Global Information Assurance Certification Paper

HYBRIS – The Worm Turns.
Greg Smith
February 5, 2001

Date line September 1999 – SANS Birds of a Feather group meeting in New Orleans track down a new virus with startling new features and name it Ring-Zero Trojan. This new virus has an ominous ability. It appears the virus has, among its many features, the ability to contact external sources and download controls that can alter its mission on the fly.

I'll See your Ring-Zero and raise you Hybris.
Ring-Zero introduced a new level of complexity in the battle against malware (malicious code) assaults and caused the security community a good deal of concern. Move the calendar forward 12 months and we have a new threat identified by the folks at Kaspersky Lab as a rework of the Hybris worm first discovered "in the wild" (a euphemism for watch out!) at the end of September, 2000. The worm was originally classified a low risk by virus specialists. In fact, many of the anti-virus web sites still list Hybris as a low risk virus.

According to an article published November 13, 2000 in Newsbytes, Kaspersky Labs warns the revamped Hybris Worm is highly dangerous. This worm spreads as an attachment to e-mail messages, works only on Win32 systems and contains components (plug-ins) in its code that are executed depending on its needs! And oh yes, can be upgraded from an Internet web site or Usenet newsgroup "alt.comp.virus". Detailed information about this worm can be found at:
http://www.viruslist.com/eng/viruslist.asp?id=4112&key=00010001300001000 44.

The article goes on to say the major worm versions are encrypted with a semi-polymorphic encryption loop. The main target of the worm is the WSOCK32.DLL. The coding technique for infecting this standard Windows DLL increases its probability of infection considerably and is a good indication of the sophistication at work in this worm. Once infected, the worm is able to intercept Windows network functions that communicate via TCP/IP such as SMTP, HTTP, FTP and any other application that makes calls to the Winsock DLL. One thing we know this worm does is look for e-mail addresses in packets and if found sends an infected e-mail message to that address, the proverbial tip of the iceberg as it were.

Ring-Zero On Steroids
The Hybris worm has taken the concept of remote control, introduced in Ring-Zero, to a new level using "plug-ins" to determine its mission. Ring-Zero employed a mechanism to download an encrypted file from an external source. This file directed the Trojan's activities, was saved locally and could be consistently identified. The Hybris "plug-ins" are downloaded and saved locally too, but are saved in encrypted form using a random naming convention making discovery much more difficult. Hybris also introduces the ability to "update" plug-ins based on the "name" and "version" of the plug-in found on

remote servers. These plug-ins are encrypted with an RSA like crypto algorithm, making it very difficult for outsiders to determine what is contained within the plug-in.

One significant concern is the ability of the worm to alter its signature with these plug-ins making detection by virus scanning tools more difficult. According to Eugene Kaspersky, head of the company's Anti-Virus Research Center, "What we have here is perhaps the most complex and refined malicious code in the history of virus writing. Firstly, it is defined by an extremely complex style of programming. Secondly, all the plug-ins are encrypted with a very strong RSA 128-bit crypto-algorithm key. Thirdly, the components themselves give the virus writer the possibility to modify his creation "in real time," and in fact allow him to control infected computers worldwide."

Compare the above comments by Mr. Kaspersky with those posted on another Anti-Virus vendor's web site in mid-November and you can begin to appreciate the extent of the challenges we face in the Information technology business:

> **"Navidad and Hybris viruses pose low threat to users practising safe computing says Sophos Anti-Virus**
>
> Sophos Anti-Virus, one of the world's leading developers of anti-virus solutions, today called for calm regarding two new viruses, Navidad and Hybris. Sophos urges computer users to follow safe computing guidelines, following media interest and a decision by the US Army to rate Hybris as 'high risk'.
>
> The viruses have been spreading in the USA and South America, and have already hit a small number of UK companies. However, they pose no real threat to users practising safe computing or to users running up-to-date anti-virus software.
>
> "No computer-savvy person would open an unsolicited executable file they received via email," said Graham Cluley, senior technology consultant at Sophos Anti-Virus. "If users took on board this simple safe computing message, viruses like Navidad and Hybris would spread about as well as frozen butter."
>
> Most anti-virus products have been capable of detecting both viruses since early November and Sophos advises users to download the latest anti-virus virus protection from their vendor."

First, e-mails with malware attachments sometimes appear to come from someone we know and the natural tendency is to trust its origins. Second, if the anti-virus vendors don't know about a particular virus/worm/trojan their products may not be able to detect it. In the case of a worm like Hybris, this could be disastrous. The user may not discover the infection and depending upon the worm's plug-in payload may inadvertently become a launch point for surveillance, destructive, or other unknown activities at some later date. And finally, if the worm can indeed change its signature regularly, anti-virus vendors may have a much harder time detecting this guy once it is in place. We know that all it takes is one mistake and we're off to the races. In many of my personal experiences

responding to virus outbreaks, the users admitted they should have known better but went ahead and clicked the attachment anyway. According to press releases and my own experience, this happens pretty often!

Incidentally, Sophos reported on February 5, 2001 the detection of Hybris.Drop, which is an executable file that drops the I-Worm.Hybris worm. Files carrying Hybris.Drop are created by Hybris using one of its upgradable components. One down, 31 (plug-ins that is) to go!

The Faster I Run the Further Behind I Get.

Malware developers have a bad habit of learning from others and incorporating the latest features into their own creations. It's a story as old as time. Man invents widget (read virus), widget is cloned into a better widget and so on. If we can agree on this one simple point, then it's easy to see the threat of malware as very compelling to us all. I've taken to using the term malware as have others in the profession simply because these applications are more frequently straddling the traditional definitions. Hybris was originally described as a worm (*self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. To get rid of a worm you just need to delete the program*) but could exhibit characteristics of a Trojan (*program masquerading as benign application but is destructive – doesn't replicate*), and certainly does sound like a Virus (*a piece of code loaded onto your machine without your knowledge and runs against your wishes – does replicate*). Maybe we need a new term – how about virman a.k.a. vermin (VIrus/woRM/TrojAN)?

With so many avenues into an organization (*incursions can happen through embedded code in Word, Excel, Powerpoint, Windows help files, screen savers, java or activex HTML, or the venerable diskette to name a few*) and with malware evolution continuing at an impressive rate, the need to assess an organization's current strategies and adjust to the realities of these new threats should be abundantly clear. Organizations should assume infection in the future is likely, that the virus infecting the organization will be as capable as the Hybris variants we've been discussing, and discovery/eradication by traditional anti-virus products may be unreliable. Motivation should be high to counter this threat with tools that can detect an intruder's presence on our systems and in our networks. It is no big stretch to develop a scenario where thousands of computers worldwide are infected with these new malware variants exposing our personal computers, our company networks, and indeed the national infrastructure to surveillance (targeted and/or nuisance), DDoS attacks, espionage, and other disruptive activities.

Vulnerable systems are all around us.

We are surrounded by threats and vulnerabilities in this new eWorld. From computers without anti-virus protection to computers plugged directly into the Internet without firewall or NAT'd router. Marketiers would have us believe this new eWorld is a wonderful place full of great things, but make no mistake – the threats and vulnerabilities are numerous and affect us all. Attacks from e-mail attachments are commonplace and I can personally speak to unprotected systems plugged directly into the Internet from my own experiences conducting security assessment audits for my customers. One of the steps in our assessment is to check the network "neighborhood" in close proximity to the

customer's Internet connect point. From these experiences, I can tell you that hundreds of systems are currently plugged into the Internet with no safeguards in place (other than the on/off switch on their computer). When I say no safeguards, I mean map a network drive to the stranger's C$ share-point without a required password ending up with read/write permissions all the way down the tree. This is not earth-shaking news to security professionals, but to the average person on the street, this is still an abstraction as are the consequences. With this level of awareness all around us, the likelihood of subversion is ensured and the repercussions are unpredictable.

Brace yourself – Incoming!

For the security conscious, all we can do is run faster, work longer, and yell louder. It seems so obvious to those of us who work in the trenches what's just over the horizon – and it's not paradise. We know what to do. Make sure the anti-virus programs are in place, current, and covering all systems small and large. Make sure all of our Operating Systems have been "hardened" – that is; file and folder permissions set properly, system control files protected, activities audited, holes plugged and patched, user ids and passwords protected, password complexity enforced. If we don't already have one, get an Intrusion Detection System (both network and host based) in place so we have half a chance of detecting an outbreak of the next generation of Hybris when it erupts. Check and double-check our backup and restore procedures regularly. Scan our HTML and FTP traffic as well as our e-mail for malicious code. Test our firewalls, proxy servers, and other perimeter defenses regularly. Encrypt all data in transit or stored on computers that we want remaining private and confidential. Make sure our telecommuters are running anti-virus and personal firewalls on their computers and their computers are checked regularly for compliance with security policies. And never, ever go to sleep.

The history of malware and anti-virus developers has always been one of cat and mouse. A new virus shows up and the anti-virus vendors quickly respond to neutralize the threat. But what if the Hybris worm can substantially change its signature and elude virus detection. And what if this worm can be manipulated remotely and it's functions altered. The means by which we are left to deal with this threat are certainly going to require a sophisticated level of expertise. If active scanning of our anti-virus software won't detect it then we're left with the more time consuming tasks of closely monitoring logs for unusual activities or hoping our Intrusion Detection Systems (IDS) pick up the anomalous entries that might give its presence away. That is, if we have the manpower and logs to monitor or if we have an IDS monitoring for us.

Businesses at the lower end of the food chain are not going to have the levels of expertise to identify they have a problem let alone eradicate it. And if these businesses were partners with larger businesses connected by way of a VPN, what effect would a breach have on their relationships?

What would the implications be for you and me if this worm was so effective at the art of stealth that it remained on our computers for months running undetected, perhaps until a Microsoft® update replaced the rogue DLL?

Let's put our rose colored glasses back on for a moment and discount the severity of this new worm. Let's pretend the anti-virus programs can effectively deal with this new threat as the Sophos release indicates. And let's pretend that it will take a couple more years or so for a revised version of Hybris to show up on the scene with new and more challenging features. And let's not worry that it took a mere twelve months from the time the Ring-Zero trojan arrived on the scene until the first reports of the Hybris worm surfaced. Based on simple math, we have seven whole months before we have to worry about this again!

References:

1. **Symantec.** "W95.Hybris.gen" 25 September 2000. Http://service1.symantec.com/sarc/sarc.nsf/html/W95.Hybris.gen.html
2. **Trend Micro Virus Encyclopedia.** "Troj_Hybris.B" 25 September 2000. Http://www.antivirus.com/vinfo/virusenclyclo/default5.asp?Vname=TROJ_HYBRIS.B
3. **Kaspersky Lab.** "AVP Virus Encyclopedia – I-Worm.Hybris" 13 November 2001. Http://www.viruslist.com/eng/viruslist.asp?id=4112&key=000010001300001000044
4. **Internet News.** "Hybris Worm Prowls the Net, Awaits Lethal Plug-ins" 13 November 2000. http://www.internetnews.com/streaming-news/article/0,,8161_509721,00.html
5. **Newsbytes.** "Kaspersky Lab Warns Over Revamped Hybris Worm". 13 November 2000. Http://www.newsbytes.com/news/00/158042.html
6. **ZiffDavis News.** "New hybrid worm is looking troublesome" 14 November 2000. http://www.zdnet.co.uk/news/2000/45/ns-19060.html
7. **Computer User.** "Kaspersky Lab Warns Over Revamped Hybris Worm". 14 November 2000. http://www.computeruser.com/news/00/11/14/news3.html
8. **PlanetIT.** "Hybris: A Stealth Virus With Plug-ins". 9 January 2001. Http://www.planetit.com/techcenters/docs/security-hostile_content/news/PIT20010109S0021
9. **National Infrastructure Protection Center.** "CyberNotes" 29 January 2001. Http://www.nipc.gov
10. **CERT/CC Current Activity.** "Virus Activity" 31 January 2001. Http://www.cert.org/current/current_activity.html