FEATURE 3

NEW MALWARE DISTRIBUTION METHODS THREATEN SIGNATURE-BASED AV

Oren Drori and Nicky Pappo
Commtouch Software, Israel

Dan Yachan
International Data Corporation (IDC)

For some time now, viruses have been designed for rapid distribution during the few hours before anti-virus update signatures are produced (as discussed in a previous article by one of the authors, see [1]). In a recent report *IDC* stated that achieving high propagation rates is one of the main design goals of malware authors today [2]. Modern viruses and worms are not immune to vaccinations – rather, they are designed to infect as many computers as possible before vaccinations become available.

As a result, a timely response has become a key factor in effective protection against malware, and a major challenge for the AV industry. We have argued that all signature-based methods need powerful complements to provide early-hour (preferably zero-hour) protection.

NEW DISTRIBUTION METHODS

In recent months, however, there has been a decided shift in malware distribution patterns. The new breed of malware is distributed in ways that enable attacks to be executed fully before they can be blocked by signatures. Widespread adoption of these new distribution methods could pose a serious threat to signature-based protection methods.

In this article, we identify two new malware distribution methods: short-span attacks and serial variant attacks. We describe their particular distribution patterns, the development of recent attacks, and the potential dangers they present.

MALWARE DISTRIBUTION PATTERNS

Classic malware uses a viral distribution pattern, in which one infected station infects another, and an epidemic develops. Traditionally, an outbreak of this type would grow gradually and peak after several days (see Figure 1a). This distribution pattern allows AV vendors valuable time to produce and distribute signature updates (although some of the viruses penetrate during the first hours). As powerful and dangerous as these attacks may be, signatures are still effective against them, unlike in the case of short-span attacks.

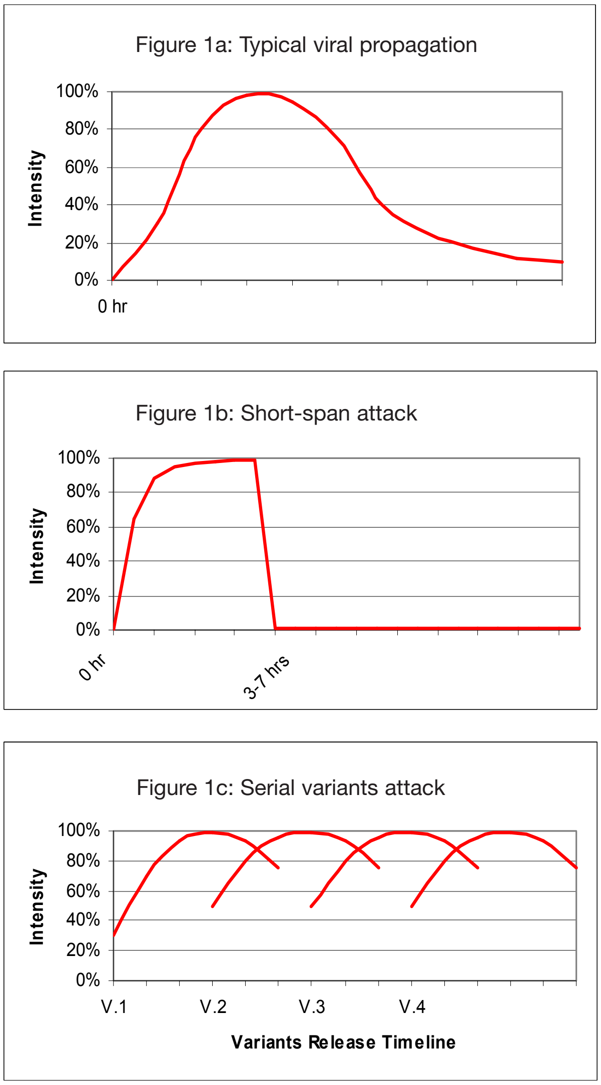


Figure 1a: Typical viral propagation

Figure 1b: Short-span attack

Figure 1c: Serial variants attack

Figure 1: Malware distribution patterns.

SHORT-SPAN ATTACKS

No doubt the increasing spam-virus symbiosis plays a part in malware distribution patterns. The short-span attack combines the distribution methods of spam with the payload of malware: this type of attack is mass-mailed, mostly without any mechanism for self-propagation.

Typically, an entire short-span attack is completed within a few hours, sometimes within as little as 20 minutes. Outbreak-scale attacks, distributed via zombie networks, can infect many millions of users before signature protection is available. As a reference, large zombie-based spam attacks distribute 100–200 million messages, within five to seven hours.

Unlike viral-propagation attacks, which die slowly, short-span attacks have a spam-like distribution pattern: rapid buildup, steady distribution rate throughout the attack, and almost instant dropping off (see Figure 1b). According to *IDC*, this technique is highly effective for Trojan distribution, and is often used in financially-motivated attacks [2].

In many short-span attacks, AV vendors avoid the trouble of developing a signature that will be obsolete by the time it is released.

During the month of June 2005 alone, *Commtouch* identified four short-span malware attacks, which were completed within one to seven hours (see Figure 2).

Short Span Attacks in June 2005				
Attack	**Named by**	**Date**	**Intensity**	**Span**
Goldun.BA	[Commtouch]	03-Jun-05	Medium	1 hour
Goldun.BB	[Commtouch]	17-Jun-05	Medium	45 minutes
Flooder.Agent-1	[ClamAV]	19-Jun-05	Low	1 hour
Flooder.Agent-1, variant	[ClamAV]	20-Jun-05	Low	1 hour
Beagle.BQ	[Symantec]	26-Jun-05	Very high	7 hours

Figure 2: Short-span malware attacks in June 2005 (measured by Commtouch Labs).

The most severe of these attacks was Beagle.BQ, which started and finished within seven hours. Of 20 major AV engines tested independently by *VirusTotal*, 10 did not manage to produce a signature before the end of the outbreak. 24 hours later, seven AV engines still had no signature for it at all (see Figure 3).

Beagle.BQ was one of the most intense attacks seen so far in 2005, perhaps the single most forceful one. Faced with it, 35% of commercial AV users obtained adequate protection only halfway through the attack, and 50% of products failed to provide adequate protection throughout the entire attack.

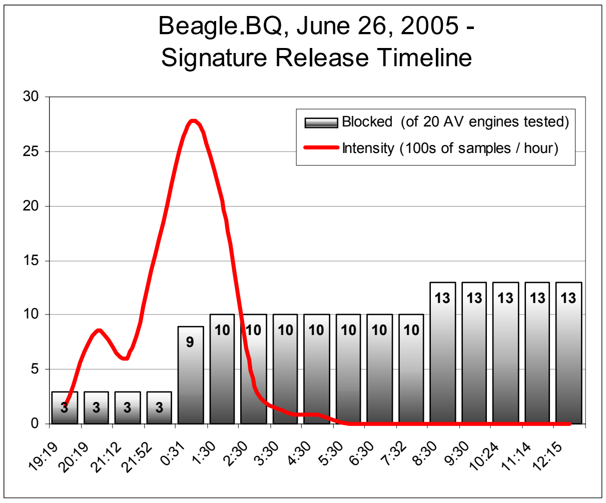


Figure 3: Beagle.BQ short-span attack. Sources: attack intensity based on data from Commtouch Software [3], signature updates based on VirusTotal [4].

SERIAL VARIANT ATTACKS

Serial variant attacks not only make use of the early-hour vulnerability window in traditional AV methods, but extend it by a cumulative factor.

A series of variants, prepared in advance, are launched at timed intervals. Each of the variants requires a new signature; each outbreak therefore enjoys its own window of opportunity, its own open distribution time, unimpeded by signatures. The overall window of vulnerability of the attack is the cumulative vulnerable time span of the individual variants (see Figure 1c).

To maximize the vulnerability period, the malware distributor uses a larger number of variants. Theoretically, if an unlimited number of variants could be added to the series, it would mean extending the window of vulnerability indefinitely.

In order to maximize distribution intensity – the number of infections or penetrations per hour – the malware distributor would aim to release the variants at very closely-spaced intervals.

Example: MyTob

One example of a low-volume, long-term serial variant attack is MyTob, releasing, on average, one new variant every day over the course of six months (see Figure 4 for the list of variants in July 2005).

Even though the functionality of the different MyTob variants is identical, a new signature must be produced for each one. Considering an average production cycle of 10 hours (see [5]), and a new variant every day, this means that the average paying AV user is unprotected from MyTob for 10 out of 24 hours, or 42% of the time.

MyTob Variants, July 2005	
27-Jul	W32/Mytob-HU
26-Jul	W32/Mytob-DX
25-Jul	W32/Mytob-BV
25-Jul	W32/Mytob-DW
23-Jul	W32/Mytob-HM
23-Jul	W32/Mytob-HN
21-Jul	W32/Mytob-IN
21-Jul	W32/Mytob-DV
21-Jul	W32/Mytob-DU
20-Jul	W32/Mytob-CX
20-Jul	W32/Mytob-DT
18-Jul	W32/Mytob-DS
18-Jul	W32/Mytob-DR
18-Jul	W32/Mytob-DQ
13-Jul	W32/Mytob-DP
13-Jul	W32/Mytob-DN
12-Jul	W32/Mytob-DM
12-Jul	W32/Mytob-DL
12-Jul	W32/Mytob-DK
11-Jul	W32/Mytob-DJ
10-Jul	W32/Mytob-DI
9-Jul	W32/Mytob-DH
8-Jul	W32/Mytob-AS
7-Jul	W32/Mytob-IU
7-Jul	W32/Mytob-DG
7-Jul	W32/Mytob-DE
7-Jul	W32/Mytob-DF
7-Jul	W32/Mytob-DD
5-Jul	W32/Mytob-DC
5-Jul	W32/Mytob-DB
5-Jul	W32/Mytob-CY
1-Jul	W32/Mytob-CW

Figure 4: Serial variants MyTob attack.

Example: Beagle

At the other end of the spectrum are attacks that maximize distribution density, by releasing multiple variants within a short time span. One good example is the Beagle attack of 1 March 2005 (Beagle.BB-BF) – an aggressive, high-volume attack that included no fewer than 15 different new variants in a single day, or almost one new variant per hour.

At the end of the day, *Kaspersky*'s team recounted the news [6]: 'Today we have already intercepted 15 new pieces of malware produced by the author of Beagle. The newest variants follow hard on the heels of our updates and we suspect that the author is creating new variants every time we release updates to block previous versions.'

CONCLUSION

In the past two to three years, malware developers have zeroed in on the early-hour vulnerability gap of traditional AV protection methods. Focusing on this 'sweet spot', they have developed new ways of distributing malware, which not only use, but also extend the early-hour gap in AV protection dramatically.

So far, these particularly pernicious types of attack are a minority on the landscape of malware. Nevertheless, these aggressive short-span attacks and serial variants have the potential of becoming the norm. If such a thing were to happen, it would represent a game-changing event in the AV industry. We believe it is crucial for the AV industry to prepare immediately the technologies to protect users from emerging early-hour distribution attacks.

REFERENCES

[1] 'Virus outbreak protection: network-based detection', Oren Drori, *Virus Bulletin*, March 2005.

[2] 'Zero hour virus protection: defending against the unknown', Dan Yachin, *IDC*, August 2005.

[3] Commtouch Software, http://www.commtouch.com/.

[4] VirusTotal, http://www.virustotal.com/, *VirusTotal* is an independent service that uses multiple anti-virus engines to analyse suspicious files. It facilitates the quick detection of viruses, worms, Trojans, and other kinds of malware detected by each of the anti-virus engines. Data documented by *Commtouch*, during the outbreak time.

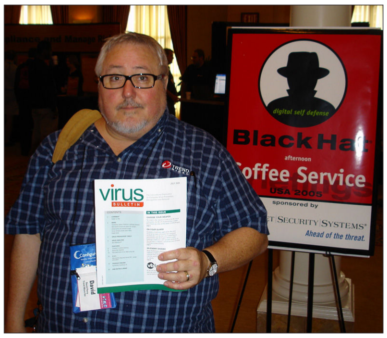
[5] Andreas Marx, AV-Test.org, http://www.av-test.org/, *Proceedings of the Virus Bulletin International Conference* 2004.

[6] Kaspersky Lab, *Analyst's Diary*, 1 March 2005, http://www.viruslist.com/.

CONFERENCE REPORT

BLACK HAT AND DEFCON – TOO HOT FOR MANY

David Perry
Trend Micro, USA



A wise man once told me that the difference between responsibility and blame is that responsibility happens before the fact, and blame happens after the fact. Bear that in mind.

I went to Las Vegas in July to attend both the Black Hat Briefings and DEFCON, at the behest of *Virus Bulletin*, who had asked me to write up a report of the proceedings as I saw them. So without digressing, I will get right to the subject at hand.

Now, you always hear about 'Black Hat *and* DEFCON', so just to set the record straight, the two are very different things. Black Hat is a very serious conference intended to illustrate top issues in the world of network security, and DEFCON is a 'through-the-rabbit-hole' con, where not only is everyone there a poseur, but everyone is proud to admit that everyone there is a poseur.

When registering for Black Hat, you are given a backpack containing the conference proceedings (a paperback volume the size of a very large phonebook) and a number of other useful items. A closer inspection of the proceedings volume showed that the rumours were true – a whole presentation had been torn neatly out of the volume – and the CD versions of the proceedings had been rudely withdrawn to a secret location where each was ceremonially destroyed under the watchful eye of a trained exorcist.

The missing presentation was Michael Linn's *CISCO* disclosure – a subject so controversial that no two people agree on what it really means. You cannot see the slides, you cannot see the video or hear the audio recordings made of the presentation (both were seized by a local court following a cease and desist order), and you can't get a clear story about exactly what happened, but I will tell you this about Michael's presentation: it was *really* crowded! After standing and listening to about 15 minutes (including the famous 'Welcome to the Eighties' line – upon which I will not elaborate here) I did what any other reasonable conference-goer would do – I went to another room, to let everyone else report on the big enchilada.