NETWORK SECURITY FOR SUBMARINE NETWORKS

Mounish Patel (Cable&Wireless Worldwide)

Email: Mounish.patel@cw.com

Cable&Wireless Worldwide, 32-43 Chart Street, London, N1 6EF, United Kingdom

Abstract: Submarine telecommunications cables are the backbone for 95% of all voice and data traffic carried around the world. Governments now view submarine telecommunications as part of the critical infrastructure of a nation that deserves the highest level of protection. Submarine telecommunications cables are an obvious target for global terrorism. The use of anti-virus software is currently non-existent on submarine system management equipment and craft terminals. Other organisations have suffered the effects of malware attacks; it is suggested that submarine system operators take action to protect their network management systems in case they become targets. This paper discusses physical as well as logical network security vulnerabilities and possible measures to protect or limit the management system and craft terminals from exposure to malware and cyber-attacks.

1. INTRODUCTION

Mr Charles Bright FRSE, one of the founders of telegraph cables and son of the famous Sir Charles Bright, is quoted as saying "he had little doubt that cables will be cut right and left in time of war" [1]. His foresight was correct as the events of the first and second world wars showed. In today's world of highly complex telecoms nothing has really changed except there are new methods of cutting cables. It is reasonable to suggest that in time of cyber war and cyber terrorism cable networks will be targeted persistently by state-sponsored hackers or terrorists.

This paper discusses the threat posed by general malware as well as targeted attacks. Also discussed is the lack of anti-virus software and physical security to protect submarine cable management systems. A report [2] by an anti-virus company McAfee Labs® predicts that the malicious behaviour by organised criminal gangs and hackers will grow in 2013. A speech given by the US secretary of defence on 12th October 2012 highlighted the threat posed by individuals, terrorists and rogue governments to wage cyber-attacks on critical infrastructures, telecommunications being one of them. [3]

2. WHAT IS MALWARE?

Computer viruses, worms, Trojan horses, spyware, key loggers etc. all come under the heading of malware.

Malware is created and used by hackers, governmental agencies and criminals to disturb computer operation, steal sensitive information, and gain access to private systems.

With the advent of personal computers and increased availability of broadband, infection rates of malware has also increased, with large corporations reporting various forms of advanced attacks into their networks on a regular basis. Whilst some of the attacks are reported, the majority are not. In May 2012 Microsoft® reported that one in every 14 downloads now contains some form of Malware. Figure 1 shows the percentage of various forms of malware in circulation in 2011.

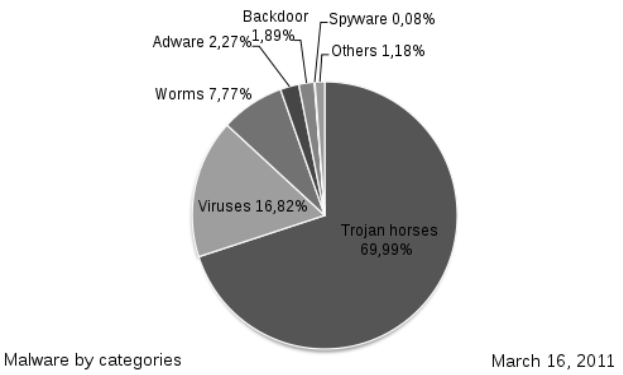

Figure 1: Malware by Categories [4]

3. OPERATING SYSTEMS AND MALWARE

Microsoft® operating systems are the dominant operating systems in use on personal and corporate computers around the world, and consequently have the highest rate of malware infections as well as attacks. In 2012 Microsoft® published a report on security [5] which showed the highest number of advanced persistent threats (APTs) was on Windows XP® operating systems, as shown in Figure 2.

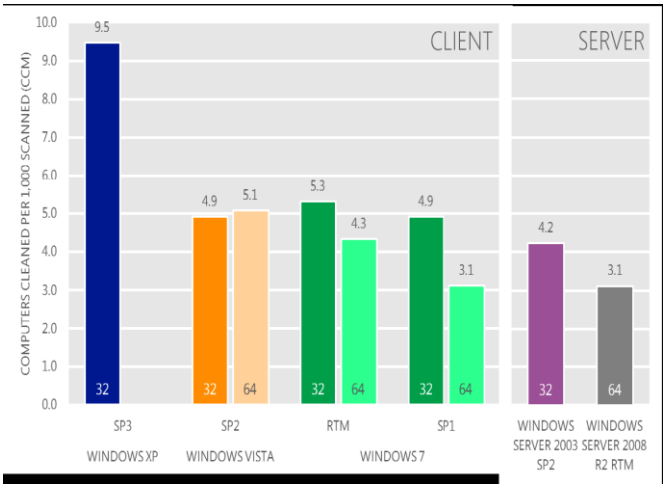

Figure 2: Chart from Microsoft Report 2012

Apple® OS (operating systems) have shown to have lower infection rate but are not invulnerable from malware attacks. In 2012 approximately 600,000 Macs were infected with a Trojan virus called Flashback. The Trojan was hidden in legitimate software and caused each of the Macs to be hijacked and used as a 'botnet' (term used for computers controlled as a group without the owner's knowledge). UNIX-based operating systems are not invulnerable and have also experienced an albeit lower level of attacks. The reason why there has never been a full scale infection is that the virus cannot reach its full potential in the UNIX operating system's hostile environment at this time, but in the future the virus code writers will probably overcome this. Both UNIX and Microsoft® operating systems are used for submarine cable network management.

4. DEFINITION AND TYPES OF VIRUSES

4.1 Virus

A virus gets its name for the way it reproduces and spreads; it is very closely analogous to the behaviour of a biological virus. In the same way that biological viruses exploit many strategies to reproduce, computer virus writers are very creative and devious. In most cases, human action is required for the virus infection to occur and spread by running a malicious program which is then spread by sharing infected files. The main virus types with their strategies are listed below. Many thousands of viruses of these types are currently circulating and are a general risk to the network management system.

- **Boot sector virus:** Attaches itself to the first part of the hard drive and is read upon boot up.
- **Micro virus**: hidden within documents like MS Word®, MS Excel®.
- **Rootkit virus:** enables remote users to gain control of the host computer.
- **Polymorphic viruses:** change their digital signature every time it replicates making it difficult to detect.
- **Logic bombs:** programs that are initiated on specific dates, times or actions.
- **Stealth Virus:** The virus hides itself in the system memory.

4.2 Reported Virus attacks

General viruses have been in circulation for many years. There are anecdotal reports of submarine network management systems being infected and suffering minor difficulties. As far as can be found by this author, no network operator has publicly admitted a problem and it seems unlikely any operator has lost traffic as a result. However, it is worth noting that Symantec® in its 2012 data breach investigations report [6] reported that Verizon® had 174 million records compromised by cyber-attack in 2011.

More serious are viruses written to attack a specific target. There were a number of high-profile targeted attacks in 2012. For instance, 30,000 workstations at the world's largest oil company (Aramco®) suffered a virus attack by a group called 'Cutting Sword of Justice' who have a grievance with the Saudi Government. Although there was no disruption in the production of oil following this attack, the consequences could have been disastrous if the safety override systems had been tampered with or shut down. Two US energy plants suffered a malware attack inadvertently introduced by an employee, who routinely used a USB memory storage device for backing up data in 2012.

In 2010 Iran's Natanz nuclear facility was attacked by a highly destructive virus called Stuxnet, introduced via a USB storage device. The attack temporarily crippled Iran's nuclear programme by destroying roughly one fifth of the nuclear centrifuges. It was made up of a Windows virus designed to infect the laptops of maintenance technicians, once the technician connected to the centrifuge process controller it then downloaded a small program to disrupt it. It was designed to attack vulnerability of the Siemens control systems and subtly confuse the operator whist damaging the equipment.

4.3 Definition and types of Worms

A worm is similar to a virus, but with an enhanced ability to replicate itself. Instead of an infected computer sending out a single copy of the worm, it sends out hundreds or even thousands of copies. Worms do not require human intervention to spread and take advantage of transport features on the system. A major infection can result in consumption of system memory or network bandwidth. Some examples of worm infections are given below.

- **The ILOVEYOU worm** attacked millions of computers running Windows in 2000. Not only did the worm send copies of itself but made a number of malicious changes to the infected computer. The ILOVEYOU worm also affected large corporations and governments, including the Pentagon in the United States. The total cost of the damage caused was $15 billion.
- **Flame** In 2012 a number of Middle Eastern sites were targeted with a Stuxnet-like worm called Flame designed to steal technical information.
- **Viper.** On 28 May 2012, Kaspersky Lab and ITU Research discovered a new and advanced cyber threat in the form of a highly sophisticated worm codenamed Viper. The complexity of this malware program exceeds all the known syber menaces to date [7].

4.4 Definition of a Trojan?

Contrary to popular belief a Trojan neither reproduces nor self-replicates so is not classed in the same category as a virus or a worm. As its name suggests from Greek mythology, the Trojan is a vessel designed to carry what appears to be useful or legitimate software, but carries an infected file. Once opened and uploaded, the results can be unpredictable. Some Trojan programs are designed to be annoying whilst others are designed to cause serious damage, or open a back door to your network or computer.

4.5 Blended Threats: a New Form of Malware

Blended threats are sophisticated forms of malware that spread using vulnerabilities in the internet and servers. Blended threats are considered the worst form of malware attacks as they spread via combinations of Trojans, worms, malicious code and viruses. The use of multiple malware gives the blended threat a greater chance of success as it uses multiple attack vectors to increase chances and speed of infection.

5. WHAT ARE THE CONSEQUENCES OF A MALWARE ATTACK ON A SUBMARINE SYSTEM?

For most general malware attacks on a submarine system, the network management system would be compromised but probably usable in some part. The network might be controllable from some terminals but not others. If all terminals were disabled the system would continue to carry traffic although there would be no visibility of its performance. It is probable in this situation that craft terminals could be used to manage the terminal equipment unless in the confusion they also had become infected. At its most severe, recovery would involve re-imaging all the affected machines. Traffic would only be lost if the attack coincided with an equipment failure thus hindering repairs.

A more serious infection would be a deliberate targeted attack. This could leave the traffic disabled while reporting to the operator that the system is working correctly. It may even be possible to make an operator believe there is a submerged plant fault. A virus writer with sufficient knowledge may be able to make the system report a repeater failure while switching off the terminal line cards. Such a deliberate attempt to confuse and disrupt could lead to a long traffic outage and a coordinated attack could leave a country isolated.

The example of Stuxnet shows such attacks are possible. It is interesting to note that although Stuxnet was highly targeted, its overall construction was generic. It could be re-written for a different target.

An attack would need to be carefully planned and would need a group of skilled software writers. Some members of the group would need to be experienced in writing viruses, but more critically some would need direct experience of working on vendors' network management systems and/or terminal software.

Members of the group would most likely be motivated by patriotism or ideology which raises a serious question for the vendors: how well do you know your software writers and what level of security clearance do you require?

6. PHYSICAL NETWORK SECURITY

Once an intruder has physical access to the equipment, all other security setups will be ineffective. Physical security should thus be designed to support network security to disable unauthorised access by an individual or individuals into the network. Network security planning requires the same level of care as is applied to the physical security of the building.

Considerations to take into account during planning include the following:

- Control of physical access by use of locks, card keys, bio scanners etc.
- Rack mounted servers and the use of racks with lockable doors
- Set up surveillance
- Secure work stations and laptops
- Secure backups
- Lockdown all unused ports on routers and switches
- Human firewall as first line of defence by raising awareness and vigilance amongst cable station and NOC employees.

7. NETWORK SECURITY

Network security should be designed to protect what the physical security cannot, such as a malware attack. Network security methods include:

- Network based Firewalls
- End Protection Antivirus Software
- IPS (intrusion prevention systems)
- IDS (intrusion detection systems)
- Robust passwords
- System and Network Backups

8. DISCUSSION

As can be seen from the examples given, any network, regardless of the operating system is vulnerable to some form of internal or external malware attack and submarine network management systems are no exception. It might be argued that submarine network management systems are connected via an internal private LAN with no external connection to the internet or the corporate network, so there is no risk. However, when external connection is provided to the supplier for maintenance purposes then the network security is only as good as the supplier's network. External physical connections are not needed to introduce malware. No matter how secure the network, all that is needed is one breach and the system is at risk. Such breaches could easily occur, for example by the use of external computers and portable media during network maintenance, by an employee plugging a media device or by a disgruntled employee.

Little attention is given to the overall security requirements of the network management system. Some consideration is given to low level security aspects such as user access. IT specialists are not normally consulted during the planning process until ports are required to be turned up on an IP switch, or a router to connect the submarine network management server. Central to submarine network protection is the use of antivirus protection which requires real time updates to the Remote Operator Positions (ROPs), as well as the Craft terminals. Antivirus is not provided by the vendors as part of the deliverables. The purchasers may also be reluctant to install weekly updates for anti-virus software.

Law 8 from Microsoft's 10 Immutable Laws of Security states that 'an out of date virus scanner is only marginally better than no virus scanner at all' [8].

There are solutions available using various hardware and software packages. Vendors and purchasers need to work together with antivirus providers to come up with the right solution for submarine systems.

9. ADDITIONAL SUBMARINE NETWORK SECURITY RECOMMENDATIONS / SUGGESTIONS

- Establish physical security rules for access to sensitive areas of the cable stations like the transmission equipment room where the suppliers usually install the NMS servers and work stations
- All servers installed in lockable racks
- Lock craft terminals when not in use
- Accompany vendor engineer when accessing sensitive areas
- Restrict network user privileges
- Set up robust passwords
- Appoint a system administrator
- Work with IT consultants during the planning process
- Install Antivirus software on ROPs and craft terminals as well as window based servers.
- Install Antivirus software on dedicated USB drives used to access the network management system

- Set up a policy for vendors for use of secure portable drives
- Security vet station employees
- Vendors to security vet software writers
- System back up policy
- Remote vendor access policy
- One way FTP
- Ensure that adjustments which could damage system components, such as a large increase in power feed current require manual intervention.
- Raise awareness and vigilance amongst cable station and NOC employees

10. FUTURE TECHNOLOGY ENHANCEMENTS

- Use of dumb terminals instead of Craft terminals with operating system on the equipment shelf controller
- Set up a VPN tunnel to the vendor and allow them to provide network security as part of the system maintenance contract
- Craft Terminals without Wi-Fi, where possible use USB/Serial to access the network / equipment, disable the NIC (Network interface card).

11. CONCLUSION AND CLOSING COMMENT

The unavoidable conclusion is that submarine cable systems are very vulnerable to cyber-attacks including targeted attack. It would require a skilled, well motivated group of software writers, but such a team could take a cable system out of traffic for an extended period.

Ralf Langner who headed the team that cracked the Stuxnet code said: "it's a cyber-weapon of mass destruction...we better face the consequences and we better prepare right now" [9]. That is the challenge of this paper to both vendors and operators.

12. REFERENCES

[1] Mr C Bright, Pall Mall Gazette, 11th May 1898.

[2] McAfee Labs, Threats Predictions 2013. http://www.mcafee.com/uk/resources/reports/rp-threat-predictions-2013.pdf

[3] M Williams, cyber-attacks could rival 9-11 October 12 2012 Future. http://www.computerworld.com/s/article/9232317/Future_cyber_attacks_could_rival_9_11_cripple_US_warns_Panetta?taxonomyId=17

[4] Wikipedia, Malware February 15 2013. http://en.wikipedia.org/wiki/Malware

[5] D Alyias, et al Microsoft 2012. Microsoft Security Intelligence Report volume 13 - Download Centre

[6] C DeBrine, weakest Links in websites Vulnerabilities Exposed November 27 2012. http://www.symantec.com/connect/blogs/weakest-links-websites-vulnerabilities-exposed

[7] Kaspersky Lab, Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat 2012. http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat

[8] Microsoft, 10 Immutable Laws of Security 2013.

[9] R Langner, A 21st century cyber weapon, TED, 29 May 2011.

[10] Ponemon Institute LLC, Perceptions about Network Security sponsored by Juniper Networks June 2011. http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

[11] J Beechey, Application Whitelisting January 18 2011.
http://www.sans.org/reading_room/whitepapers/application/application-whitelisting-panacea-propaganda_33599

[12] P V.Radatti, The Plausibility of UNIX Virus Attacks. IWS Information Warfare Site 1993.
http://www.iwar.org.uk/comsec/resources/plausibility.htm

[13] Symantec T Katsuki Crisis: The Advanced Malware November 2012.
Symantec, Analysis of Flamer C&C Servers November 2012.
Symantec, Rootkits. March 2012.
http://www.symantec.com/security_response/whitepapers.jsp

[14] S Barlas, A Earls, M Fitzgerald, J Ledford and D Mccafferty US critical infrastructure security 2004.
http://searchsecurity.techtarget.com/US-critical-infrastructure-security-Highlighting-critcal-infrastructure-threats

[15] S Convery, Cisco General Design Considerations for Secure Networks 2004.
http://www.ciscopress.com/articles/article.asp?p=174313

[16] K Scarfone and P Hoffman
Guidelines on Firewalls and Firewall Policy September 2009.
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

[17] R Ben Nahorney Symantec Intelligence November 2012.
http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11_2012.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Dec_worldwide_NovemberIntelligence

[18] Black Box, network services Physical Security 2013.
http://www.blackbox.co.uk/gb-gb/page/5351/white-papers.

[19] K Scarfone & P Hoffman, Guidelines on Firewalls and Firewall Policy September 2009.

[20] B Schneier, Secrets and Lies Digital security in a Networked world 2000.

13 ACKNOWLEDGEMENTS

The author would like to thank the following people for the useful and thought provoking conversations.
Mr Phil Lancaster, Senior System Engineer (Cable and Wireless Worldwide).
Mr Edward West, Principle Engineer (Cable and Wireless Worldwide).
Mr John Kincey, Principle Engineer (Cable and Wireless Worldwide).