc. http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.
12 Adobe Flash ActionScript Parsing Memory Corruption Vulnerability (ID# 492133, July 20, 2009).

of one vulnerability;[13] the exception was an integer overflow vulnerability that emerged from the Black Hat 2010 conference in Las Vegas, which could allow an attacker to execute arbitrary code on a targeted host.[14]

1.2.2 Changing Vulnerability Disclosure Landscape

The vulnerability disclosure landscape dramatically changed over the course of the year. The emergence of multiple vendor bounty programs, increase in standard payment for vulnerabilities, and the creation of coordinated vulnerability disclosure reenergized relationships between security researchers and vendors.

Early this year, Google announced it would offer researchers cash rewards for bugs and vulnerabilities found in its browser, Chrome. This program, similar to Mozilla's Firefox bounty program, received criticism because security researchers felt the cash reward was too small. Security researchers could sell their work to brokers for a much larger compensation. Mid-year, Mozilla announced it would pay researchers up to $3,000 US for critical vulnerabilities found in its browser, Firefox. Google quickly responded by offering security researchers up to $3,133.73 US. Thus, a bidding war began for researchers' efforts, raising the industry's standard payment for vulnerabilities.

The price bump signified a change in the overall posture by vendors for vulnerability research. Vendors are embracing the overall change in the economics of vulnerability research. Vulnerabilities and bugs are no longer free. Rather than rewarding researchers with T-shirts and recognition, vendors are giving security researchers real cash incentives for helping make vendors' products more secure. This once one-way street has become a two-way street for security researchers and vendors. The cash incentive has proven very effective in the case of Google. The number of bugs and vulnerabilities that people have submitted to Google has dramatically increased since the bounty prize increase. The success of Chrome's bounty program spawned Google's latest bounty program, which it designed to fortify Google's array of Web applications.

"Vendors are embracing the overall change in the economics of vulnerability research. Vulnerabilities and bugs are no longer free."

Microsoft outlined a new form of responsible disclosure. Microsoft coined the new disclosure type "coordinated vulnerability disclosure" or CVD. CVD follows the core principles of responsible disclosure but further defines coordination with three basic philosophies: vendors and discoverers need to work closely toward a resolution; vendors should make extensive efforts to respond in a timely manner; and only in the event of active attacks should vendors use public disclosure, which should focus on mitigation and workarounds.[15]

Microsoft created CVD in response to two opposing views on the disclosure of vulnerabilities: responsible disclosure and full disclosure. Responsible disclosure gives vendors a chance to patch vulnerabilities before the public knows about them; however, this type of disclosure can result in vendors

13 Adobe Reader and Acrobat 9.3 LibTiff Integer Overflow Vulnerability (ID# 572570, Feb. 16, 2010); Adobe Flash Player 10.0.45.2, Reader 9.3.2 and Acrobat 9.3.2 Remote Code Execution Vulnerability (ID# 595312, June 5, 2010); Adobe Acrobat and Reader Cooltype.dll Memory Corruption Vulnerability (ID# 614986, Sept. 18, 2010).

14 Adobe Acrobat and Reader CoolType.dll True Type Font Integer Overflow Vulnerability (ID# 607161, Aug. 4, 2010).

15 Thomlinson, Matt. "Announcing Coordinated Vulnerability Disclosure." July 22, 2010. Microsoft. http://blogs.technet.com/b/msrc/archive/2010/07/22/announcing-coordinated-vulnerability-disclosure.aspx.

delaying the fix of vulnerabilities, which may allow a miscreant to discover such vulnerabilities and use them in targeted attacks. Full disclosure provides malicious users with details to use against unpatched software but could also enable immediate preventive action, and it pressures vendors to quickly develop a fix for such vulnerabilities.

Tavis Ormandy, a security researcher for The Google Security Team, released details for a critical vulnerability in Microsoft Windows on Full Disclosure on June 10.[16] Microsoft acknowledged the vulnerability the same day and reiterated that it advocates responsible disclosure and encourages security researchers to work with it on providing mitigation for an issue and coordinating the release of details.[17]

The Google Security Team responded in its blog with Google's stance on disclosure policies. The blog discussed the differences, benefits and shortcomings of the two disclosure models (responsible disclosure and full disclosure).

Microsoft's efforts to redefine responsible disclosure into coordinated vulnerability disclosure are the software giant's way of realigning itself with the evolving vulnerability disclosure landscape. Vendors such as Google and Mozilla realize that vulnerability research is no longer about recognition but rather has evolved into a source of income for many professional security researchers. This year marked many changes in the security field, but none of those changes were as dramatic as the change between vendor and security researcher relationships.

"Full disclosure provides malicious users with details to use against unpatched software but could also enable immediate preventive action, and it pressures vendors to quickly develop a fix for such vulnerabilities."

1.2.3 Vendor Bounty Programs

1.2.3.1 Mozilla Security Bug Bounty Program

Mozilla initiated a bug bounty program in August 2004,[18] in which it compensated security researchers $500 US and a T-shirt[19] to report critical security bugs in both Thunderbird and Firefox. In July of this year, the bounty increased to $3,000 US. The increase was due the evolving cyber landscape. A movement called "No more free bugs" was a contributing factor to the change; this movement supported the idea that security researchers believed that vendors should compensate them for newly discovered security vulnerabilities. Security researchers Charlie Miller, Dino Dai Zovi and Alex Sotirov advocated these sentiments in 2009 during CanSecWest.

Mozilla's security engineering director, Lucas Adamski, acknowledged the transitioning cyber landscape and believed that increasing the compensation would improve relations between security researchers and Mozilla. Additionally, this would prompt researchers to responsibly disclose the vulnerabilities to Mozilla and improve the safety of its products.

The higher compensation by Mozilla has the potential to drive more security

16 Microsoft Windows Help and Support Center Malformed Escape Sequence Vulnerability (ID# 595633, June 10, 2010).
17 Reavey, Mike. "Windows Help Vulnerability Disclosure." June 10, 2010. Microsoft. http://blogs.technet.com/b/msrc/archive/2010/06/10/windows-help-vulnerability-disclosure.aspx.
18 Staff. "MOZILLA FOUNDATION ANNOUNCES SECURITY BUG BOUNTY PROGRAM." Aug. 2, 2004. Mozilla Foundation. http://www-archive.mozilla.org/press/mozilla-2004-08-02.html.
19 Staff. "Mozilla Security Bug Bounty Program." Aug. 11, 2010. Mozilla Foundation. http://www.mozilla.org/security/bug-bounty.html.

researchers to present high-quality bugs; however, the program has been in place since July of this year and it is too soon to tell the effectiveness of the program. Since the increase, the number of vulnerabilities has increased slightly, but one could attribute this to the increase in the number of existing vulnerabilities over the years. The number of Mozilla vulnerabilities year over year has increased on average about 11 percent.

1.2.3.2 Google Security Bug Bounty Program

Google presented a similar program to reward security researchers for their work. Payment for general vulnerabilities was $500 US and for severe vulnerabilities, $1,337 US. Google considered severe bugs "leet," which is hacker slang for elite. The program received scrutiny from security researchers stating that the amount was too low. Mozilla also offered $500 US for bugs—the same amount that it provided in 2004. The first 6 months of Google's bug bounty program yielded 21 bugs. Google considered one the 21 bugs to be "leet."

Soon after Mozilla increased its bounty to $3,000 US, Google reacted by increasing its maximum bounty to $3,133.73 US. This amount is the numeric translation of "elite." The increase in the bounty generated greater interest and resulted in the disclosure of more vulnerabilities in a shorter period of time than previous bounty amounts did.[20]

The addition of the sandbox feature in Chrome makes it difficult for security researchers to discover high-severity vulnerabilities.[21] Chris Evans of Google Chrome Security stated that the sandbox feature in Chrome requires security researchers to spend more time discovering bugs. Google justifies the high bounty by the amount of work that goes into researching those bugs. The limited number of security researchers and the amount of time that goes into discovering bugs requires researchers to focus on one particular browser. This situation can drive researchers to research bugs in the browser that pays out the most.

On Nov. 1, 2010, Google announced a new, experimental bounty program that extends to Google Web properties.[22] Such Google Web properties include .google.com, .youtube.com, .blogger.com and .orkut.com.[23] The same rules and bug bounty rewards apply to newly discovered bugs. Google plans to extend the program to its client-based applications in the near future, which include Android, Picasa and Google Desktop.[24]

Even though the program started on the wrong foot, Google's bounty program has reported more vulnerabilities since its bounty increase. Since the increase, the amount of $1,337 US bounties has quadrupled, but Google has yet to pay out the "elite" amount. The increase in disclosures is a clear indicator that more researchers are dedicating more time to find higher-quality bugs

20 "Security Hall of Fame." Sept 9, 2010. Google Inc. http://dev.chromium.org/Home/chromium-security/hall-of-fame; Evans, Chris. "Celebrating Six Months of Chromium Security Rewards." July 20, 2010. Google Inc. http://google-chrome-browser.com/celebrating-six-months-chromium-security-rewards.
21 Ibid.
22 "Rewarding web application security research." Nov. 1, 2010. Google Inc. http://googleonlinesecurity.blogspot.com/2010/11/rewarding-web-application-security.html.
23 Ibid.
24 Ibid.

in Chrome. With the extension of the experimental bug bounty program to Web-based applications and the hard learn lesson from the beginning of the program, Google can expect a similar turnaround of high-quality bugs.

2 Disruptors

2.1 Introduction

In 1997, Clayton Christensen published his book "The Innovator's Dilemma,"[25] in which he postulated a theory about disruptive technology. Essentially, innovations can emerge that fundamentally change how an industry services its customer base. Some businesses fail because leadership does not recognize the change fast enough to compete.

These business catalysts are not enhancements or improvements to existing ideas, but rather are radical and innovative solutions that sometimes, at first glance, appear only to service a niche audience. Over time, use of these innovations builds momentum and eventually dominates the space. The heretofore best practice solutions wither and die while the innovation takes over. One example that Christensen uses to prove his point is the size reduction of computer disk drives.[26]

Hard drives have gone through repeated design innovations from the early 1960s to the early 1990s. The disruptive technology that caused some businesses to fail came with each reduction. For example, when the 5.25-inch floppy drives started to appear on the personal computer market, the dominant floppy drive manufacturers were producing 8-inch floppy drives for minicomputers. According to the Christensen, the 8-inch producers did not anticipate the demand for the 5.25-inch floppies until it was too late and businesses failed.

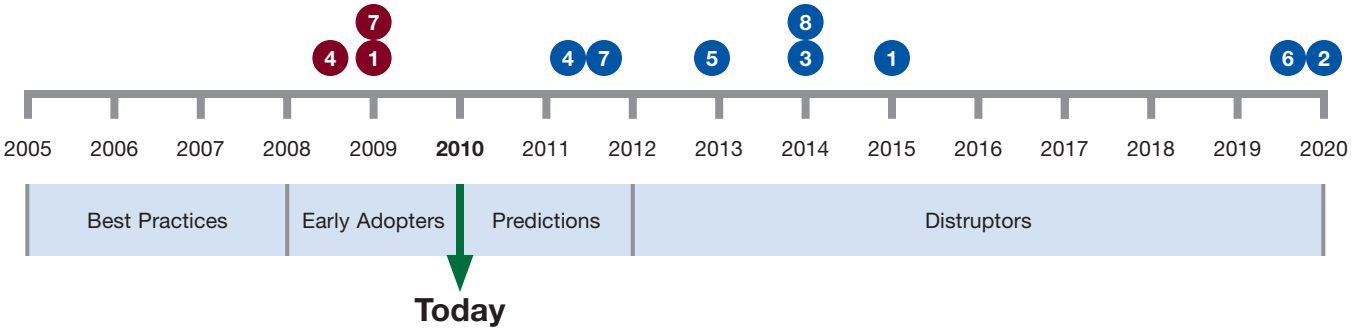
In 2007, iDefense introduced the concept of the cyber security disruptor: new ideas, technologies, government policies or events (cyber security catalysts) in the next 5-10 years that could fundamentally change how organizations protect their cyber assets.[27] Since 2007, iDefense analysts have identified disruptive catalysts worthy of the disruptor definition. Each of these catalysts represents a technology, law or forecasted event that will completely change the security community at some level. This type of change is at the heart of the disruptor. Change is the reason that iDefense spends so much time trying to describe the concept and identify the key disruptors. The idea is to give the security community leadership a chance to prepare for a completely different way of doing business.

"Since 2007, iDefense analysts have identified disruptive catalysts worthy of the disruptor definition. Each of these catalysts represents a technology, law or forecasted event that will completely change the security community at some level."

Consider the timeline in Exhibit 2-1. The far right outlines predictions 10 years into the future. This is the event horizon when iDefense analysts begin to track the innovations that will affect the future enterprise.

At the far left is the past: 2005 and prior. This is the area where current security best practices reside, where technology leaders have agreed that certain solutions work well to mitigate specific security problems. In the case of disruptors, these mitigation options have become industry-accepted solutions. Technologies such as firewalls, anti-virus engines and IDS reside here.

25 Christensen, Clayton M. "The Innovator's Dilemma." Harper, 1997.
26 Ibid, pp. 15-19.
27 Cyber Disruptors: the Next Five Years (ID# 465310, Nov 5, 2007).



1 1 **Concept:** Developing Nations' Use of the Internet → **Impact:** These nations have seen increased volumes of malicious cyber activity. → **Enterprise Change:** There will be a shift in the center of gravity away from commercial entities and toward governments in terms of budget and compliance laws.

2 **Concept:** Massively Multiplayer Online Environments (MMOs) and the Metaverse → **Impact:** This is a new type of Internet interface. → **Enterprise Change:** Robust solutions around identity management

3 **Concept:** SCADA Attacks → **Impact:** As SCADA systems become more and more connected to the Internet, they become more vulnerable to cyber attacks. → **Enterprise Change:** Traditional security teams, not facility teams, will manage the SCADA security infrastructure.

4 4 **Concept:** Mobile Platforms → **Impact:** Powerful untethered computing devices become ubiquitous. → **Enterprise Change:** Robust security suites dedicated to protecting the platform

5 **Concept:** Political and Strategic Hacking (Advanced Persistent Threat) → **Impact:** Intellectual property is seriously at risk. → **Enterprise Change:** Data loss prevention tools become mainstream.

6 **Concept:** Cyber Terrorism → **Impact:** The first death via a cyber threat alone will cause all organizations to rethink their security practices. → **Enterprise Change:** Extreme compliance laws and privacy erosion

7 7 **Concept:** Cloud Computing → **Impact:** As corporations are moving toward the use of cloud computing, increasingly, more corporate resources are not directly controlling the enterprise. → **Enterprise Change:** Development of robust oversight groups

8 **Concept:** Application Stores → **Impact:** Application stores are trusted sources for software. → **Enterprise Change:** The importance of anti-virus technology will diminish.

Exhibit 2-1: Cyber Security Disruptor Timeline

In the middle of the timeline is today: 2010. This is the precipice where security leaders make critical technological and budgetary decisions about how best to protect their enterprises. This is also where iDefense analysts attempt to predict what the next year will bring to help its customers, who are some of the largest enterprise leaders in the world, make informed decisions.

In the near past is 2008, where brave technologists have deployed technologies early because they recognize the great potential for disruption. As such, they are willing to weather the bumps and bruises normally associated with early deployment of a technology that is not quite ready for wide distribution.

The numbered circles on the timeline show the iDefense estimates on how far out it considers each of these disruptors to be. The placement of the circles is based on iDefense research and observations made by the security community. As disruptors get closer to the present, they begin a transformation: within a year of the present, iDefense often identifies them as predictions for the following year. As each disruptor moves farther into the past, they most often take the form of security solutions. At this point, iDefense analysts consider them best practices and no longer disruptors.

It is worth noting that for any particular time, iDefense analysts will move each of these disruptors up and down the timeline depending on a number

of factors that affect how quickly the security community reacts to each disruptor. For example, two of the disruptors–massively multiplayer online environments (MMOs) and cyber terrorism–exist at the far end of the event horizon of 8-10 years. Others, such as cloud computing, developing nations and mobile platforms, already have early adopters but are probably 2-5 years from mainstream adoption. The remaining disruptors, including application stores, SCADA attacks, IPv6/DNSSEC/IPSEC deployment, and political and strategic hacking, have no real early adopters but are probably also 2-5 years from mainstream adoption.

In the following sections, iDefense updates the status of the original disruptors and provides additional depth on two: application stores and cloud computing. These sections are meant to highlight disruptors that iDefense believes require a closer look. For instance, iDefense malware analysts believe strongly that application stores will fundamentally change the way that organizations secure themselves from software-based threats. Likewise, many iDefense vulnerability specialists believe that a vulnerable cloud will fundamentally change the perception of the cloud as a security solution. These discussions are less identifications of new disruptors than deeper looks at disruptors that iDefense has previously discussed.

2.2 Disruptor: Convergence of the "App Store" Model and Traditional Computing

The "app store" distribution model has become the de facto standard method for users to install programs onto mobile devices such as smartphones. Apple's App Store is the largest application store in the market with more than 250,000 available applications and more than 6.5 billion downloaded applications; however, many mobile vendors, including Google, RIM, HP/Palm, Nokia and Microsoft, have implemented their own platforms.

Mobile devices with application stores have two security advantages over their traditional computing counterparts such as desktop and laptop PCs. First, only applications that developers have signed with a certificate provided by the app store proprietor can execute on the devices. The effect of this protection is that only applications created by known developers can run on the devices; if an application store proprietor discovers that a particular program is malicious, he or she can execute a "kill-switch" for the application by revoking the certificate. Second, app stores act as gateways between malware authors and the devices on which those authors want to run their malware. The proprietor of an app store can conduct reviews of programs before making them available to users, which prevents most malware from ever entering their platforms' ecosystems.

These protections are far from perfect, as attackers have already introduced malware into app stores and discovered ways to disable the signed-code requirement that prevents the execution of unsigned programs. Despite these problems, systems that use the application store model have a much more defensible architecture than traditional desktop operating systems.

28 Walters, Audrey. "Gartner Hype Cycle 2010: Cloud Computing at the Peak of Inflated Expectations." Oct. 8, 2010. ReadWriteWeb. http://www.readwriteweb.com/archives/gartner_hype_cycle_2010_cloud_computing_at_the_pea.php.

29 Staff. "iPhone OS 4 Adds Much Needed Security Features." April 8, 2010. Security Week. http://www.securityweek.com/content/iphone-os-4-adds-much-needed-security-features.

Cloud Computing

Year: 2011

Concept: Outsourcing automation resources to third-party vendors at greatly reduced costs compared to the costs of performing those tasks in house.

Impact: Adopting cloud computing services within an enterprise effectively moves critical infrastructure and intellectual property out of direct control by the enterprise. Conversely, having all data centrally located will likely provide increased incentive for attackers to compromise the cloud.

Enterprise Change: As cloud computing becomes more popular, the teams that are tasked with monitoring these third-party vendors will grow and will become a dominant player in the security organization. Increased malicious scrutiny may prove the cloud to be less than ideal as a security solution.

Early Adopters: Yes (2009)

What has changed this year: According to Gartner, cloud computing has reached its peak of inflated expectations and is 2-5 years from mainstream adoption.[4]

Mobile Platforms

Year: 2011

Concept: There has been a ubiquitous explosion of powerful computing devices on enterprise networks that both businesses and individuals use. As Walt Mossberg has said, the difference between a BlackBerry and a smartphone is that a BlackBerry is a cell phone that uses SMS trickery to allow Web browsing.

Impact: Security features for these devices have not traditionally been strong.

Enterprise Change: Organizations are struggling to develop policy for use and basic enterprise protection.

Early Adopters: Yes (2008)

What has changed this year: Apple made a play to be an enterprise smartphone vendor by offering security features that heretofore have only been available on the BlackBerry.[5] In addition, Apple launched the very popular iPad in 2010.

Many environments, including those of large enterprises, would benefit from using an OS that required that a trusted authority sign and vet every application. This whitelisting approach could be much more effective than the current solution driven by AV programs that seek out bad programs and remove them.

On Oct. 18, 2010, Apple announced its plans to create a Mac App store, similar to the iOS App store, but for Mac OS X desktop applications.[30] Adobe has also introduced the Adobe AIR Marketplace, an app store for programs that work through Adobe's AIR platform.[31] Intel's AppUp is an app store that distributes applications specifically designed for Netbooks running Windows or Moblin.[32] Many Linux distributions, such as Ubuntu and Fedora, already maintain software repositories that maintainers vet; users can access such repositories to install common programs. The app store model is already spreading to desktops, but the security benefit from this model is minor if the OS does not prevent untrusted programs from executing.

Multiple technologies already exist that prevent untrusted programs from running on Windows. Windows 7 includes AppLocker, which allows administrators to configure policies that define applications that will and will not run on protected systems. AppLocker can prevent and allow the execution of programs based on their location on the system, their publisher and file hash. Third-party solutions, such as Bit9 Parity, perform a similar function by restricting executables that do not match characteristics defined by administrators. It is already possible to configure a Windows system that will not run any untrusted programs unless the attacker has exploited a vulnerability in the system.

These whitelisting technologies have yet to gain widespread adoption because they are either too complex to maintain or users view them as overly restrictive. A solution to both of these problems may be to deploy the app store model for traditional operating systems. Smartphone users have already accepted this model for their mobile devices and may be open to using a similar system for their desktop and laptop computers. A user-friendly app store for distributing software that administrators deem acceptable but do not include in default builds is key to gaining user acceptance. The application store model would allow administrators to distribute updates for these programs and keep track of every application in their environments.

The logistics around the app store model on Windows may prove to be complex. Microsoft has faced allegations of monopoly practices in the past; if Microsoft in fact acted as its own vetting authority for all programs running on Windows, courts around the world could rule against the company. Microsoft's dominance in the OS market means that no other player can have a significant impact on worldwide security by implementing the app store model. To implement the app store model in an acceptable way that provides a more secure platform, Microsoft would have to do the following:

Political and Strategic Hacking (APT)

Year: 2012

Concept: Nation-state cyber operations target government and commercial organizations for the purpose of intelligence gathering.

Impact: Intellectual property is seriously at risk.

Enterprise Change: Data loss protection services will become mainstream.

Early Adopters: Yes

What has changed this year: While most government entities have known about this issue for more than a decade, many commercial entities became aware of the seriousness of the issue with Google's very public outing of Operation Aurora.

Application Stores

Year: 2014

Concept: Attempts to provide application verification, such as code signing, are not new; however, "app stores," made popular by the iPhone, are the accepted medium through which to install applications on many mobile devices. Application repositories will become the default method of choosing and installing applications for all automation needs to the home and the business, effectively creating application whitelisting services for the general population.

Impact: The enterprise will have a trusted source to ensure that no malicious software is on an employee's desktop or laptop.

Enterprise Change: The importance of anti-virus technology will diminish.

Early Adopters: No

What has changed this year: There are more than 103 applications stores in existence today.[9]

30 Mac App Store homepage. http://www.apple.com/mac/app-store/. Accessed on Nov. 5, 2010.
31 "Adobe Air Marketplace." Accessed on Nov. 5, 2010. Adobe Systems Inc. http://www.adobe.com/cfusion/marketplace/index.cfm?event=marketplace.home&marketplaceid=1.
32 Intel AppUp. http://www.appup.com/applications/index. Accessed on Nov. 5, 2010.
33 "App Store Report – November 2010: How Many App Stores Is Too Many." Accessed during November 2010. Wireless Industry Partnership. http://www.wipconnector.com/download/WIPAppStoreReport-Nov2010.pdf.

- Provide multiple versions of Windows—one that allows untrusted code to execute and one that does not. Enterprises and users who do not require the freedom to run any application they like should use the trusted-only version. It is important that the trusted-only version does not allow an attacker to easily subvert the requirements via either technical or non-technical (social engineering) means.

- Create a process and the necessary technology that allows for the vetting and creation of app stores. Microsoft cannot be the sole maintainer of app store control; it must transfer its authority to other entities in the same way that trusted root certificates built into Windows must allow others to use secure socket layer (SSL) sessions on the Internet. It is unlikely that Adobe would provide its source code to Microsoft for review and distribution through a Microsoft app store, but Microsoft could allow code from an Adobe app store to execute on Windows through a chain of trust.

The app store model could work differently for home and enterprise users. Home users may get their applications directly from app stores that passed Microsoft's vetting process. Microsoft would add vetted app stores' signing certificates to the list of approved-to-run programs on Windows (see Exhibit 2-2, left). If those app stores began distributing malware, Microsoft could prevent any programs signed by that store after a particular date from running. Additionally, the app store could also revoke the certificate of a particular application if it deemed that application malicious.

In a corporate environment, the information technology (IT) department would act as a gateway between app stores and users (see Exhibit 2-2, right). The gateway would also allow the IT department to control which applications users install and to keep accurate data on precise software versions that systems in the network are running.

Within the next 5-10 years, it is possible that Microsoft will enable the development of desktop app stores that create a more secure computing Windows environment. The primary hurdles preventing this model from succeeding on Windows are not technological but political, as this model restricts freedom in a way that software developers would almost certainly challenge. If Microsoft can implement this model in a way that is acceptable to third-party developers and users, it could have a major impact on computer security as a whole.

SCADA Attacks

Year: 2014

Concept: SCADA systems are man-machine interface devices that allow for the management and monitoring of critical infrastructure such as power and water. The designers of these systems initially designed them to be isolated; therefore, the designers of the protocols did not pay much attention to security. Recently, these systems have become more interconnected with public IP networks to provide easy access for engineers and maintenance crews. The security of these devices is generally not the responsibility of the enterprise security staff. That responsibility generally falls to enterprise infrastructure teams. Patches on SCADA systems require extensive application testing and generally have not been deployed with the same frequency as traditionally deployed software to the desktop.

Impact: As SCADA systems become more and more connected to the Internet, they become more vulnerable to cyber attacks.

Enterprise Change: Traditional enterprise security teams will eventually take over the management of the SCADA space within the enterprise and will demand the same performance from SCADA vendors that they are now getting from enterprise software vendors.
Early Adopters: No

What has changed this year: The Stuxnet worm emerged this year and successfully infiltrated SCADA systems in Iran, China and other countries.[10]

34 Schneier, Bruce. "The Stuxnet Worm." September 2010. Schneier on Security. http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html.

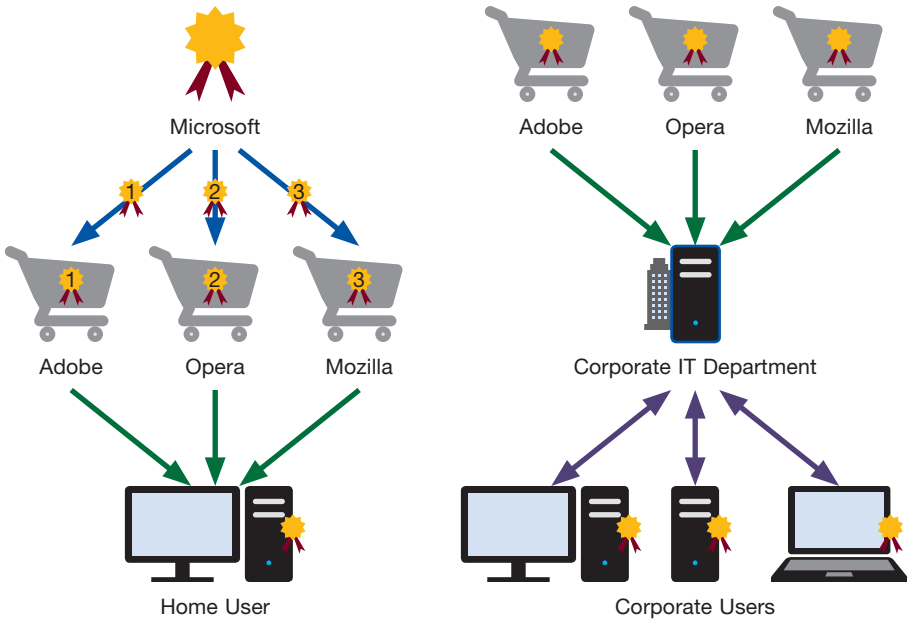


Exhibit 2-2: Home Users Receive Code Directly from Application Stores (Left); Corporate IT Departments Control Application Store Access (Right)

The development of desktop app stores would cause a fundamental shift in the way enterprises protect systems from compromise. AV software would no longer be a necessity, as the malware detection phase would move into the evaluation process before a program enters the app store. Additionally, attackers will need to refocus their efforts, not on creating malware that can evade detection on a host, but in two additional areas. First, attackers may attempt to circumvent the protections put in place by the OS in the same way users jailbreak their mobile devices to remove protections. Subverting security controls typically involves discovering a vulnerability in the OS that allows the attacker to execute his or her code within the context of an already-trusted application and then alter the OS to disable the protection for other applications. The second place attackers may focus their efforts may be in sneaking into app stores while masquerading as a legitimate program. By creating a program that has hidden features that the app store evaluators are unable to detect, attackers can create a traditional Trojan horse and sneak their program onto the system.

2.3 Disruptor: The Vulnerable Cloud

Cloud computing is a new computing model that leverages the Internet to deliver applications, storage and other computing resources on demand. Using cloud computing, an organization is able to purchase exactly the amount of computing power that it needs at any given time, without the overhead of purchasing and managing its own physical servers.

Although many often discuss server virtualization at the same time as cloud computing, server virtualization is an important topic on its own. By completely isolating multiple OS environments on a single server platform,

Developing Nations' Use of the Internet

Year: 2015

Concept: The developed world had to invent malicious cyber activity; the rest of the world can simply adopt it and refine it. This is not an argument that people from the developing world are more likely to become cyber criminals, though in some cultures, they are. Rather, the sheer number of people in meager circumstances who will soon have online access is great enough to cause a serious drain on the world's cyber defense resources.

Impact: Increased volume of malicious cyber activity

Enterprise Change: Shift in the Center of Gravity away from commercial entities and toward governments in terms of volume of money spent on cyber defense and the quantity of compliance laws passed.

Early Adopters: Yes (2009)

What has changed this year: The US government created the US Cyber Command[11] and the UK government classified cyber crime as a tier 1 threat, putting it in the same category as international terrorism.[12] Other countries have moved in similar directions.

35 Page, Lewis. "US Cyber Command becomes fully operational." November 2010. The Register. http://www.theregister.co.uk/2010/11/04/cyber_command_go/.

36 Broersma, Matthew. "Home Secretary Calls Cyber Warfare a Growing Threat." Oct. 18 2010. eWeek Europe. http://www.eweekeurope.co.uk/news/home-secretary-calls-cyber-warfare-a-growing-threat-10689.

organizations are able to cut down on the number of physical servers in datacenters, saving a potentially large sum on electricity and maintenance costs. Adoption of virtualization technology into the datacenter, which started about 5 years ago, has now reached a point where it is entrenched in many environments. Though implementing virtualization brings about a number of savings in management and maintenance, it also brings about several new and complex security considerations.

Cloud computing has become an increasingly important part of the IT landscape and is making inroads into most corporations. The use of virtualization along with cloud computing is one marriage of technologies that reaps in a lot of profit and ease of use for enterprises; however, while there are many tangible benefits to adopting cloud computing as either a supplement or replacement to traditional client-server environments, there are many potential security pitfalls also.

Cloud computing is a disruptor to the current model of doing business because the majority of enterprises currently rely on local hardware and software for most of their needs. The concept of sending data to a cloud for processing or having hardware resources within a cloud is still alien and still sounds like a risky proposition; however, recently, more and more enterprises are moving toward the cloud. This increased movement toward the cloud is in spite of the threats and risks associated with using the cloud. iDefense predicts that a large part of the enterprise community will shift to using the cloud within the next 5 years.

Once the shift to the cloud happens, the whole security industry will be in a state of flux. Security service providers will have to learn to deal with the new attack vectors and threats that the cloud model brings in; employees will have to relearn safe computing habits. On the other side, malicious actors will have to create new malware and delivery mechanisms that can attack the cloud. For a few years, the security community will witness an escalating arms race between security companies and malicious actors.

Given the eventuality in the migration to the cloud, it is interesting and a learning experience to try to foresee what would happen if the cloud model were to collapse. What changes would businesses have to make? What would the economic costs be? Would it even be possible to rapidly move out of the cloud? The next few sections explore the answers to these questions in a post-attack cloud world.

It is an undisputable fact that any new technology faces umpteen numbers of hidden threats. Cloud technology is also susceptible to many unknown threats apart from the threats that can be foreseen. iDefense has written about the various possible threats in iDefense's Topical Research Report "Cloud Computing."[37] For the purposes of this discussion, assume that one or several of the threats mentioned in that paper have occurred and have brought the cloud to its knees.

The cloud being the single point of failure, companies will have to figure out ways to move quickly from one cloud to another. If the cloud vendor itself has

Cyber Terrorism

Year: 2019

Concept: This is the act of engaging in terrorism practices via a cyberspace vector alone that causes fear to the general populace by threatening or creating violence, in some cases instigating significant socio-economic or political disturbances.

Impact: The cyber security community has discussed cyber terrorism for more than a decade. Those discussions have not produced any tangible remedy that is not general in nature and can be applied to other kinds of malicious activity (cyber war, cyber crime, cyber espionage, etc). When the first death occurs as a result of a cyber terrorist attack, the game will change.

Enterprise Change: Enterprises will react to draconian compliance laws, which some governments enacted in an effort to keep their citizens safe.

Early Adopters: No

What has changed this year: Nothing significant

37 iDefense Topical Research Report: Cloud Computing (ID# 485851, May 1, 2009).

a large physical presence, it can also move operations around the globe in an attempt to allay the threat.

If the enterprise were using the cloud as an infrastructure, as in the concept of "infrastructure as a service" (IaaS) hosting place, an attack on the cloud would mean that, internally, the employees of the company would not be able to access the servers (those containing databases, e-mail, etc.), and, externally, the customers will not be able to access the services the servers provide. This is the worst-case scenario for cloud services since an enterprise in such a situation will not be able to move quickly across cloud service vendors or to quickly bring up its own hardware. What will perhaps emerge as a solution to this issue is the use of backup clouds. In such a solution, enterprises can have infrastructure in the cloud as a backup mechanism at a lower cost. Enterprises will likely choose to use a different vendor for the backup cloud.

Closely related to the discussion of failure in IaaS is the issue of failure in the virtualization model of operations. In the event of a threat to virtual machines becoming real, enterprises will have to quickly fall back to using physical machines instead of virtual machines. This reversal will impact the operating cost severely and will require not only great financial inputs to buy the required hardware but also skilled labor to start and maintain the physical systems. Such a disruption has already occurred in a small way in the field of malware analysis. Advanced malware, which can detect virtual machines, have to be executed and observed in a lab that has physical computers instead of virtual machines.

In the event of the failure of cloud services for platform as a service (PaaS), the applications that the enterprise hosts for its employees and for the customers will become inaccessible. It will not be possible to move these applications around quickly since they are tailored for particular platforms. This limitation will result in downtime and economic losses. Maintaining applications in the conventional way (as it is generally done today) on enterprise servers can be a backup strategy, but this strategy would negate the use of the cloud as the platform for applications.

The last cloud service model is the one whereby the enterprise uses the cloud to run software (software as a service, or SaaS). The recovery from the disruption of cloud services that provide software (presumably to employees) is easy. Apart from making a financial investment in buying requisite software for the client machines, the enterprise will have to hire skilled administrators who can have the system running quickly.

Among the new policy measures that enterprises have to consider is the ability to move to another cloud service provider quickly in the event of a disruption of services. Another possible solution is to move to an internal (private) cloud for the duration of the service disruption, but the latter solution would mean that the enterprise maintains an internal cloud all along, which will increase the cost of operation. The last fallback strategy is to maintain a part of the conventional operating process in parallel with using the cloud. It is not necessary for this backup to be capable of taking the full load of services

38 Sinclair, Brendan. "Blizzard Real ID System Sparks Controversy." July 8 2010. Cnet. http://news.cnet.com/8301-17938_105-20010022-1.html.

MMOs and the Metaverse

Year: 2020

Concept: Neal Stephenson coined the term "Metaverse" in his 1992 novel "Snow Crash." In the novel, people interface with the Internet through their personal avatars and autonomous software agents in a three-dimensional space. In the real world, the gaming community has adopted Stephenson's Metaverse blueprint for how to build MMOs such as Second Life and World of Warcraft. Once someone solves the technical problem of how to move an avatar from one MMO to another, the essential characteristics of Stephenson's Metaverse will emerge.

Impact: This will become a completely different way to access the Internet, one that moves away from browsers and toward the use of personal avatars.

Enterprise Change: Robust solutions around identity management will emerge. Global law will change in regard to national sovereignty.

Early Adopters: No

What has changed this year: The hype has gone down, but slow technology advances have occurred. Blizzard Inc. launched RealID,[14] an optional additional layer of identity verification for players in any Blizzard game that allows cross-platform communication across all Blizzard games. Steam Inc. installed a similar communication system with all of its supported games but did not adopt the identity layer.

"Among the new policy measures that enterprises have to consider is the ability to move to another cloud service provider quickly in the event of a disruption of services."

when the cloud fails, but even if it could replace the cloud partially, the enterprise could have some operations running during the disruption.

To sum it up, in the event of a major disruption of cloud services, enterprises must be ready to either move all their operations to another service provider, move to an internal cloud or move back completely to not using the cloud. iDefense foresees that a hybrid approach of an internal cloud and internal infrastructure will emerge as the best fallback mechanism. New services such as backup clouds, which do not currently exist, may also provide new ways of recovering from the disruption of cloud services.

2.4 Disruptors Conclusion

Ten security catalysts—cyber security disruptors—may fundamentally change how the security community protects the enterprise. Some disruptors will occur sooner than others. Indeed, some companies have decided to become early adopters of these changes. Other disruptors may never happen. They are so far down the timeline that other security events, technologies or laws could derail them. Regardless, enterprise security leadership should consider all of these disruptors in their planning process, especially the disruptors within 3 to 5 years. Planning must begin in order for leadership to fully understand the change that is coming and how that might affect the enterprise.