Painting the Internet: A Different Kind of Warhol Worm

John Aycock
Department of Computer Science
University of Calgary
2500 University Drive N.W.
Calgary, Alberta, Canada T2N 1N4
aycock@cpsc.ucalgary.ca

TR 2006-834-27, May 2006

Abstract

Some people have argued that software is artistic. If so, what about malware?

Only occasional, small-scale attempts have been made to create art using malware. We present "art worms," worms which allow an artist to use the entire Internet as a canvas. These worms could be interactive, allowing an artist to stage a global performance, or non-interactive and automatic. Examples are given of artworks that could result from these worms. Art worms raise a variety of questions about the very nature of art: what constitutes art? must art be seen in order to exist? should art be destroyed?

Two major technical aspects of art worms are communication and geolocation. Both aspects ensure that art worms behave correctly to create an overall picture. We look at a number of ways that malware can perform these tasks, which have broader applications to malware targeted at specific countries for the purposes of terrorism or information warfare.

1 Introduction

> 'There is no reason not to consider the world as one gigantic painting.'
> – Robert Rauschenberg, American artist[1]

It is unusual to find any connections to art in the field of computer security. Even Warhol worms, named after Andy Warhol, refer not to Warhol's art but his famous quote [22]: 'In the future everybody will be world famous for fifteen minutes.' (Warhol worms may infect their targets in less than fifteen minutes [35].)

There is no reason that art and computer security cannot meet. To explore this idea, we present *art worms*. An art worm is a new type of computer worm that turns

[1] Rauschenberg said this in 1961, as quoted by [23, page 255].

infected computers into active participants in an artwork; effectively, the entire Internet becomes the artist's canvas.

Art on this massive scale has been done in the real world. For example, Christo and Jeanne-Claude have used fabric to surround islands in Florida and wrap the Reichstag in Berlin [4]. Large-scale art has not made the transition to the virtual world, but there is every reason to expect that it will. Whether we end up in a dystopian cyberpunk future or not, the Internet is indisputably a critical part of our society today. Given its societal importance, it is inevitable that the Internet will become both a major subject of artistic statements and the medium through which those statements are expressed.

Art is also used to make political statements. The Internet is a tool of capitalism [27]; the Internet is described using distinctively American terms [19]. Either argument, right or wrong, is sufficient to make the Internet an attractive target for anti-capitalist or anti-American artistic statements.

Why has this not been done before? There is in fact some prior art. The possibility of viruses and worms used for art was mentioned in passing in a 2005 article [8], but had already been realized. The Italian artist Luca Bertini released two email worms in 2004, *Yazna* and ++, one seeking the other [6]; it was interpreted as a statement about love [3]. In 2001, the [epidemiC] and 0100101110101101.ORG groups released a virus called *Biennale.py* into the wild for artistic purposes [1]. *Biennale.py* has been interpreted in various ways: performance art [13]; a means of highlighting the elusive nature of computer viruses [10]; a rejection of the computer virus as an evil entity [25]; a demonstration of the link between viruses and the media and, more generally, as a political statement against capitalism [27].

It is thus clear that malware can be used in an artistic sense. But to date, there have not yet been any large-scale examples of malware-as-art such as art worms. In the remainder of this paper, we introduce art worms in detail, examine some artistic questions that art worms raise, and give some other possibilities for how art worms may manifest themselves. We then turn to technical issues presented by art worms, and finally explore the relevance of art worms to computer security.

2 Art Worms

A basic art worm would spread to a computer in some country in the world, find what country the infected computer is located in, and announce a color based on the infected computer's country. To an outside observer, the net result is that every country on a map of the world is given a color.

Even at this crude level of granularity, an art worm can produce pictures. Figure 1 shows a "Coca-Cola" logo – a twisted silver ribbon cutting horizontally through a red background – splashed across the entire globe. This particular example could be interpreted as a statement about "Coca-colonization" occurring via the Internet.

More specifically, an art worm would operate in the following sequence:

1. The art worm's author prepares the worm for release, supplying it with a color table that maps country names into colors. For example, the smiley in Figure 2 – its mouth split in two by the Mediterranean Sea – results from the table below.

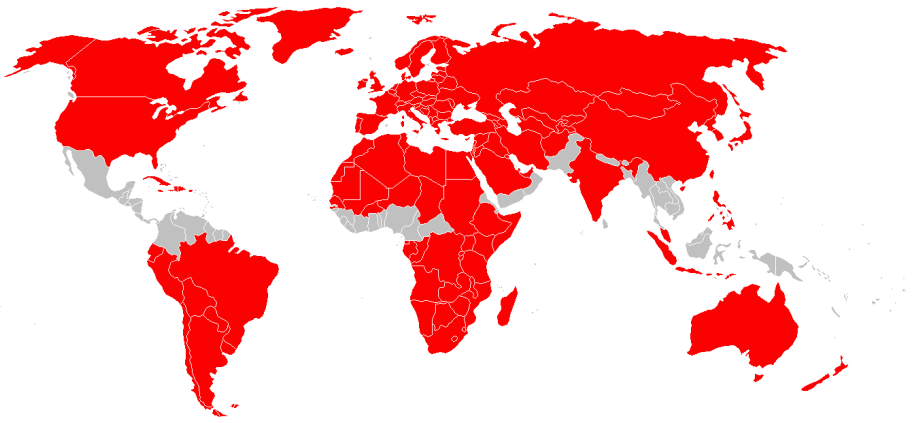

Figure 1: “Coca-Cola” logo on a Robinson projection

Brazil	black	*left eye*
United States	black	*right eye*
Morocco, Western Sahara	black	*nose*
Albania, Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Egypt, Germany, Greece, Hungary, Macedonia, Poland, Romania, Serbia and Montenegro, Slovakia, Slovenia, Sudan	black	*mouth*
All others	gray	

2. The art worm is released into the wild.

3. On every new machine it infects, the art worm determines what country the machine is physically located in. This geolocation is discussed in Section 5.

4. The art worm lies dormant until its activation is triggered. Once triggered, the art worm announces its countries’ color to a central display site established by the art worm author.

   The art worm could easily transmit the color using a protocol unlikely to be blocked by egress firewalls, like HTTP or DNS. For example, an art worm in Brazil with the above color table could do a DNS lookup on `brazil.black.example.com`. If the art worm author’s DNS is authoritative for `example.com`, then all DNS lookups (i.e., color transmissions) can be monitored.

   The trigger itself must be a signal that all infected machines can see at the same time, yet checking for the signal should not produce suspicious network traffic or disclose the location of the art worm author. The signal could simply be a predetermined UTC time and date, in which case no network traffic is required, but a captured art worm will reveal the triggering details. The signal could instead be placed in a web page by the art worm author; the art worm could periodically

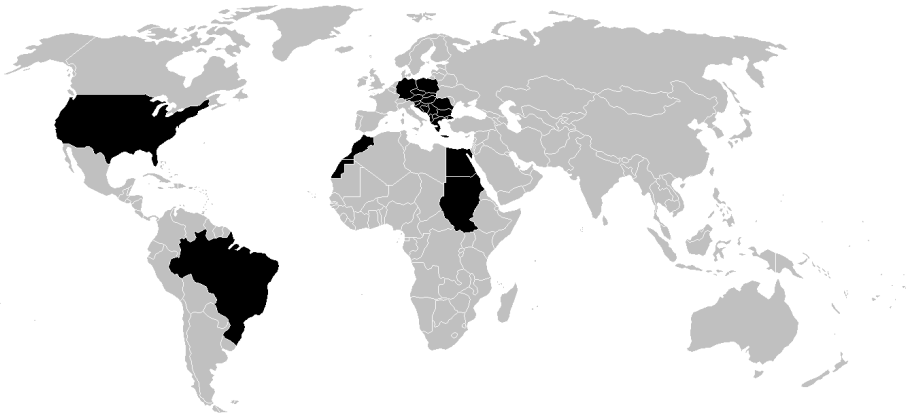

Figure 2: Smiley on a Robinson projection (rotate clockwise 90° to view)

use a web search engine to look for the signal without attracting undue notice. More elaborate trigger mechanisms are also possible (e.g., [24]).

5. The central display site aggregates responses from the worm and shows them on a map. The color a country is rendered in would be based on the majority of responses received that claimed to be in that country, to filter out noise. Noise may be introduced various ways: the geolocation done by the worm may be somewhat inaccurate, and portable devices like laptops and mobile phones may cause an infection to move from country to country.

The maps in Figures 1 and 2 are Robinson projections [31], a commonly-used map projection for world maps. The central display site may of course use this or any other type of map projection. More generally, the world map can be abstracted into a graph, where countries are nodes; an edge connects two nodes *A* and *B* if country *B* can be reached from country *A* by traveling in a straight line, without passing through any other countries. Section 4 gives applications of this graph representation.

3 Questions Raised

Art worms raise a number of artistic questions. This section looks at three key questions, whose answers shed light on whether or not an art worm will exist, what form it will take, and the interaction between art worms and worm defenses.

3.1 Is an Art Worm Art?

This question can be interpreted two ways. First, does art result from the actions of an art worm? It must: the art worm is providing an Internet-scale virtual canvas upon which pictures can be painted. As with any canvas, those pictures could be considered art. Perhaps not *good* art, but 'bad art is still art' [12, page 74].

Second, is the art worm itself art? As mentioned in the Introduction, the Internet is an attractive target for artistic statements about modern society and politics, and the art worm is a way of doing this. There is even a genre of art called "Internet art" [18]. That, plus the fact that *Yazna/++* and *Biennale.py* were interpreted artistically, makes a strong case that art worms would be treated the same way.

Nor is legality necessarily a limiting factor in art. This is a consideration because releasing worms and viruses is illegal in many (if not most) jurisdictions. Yet *Yazna/++* and *Biennale.py* were released in spite of this. Graffiti – some examples of which are definitely artistic – continues to flourish in the real world regardless of laws against it, and the picture an art worm produces can be thought of as graffiti on a global scale.

3.2 Must Art be Seen to be Art?

An art worm could simply perform its task by changing the background color of an infected machine. Neither the artist nor the victims of the art worm would be able to see the whole artwork. Somewhat surprisingly, this would still be considered art even if no one could view it in its entirety.

There are many different theories of art. Some, like expression theory, require art to have an audience in order to be art [12]. However, even this theory does not require all of an artwork to be seen. There are also some works of art where it is physically impossible to experience the whole thing:

- John Cage's piano composition *ASLSP*, which stands for "as slow and as soft as possible" [29], is having its title taken in a very literal sense. The work is currently being played on an organ in Halberstadt, Germany; the performance will take place over a period of 639 years [32].
- Walter de Maria's piece *Vertical Earth Kilometer* [5] is a one-kilometer-long rod sunk into the ground in Kassel, Germany. Only the very top is visible.

Despite these exceptions, it is fair to say that the vast majority of art does admit an audience. If the product of art worms was not viewable somehow, it would severely limit their artistic utility. We must assume that art worms will transmit their color to a central site where the artwork can be seen as a whole.

3.3 Should Art Worms be Removed?

If an art worm is art itself, or is helping to create part of an artwork, then disinfecting a computer and removing the art worm in effect destroys the art. It is safe to assume that anti-virus companies would not hesitate to have their products remove art worms, but is this akin to burning books?

We argue that it is both practically and philosophically sound for malware defenses to remove art worms. Many forms of art are temporal in nature, like music and dance. Ice sculptures are made with the expectation that they will eventually melt. Art worms are temporal, too, created with the knowledge that worm defenses will turn each art worm into an endangered (but maybe not extinct) species.

It is also possible to view disinfection not as the end of an art worm's life cycle, but as the beginning. In other words, the pattern of worldwide disinfection would itself be the art, making anti-virus vendors and computer users active participants in the artwork.

4 Other Artistic Possibilities

There are many other possibilities for art worms beyond the basic version described in Section 2. We consider four in this section.

First, the type of art can be changed. A musical tone could be played instead of painting a color. Or a collage could be constructed: each art worm would contribute a picture or document from an infected machine, which would be made into a collage at the central display site. The latter task need not involve a human artist, because automatic techniques for making aesthetically-pleasing collages are known [15]. A slight variant on this theme is to construct photographic mosiacs with pictures from infected machines. Again, there are automatic techniques for doing this [34]. Art worm collages and photographic mosaics obviously present enormous privacy problems.

Second, animations could be made instead of static pictures. Like the color table, animations could be arranged in advance by the art worm author and distributed with the worm. A series of trigger signals is indicated, probably time-based, to keep the worms in synchronization as they play the animation to the central display site.

Third, the art worms could produce the artwork themselves. This is the realm of "generative art" [16]; the art worm author would not provide a color table, but would supply rules the art worm would use to generate its own painting, possibly through interaction between infected machines. This explains why the central display site does not simply colorize countries itself, rather than use color information from the worms – the display will not know what colors to use if they are generated by the worms.

Models of computation like cellular automata [33] and swarm intelligence [7] are well-suited to art worm interactions, because these models only require local communication. The graph-based world map representation mentioned in Section 2 is useful here: each graph node can be a cell, or the graph topology can be traversed by a swarm. This naturally leads to the idea of having the art worms generate an animation. For example, infected machines could play Conway's Game of Life [17] amongst themselves, transmitting the state to the central display site after each generation.

Fourth, the art worms could be interactive – the art worm author or Internet users could "conduct" an art worm performance. Conducting can range from influencing a moving swarm [9] up to real-time painting on the art worm's canvas. The communication required for conducting presents some interesting technical challenges.

5 Technical Issues

We look at two technical issues in this section: geolocation and conducting communication.

5.1 Geolocation

Geolocation is the determination of the geographical, real-world origin of a network connection. It is commonly pitched on the basis of delivering content customized to a particular location [21] or as a fraud prevention measure [21, 28]. *Reverse geolocation* is the related problem of having a computer determine where it is geographically located [11]. Intuitively, geolocation asks "where are you?" and reverse geolocation asks "where am I?"

To the best of our knowledge, no malware is currently performing either type of geolocation. Art worms require a solution to the reverse geolocation problem,[2] though, so they can identify the country of an infected machine. We limit our discussion here to practical solutions which are amenable to automation in malware; a fuller geolocation survey can be found in [26].

There are four likely candidates for reverse geolocation by malware. The first two are high-accuracy, the last two less so:

Ask. An increasing number of mobile computing platforms like cellular phones have the capability to pinpoint their location. This information can be used by emergency services and applications providing map directions, for example [36]. An art worm located on such a mobile platform may simply be able to ask for its position, which can be mapped into a country name.

Use existing services. Art worms can leverage existing Internet services whose web pages attempt to geolocate a connecting site, like `www.ip2location.com` or `www.hostip.info`. This approach has a number of advantages, because the art worm's reverse geolocation will look like ordinary HTTP traffic, and an established geolocation provider may already use a plurality of methods to gather its information [2] that the art worm need not duplicate. Some geolocation providers claim country-level accuracy rates as high as 95% [20] and 99.9% [28]. Art worms could try using information from existing `whois` services in a similar fashion.

TLD information. Some domain names have country codes for their top-level domain (TLD), like `.ca` (Canada) or `.uk` (United Kingdom). The TLD could be used by an art worm for reverse geolocation. However, there are major TLDs that are not country-specific, such as `.com`, and some TLDs have actively sold their subdomains worldwide (e.g., `.tv`).

Latency information. Reverse geolocation has been attempted by trying to correlate network latency with geographic location [11]. One of the main drawbacks to this approach, from the art worm point of view, is that lots of network traffic is required to take latency measurements. This traffic might prematurely reveal the presence of an art worm on an infected machine.

The precision of reverse geolocation is critical to the resolution of the art worm canvas. Advances in (reverse) geolocation will directly benefit art worms.

[2] Strictly speaking, a worm could attempt to geolocate a targeted computer upon infection instead of reverse geolocation after infection. Most of the solutions discussed here apply to either scenario.

5.2 Conducting Communication

Unless an interactive art worm is meant to be obvious and short-lived, then there are a severe set of constraints on communication for conducting the worm. Communication must be covert; it need not reach all infected machines; it must be scalable; transmissions should be limited; it should be very hard to trace the communication source; it should be resistant to false signals being inserted; it should be sustainable over a long period of time; it should be (near) real-time. We are currently looking into mechanisms that meet these criteria.

6 Who Cares?

While co-ordinated, large-scale virtual art has not yet been seen, the prospect of art worms appearing increases with our society's dependence on the Internet.

The techniques used by art worms have wider application. Methods are already known to construct malware that is strongly resistant to analysis and that can target specific groups of people [14, 30]. Malware using geolocation and reverse geolocation for targeting has not made its debut, as far as we know, but it has obvious applications for information warfare and Internet-enhanced terrorism. Conducting communication could be used for directing extended network attacks.

Research can and should be undertaken now to address art worms and their attendant applications.

7 Acknowledgments

The author's work is supported in part by a grant from the Natural Sciences and Engineering Research Council of Canada. Margaret Nielsen and Leila Sujir pointed me to several art resources, Ehud Sharlin mentioned the German *ASLSP* performance, and Jörg Denzinger provided a translation of [32]. The blank Robinson projections are by Vardion and are in the public domain.

References

[1] 0100101110101101.ORG. Contagious paranoia. http://0100101110101101.org/-home/biennale_py/story.html, Retrieved 14 April 2006.

[2] M. Anderson, A. Bansal, B. Doctor, G. Hadjiyiannis, C. Herringshaw, E. E. Karplus, and D. Muniz. Method and apparatus for estimating a geographic location of a networked entity. United States Patent #6,684,250, 27 January 2004.

[3] M. Antonini. Secretly out there. *NY Arts Magazine*, 9(9/10), 2004.

[4] J. Baal-Teshuva, editor. *Christo: The Reichstag and Urban Projects*. Prestel-Verlag, 1993.

[5] G. Baker and C. P. Müller. A balancing act. *October*, 82:95–118, 1997.

[6] L. Bertini. Vi-Con. http://vi-con.net, Retrieved 14 April 2006.

[7] E. Bonabeau, M. Dorigo, and G. Theraulaz. *Swarm Intelligence: From Natural to Artificial Systems*. Oxford University Press, 1999.

[8] G. W. Bond. Software as art. *Communications of the ACM*, 48(8):118–124, 2005.

[9] J. E. Boyd, G. Hushlak, C. J. Jacob, P. Nuytten, and M. Sayles. SwarmArt: Interactive art from swarm intelligence. In *Proceedings of the 12th Annual ACM International Conference on Multimedia*, pages 628–635, 2004.

[10] R. Buiani. Marginal networks: The virus between complexity and suppression. *fibreculture*, 4, 2005.

[11] C. G. Carr III. Reverse geographic location of a computer node. Master's thesis, Air Force Institute of Technology, 2003. AFIT/GCS/ENG/03-04.

[12] N. Carroll. *Philosophy of Art: A Contemporary Introduction*. Routledge, 1999.

[13] J. Farman. The virtual Artaud: Computer virus as performance art. *Extensions: The Online Journal of Embodied Technology*, 2, 2005.

[14] E. Filiol. Strong cryptography armoured computer viruses forbidding code analysis: The Bradley virus. In *Proceedings of the 14th Annual EICAR Conference*, pages 216–227, 2005.

[15] J. Fogarty, J. Forlizzi, and S. E. Hudson. Aesthetic information collages: Generating decorative displays that contain information. In *Proceedings of the 14th Annual ACM Symposium on User Interface Software and Technology*, pages 141–150, 2001.

[16] P. Galanter. What is generative art? Complexity theory as a context for art theory. In *GA2003 – 6th Generative Art Conference*, 2003.

[17] M. Gardner. The fantastic combinations of John Conway's new solitaire game "life". *Scientific American*, 223(4):120–123, October 1970.

[18] R. Greene. *Internet Art*. Thames & Hudson, 2004.

[19] S. Helmreich. Flexible infections: Computer viruses, human bodies, nation-states, evolutionary capitalism. *Science, Technology, & Human Values*, 25(4):472–491, 2000.

[20] IP2Location. IP2Location IP-country database FAQ. http://-www.ip2location.com/README-IP-COUNTRY.htm, 2006.

[21] IP2Location. IP2Location: Bringing geography to the Internet. http://-www.ip2location.com/ip2location.pdf, Retrieved 14 April 2006. Brochure.

[22] E. Knowles, editor. *The Oxford Dictionary of Quotations*. Oxford University Press, 1999.

[23] M. L. Kotz. *Rauschenberg: Art and Life*. Harry N. Abrams, Inc., new edition, 2004.

[24] H. H. Lee, E.-C. Chang, and M. C. Chan. Pervasive random beacon in the Internet for covert coordination. In *7th International Workshop on Information Hiding*, pages 53–61, 2005.

[25] A. Ludovico. Virus charms and self-creating codes. I love you – computer_virus_hacker_culture, 2003. digitalcraft's exhibition on computer viruses.

[26] J. A. Muir and P. C. van Oorschot. Internet geolocation and evasion. Technical Report TR 06-05, School of Computer Science, Carleton University, April 2006.

[27] J. Parikka. Digital monsters, binary aliens – computer viruses, capitalism and the flow of information. *fibreculture*, 4, 2005.

[28] Quova. Geolocation – fraud prevention for online financial services, 2005.

[29] J. Retallack, editor. *Musicage: Cage Muses on words, art, music*. Wesleyan University Press, 1995.

[30] J. Riordan and B. Schneier. Environmental key generation towards clueless agents. In *Mobile Agents and Security (LNCS 1419)*, pages 15–24, 1998.

[31] A. H. Robinson. A new map projection: Its development and characteristics. *International Yearbook of Cartography*, XIV:145–155, 1974.

[32] K. Rohring. As slow as possible. *Musik und Kirche*, pages 348–349, 2000.

[33] P. Sarkar. A brief history of cellular automata. *ACM Computing Surveys*, 32(1):80–107, 2000.

[34] R. S. Silvers. Digital composition of a mosaic image. United States Patent #6,137,498, 24 October 2000.

[35] S. Staniford, V. Paxson, and N. Weaver. How to 0wn the Internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, 2002.

[36] G. Sun, J. Chen, W. Guo, and K. J. R. Liu. Signal processing techniques in network-aided positioning. *IEEE Signal Processing Magazine*, pages 12–23, July 2005.