

# Q3 ROUNDUP 2005

There was a wave of seven alert malware last quarter, four MYTOB variants, a SOBER worm, a WURMARK worm, and the BOBAX worm. For this quarter, there are two. Most notably, the two alert malware, WORM\_ZOTOB.D and WORM\_RBOT.CBQ (later renamed to WORM\_ZOTOB.E) both exploit the Windows Plug and Play vulnerability, MS05-039. The evil genius behind the said attacks is a certain Farid Essebar, an 18-year-old Moroccan hacker who goes by the name, Diab10. His codename definitely rings a bell, because he was also believed to be among the masterminds behind the first WORM\_MYTOB variants. Consequently, he and his cohort Coder (Atilla Ekici, aged 21) were arrested two weeks after the outbreak. It's definitely kudos to the cyber cavalry for the very quick response.

## New Notables

### Worm Drops a Dropper of its Dropper

It is neither a practical joke, nor mere wordplay. It was first observed with WORM\_BOBAX.P, which came with a Trojan component, TROJ\_SMALL.AHE, which it sends out via email as an attachment. The said Trojan then downloads a copy of the said worm. This quarter's WORM\_BAGLE.DA takes it a step further, with two Trojan components. WORM\_BAGLE.DA mass-mails TROJ\_BAGLE.DA. Following this initial line of thought, the Trojan component should be downloading a copy of the worm, but alas no, instead it downloads yet another Trojan, TROJ\_DLOADER.ACT. The last Trojan is finally the one that downloads the worm. Since then, a MYTOB variant has again used the worm-dropper tandem: WORM\_MYTOB.KM and TROJ\_DROPPER.LV.

The cycle of doom (first introduced by WORM\_BOBAX.P) has just been brought to a new level. Antivirus and security companies can only brace for what will come next.

Another trend that's frequently being used these days is that lately, instead of directly attaching the malware file on spammed email messages, malware authors instead incorporate a link in the message body.

"This technique can bypass the filters used by enterprise companies in their email

scanning systems or applications that scan or block malicious or even suspicious attachments," said Ivan Macalintal, Trend Micro's Senior Threat Analyst. The logic is simple yet effective—if the attachment can be blocked, then do not include one—a link will suffice. This technique drops the burden back to the user, since mechanical intervention (read: attachment blocking) is not an option anymore. To malware authors, it's back to banking on trust and gullibility, whichever is more convenient.

"A savvy and novel social engineering trick would then complete the intention of the malware authors – to entice users to click on the malicious link included in the mail message body, and BOOM! The user becomes a part of the downloader1-downloads-downloader2-downloads-worm-because-the-user-clicked-on-the-link cycle," Macalintal notes.

Jamz Yaneza, Senior Antivirus Consultant at Trend Micro believes that this new technique brings "URL blocking" features to the fore, as malware coders, spammers, and phishers use the said technique to propagate their malicious creations. "Hope looms on the horizon as many technologies, used in newer antivirus solutions and as browser plugins, start to incorporate validation of links prior to allowing users to proceed," Yaneza said.

## Roaming Malware: From Your Phone to Your PC

Next generation phones provide not only communication functions, but complex computing functions as well. From taking snapshots to capturing audio and video, from short memos to documents, a mobile phone is almost like a handheld PC. And like a PC, with nearly the same functions, it also inherits the vulnerability for malicious attack. The advent of wireless technologies including Bluetooth and high-speed WiFi from 3G networks made anonymous and wireless connection possible. It also provided another medium for malware to propagate. The first SYMBOS variants modified an affected phone's logos and icons and still others dropped malware.

And then came SYMBOS\_CARDTRP. Taking advantage of mobile phones' nifty storage capability, this mobile malware drops PC malware into an affected phone's memory card. If that's confusing, then think: this malware not only affects your phone, it's also a medium for malware to infiltrate your PC. Not only that, it also renders several phone applications unusable. So far, CARDTRP drops WORM\_WUKILL.B and BKDR\_BERBEW.A.

Suddenly, the definition of a "blended threat" evolved. "Previously, we had come to define an example of a 'blended threat' as a Windows worm that either spreads via multiple propagation vectors such as email, IM, network shares and application vulnerabilities, and/or a worm that has capabilities of other malwares such as file-infectors, backdoor Trojans or even spyware," Macalintal explains. With the coming of the SYMBOS\_CARDTRP variants, another dimension can be added to how people see a blended threat - A mobile malware that has the capability to affect Windows desktop platforms!

Macalintal believes the blended-threat feature may also have come with a calculated social-engineering goal targeting affected users of a keener sense of antivirus knowledge. These people have a higher

tendency to attempt to remove the virus at the first sign of infection, or even at the slightest hint of suspicious activity.

Basically, when the user suspects possible infection in his or her mobile phone memory card, most probably the course of action taken is to insert the "possibly infected" memory card into the PC for disinfection.

And the moment the memory card is inserted to the PC (supposing it was CARDTRP, and not merely another member of the popular CABIR family), then wham! Another victim of the new PC-infecting SYMBIAN malware.

"Memory cards in various forms including MMC, SD, and CF are new touted mobile storage solutions providing easy means of transferring data across initially incompatible devices," added Yaneza.

"How can he know that there wasn't only CABIR, but an altogether new strain of a blasted Symbian-PC-infecting bug?!" said Macalintal, pondering on the technique. "Even now, there may be a user out there who hasn't got a single inkling where he got a WORM\_WUKILL.B or BKDR\_BERBEW.A infection!" he added.

What if the affected memory card is inserted to a PC that is part of a large corporate environment? The threat becomes multiplied. Needless to say, antivirus companies must then continue to reinforce stricter guidelines and educate users on more safety measures in preventing and mitigating these security threats.

Mobile threats, similar to PC threats continue to evolve parallel with each other. The threats increase both in number and in technique as more and more devices gain the capabilities of the computer. "It is highly probable that we will see more threats similar to this - but ones that will be utilizing more effective distribution and social-engineering techniques, therefore carrying a higher potential for vast infections. Ergo, let the battle-cry linger on - Let's continue to be vigilant..." Ivan Macalintal concludes.

## Malware Detections

This quarter's malware detections follow the trend established by last months' recent spikes. With only the first quarter as an exception – as malware detections during the said period in 2004 and 2005 meet at nearly the same amount of 1300 – Q2 and Q3 from 2004 to 2005 doubled in total malware detections. Last years Q3 count was at 2675, and this year's number almost hit 5000, with 4716.

The rise, however, from the previous quarter is a mere 648, coming off Q2's 4068 malware detections. The spike came earlier with the transition from Q1 to Q2, when malware detection count leaped by nearly 3000. From the current figures, the number has stabilized for the moment. It is still quite notable that the previous year followed a more sedate pace early on, rather than this year's spike right on the first quarter.

Figure 1.2 shows how the numbers are divided in terms of malware type. While the inclusion of Trojan spyware to Q1 and Q2 (551 and 842 respectively) may also add to the mentioned spike earlier, it can also be noticed that the worm count also doubled on its own. Trojans made a leap last quarter, coming off 403 to 1514. Its figures dropped for this quarter but the influx of worms, Trojan spyware, and a remarkably high "others," still managed to give this quarter a steady albeit considerably lower rise.

## Infection Counts

As with the data previously presented, infection counts remain consistent with the high rise. This time the jump was from last quarter to the present, with almost 120% rise. The quarter has only seen two alerts, very meager compared to last quarters seven yellow alerts. These alerts were courtesy of two worms exploiting the Windows Plug and Play vulnerability, but both alerts caused a jump of millions in infections counts. The fact that these two alerts were almost zero-day outbreaks led to this jump.

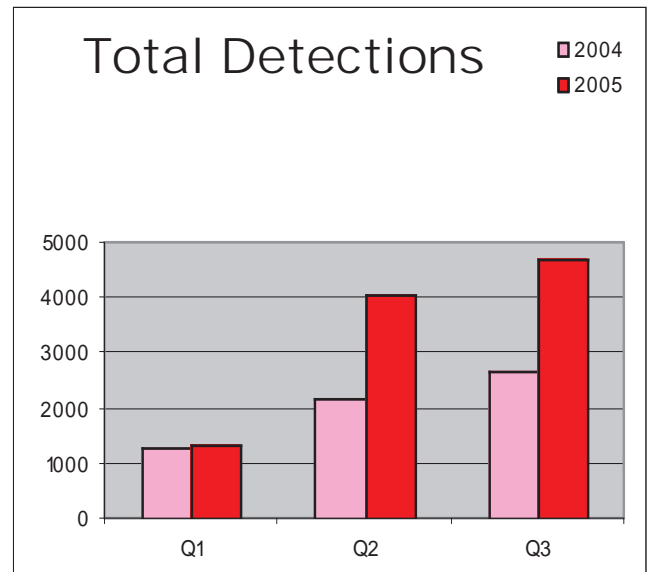


Figure 1.1 Quarterly Malware Detections

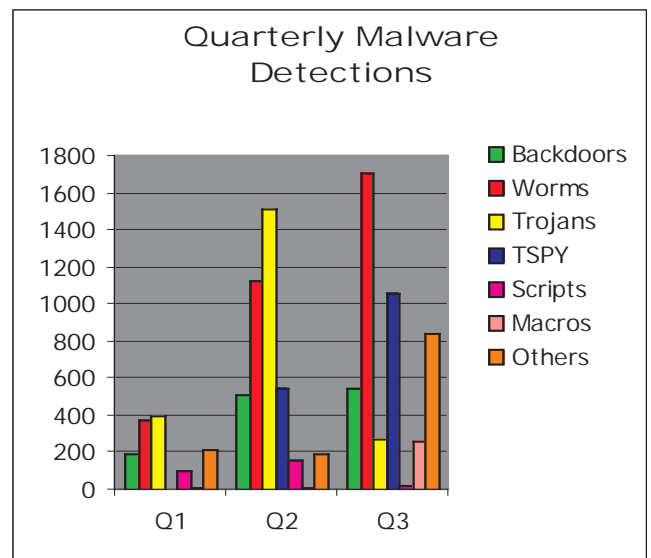


Figure 1.2 Quarterly Malware Detections. Broken down to Malware types

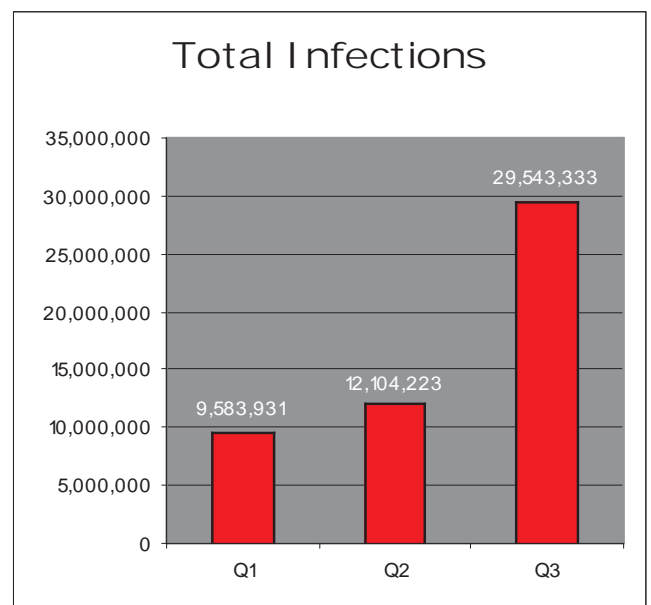
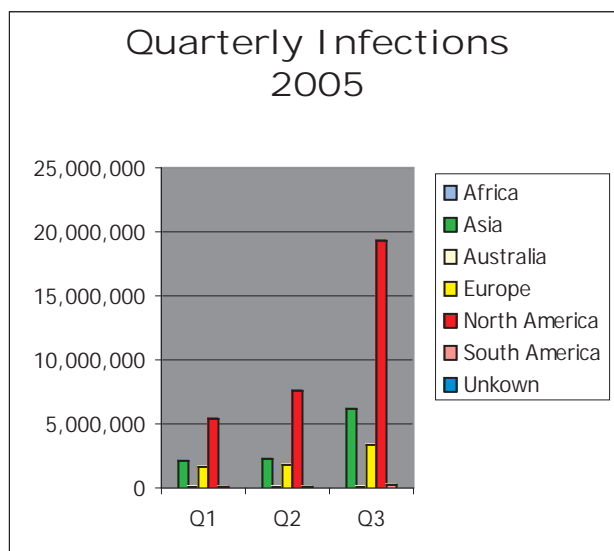


Figure 2.1 Quarterly Infections



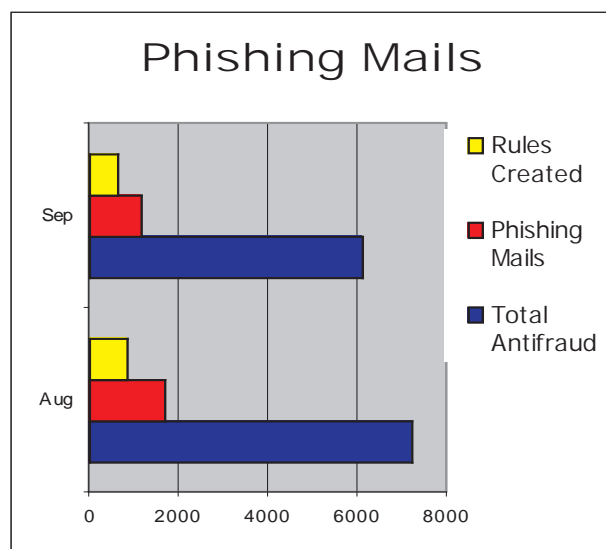
**Figure 2.2** Quarterly Infections. Broken Down by Continents

North America garnered nearly 70% of this quarter's total infections. As shown in figure 2.2, the next two at least visible continents on the chart are Asia and Europe. Both continents combined still do not catch up to North America's infection counts. Again, a display of a sudden leap, Q1 to Q2 was slow and easy, but the jump in infections from Q2 to this quarter, is clearly noticeable.

## Phishing and Spam

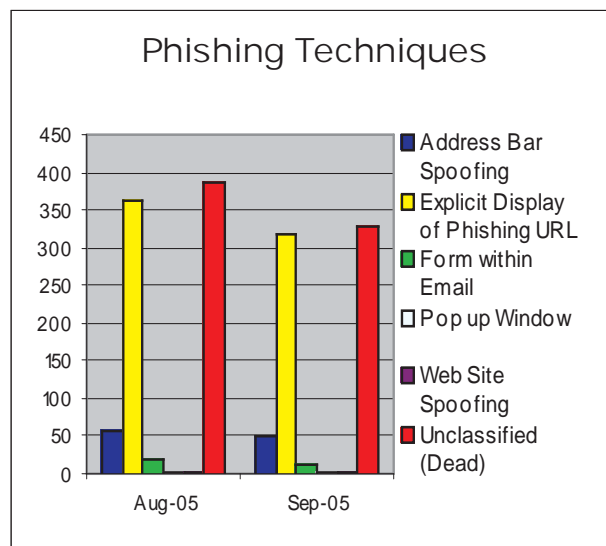
Unlike the sudden jumps in malware detection and infection figures, phishing figures remain proportionally steady, though the total of antifraud mails received for September are slightly lower than last month's. The ratio of the total phishing mails vis-à-vis the rules created remains the same.

"There have been theories that growth in various regions have peaked. However, the more probably reason would be the timing in terms of computing usage. As seen by historical data, North America contributed numbers are majority. The quiet months of August to October yearly over time figure into the start of the school months and focuses are elsewhere rather than new purchases," Yaneza explains.



**Figure 3.1** Antifraud Mails, Phishing Mails, Rules Created

Still consistent with the previous month, Explicit Display of Phishing URL is still on the top technique used by phishers. Also in accordance with the slight drop in total antifraud mails received, figures in the phishing techniques dropped as well. Most of the phishing techniques recorded are still filed under Unclassified.



**Figure 3.2** Phishing Techniques

As for the top targeted companies, Paypal and eBay are still on top. Amazon, went from number ten to number three this month. Bank of the West, Earthlink, Chase, and Sky Bank are new to the top ten list. ANZ, Deutsche Bank and, Natwest got off the hook for September.

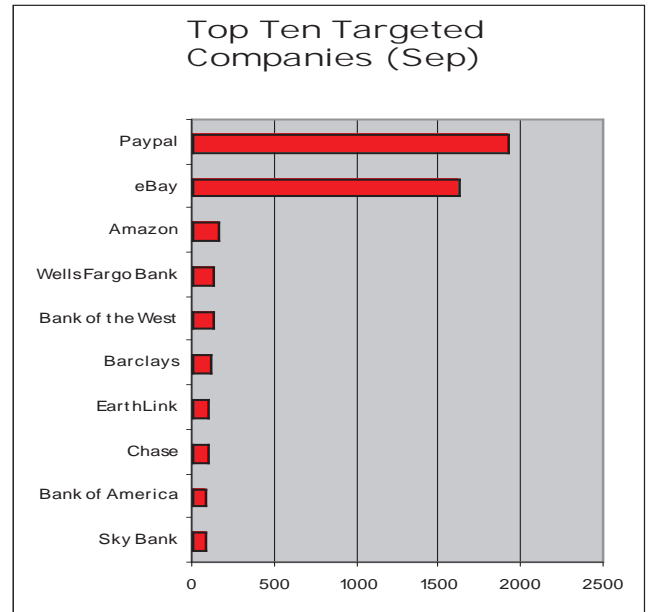
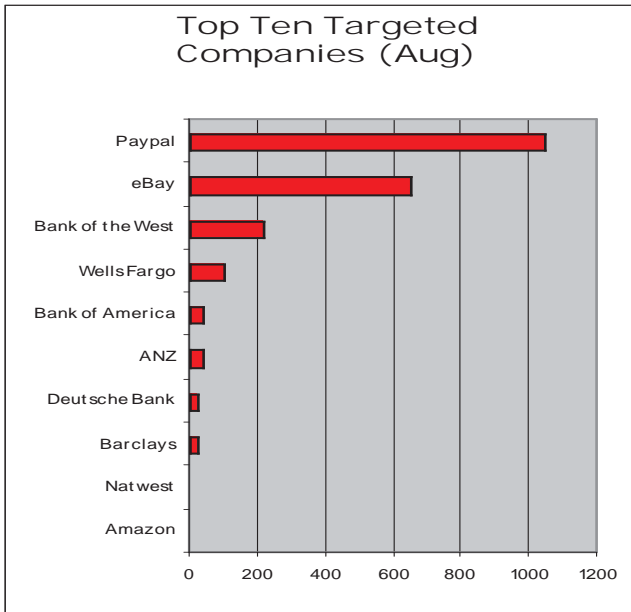


Figure 3.3 (left) and (right) 3.4 Top Ten Targeted Companies for September and August

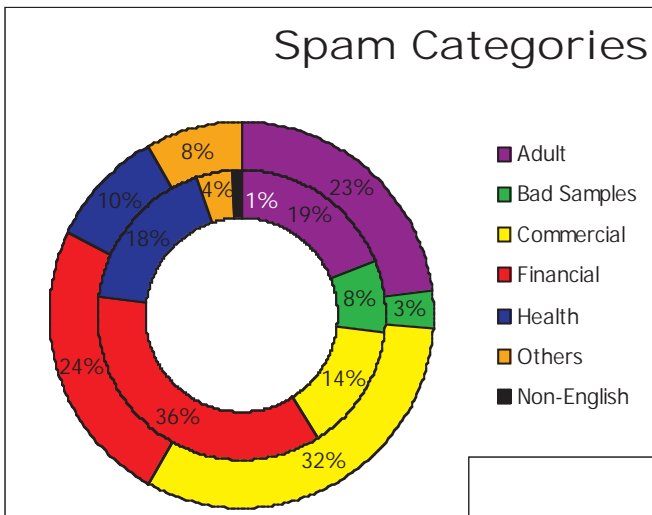
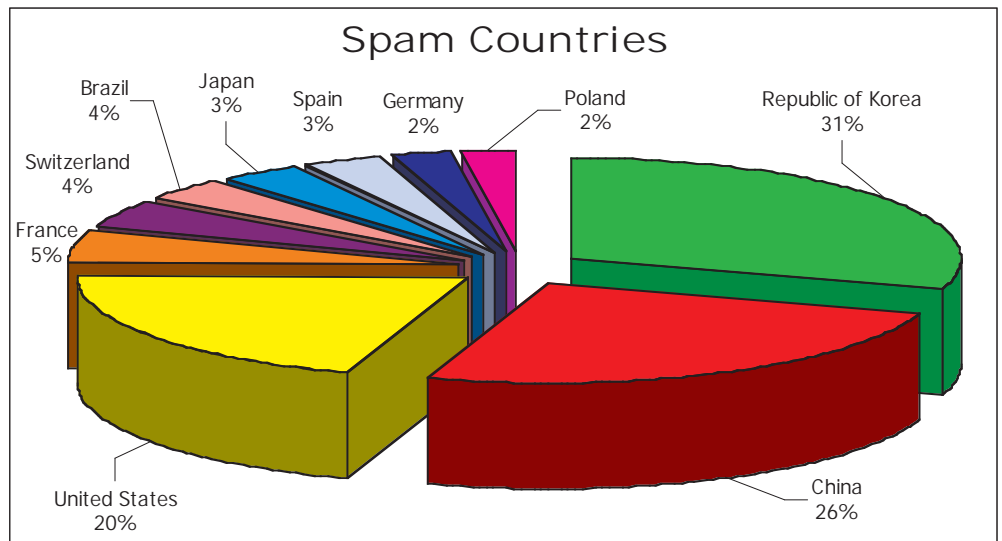


Figure 3.5 Spam Categories for August (inner ring), and September (outer ring)

The chart on the left shows the spam categories for both August and September. The outer ring represents September, while the inner ring is August. Commercial-related and Adult-related spam increased this month, while the rest decreased.



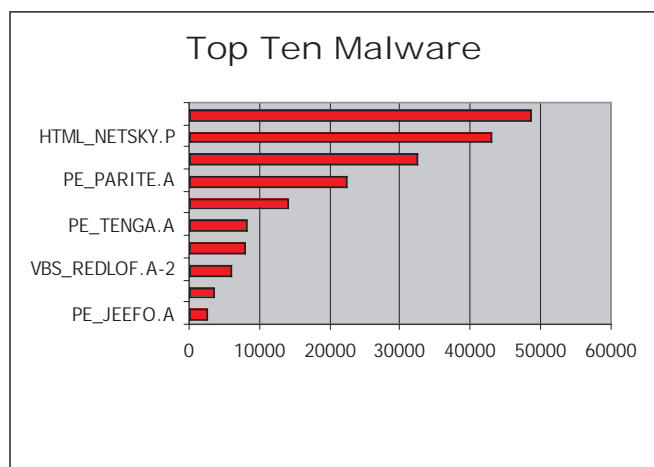
Korea retains the top spot for this month, gathering 31% of the world spam. China managed to slip past United States of America and take the second spot.

As of September 25, Korea, China and Japan combined hold 59% of the total spam.

Figure 3.6 The Top Ten Countries in terms of Spam. Korea retains top spot. (As of September 25, 2005) Trend Micro's Spam Report Map <http://www.trendmicro.com/spam-map/default.asp>

## Prevalence Charts

### Slipped Through At Last



JAVA\_BYTEVER.A, the ever so handy applet used by a lot of spyware and adware to propagate via email has finally risen to the top. After nine months of watching NETSKY at the top, the Java applet overtook the HTML component of Netsky with a slim margin of roughly six thousand counts.

## Roundup Special

### Sizzling Spyware

This quarter's spikes in malware detections and infections are attributed mainly to two things—the rise in computing population and the introduction of the Trojan spyware. Jamz Yaneza said August's monthly global perspective shows quite an alarming number of attacks against "Legend of Mir" and "Lineage", both popular MMORPGs (massively multiplayer online role playing games).

Attacks to online game accounts are nearly as hot as attacks to bank accounts. Video gaming has evolved to highly cinematic and interactive experiences. MMORPGs like it's ancestor, the board game Dungeons and Dragons, have followings like cults and gamer communities are geeking out with every new in-game item, every scrap of armor, and every last bit of that potent elixir. Consequently, the items values in the make-believe world of MMORPGs crossed over to the real world, with rare swords and armor sets getting sold for hundreds of dollars, not just virtual currency.

Yaneza said that while Legend of Mir players are predominantly based in mainland China, Lineage devotees are mostly in Taiwan and the greater United States. The developers of both games are based in South Korea and have business partners in North America.

Banks and online characters—equally valuable for its patrons—remain the biggest targets for Trojan spyware. Most of the banks targeted currently are based in Brazil and South America, yet on an interesting side note, while TSPY\_BANCOS.AFG is meant to target banks in Brazil, the larger part of infected systems actually come from North America which accounts for triple the numbers coming from South America.

**"There is an underground growing demand for virtual weapons and character capabilities in online games such that an industry has sprouted. In fact, people are willing to kill for these."**

**- Yaneza**