

April 1, 2004

2003 in Review, 2004 Predictions

Malicious Code

© iDEFENSE Inc. 2004, All Rights Reserved. Distribution of this document by permission only.

Presented by: Ken Dunham, Director of Malicious Code

2003 Malicious Codes

- » Top Codes
- » Top Families
- » Calendar of 2003 Events
- » Trends for 2003 Malicious Code

Characteristics of Cyber-Criminals & Crimes

- » Means & Motives
- » Prolific Phishing
- » Rapid Exploitation

2004 Malicious Code Predictions

Closing Discussion: Q&A

2003 Malicious Code Overview



- » 2003 was the worst year to date for malicious code attacks.
 - » Avron, Slammer, Fizzer, BugBear.B, Blaster, SoBig, Welchia, Dumaru, Swen, MiMail, Gaobot and others
- » Phishing became a household term as attacks escalated throughout the second half of the year.
 - » Multiple new techniques emerged for Phishing throughout 2003.
- » Malicious code grossly underreported by the anti-virus industry.
 - » Swen: 45,000 interceptions noted, over 1.5 M computers infected!
- » Dozens of variants of released.
 - » Progressive Dumaru attacks and silent updates.
 - » Hacker for hire and Gaobot worms/Trojans.
- » Increased blended attacks combined with vulnerability exploits.
- » Technology proven to be reactive and incomplete against emerging malicious code threats.

2003 Malicious Code Impact



Banking and identify theft, stolen software and keys

- » Election and related online activities significantly disrupted
- » Welchia likely involved with the great 2003 blackout
- » Root servers of the Internet impacted by outbreaks
- » 911 System taken down incidentally by network attack worm
- » Flights delayed
- » Railway services interrupted
- » ATM services interrupted
- » Government websites singled out and successfully attacked
- » Navy network and highly secure networks unable to avoid infection
- » **Sasser in 2004, incidentally, stranded 300,000 railway passengers, delayed flights and took out the UK Coast Guard network.**

Top 2003 Codes 1-5



1. SoBig	6 variants, nosiest worm in history of computing, 3 stage attack worm
2. Yaha	Long-term success, political and religious motives, country/state specific attacks
3. BugBear	Long-term success, targets over 1,300 financials
4. Blaster	Multiple variants, spread rapidly, mass disruption, exploited a new vulnerability
5. Dumaru	Multiple variants, Eastern European Attackers, tied to spam, DDoS, and identity/banking theft

Top 2003 Codes 6-10



6. MiMail	Multiple variants launched in waves of attacks. Motivated by financial gain, slick executable GUI.
7. Swen	One of the most underreported worms to date, 50K to 1.5 M. Slick HTML interface that looks legitimate.
8. Welchia	Spread via two vulnerabilities, RPC and WebDAV. Associated with the blackout and Navy network incident.
9. Slammer	Slammed the net and started 2003 with a big bang. Patching problems and integrated solutions contributed.
10. Klez	Widespread to 10 worm from 2002, spoofs e-mail.

Top 2003 Code Comments



- » The top three codes spread via e-mail.
- » E-mail worms tend to rank higher because they stay in the top ten for a longer period of time as compared to network attack worms.
- » Network attack worms tend to not require human interaction and spike and die out more rapidly than other types of code.
- » Three of the top ten codes are network attack worms
 - » Blaster
 - » Welchia
 - » Slammer

January

- » Avron.A is first major outbreak of the year.
- » Otto von Guttenberg plans attacks; Avron.C.
- » Slammer/SQL worm causes havoc.
- » Sadhound dropper installs backdoor Trojan.

February

- » LoveGate.C and LoveGate.D spread in the wild.
- » Gibe.B worm gains ground in the wild; social engineering.

March

- » SMB DoS worm discovered in the wild.
- » Deloader worm targets home users.
- » Yaha.Q worm discovered.
- » Ganda worm spreading in English and Swedish.
- » LoveGate.F worm attack networks with brute force.

May

- » Fizzer worm installs Trojan horse.
- » LoveGate.H, J, and K discovered.
- » Palyh worm discovered (SoBig.B).
- » MMS.A, Flood.BV worms provide backdoor access.
- » SoBig.C discovered in the wild.

April

- » No significant malicious code events during this month!

June

- » BugBear.B worm targets over 1,300 banks and others.
- » MuMu network attack worm in the wild.
- » SoBig.D and SoBig.E worms surface in June.

July

- » Trojan authors begin exploitation of RCP-DCOM 026.

August

- » MiMail worm is seen as a significant threat.
- » Blaster worms emerge in the wild, mass disruption.
- » Welchia worms spread and hit many networks.
- » SoBig.F is the nosiest most widespread worm of all time.

September

- » Swen worm spreads in the wild as an HTML e-mail that looks like it comes from Microsoft Corp.
- » Smibag worm spreads through MSNM.
- » Widespread zero-day attacks underway against IE.

October

- » Qhosts zero-day exploit of IE, installs Trojan.
- » MiMail.C gains ground in the wild.

November

- » MiMail.I, aka Paylap, steals credit card data.
- » MiMail.J

December

- » Scold.A worm spreads via e-mail.
- » Sober.C spreading in the wild, targets German speakers.

General Attack Periods

- » First and last week of January
- » Last week of February
- » First week of March and spring break time frame
- » Last two weeks of May
- » Middle of June
- » Entire month of August
- » Second and third weeks of September
- » Second and third weeks of November

2003 Trend Statistics



2002	840 mass mailing worms
2003	1,007 mass mailing worms
2002	1,484 backdoor/remote access Trojans
2003	2,205 backdoor/remote access Trojans (67% increase)
2002	142 linux/unix malicious code
2003	170 linux/unix malicious code (only 466 total)
2002	508 macro viruses
2003	436 macro viruses (dropped)
2002	196 P2P malicious code
2003	436 P2P malicious code (significant increase)
2002	438 IRC component in malicious code
2003	619 IRC component in malicious code (1,698 total)

E-mail Codes on the Rise



1999	9,184 viruses intercepted: 1553 ratio
2000	184,257 viruses intercepted: 911 ratio
2001	1,798,872 viruses intercepted: 381 ratio
2002	9,332,627 viruses intercepted: 215 ratio
2003	58,580,646 viruses intercepted: 92 ratio
2004	? MyDoom, Bagle, NetSky, Sasser...

*MessageLabs Corp. data, <http://www.messagelabs.com/>

- » Attacks are becoming more sophisticated and diverse as financial, political, and religious motives drives cyber-attacks.
- » Traditional motives of notoriety and personal challenge are now overshadowed by motives for money and power.
- » Malicious code attacks are now more commonly associated with vulnerabilities, very rapidly, as seen with Blaster and RPC, Data Object zero-day attacks in the fall against IE, and WebDAV attacks throughout 2003.
- » Opportunistic attacks are also on the increase, especially in P2P and e-mail environments.
- » The number of vectors for piercing through a network perimeter or to attack a various workstation has increased significantly.

Means & Motives 2



- » The middle class coder has grown in number. Organized criminal groups are interfacing with this group for multiple activities. This includes DDoS attacks, hacker for hire, affiliate advertising, and spam (to mention a few).
- » The carding market in particular reveals how organized the exploitation side of attacks has grown over the Internet in recent years.
- » Microsoft Corp. and others have offered thousands to catch criminals of high-profile malicious code attacks. Few have been arrested for such crimes to date but it appears that this is starting to work.
- » A relative small number of identity theft cases are actually reported and even fewer result in an actual arrest. Attackers can attack anonymously without fear of prosecution.
- » Hacktivists appear to have some support when tensions run high.

- » Phishing became a household term in 2003.
- » A dramatic increase in phishing attacks occurred in the summer and fall of 2003.
- » Multiple techniques are used to launch phishing attacks:
 - » Nigerian Letter Scams
 - » BiBrog and MiMail Malicious Code Attacks
 - » IP Address
 - » @ URL Hijacking
 - » Encrypted URL Data for Obfuscation of the Hijack
 - » Layered Windows Loaded From Hostile Website
 - » IE Vulnerability (MS04-004, Feb. 10, 2004)
 - » **Toolbar replacement via JavaScript in 2004**
- » Implications of the APWG, AVIEN, and others.

Rapid Exploitation



- » WebDAV Trojan, March 2003
- » RPC Trojans, July/August 2003
- » RPC Tool, July 2003
- » Blaster, August 2003
- » Welchia, August 2003
- » Data Object Zero-Day*, August – November 2003
- » ADODB.Stream Zero-Day*, August – November 2003
- » Agobot Worms, Fall 2003
- » BugBear/Others, IE Spoofing Zero-Day*, Dec. (03) – Feb. 2004
- » Witty, March 2004, within 2 days of patch made available
- » Phatbot, Sasser, MS04-011 exploitation within 30 days or less

*zero-day = attacks that occur before a patch is made available.

2004 Malicious Code Predictions 1



- » Increased malicious code attacks in 2004 overall, despite new bounties, laws and actions by authorities.
- » Multiple new variants to emerge in a pattern of attacks with successful families. This has been seen in many worms such as SoBig, BugBear, Yaha and MiMail. Waves of attacks are likely in 2004, such as a new worm with two or more variants, a time of rest and then another wave of attacks.
- » Blitzkrieg attacks likely in 2004. A large amount of variants launched into the wild within a short period of time, which will overwhelm anti-virus companies and help some variants to survive in the wild for extended periods of time.
- » Increased use of randomization techniques and simple social engineering to spread e-mail worms.
- » Increased use of ZIP attachments to bypass corporate gateways.
- » Increased blended threat attacks and multiple mediums to spread malicious code, such as P2P and IRC networks. Backdoor Trojan horse components will continue to become a common component of blended threats.

2004 Malicious Code Predictions 2



- » Increased customization of packers to make anti-virus detection and analysis more difficult.
- » Increased impact of malicious code upon infrastructure as seen with Slammer, Blaster and Welchia/Nachi in 2003.
- » Increased organization and development of cohesive hacking and malicious coding groups to launch targeted and opportunistic attacks.
- » Continued rapid exploitation of new vulnerabilities, occurring within days and weeks rather than months.
- » Increase in proxy Trojans often used to send out spam or protect the identity of an attacker.
- » Decrease in older and less effective mediums such as macro viruses and boot sector infecting viruses.

2004 Malicious Code Predictions 3



- » Increased number of computers on which anti-virus software is not used and that are easily or continually infected with malicious code. These computers will be used for significant DDoS attacks and the launching of more severe criminal attacks tunneling through such victimized computers.
- » Increased merging of spam, Trojans and worm technologies for criminal gain.
- » An increase of groups that work together to launch new malicious code attacks. Increased organization overall.
- » Continued increase in malicious code and techniques that terminates, deletes or attempts to undermine anti-virus and security related products.
- » Increased number of vulnerabilities that may be exploited to gain unauthorized access or spread a network attack worm. Increased speed of attack of some malicious code outbreaks, such as network attack worms.
- » Increased spam and DoS type attacks against mobile devices.
- » Increased utilization of wireless solutions to perform criminal acts and abuse.

Acknowledgements

Thanks to the following individuals for their efforts:

- John Watters, Chairman and CEO, iDEFENSE Inc.
- Jim Melnick, Director, iDEFENSE Inc.
- Sunil James, Director, iDEFENSE Inc.
- Gertjan Vroon, Ing. Senior (Anti)-Virus Expert, DFCAE, FSCFE, FSCSE
- Malcode Team, iDEFENSE Inc.
- Mike Wallace, Editor, iDEFENSE Inc.

Q&A: Ken Dunham: kdunham@idefense.com

End of Presentation