

THE STATE OF Malware Today

Fortinet has reviewed Malicious Code Activity During
September 2005.

This month's highlights:

- ▶ Bagle/Mitglieder - The Most Significant Threat in September
- ▶ Rise of Spyware - Top Ten Threats in September Highlight a Striking Trend
- ▶ Phishing Attempts Take Advantage of Hurricane Katrina
- ▶ Most Unique Outbreak for the Past Several Months
- ▶ Trojan Masquerading as Security Patch Install Update from Microsoft

Bagle/Mitglieder - The Most Significant Threat in September

The week starting on Monday, September 19, essentially consisted of an absolute Mitglieder (aka "Bagle downloader") Trojan frenzy, with several variants hitting the scene every day. As Trojans, Mitglieder don't replicate by themselves. They were mostly sent out very aggressively with the intent for users to download a copy of Bagle - and appear to have been sent more aggressively than any Trojan previously.

According to Fortinet Threat Response Team Leader - EMEA, Guillaume Lovet, "The high frequency of new variant releases, which correspond to slight modifications in the code before packing, may indicate that authors tried to challenge antivirus vendors - much like MyTob

authors did back in May of this year. This obviously failed, as most vendors responded quickly with generic signatures - and above all because of my knowledge, Bagle copies haven't ever been available for download. Proof is that the first Bagle variant to appear in Fortinet's virus activity top 100 list is down around 50th place, with less than 1% of the global activity."

Rise of Spyware - Top Ten Threats in September Highlight a Striking Trend Whereas, historically, Fortinet's monthly top 10 threats list has been a list of the most active mass-mailing worms, nearly half of September's top 10 threats are not worms. In addition to HTML/Ebay-phish and Adware/ 180 Solutions, the September top 10 threats list now features two additional spyware threats: ZangoSA, a so called "browser helper object," which spies on users' browsing habits, and the one year old Download/Px, a shady installer, which silently downloads and runs an impressive list of spyware.

How can simple spyware, which unlike worms do NOT replicate (let alone embed a mass-mailing engine), kick several well-implemented mass-mailers such as Zafis or MyTobs out of the top 10?

Let's consider the three main ways to get infected by spyware:

To secure against phishing sites, Fortinet highly recommends using a Web filtering service that blacklists malicious sites used for phishing attacks

Top 10 countries reporting infections in September 2005:

▶	United States of America	29%
▶	Korea, Republic of	8%
▶	China	5%
▶	Taiwan, Province of China	5%
▶	Mexico	5%
▶	Japan	4%
▶	Italy	4%
▶	India	3%
▶	Canada	3%
▶	Thailand	2%

Top 10 threats caught by Fortinet's FortiGate security appliances in September 2005:

▶	W32/Netsky.P-mm	8%
▶	HTML/FileDownload.E	7%
▶	HTML/Ebay-phish	3%
▶	Download/Px	3%
▶	W32/Zafi.B-mm	3%
▶	W32/MyTob.EK-mm	3%
▶	Adware/180Solutions	2%
▶	W32/MyTob.AS-mm	2%
▶	Adware/ZangoSA	2%
▶	W32/Zafi.D-mm	2%

- ▶ A user visits a malicious Webpage with an unpatched browser (usually following a link in a malicious email)
- ▶ A user clicks the attachment in a malicious email
- ▶ A resident virus is instructed to install spyware on the infected host

"Most malicious emails are spammed via infected hosts, so a raise in spyware activity likely reflects a trend in cyber-criminal activity. Now that large-scale nets of infected hosts (i.e., botnets) have been well established for a while, the commercial activities of their owners are flourishing - the two most lucrative ones being spam and phish relaying and aggressive seeding of spyware," said Lovet.

Phishing Attempts Take Advantage of Hurricane Katrina

Unfortunately, as more proof that greed sometimes doesn't stop before suffering, numerous phishing attempts taking advantage of Hurricane Katrina related events were reported in September. These phishing emails urge users to log into malicious Websites posing as charities and prompting users to donate relief funds. This follows the numerous scams that made use of other major catastrophes such as the Tsunami or the London Underground attacks, and precedes those, which will most likely appear in regards to Hurricane Rita's related events (several domain names have been registered already, such

as "HURRICANE-RITA-RELIEF.net" or "RITA-DONATIONS.com").

"It's sad to say, but experience proves that whenever an important event is hitting the news, and the more it generates commiseration and donations, the more phishing attempts pop up in response - so be cautious. Additionally, to secure against phishing sites, Fortinet highly recommends using a Web filtering service that blacklists malicious sites used for phishing attacks, in addition to a complete security strategy for Internet gateways and host systems."

Malicious emails claiming to be from Microsoft, and urging users to install the attached security patch continue to be distributed in September.

Most Unique Outbreak for the Past Several Months

September quite possibly could have produced the most unique outbreak of the past few months. Emails in German, mimicking the eBay look and feel and claiming to originate from ebay.de, were heavily spammed with an attached file named "Ebay rechnung.pdf.exe." While the "click the attachment" social engineering payload was everything but original, the file was a lot more surprising. Either the file was a small non-malicious application implementing a very basic cipher/decipher operation (Caesar's cipher...), or it was a downloader (W32/Agent.UF-dldr) that would first retrieve a text file containing the following data:

```
jvvr8--ig***.`caiwr,gzg
jvvr8--hmntcf,***,gzg
jvvr8--qkvc`mp,amo-***-20,gzg
jvvr8--qxc`cfcnokic***mpi-q(q,vzv
jvvr8--uuu,`qcvpqlq,***-nmeq-
3nm,gzg
```

This data looks like URLs encoded by a simple shift-cipher, and indeed, it is. Using the small application mentioned above, this data translates to the below locations where the malware would

download copies of a P2P Worm called W32/Goldun.A-net (as a second step in its infection process.):

```
http://keraker.hu/***.exe
http://jolvad.hu/***.exe
http://sitabor.com/****/****/****.exe
http://szabadalmikamara.hu/****/****.txt
http://www.bsatrans.com/
****/****/****.exe
```

According to Fortinet Threat Response Team Leader - EMEA, Guillaume Lovet, "The benefits of downloading a file, which in turn contains a list of locations (vs. reaching those locations directly) are unclear. Most likely, the authors thought that since the file was meaningless plain text, Web hosting companies hosting it would not take it offline, despite complaints from threat researchers. That way, sites hosting the actual malware could be shut down - authors would just relocate samples elsewhere and change the ciphered locations list."

User Trojan Masquerading as Security Patch Install Update from Microsoft

Malicious emails claiming to be from Microsoft, and urging users to install the attached security patch - which is actually a casual Trojan - continue to be distributed in September. This time around it's called W32/Zapchast.F-tr, and follows in the footsteps of many other threats that thrived on the same type of social engineering: W32/Swen.A, W32/Sober.D, W32/Dumaru, W32/MyDoom.AD and W32/Pandem.B to name a few.

According to Fortinet Manager of Antivirus Escalation and Research, Nick Bilogorskiy, "Social engineering like this can only be countered through user education and increasing awareness. Users must develop a habit to distrust any incoming email attachment by default. Whether it claims to be from Microsoft, a financial institution, or even your own system administrator or ISP, be suspicious and exercise good judgment. And remember, Microsoft never emails patches out." **CTOP**