FEATURE 2

Are You Being [Opa]Serve[d]?

Martin Overton
Independent Researcher, UK

W32/Opaserv, which first appeared as a 'minor' curiosity at the end of September 2002 (see *VB*, December 2002, p.6), is fast becoming a major headache not just for the 'great unwashed' (the public) with their xDSL/Cable/Modem Internet-connected systems, but for a large number of organisations too.

Underestimating

It appears that many people did not consider Opaserv to be a threat because they felt that it couldn't become widespread using Windows Shares as its only infection vector.

This 'incorrect' thinking was partly due to the fact that many companies (quite rightly) do not allow Windows Share (SMB) traffic to traverse their corporate firewalls (Port 137 UDP 139 TCP).

Furthermore, a subset of these companies prohibits the use of 'open' shares on their internal network(s). An even smaller subset prohibits P2P use, for the same reasons – fear of confidential data leakage, copyright infringement, malware, and other security risks.

However, the 'great unwashed' have shown that they have little understanding of security. They do not seem to understand the need to run anti-virus products or personal firewalls, and do not comprehend how 'open' their systems have been left as a result of not following basic safe computing guidelines.

Not only have they left their systems exposed to the likes of Opaserv, but also to the mounds of other malware, including RATs and DDoS bots/zombies and to the ubiquitous 'hackers', 'script kiddies' and other mischief makers. Furthermore, they may unwittingly be exposing their personal data, including personal documents and correspondence, credit card details, passwords, ISP details and who knows what else.

The Quiet One

In many ways, Opaserv is the quiet twin of Klez; like Klez it is very widespread but it uses a different infection vector (Windows Shares [SMB] rather than email [SMTP]) to achieve its ends. (Allegedly Klez can spread via Windows Shares, however this is a secondary 'vector' for it, and I have yet to see a sample that has been dropped to my worm lure via this route.)

Although Opaserv is relatively harmless, it has caused similar traffic patterns to those caused by Nimda and CodeRed. Thankfully, Opaserv is not as aggressive in its scanning of a network for new victims.

Let's have a look at some of the reasons why Opaserv and its increasing number of variants are spreading so far and so quickly.

Evolution

Over the last few months a number of new variants of Opaserv have been created. In the majority of cases the changes have been subtle – for example, new website addresses from which the worm grabs updated versions of itself, and the use of varying file compression and/or encryption tools in an attempt to conceal the modified malware.

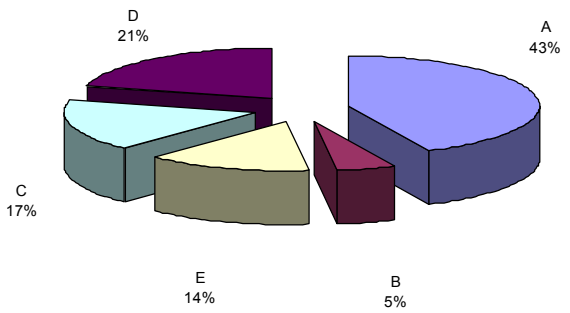
The table below shows the dates when these new (i.e. unknown) variants were first detected by my Internet-facing worm lure. The lure is used to catch new malware In the Wild and to monitor how widespread a particular piece of malware using this infection vector becomes (along with other tools for malware which use other infection vectors). In most cases the 'new variants' of Opaserv were caught by my worm lure within hours of their initial deployment by the author(s).

The samples were catalogued, and the information that was gleaned from the initial (brief) investigation and testing was sent to a number of anti-virus vendors, along with the trapped samples. In addition, the data was transmitted to the AVIEN mailing lists (minus the samples), to give members a 'heads-up' on the new threat.

Shown below is the timeline of new Opaserv variants trapped (the variant naming used for this timeline is from *F-Prot* [F] and *NAI/McAfee* [N]):

Filename	***Date Trapped***	***F/N***
Scrsvr.exe	N/A	A/A-D
Brasil.pif	19 October 2002	A/E
Brasil.exe	20 October 2002	A/F
Alevir.exe	22 October 2002	C/G
Marco!.scr	28 October 2002	D/I
Puta!!.scr	7 November 2002	?/?
Instit.bat	10 November 2002	E/K

(Brasil.exe was first spotted by AVIEN member Mark Ackermans.)



Change for Change's Sake

The pie-chart above shows the distribution spread of almost 10,000 trapped samples of the current (as of 26 November 2002) known variants of Opaserv. The variant naming used for this chart is that used by *F-Prot*.

As can be seen, some variants have spread more quickly and widely than others. In many cases it may be the changing filenames and the use of packing and encryption tools that have allowed new variants to gain a 'beachhead'.

It seems clear that many anti-virus companies need to improve their handling of packing and compression tools. It appears that plenty of malware authors are well aware that a number of anti-virus products are 'limited' in this area.

Risky Business

Known MS Security Holes

Opaserv takes advantage of the password exploit on *Windows 9x/Me* which is fixed by installing MS00-72. Luckily *Windows NT/2000/XP* are not vulnerable to this specific attack.

Holey Network Batman!

Opaserv takes advantage of Windows Shares, including password protected shares, as long as:

1. The whole of drive C: is shared as 'C'.
2. It is either open (with no password) or it is password protected but not patched with the MS00-072 (*Win 9x/Me* only).
3. It is writeable.
4. The share is visible to an infected system on the network (internal/home) that it lives in, or the system has Netbios over TCP/IP enabled (which makes Windows Shares available to other Internet systems and/or users).

What are the risks in a corporate environment, where the corporate firewall does not allow SMB traffic to/from the Internet?

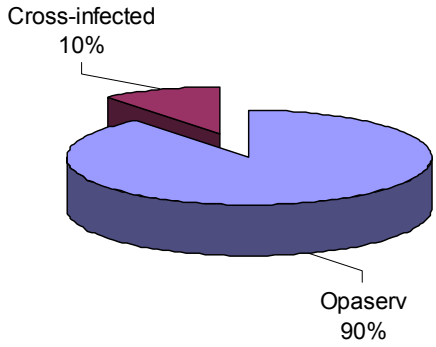
Opaserv can still get in. Let's investigate possible back- and side-doors that it could use to bypass the front-door bouncers (firewall and perimeter AV).

These include:

- Modems on desktops, laptops and servers.
- Laptops that are taken home or to customer sites.
- VPN installations that allow dual-access (Internet and corporate network at the same time) for home-based workers or those on customer networks.
- Other remote access software for home-based workers via their xDSL/Cable/Modem connection.
- Web-based email (yes, I have seen Opaserv sent as a file attachment via email).
- P2P, such as *KaZaA*, *WinMX*, *Gnutella* (maybe disguised as another piece of software).
- Hacked or back-doored systems.
- Disgruntled employees.
- Re-packaged with a compression/encryption tool that the perimeter AV can't handle or doesn't recognise, but doesn't quarantine.

Cross infection

The following chart clearly shows that Opaserv is acting as a 'carrier' and is transporting other malware along with it (unbeknown to Opaserv) – acting as a sort of binary 'Typhoid Mary'.



This could also explain the resurgence of W32/Funlove (especially with W32/Braid dropping W32/Funlove too), as this virus was the most common 'passenger' on files dropped by Opaserv.

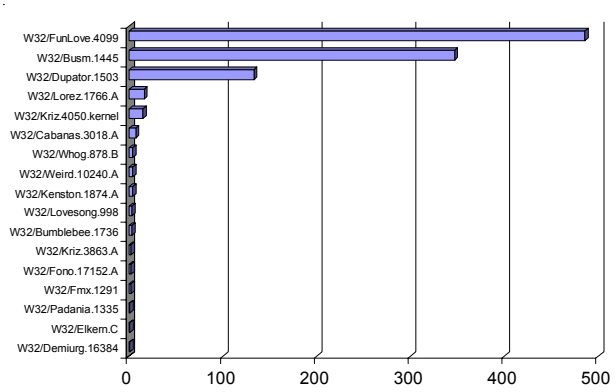
On the following page is a bar chart showing the full list of 'passenger' malware that has been found hitching a ride on the Opaserv malware transit system so far.

I Can See You

Not only does Opaserv drop files onto a new victim system, it also makes changes to ensure that it is executed the next time the system is restarted.

Dropped Files

An integrity system will alert on new files and system modifications which may indicate that Opaserv or another



SMB-aware (or other infection vector-based) piece of malware is active on a system.

To date, Opaserv has dropped files masquerading as .BAT, .EXE, .PIF and .SCR file extensions with fixed names (Brasil.exe, Brasil.pif, marco!.scr, scrsvr.exe, scrupd.exe, puta!!.exe, alevir.exe and instit.bat). Luckily, it hasn't (yet) used random or similar (list) filename generation.

System File Modifications

Opaserv modifies WIN.INI by changing the 'run=' line to read as follows:

```
run=c:\windows\<variant_name.variant_extension>
```

In some cases this line can contain multiple variants on the same line, for example:

```
run=c:\windows\scrsvr.exe,c:\windows\marco!.scr,
c:\windows\Brasil.exe,c:\windows\alevir.exe,
c:\windows\instit.bat
```

On systems that have been infected it is quite likely, even though the worm has been blocked or removed by an on-access or on-demand anti-virus solution, that the WIN.INI will still be modified and contain numerous references to the worm files, which will cause errors to be displayed when the system is next restarted. This seems quite ludicrous!

I have even seen several cases in which the WIN.INI file has become truncated or corrupted due to modification by Opaserv.

Once Opaserv has been run (usually via the modification it made to the WIN.INI 'run=' line) and the system has been restarted, it adds an entry and a call to itself in the following Registry key, which ensures that the worm is loaded when the system starts (even if the WIN.INI call has been removed):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run
```

There has been a lot of confusion as to whether Opaserv can (and does) drop copies of itself on *Windows NT/2K* or *XP*-based systems.

The worm lure I use is based on *Samba* running on *Linux*. However, to other *Windows* systems this appears to be a *Windows NT 4.0* server. Opaserv will happily drop copies of itself onto this system and modify the WIN.INI file as if it is a 'real' *Windows* system. However, most anti-virus companies' descriptions claim that Opaserv can work and drop copies of itself only on *Windows 9x/Me*-based systems. A little clarification is needed! While Opaserv will successfully copy itself to *Windows NT/2K/XP* machines as long as it finds an open (not password-protected), writable share 'C' with the directory 'Windows', the chances of meeting those requirements are much slimmer that finding the suitable conditions on *Windows 9x/ME*.

Personal Firewalls

Firewalls can be used as an effective way to slow or even block Opaserv, by enabling the 'Windows File and Print Sharing on the Internet protection' (the exact wording depends on your personal firewall product).

Most personal firewall products have this 'rule' or 'protection' switched on by default. However, this will not slow Opaserv down on the user's 'home' or 'corporate' network. To resolve this would require the addition of a 'custom' rule.

Desktop Anti-Virus

Yes, desktop (and perimeter) anti-virus packages have their part to play and, once they have been updated to detect the new variants of Opaserv, they can and do block the Opaserv 'dropped files'.

However, it seems that, although the anti-virus packages block the files, the end-user is left to clean out WIN.INI after each infection attempt – in most (if not all) cases, anti-virus programs do not stop Opaserv from modifying this file.

As I have been seeing up to 1000 such modifications each day, I imagine that this soon becomes a major chore for the Opaserv-afflicted, but AV-protected, user.

Caught Red-Handed

Intrusion Detection System

Yes, you can use an IDS as an anti-malware detection and/or blocking tool.

It is fairly straightforward to create custom malware signatures or rules (especially for SNORT). These can then be used either to log attempts (for later remediation) or to block/drop specific requests or connections.

This is very useful when dealing with new malware for which the anti-virus companies have not yet added detection, or for blocking 'self-updating' or 'phone-home' malware and related risks.

SMB Lure

Since Opaserv first appeared (approx. two months ago), my Internet-facing SMB Lure has trapped over 14,000 samples, yes samples, as I have made some major changes to the basic SMB Lure design that was created by John Morris of *Nortel Networks*. These changes include:

- Sample capture, once the dropped/modified file is completed.
- Intrusion Detection with custom malware signatures (logs IP addresses).
- Integrity checking, so that changed, added or removed files can be handled accordingly.
- MD5 hash table to compare trapped samples against known MD5 hashes of specific malware and variants.

And more improvements are planned.

Router/Firewall/Proxy Logs …

Regular reviews of log files looking for (unusual) quantities of outbound traffic on port 80 to the known 'Opaserv update' or 'non-mainstream' websites:

- http://www.opasoft.com/
- http://www.n3t.com.br/

How Opaserv can be Beaten or Held at Bay

Patching, Patching, and More Patching

Regular system maintenance is imperative. If you didn't learn this from Kak, CodeRed and Nimda, as well as the myriad other malware that have exploited security holes in either an operating system or an application, then you are forever cursed to suffer from such malware until you learn the lesson that malware history has desperately been trying to teach you.

Don't Share

Stop sharing, or change the way you use shares. Windows shares are useful, but should be used as a last resort, and never across the Internet! If you must use Windows shares, then:

1. Ensure that your system is fully patched.
2. Do not share the whole hard disk; share the directories that you need only.
3. Do not allow write access unless you really need to.
4. Use 'User-level access control' rather than 'Share-level access control' as this is slightly more secure.
5. Use a complex password of at least eight characters, and use non-alphanumeric characters too, not just alphanumeric.
6. Use a firewall and/or unbind Netbios over TCP.

Unbind Netbui/Netbios

Unbinding Netbui/Netbios over TCP/IP from Internet interfaces (i.e. Modem/xDSL/Cable) is strongly recommended. See http://www.mikeshardware.com/howtos/howto_disable_netbios.html for details of how to achieve this.

If you must use Netbios over TCP, then install a firewall. Configure the firewall correctly to block Netbios traffic to/from the 'Internet' by default, then set up specific rules to the IP addresses that you require Netbios over TCP for on your 'home' or 'corporate' network.

Conclusions

W32/Opaserv has surprised many people by becoming so widespread. It is highly likely that its success in terms of propagation has been noticed by other malware authors, and that they will add 'SMB' as an extra infection vector to their upcoming releases.

We (at least, the 'great unwashed') should be thankful that the current versions of Opaserv have not been destructive, nor had a nasty payload.

The fact that you are on a 'corporate' network does not mean that you can't or won't see Opaserv.

SMB Lure-based trap systems are useful additions to corporate networks, as they can log the IP addresses of 'internally' infected systems which are looking for new victims to infect. This will allow remedial action to be taken more quickly than would be possible when relying on the network team to notice and/or mention 'strange' or enlarged quantities of SMB traffic and large numbers of outbound requests to a specific site.

Like Roger Thompson's *WormCatcher* (see *VB*, December 2001, p.4), SMB Lure is a very useful early-warning system, and compliments *WormCatcher* well. It is well worth the minimal trouble in setting it up and maintaining it.

Both early warning systems should be considered seriously by organisations to be included as part of a defence-in-depth approach to malware.

With simple modifications SMB Lure can easily be turned into a semi-automated share-aware sample capture system. This is especially useful when Internet facing.

Anti-virus products should block the WIN.INI modifications, as this blocks the worm itself. This would not be difficult to implement, and the inclusion of this feature would help avoid unnecessary panic and anger among the AV product user base.

Finally, have we seen the last of the Opaserv variants? I do not think so … at the time of writing, my trapped sample count has exceeded 18,000.