

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or control room environment.

1Q 2011 Crimeware Report

Trend Micro, Incorporated 

TrendLabsSM

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

A Trend Micro Quarterly Report | 1Q 2011

1Q 2011 CRIMEWARE REPORT

Continuous technological advancements have made the Internet the preferred platform to quickly and easily conduct all kinds of transaction. Banks and other financial institutions are aware of and are taking advantage of these by creating more robust online services to reach out to and to better serve their clients' needs.

The convenience and ease of using the Internet as a service platform, however, also entails certain security risks. In fact, information theft and the conduct of unauthorized online banking transactions are just two of the security issues that organizations have to deal with on a regular basis. In line with this, we at Trend Micro have decided to compile our findings on the latest threats targeting the financial industry.

• The convenience and ease of using the Internet as a service platform entails certain security risks.

In the first quarter of 2011, we discovered that established banks such as HSBC Holdings Plc; the Australia and New Zealand Banking Group Limited (ANZ); Lloyds TSB Bank Plc; Banco Santander, S.A.; and Western Union Bank made it to the top 10 list of cybercrime targets—for both email phishing and site-spoofing attacks.

Rank	Organization
1	PayPal
2	eBay
3	Yahoo!
4	Facebook
5	Pharmacy Express
6	HSBC
7	ANZ
8	Lloyds TSB Bank
9	Banco Santander
10	Western Union Bank

Table 1. Top 10 cybercrime targets in 1Q 2011

Notable Incidents

ZeuS Updates

ZBOT malware, Trend Micro's detection for ZeuS variants, **are notorious for stealing user information**, particularly victims' online banking login credentials. Since it first reared its ugly head, ZeuS remains a significant threat even in the current landscape. This quarter alone, Trend Micro detected several ZBOT system infections led by the 10 variants in the table below.

Rank	Variant
1	TSPY_ZBOT.SMG
2	PE_ZBOT.A
3	TSPY_ZBOT.SMOI
4	TSPY_ZBOT.SMAM
5	TSPY_ZBOT.SMGS
6	TSPY_ZBOT.SMDM
7	TSPY_ZBOT.SMEQ
8	TSPY_ZBOT.SMB
9	TSPY_ZBOT.SMO
10	TSPY_ZBOT.SMHA

Table 2. Top 10 ZBOT variants in 1Q 2011 based on Trend Micro™ Smart Protection Network™ data

ZeuS-SpyEye Merger

Security experts have been continuously monitoring developments with regard to the ZeuS-SpyEye merger. In line with this, TrendLabsSM engineers got hold of and analyzed what seemed to be a product of the said merger—the **beta version of the SpyEye Builder 1.3.05 toolkit**. This toolkit allows the use of encryption keys, among other features.

A month after our security researchers found the merged toolkit version, they came across an updated version in the **SpyEye Builder 1.3.X toolkit**. This update came with three control panels in order to accommodate ZeuS and SpyEye's varying control panels.



Figure 1. SpyEye Builder 1.3.05

Improved ZeuS Builds

Apart from its recent merger with SpyEye, TrendLabs engineers also found nastier ZBOT variants created with new and improved ZeuS toolkit versions in the wild. These include the following:

- One such variant, a *Symbian* malware detected as **SYMBOS_ZBOT.B**, has the ability to **bypass the two-factor authentication measures** banks commonly use to protect their clients. To do so, the malware monitors an affected user's text messages and forwards relevant ones to a remote user. This allows cybercriminals to get hold of the authentication codes banks send to users. Obtaining these codes allows the cybercriminals to access and steal from affected users' bank accounts.
- TrendLabs engineers also targeted organizations that relied on Automated Clearing House (ACH) systems. Spammed messages urged recipients to click a link to a site in order to obtain more details regarding a supposed rejected transaction. To obtain the promised information, however, the users were prompted to download a *Java* update, which was actually an exploit kit detected as **PE_LICAT.SM-O**. The malware then infects .EXE files currently running on affected systems, turning these into **PE_LICAT.SM**, which were designed to randomly generate and access certain domains in order to download more malware.

In a similar attack, a link embedded in spammed messages led users to a site that hosted **TSPY_ZBOT.GBX**.

- As if attacking user systems was not enough, ZeuS also **began targeting more mobile phone users** with a data-stealing Trojan detected as **BBOS_ZITMO.B**. This Trojan remains hidden, as it does not make use of a graphical user interface (GUI) and is not listed as an app. Once installed, it sends a confirmation message to the attacker that the device is ready to receive commands. To evade removal, it allows the attacker to remotely alter an infected device's administrator number. This way, even if the original administrator number becomes unavailable, the attacker can simply send a command to change the number so the device can continue to receive the commands he sends.



Figure 2. SMS sent to the bot master

- TrendLabs engineers also found a ZeuS 2.0 variant dubbed version 2.0.8.9 still being peddled in online forums. What was notable about this toolkit was the presence of a so-called *Ghost Panel*, which allowed cybercriminals to choose what user information variants created with it should save in their database via the use of *No-Sh*t Reports*. This feature thus filtered out nonfinancial-related information such as users' social networking site credentials from the stolen data.

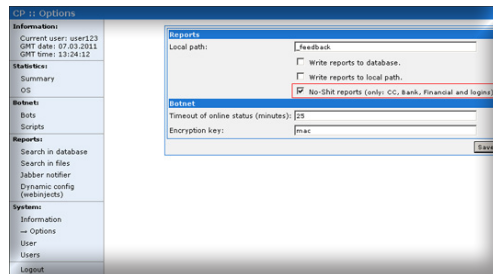


Figure 3. Ghost Panel feature that allowed the creation of No-Sh*t Reports

Other Noteworthy Crimeware

ZeuS was not the only threat banks and other financial institutions faced this quarter. A third-generation QAKBOT worm as well as the Tatanga and other banking Trojans also reared their ugly heads in the past three months.

Third-Generation QAKBOT Variant

Even though QAKBOT does not have the same level of notoriety as fellow banking Trojans ZeuS and SpyEye, it still manages to inflict considerable damage to the companies it affects. Like ZeuS, however, QAKBOT also recently underwent a “face-lift” with the release of a third-generation variant into the wild. This variant was notable in that it had enhanced propagation methods.

Session-Hijacking Trojans

This quarter, TrendLabs engineers came across two notable session hijackers in the form of the Tatanga Trojan aka TSPY_PINCAV.GEK and of TSPY_ODDJOB.SMA. Session hijacking or the unauthorized exploitation of a system session to gain access to confidential information is now often employed by cybercriminals targeting online banking and other financial sites.

The Tatanga Trojan is capable of gathering all sorts of Web tracking logs, including passwords, which it then sends it to a malicious remote user. TSPY_ODDJOB.SMA, on the other hand, hijacks online sessions by keeping these open even after their legitimate owners have already logged off.

Stealing via Malicious Apps

Spamming users and tricking them into downloading Trojan spyware onto their systems and hijacking sessions seem to be no longer enough for cybercriminals. Trend Micro senior threat researcher Ranieri Romera recently came across an application that claimed to be capable of checking Brazilians' credit scores and criminal records. Upon further analysis, however, the said application not only did what it said it would. It also downloads a BANCOS Trojan detected as **TROJ_BANKER.LEB** onto the user's system in the background. This Trojan downloads another malware onto the infected systems and steals Brazilians' social security numbers. Even though this application currently only targets Brazilians, other cybercriminals may use the same concept to target users in other parts of the world.

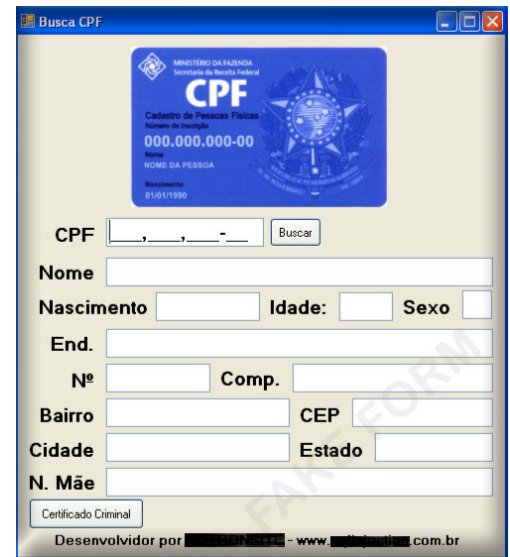


Figure 4. Malicious application's main window

Routine Developments

As security measures constantly improve, so do cybercriminals come up with more ingenious tricks of their own. They create new features and augment the specifications of already-existing threats to continue profiting from the online transactions users conduct. The following are noteworthy routine developments in the previously discussed threats:

- **ZeuS-SpyEye merger.** The ZeuS-SpyEye merger gave birth to a stealthier and more resilient toolkit. After careful analysis, Trend Micro researchers surmised that SpyEye author Gribodemon may have received help from other cybercriminals to polish the toolkit. The most notable changes to this version were the addition of the *cc grabber* plug-in and of the *Anti-Rapport* option. The *cc grabber* plug-in collects credit card numbers by analyzing a user's POST requests and checking these against the **Luhn algorithm**. The *Anti-Rapport* option, on the other hand, helps cybercriminals evade Rapport Trusteer software, which provides Web access service security.



Figure 5. SpyEye Builder with cc grabber plug-in

Apart from the previously mentioned enhancements, the merged toolkit also had the *customconnector* plug-in, which tells the bot what command-and-control (C&C) server to communicate with, most probably for backup purposes. In previous versions, this was only part of a file named *maincps.txt* in the configuration file.

Obtaining a copy of the merged toolkit also differed in that buyers first got an email message with a set of instructions, the author's own version of two-factor authentication. The email message required the buyer to send the nickname and email address that he will use for the purchase via *Jabber*. Only after this will the SpyEye creator send the buyer a message that contains the download links.

- **Pseudorandom domain generation algorithm (DGA) routine.**

Zeus variants also underwent an upgrade in the form of LICAT. Apart from plain information theft, Zeus variants now come with the ability to **pseudorandomly generate domains** from which to download updates. This makes it harder for security experts to take their C&C servers down.

- **Bypassing two-factor authentication systems.**

Zeus variants have recently taken to attacking mobile devices as well in the form of SYMBOS_ZBOT.B. Even though this behaved quite like its predecessor **SYMBOS_ZBOT.A**, it climbed up a notch, as it is capable of bypassing banks' two-factor authentication measures. This made cybercriminals' task of directly stealing money from their victims a lot easier in that they only had to intercept relevant messages to obtain the users' authentication codes.

- **Hijacking user sessions.** Two of the banking Trojans featured in this report are capable of hijacking users' sessions. If in the past, banking Trojans only logged keystrokes and captured screenshots while users logged in to their online banking accounts, today's variants now actually hijack entire sessions. This enables cybercriminals to continue accessing their victims' accounts even after the legitimate owners have already logged out, allowing them to directly siphon money off their accounts to money mules.



What's to Come?

To keep up with the security enhancements banks and financial institutions implement as well as with technological advancements, cybercriminals constantly improve their tools and tactics to continue profiting from malicious schemes.

The following describe what our analysts and researchers think the financial industry threat landscape will be like in the near future.

Bypassing Two-Factor Authentication Measures and Targeting Mobile Devices

The increasing use of mobile devices will bring about a shift in the current threat landscape. Trend Micro threat analyst Patrick Estavillo believes that cybercriminals will increasingly target mobile device users, especially since these are still insufficiently protected at present. As such, bypassing two-factor authentication measures via exploiting vulnerabilities is set to become a norm. The fact that the majority of mobile online banking users still lack awareness of the threats this poses is only likely to bring about more risks.

The Future of Banking Trojans

Trend Micro senior threat researcher Kevin Stevens does not believe ZeuS will undergo further enhancements apart from the most recent addition of DGA capability in ZeuS-LICAT variants and from its recent merger with fellow data-stealing Trojan toolkit SpyEye.

It is interesting to note, however, that pieces of ZeuS' source code have been made public. Stevens believes that in the next few weeks, 80–100 percent of the source code will be leaked, enabling just about anyone to get his own copy. If this happens, there may be some advances in ZeuS variants, including LICAT and ZeuS-SpyEye. Even though he is not 100 percent sure if the LICAT part of the code is also floating around, we may still see other malware rip this, which may stir some major issues with regard to tracking C&C servers.



Although the Tatanga banking Trojan's capability to capture videos of users' sessions is indeed unique, Stevens believes it is not very useful, as it takes up precious hard drive space. He also predicted the increasing use of session hijacking among malware in the future.

No matter how crafty cybercriminals become, however, Trend Micro will continue to protect its customers with the help of the Smart Protection Network.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651

Phone: 1 +408.257.1500

Fax: 1 +408.257.2003

www.trendmicro.com

