Symantec™
Security Response

Symantec Intelligence Quarterly
July - September, 2011

Introduction

This report discusses notable aspects of malicious activity that Symantec observed from July 1 to September 30, 2011. It also includes a timeline of notable events for the period, as well as a brief article on the state of mobile security.

Symantec has established some of the most comprehensive sources of Internet threat data in the world with the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries and territories monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and third-party data sources.

Symantec also gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, the Symantec distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attack methods.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 40,000 recorded vulnerabilities (spanning more than two decades) affecting more than 105,000 technologies from more than 14,000 vendors. Symantec also facilitates the BugTraq™ mailing list, one of the most popular forums for the disclosure and discussion of vulnerabilities on the Internet, which has approximately 24,000 subscribers who contribute, receive, and discuss vulnerability research on a daily basis.

Contents

Spam and phishing data is captured through a variety of sources including: the Symantec probe network, a system of more than 5 million decoy accounts; MessageLabs™ Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and, other Symantec technologies. Over 8 billion email messages (as well as over 1 billion Web requests) are processed each day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and over 50 million consumers.

These resources give Symantec security analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

This and other Symantec Intelligence quarterly reports are available online at: www.symantec.com/business/threatreport/

An important note about these statistics

The Symantec Global Intelligence Network uses automated systems to map the IP addresses of the attacking systems to identify the country in which they are located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking systems may differ from the location of the attacker.

Highlights

- Symantec observed approximately 155 million unique malicious code threats from July to September, 2011.
- Approximately 1 billion attacks were blocked during this quarter.
- The compromise of a popular e-commerce shopping cart software package affected 6 million websites.
- Noteworthy scams observed during the quarter featured Hurricane Irene, the death of Amy Winehouse, and the potential release of the iPhone 5.

Metrics

Total Unique Malicious Code Threats

Background

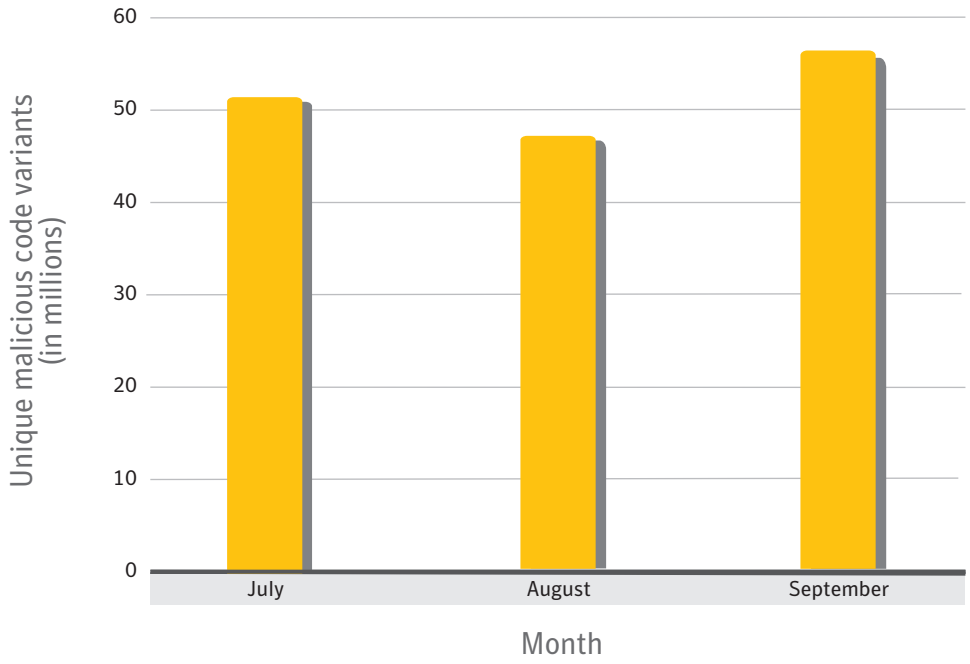
Symantec analyzes unique samples of new and existing malicious code variants to determine which threat types and attack vectors are being used in the most prevalent threats. The number of unique malicious code threats observed in a specific period can provide insight into activity changes in the threat landscape.

Methodology

Symantec assesses the number of unique malicious code threats that are observed during a reporting period. Malicious code threats are made unique from each other when the code is generated using different parameters. The parameters may change depending on the preferences and requirements of the attacker generating them. For example, when an attacker defines which IP address the malicious code should report to after a successful installation, the malicious code will be unique from that which uses a different IP address. There are a multitude of parameters possible, including port numbers, command-and-control (C&C) IPs, activation dates, and specific files to download after installation, to name a few. These numbers are based in part on telemetry data of opt-in participants; therefore, they may not directly reflect the overall number of variants active during the period.

Data

Figure 1
Unique malicious code threats



Observations

By the numbers: Approximately 155 million unique malicious code threats were observed by Symantec this quarter. The month-to-month variations were consistent overall and may indicate steady threat development activity among different sources. This may also suggest that attackers are continuing to use a large pool of consistently effective variants and requiring fewer new variants.

Total Blocked Attacks

Background

Attacks can stem from a variety of sources and may use vastly different techniques. The number of attacks blocked by intrusion detection and prevention technologies deployed on enterprise sensors and customer computers in a specific period can provide insight into the overall levels of attack activity in the threat landscape.

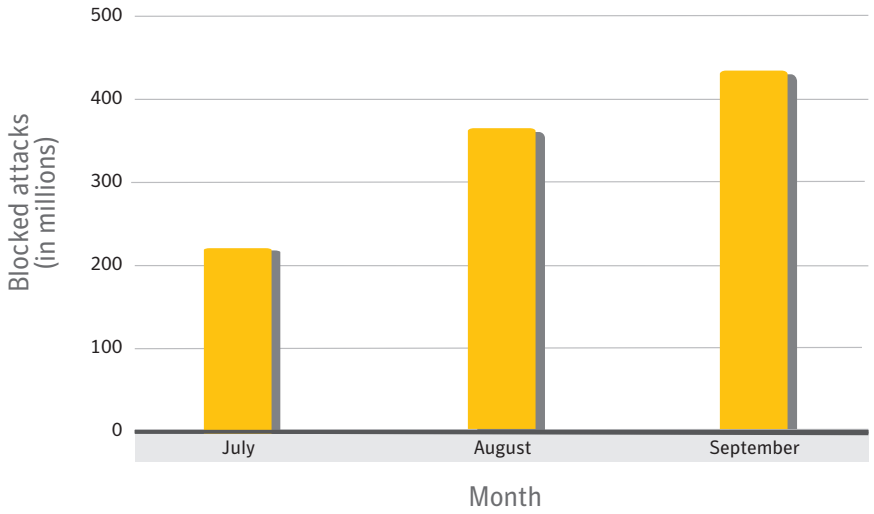
Methodology

Symantec assesses the number of attacks observed during the reporting period. These numbers are based in part on telemetry data of opt-in participants and, therefore, may not directly reflect overall attack activity during the period.

Data

Figure 2

Total Blocked Attacks



Observations

By the numbers: Approximately 1 billion attacks were blocked by Symantec during the third quarter of 2011. The number of attacks increased considerably in August and September. This increase is the result of attacks taking advantage of big events in conjunction with attackers rebuilding their botnets (discussed next).

Rebuilding botnets: Increases in the number of blocked attacks during this quarter and from the previous quarter to this one continue to indicate that attackers are rebuilding their botnet infrastructures. Furthermore, a number of events during the period allowed attackers to expose users to attacks by tricking them into falling for scam messages. These attacks typically involve apparent news of a major event along with a link that leads to a malicious website. Some of the bigger headlines driving the malware scams promised news about Google+, great deals on the pending release of a new iPhone, pictures of the deceased Amy Winehouse, and the release of the last installment in the Harry Potter series.

- Scammers prey on those interested in Google+
- iPhone release used to launch malware
- Spammers exploiting death of Amy Winehouse
- Scams involving the release of the final Harry Potter film

Malicious Activity by Source

Background

Malicious activity usually affects computers that are connected to high-speed broadband Internet because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than other connection types, faster speeds, the potential of constantly connected systems, and typically more stable connections. Symantec categorizes malicious activities as follows:

- **Malicious code**: This includes viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, or compromising the security or integrity of a victim's computer data.
- **Spam zombies**: These are compromised systems that are remotely controlled and used to send large volumes of junk or unsolicited emails. These emails can be used to deliver malicious code and phishing attempts.
- **Phishing hosts**: A phishing host is a computer that provides website services for the purpose of attempting

to illegally gather sensitive, personal and financial information while pretending that the request is from a trusted, well-known organization. These websites are designed to mimic the sites of legitimate businesses.

- **Bot-infected computers**: These are compromised computers that are being controlled remotely by attackers. Typically, the remote attacker controls a large number of compromised computers over a single, reliable channel in a bot network (botnet), which is then used to launch coordinated attacks.
- **Network attack origins**: This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- **Web-based attack origins**: These are sources of attacks that are delivered via the Web or through HTTP on other systems. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Methodology

This metric assesses the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, including malicious code reports, spam zombies, phishing hosts, bot-infected computers, and network and Web-based attack origins.

The proportion of each activity originating in each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question and the rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Data

Figure 3

Malicious activity by source, overall

Source	Rank	Percentage
United States	1	22%
China	2	11%
India	3	7%
Brazil	4	5%
Taiwan	5	4%
Russia	6	3%
Germany	7	3%
Italy	8	3%
Vietnam	9	2%
United Kingdom	10	2%

Figure 4

Malicious code by source

Source	Rank	Percentage
India	1	18%
United States	2	12%
Indonesia	3	7%
China	4	6%
Vietnam	5	4%
Egypt	6	3%
Japan	7	3%
Brazil	8	3%
United Kingdom	9	3%
Bangladesh	10	3%

Figure 5
Spam zombies by source

Source	Rank	Percentage
India	1	16%
Brazil	2	10%
Russia	3	9%
Vietnam	4	8%
Pakistan	5	5%
Ukraine	6	5%
Indonesia	7	4%
Taiwan	8	3%
Romania	9	3%
Belarus	10	2%

Figure 6
Phishing hosts by source

Source	Rank	Percentage
United States	1	51%
Germany	2	7%
United Kingdom	3	4%
Canada	4	3%
China	5	3%
Russia	6	3%
Brazil	7	3%
France	8	3%
Netherlands	9	2%
Spain	10	2%

Figure 7
Bots by source

Source	Rank	Percentage
Taiwan	1	17%
Brazil	2	12%
United States	3	11%
Italy	4	9%
China	5	8%
Hungary	6	7%
Poland	7	6%
Germany	8	5%
Japan	9	5%
Argentina	10	3%

Figure 8

Network attack origins by source

Source	Rank	Percentage
China	1	38%
United States	2	13%
Russia	3	4%
Brazil	4	3%
India	5	3%
Italy	6	3%
United Kingdom	7	2%
Taiwan	8	2%
Canada	9	2%
Japan	10	2%

Figure 9

Web-based attack origins by source

Source	Rank	Percentage
United States	1	45%
China	2	13%
South Korea	3	6%
Germany	4	4%
United Kingdom	5	3%
Japan	6	3%
Netherlands	7	2%
Russia	8	2%
France	9	2%
Canada	10	1%

Observations

E-commerce hit hard: Sharing information and shopping are two of the most popular uses of the Web and when both are used in attacks they can be very effective. During the third quarter of 2011, a popular shopping cart software package was widely infected by attack kits in the United States. This new attack activity helped maintain the prominence of the United States in Web attack activity during the period.

- Willysy malware infects millions of e-commerce sites
- Is that a virus in your shopping cart?

Big hurricane means big phishing opportunity: Scammers bent on stealing information for profit tend to exploit major global or regional events. Hurricane Irene was a big opportunity, as attackers took advantage of peoples' desire to help others in need by offering fake donation scams. With the coast of the United States under threat, it was viable opportunity that helped the United States remain a major source of phishing hosts.

- DHS warns that Irene could prompt phishing scams

Smartphones and smart scams: Although Apple did not officially announce the iPhone 4S until the fourth quarter of 2011, there was rampant speculation about the device months prior to any official statements, with fans expecting it to be iPhone 5. During the third quarter of 2011, scammers exploited the growing hype surrounding the anticipated release of the iPhone 5 with promises of being able to win or test the new device in order to entice potential victims into providing sensitive information.

- Read more about scams involving the anticipation of iPhone 5

Web-based Attack Prevalence

Background

The circumstances and implications of Web-based attacks vary widely. They may have specific targets or they may be widespread attacks of opportunity that exploit current events, zero-day vulnerabilities, or recent vulnerabilities against which some users are not yet protected. While some major attacks garner significant attention, examining Web-based attacks overall provides insight into the threat landscape and how attack patterns may be shifting. Moreover, analysis of the underlying trend can provide insight into potential shifts in Web-based attack usage and can help determine the likelihood of Web-based attacks increasing in the future.

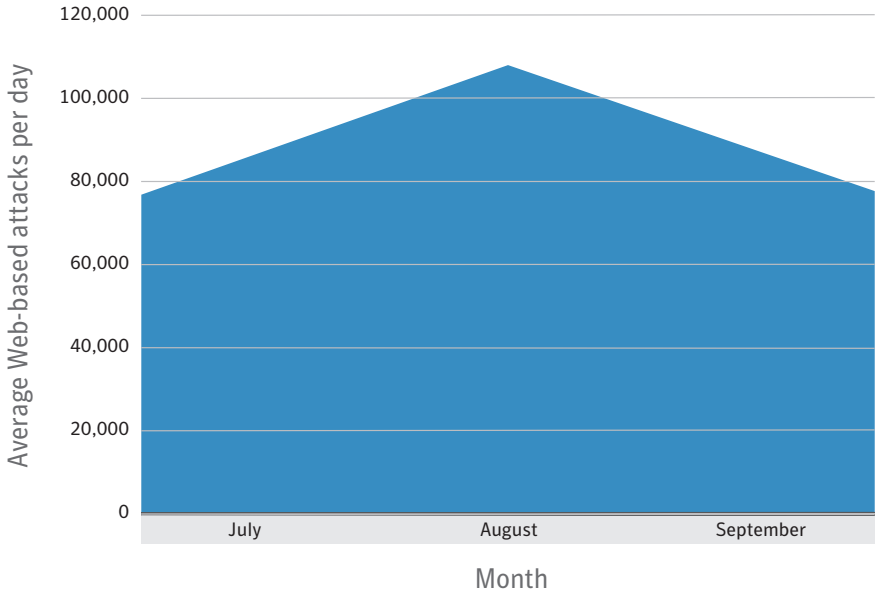
Methodology

This metric assesses changes to the prevalence of Web-based attack activity by comparing the average number of attacks per day in each month. The averages are based on telemetry data of opt-in participants and, therefore, may not be directly synonymous with overall activity levels or fluctuations that occurred as a whole. However, underlying trends observed in the sample data provide a reasonable representation of overall activity trends.

Data

Figure 10

Web-based attack prevalence



Observations

The browser is still the best way in: Attackers are still focused primarily on the Web as the best way to break into computers. With the amount of information shared through HTTP from so many hosts and sites that have dynamic content such as social networks it is very difficult for organizations to properly secure Web traffic. It is because of this that the prominence of Web attacks remained fairly constant throughout the third quarter of 2011.

Shopping cart parasites: A very popular shopping cart software package was exploited by attackers in August to carry out attacks against would-be online shoppers. Six million websites running older versions of the software were infected, which added substantially to the attack landscape during August and to the quarter over all.

- Willysy malware infects millions of e-commerce sites
- Is that a virus in your shopping cart?

Top Malicious Code Samples

Background

Symantec analyzes new and existing malicious code samples to determine which threat types and attack vectors are being employed in the most prevalent threats. This information also allows administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

Methodology

This metric assesses the top malicious code samples detected in the current reporting quarter. To determine this, Symantec ranks each malicious code sample based on the volume of potential infections reported during the period. The top 10 malicious code samples are analyzed for this metric.

Data

Figure 11

Top malicious code samples

Rank	Name	Virus	Worm	Backdoor	Trojan	Propagation Mechanisms	Impacts/Features
1	Sality.AE	•	•			Removable drives/executables	Removes security applications and services and downloads files from remote addresses
2	Ramnit	•	•			Removable drives/executables	Infects executable files
3	Bamital				•	N/A	Modifies Internet search results to include advertisement URLs
4	Ramnit.B	•	•	•		Removable drives/executables/ remote vulnerability	Infects executable files and allows remote access
5	Downadup.B		•	•		P2P/CIFS/remote vulnerability	Disables security applications and Windows Update, downloads and installs additional threats
6	SillyFDC.BDP		•			CIFS/removable drives/remote vulnerability	Downloads additional threats and sends fake DHCP packets to hijack DNS configurations
7	Virut.CF	•		•		Executables	Downloads additional threats, infects executables and allows remote access
8	Almanahe.B	•	•			CIFS/mapped drives/removable drives/executables	Infects executable files, ends security related processes and installs additional threats
9	Mabezat.B	•	•			SMTP/CIFS/removable drives	Encrypts and infects files
10	Virut	•		•		CIFS/mapped drives/removable drives/executables	Downloads additional threats, infects executables and allows remote access

Observations

Steady as she goes: The top malicious code samples for this quarter remain consistent with previous quarters and their continued shifting in rankings with each other is a testament to their comparable proliferation.

First discovered in November 2010, Ramnit.B is functionally similar to its predecessor. Ramnit.B, though, has extended its ability to propagate by exploiting the same vulnerability that was exploited by Stuxnet—the "Microsoft Windows shortcut 'LNK/PIF' files automatic file execution vulnerability." Ramnit.B also installs a backdoor on compromised computers, allowing remote access for attackers.

- Read more about Ramnit
- Read more about Ramnit.B
- Read more about Sality.AE
- Anatomy of Bamital: a prevalent click-fraud Trojan

The SillyFDC.BDP worm: SillyFDC.BDP was detected in March 2011 and has quickly become one of the top 10 reported samples, rising up to sixth rank this quarter—up from eighth previously.

While able to propagate similar to other SillyFDC variants by copying itself to removable drives, SillyFDC.BDP can also copy itself to network shares. As with Ramnit.B, it also exploits the "Microsoft Windows shortcut 'LNK/PIF' files automatic file execution vulnerability." It also exploits the "Microsoft Windows Server service RPC handling remote code execution vulnerability."

Once installed on a compromised computer, the worm will download and install additional threats. One of the threats is known to be the Tidserv worm, which subsequently sets up a backdoor. SillyFDC.BDP also sets up its own DHCP server and hijacks the DNS configurations of computers on the same network that attempt to renew their IP addresses.

- Read more about SillyFDC
- Read more about SillyFDC.BDP
- Read more about Tidserv
- Microsoft Windows shortcut 'LNK/PIF' files automatic file execution vulnerability
- Microsoft Windows Server service RPC handling remote code execution vulnerability

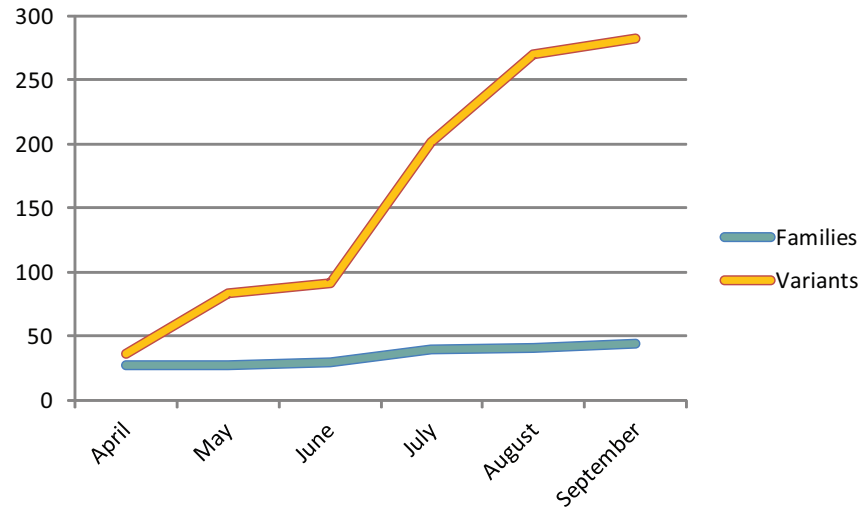
Article

The State of Mobile Threats

The increased use of smartphones as well as the rising use of tablet devices has lead to speculation about how malicious code and cybercriminal activity will affect these devices and their users. The integration of smartphones and tablets into both personal and business life is quickly rising and, therefore, presents a much larger pool of potential victims for cybercriminals to target. As such, the general hype about mobile malicious code gives the impression that there will be a massive wave of new threats. Symantec has observed an increasing number of threats targeting mobile devices (figure 13) – with the Android platform being particularly targeted. Although rising significantly, the overall number is still dwarfed by number of PC based threats in common circulation. This is likely due, in part, to the many additional hurdles that cybercriminals are faced with when targeting mobile devices as opposed to traditional computers.

Figure 12

Increases to known mobile malicious code



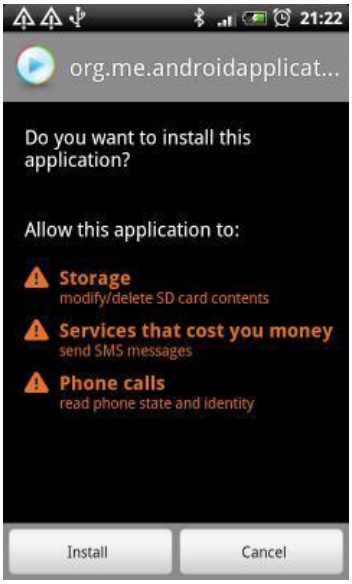
As discussed in the Symantec whitepaper, *A Window into Mobile Device Security*, released in June 2011, smartphone platforms have been designed from the ground up to be more secure than traditional computers. While the integrated security features alone present a challenge for malicious code writers, another challenge is that the pace at which these platforms are changing is faster than that of traditional computers. The platform changes can be significant enough that malicious code family works only for a small subset of a particular mobile operating system. Thus malicious code will potentially require additional development to run effectively across multiple versions of an OS.

Mobile devices are built on rapidly evolving hardware, resulting in myriad differences between devices. Some hardware may be unique to a small group of devices or even a single device. Because of this, changes to the OS are often necessary to accommodate the unique hardware in specific devices. In turn, this can hinder the effectiveness of malware across device types and versions for malicious code developers. The additional effort required by a malicious code author to have code run effectively across these different variants on multiple devices may not be worth his or her time, monetarily.

The most recent *Symantec Internet Security Threat Report* suggested that the move to mobile threats by cybercriminals was hindered by lack of opportunities to profit from the attacks. It is reasonable to assume that as more opportunities for profitable criminal activity emerge on mobile devices, more effort will be put towards mobile threat development. This is already starting to unfold with mobile malicious code that is linked to high profile banking Trojans, Zeus, and SpyEye. When installed on a user's computer, these Trojans may attempt to install malicious code on the user's mobile device as well. Some financial institutions have begun to implement

online authentication procedures that require the entry of one-time passcodes, sent to the customer via SMS. When customers log into their accounts, they receive an SMS and enter the one-time passcode to complete the authentication process. By installing malicious code on victim mobile devices, banking Trojans can intercept SMS passcodes and gain unauthorized access to a customer's account.

Figure 13
FakePlayer install prompt



Criminals are also profiting from mobile malicious code with threats—such as FakePlayer, Geinimi and Pjapps for the Android OS—that send SMS messages and long distance calls to premium services that charge the victim a hefty fee (figure 14). Other tactics include locking the screen and displaying messages that demand that victims send money to the attacker in order to have their screens unlocked, as was seen in 2009 with the iKee.B worm that affects iOS (figure 15).

The monetization schemes behind these and other profit-based threats, such as the pay-per-click Bgserv Trojan, are detailed in the Symantec whitepaper, *Motivations of Recent Android Malware*, in which several potentially effective strategies are explored. While some are unique to mobile devices, such as the GPS location tracking abilities of the Tapsnake threat, most are mobile versions of strategies employed against traditional computers, such as adware installation and black hat search engine optimization. Despite their potential harm, none of these threats appear to have proven profitable enough to justify other attackers from copying the threats or creating direct competition.

The existing examples of profit driven mobile malicious code suggest that the speed at which new malware is being developed seems to be slower than commonly anticipated. Until such a time when the return on investment for targeting traditional computers becomes less profitable than it does for mobile devices, many cybercriminals may continue to focus their efforts on what is already working for them—traditional computers. This will likely change as mobile banking apps become more commonplace or if a significant number of users begin to use mobile devices exclusively, abandoning the traditional computer entirely.

Figure 14
Ikee.B scam message

The future adoption of near-field payment technology will also play a role in where cybercriminals focus their efforts. Near-field payment technology allows customers to wave a chipped object or device (such as a smartphone) within a close vicinity of a payment scanner to complete a monetary transaction. As mobile devices become an accepted replacement for transactions that currently scan debit and credit cards, malicious code that exports related information will emerge. The ability to intercept sensitive information could allow cybercriminals to load that information onto their own device and use it to buy things at the victim's expense.

At present, mobile malicious code appears to be in an exploratory phase where a small number of ambitious authors are testing the viability of their wares. Even for high-profile threats such as Zeus and SpyEye, the introduction of mobile code serves only to increase the effectiveness of their traditional functionality. The landscape is beginning to change as mobile technology grows, but traditional computers remain more attractive targets…for the time being.

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Credits

Eric Johnson, Editor
Security Technology and Response

Téo Adams, Threat Analyst
Security Technology and Response

Joseph Blackbird, Threat Analyst
Security Technology and Response

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com