Journal of Policing, Intelligence and Counter Terrorism
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rpic20

Stuxnet: the emergence of a new cyber weapon and its implications

Sean Collins [a] & Stephen McCombie [a]
[a] Centre for Policing, Intelligence and Counter Terrorism (PICT), Macquarie University, Sydney, Australia
Published online: 21 Mar 2012.

To cite this article: Sean Collins & Stephen McCombie (2012) Stuxnet: the emergence of a new cyber weapon and its implications, Journal of Policing, Intelligence and Counter Terrorism, 7:1, 80-91, DOI: 10.1080/18335330.2012.653198

To link to this article: http://dx.doi.org/10.1080/18335330.2012.653198

Journal of Policing, Intelligence and Counter Terrorism
Vol. 7, No. 1, April 2012, 80–91

FORUM

Stuxnet: the emergence of a new cyber weapon and its implications

Sean Collins and Stephen McCombie*

Centre for Policing, Intelligence and Counter Terrorism (PICT), Macquarie University, Sydney, Australia

The malware Stuxnet was designed to sabotage the Iranian nuclear programme by targeting industrial control systems (ICSs). The potential for cyber attacks to be a significant threat to critical infrastructure has been discussed over the last 15 years, but it was only in 2010 that this potential was finally realised with the advent of Stuxnet. Stuxnet, unlike the malware that came before it, is highly targeted and designed to achieve a real-world outcome. Stuxnet has challenged assumptions about environments not connected to the internet and the belief that network defences will protect facilities from vulnerabilities in software applications. This paper examines Stuxnet's forerunners, Stuxnet in detail, its target, and its implication for critical infrastructure. Whatever the cost to create Stuxnet, it was far less than the cost of a traditional military attack. Future versions of Stuxnet may be used by nation states, terrorist groups, hacktivists and cyber criminals to achieve their own goals. In the future, cyber weapons may not be as restrained as Stuxnet. This malware has started a new arms race, and has created serious implications for the security of critical infrastructure worldwide.

Keywords: cyber attack; cyber warfare; Stuxnet

Introduction

The potential of cyber attacks to be a significant threat to critical infrastructure has been discussed over the last 15 years (Denning, 1999; Power, 2000; Schwartau, 1996; Vatis 2001; Verton, 2003). In 2010 this potential was finally realised with the advent of the malware Stuxnet. Stuxnet, unlike the malware that came before, is highly targeted and designed with a real-world outcome in mind.

A cyber weapon, Stuxnet was designed to sabotage the Iranian nuclear programme by targeting ICSs. Stuxnet also showed a level of sophistication not previously seen in malware. Despite those differences, Stuxnet is part of an evolution in cyber attacks that started with early malicious software from the period 1988 till 2002, which was mostly about showing off technical prowess and protesting, and the crimeware developed from 2004 to the present by cyber crime groups to enable fraud. Similarly, it evolved from other types of cyber attacks such as denial of service (DoS) and website defacement.

This paper examines Stuxnet's forerunners, Stuxnet in detail, its target, and its implications for critical infrastructure. Stuxnet and the future cyber weapons it will inspire have fundamentally changed the scope of cyber threats.

*Corresponding author. Email: stephen.mccombie@mq.edu.au

ISSN 1833-5330 print/ISSN 2159-5364 online

http://dx.doi.org/10.1080/18335330.2012.653198
http://www.tandfonline.com

Definitions

Malware defined

Malware or malicious software falls broadly into three categories: viruses; worms; and Trojan horses. A virus is a self-replicating program that needs to attach itself to a host program in order to spread. Often viruses are said to only reside in the host computer. They can blindly infect every file or be written to attack specific executable files. A worm is also a self-replicating program, but does not need another program to assist in replication. Worms are standalone programs that do not need any human interaction to instigate their attack.

The main difference between a worm and a virus is in the way they replicate. Viruses replicate on a host system while worms replicate over computer network connections. A Trojan horse is a program that performs unknown or unwanted actions, while posing as a legitimate program (Karresand, 2003). A Trojan horse is often used as a delivery system rather than the ultimate payload. Crimeware on the other hand is merely malware designed for fraud, such as key loggers to capture online banking credentials. Crimeware can take the form of viruses, worms and Trojan horses, or a blend.

Other cyber-attack vectors defined

DoS and distributed denial of service (DDoS) are attacks on the availability of internet systems through various technical means. The most common method is to exhaust the availability of services on a system by flooding the network, systems or application. While there is nothing stealthy about DDoS attacks, they can be hard to trace given the anonymity of robot networks of compromised computers (botnets) that are often used to execute the attacks. Another common form of cyber attack is web defacement, where an attacker gains access to a web server and changes the content of a webpage. In many cases this is done as a protest or just to show the technical skill of the attacker.

Evolution in cyber attacks

Morris worm

Robert Tappin Morris was the inventor of the computer worm. On 2 November 1988, Morris, a Cornell graduate student in computer science whose father had worked for the National Security Agency (NSA), released the first ever computer worm, attacking 1 in every 20 UNIX-based computers connected to the research network which was the early internet. By the morning of 3 November, these computers were running on a small percentage of their actual capacity, having been overwhelmed by Morris's worm. It had a severe impact on the internet, albeit not the critical network it is today. Morris's aim was claimed to be purely experimental and the outages caused an unforeseen result; despite this he was charged under the US Computer Fraud and Abuse Act 1984 and was sentenced to probation (Hafner, 1991).

Yahoo DDoS

In February 2000 a number of DDoS attacks took place against internet giants Yahoo, CNN, eBay, and other major websites. According to one estimate, the attacks

caused US$1.2 billion in losses. These acts clearly demonstrated the impact of information warfare on dot coms whose business is totally reliant on internet communication. Yahoo, then the second most visited internet site, was inaccessible for several hours. It was receiving one gigabit of traffic a second, more than most sites received in a year at that time. The cause was teenage vandalism rather than calculated commercial assault on these companies (McCombie & Warren, 2000). While there have been numerous DDoS attacks since, this was the first one to significantly impact the commercial internet; it has since served as the model for other attacks in terms of execution, if not motivation.

Maroochy Shire Council

Attacks on supervisory control and data acquisition (SCADA) systems are extremely rare, but in February 2000 an attack was initiated by an employee (Vitek Boden) of Hunter Watertech, who installed the SCADA system for the Maroochy Shire Council in Queensland, Australia. After a disagreement with Hunter Watertech and the council over employment opportunities, Boden decided to take revenge. With a carload of stolen wireless and computer equipment, he issued commands to the SCADA system to release 800,000 litres of raw sewage into local parks and rivers. The sewage caused severe damage to the local ecosystem and created a health risk for residents (Abrams & Weiss, 2008). While often used as an example of an attack on critical infrastructure, it needs to be remembered that Boden installed the SCADA system and had intimate knowledge and equipment to execute commands; there was no need to penetrate security measures as no cyber security existed. Boden did not write malicious code or create a worm to do his bidding; he basically exploited known security exposures to achieve his objective. It was, in effect, a disgruntled insider attack.

Code Red worm

On 1 April 2001 a US signals intelligence aircraft collided mid-air with a Chinese fighter while near the Chinese island of Hainan. The US aircraft had to make an emergency landing in China and the Chinese fighter jet crashed, killing the pilot. This, and the surrounding foreign policy crisis, set off a cyber protest on both sides of the dispute. One of the most prominent elements of this cyber protest was the Code Red worm, presumably created by Chinese sympathisers. On Thursday 12 July 2001, the Code Red was launched. By 19 July Code Red had infected more than 250,000 computers. The Federal Bureau of Investigation (FBI) issued an alert on the worm, stating that it presented a serious threat to internet users and the disruption of e-commerce and emails. After the worm was first identified by a senior security engineer from Chemical Abstract Services, anti-virus researchers reverse-engineered the worm, finding that it originated from a university in China. The worm exploited a vulnerability in Microsoft's Internet Information Services that was installed on millions of machines worldwide (Berghel, 2001). It also defaced websites with a message of protest about the incident.

The US government security team examining Code Red found that it was eventually to terminate propagation and launch a DoS attack on the White House webserver at midnight on 19 July 2001. However, the worm was created to attack the White House IP address and not the URL, which allowed the White House to simply

change to another IP address before the DoS attack. By CNET estimations, on the night of the DoS attack Code Red had over 359,000 systems with each releasing 400MB of useless data aimed at the White House webserver. The intended target was never attacked, thanks to the retrieval of the worm's plans from its code (Berghel, 2001).

SQL Slammer worm

MS SQL is a Microsoft server application used in databases worldwide. The SQL Slammer worm was written to exploit a known vulnerability in this software. In 2003, the SQL worm penetrated Ohio's David-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours. This was a surprise to workers at the plant who believed the network was protected from the internet by a firewall. The worm, however, found a way into the plant via a dedicated network link to a David-Besse contractor. This link bypassed the firewall and allowed the SQL worm into the plant's network (Poulsen, 2003).

The worm entered the plant and systematically crashed all the safety monitors, which are vital to reactor core maintenance. It appears the worm found entry into the plant via the computer of an engineer who had failed to update the computer's Microsoft SQL vulnerability with a patch that had been released six months earlier. Fortunately there were redundant analogue safety monitors that were used until the system could be restored (Poulsen, 2003). Compared to Stuxnet, SQL was loud, not attempting to hide itself or use subterfuge, and it also appears that the action of the worm on the nuclear power plant was not intentional and was a random event. However, it does show how worms far less sophisticated than Stuxnet can severely impact upon critical infrastructure.

Estonia and Georgia cyber attacks

In April 2007, the Estonian government decided to move a war memorial that was constructed in honour of the Soviet liberation from Nazi occupation in World War Two. The memorial was moved to a less prominent area of Estonia, sparking outrage amongst the Russian-speaking minority. Rioting ensued and cyber attacks commenced from Russian patriots against Estonian sovereignty. Like many Western nations Estonia relies heavily upon the internet for its critical infrastructure, providing a wealth of targets for disgruntled Russian hackers. Estonia relies so much on IT that its minister for defence stated that Estonia had a paperless government (Herzog, 2011).

The attacks were perpetrated from inside Russia and used botnets to execute DDoS attacks on government and banking critical infrastructure. Government and banking websites, which normally received 1000 visits a day, crashed when they started receiving up to 2000 visits a second (Herzog, 2011).

The cyber attacks on Georgia were brought about by political and military tensions over the independence of South Ossetia, which falls on the Russia/Georgia border. The attacks were coordinated with kinetic attacks in 2008 and included the defacement of government websites, DoS/DDoS attacks against government, business, finance and media IT communications, and the creation of forums distributing malware with instructions on how to attack Georgia. Even though the attacks did not have significant lasting effects, their use in conjunction with kinetic

attacks served to disrupt the Georgian military response to the Russian military campaign (Tikk, Kaska, Runnimeri, Mari, Taliharm & Vihul, 2008).

Conficker worm

In 2008, the Conficker worm was released and began infecting millions of computers that failed to install a Microsoft patch of a known vulnerability weeks earlier. Five variants of the worm would later be released to increase propagation. When Conficker B was released, it could hide in USB port devices, infecting any host connected to it. The worm was created to infect computers and turn them into 'bots' to create a vast botnet. With millions of computers under the worm's control, researchers estimated the type of damage that could be done by such an army to be significant to critical infrastructure (Conficker Working Group, 2010).

Notably, Stuxnet used the same remote procedure call (RPC) vulnerability to propagate through unpatched computers. RPC is a program command that causes a sub-routine or procedure in another address space (commonly another computer on a shared network).

Stuxnet

Introduction to Stuxnet and SCADA

Stuxnet was a worm designed to destroy centrifuges used in Iran's nuclear programme via SCADA systems. SCADA systems are computer-based mechanisms that monitor and control physical operations. These systems usually comprise network devices such as sensors, actuators, controllers and communications devices. Central data acquisition and control over distributed assets is pivotal to the operation of SCADA systems (Moteff & Parfomak, 2004). These distributed assets or distribution systems could be electrical power grids, water distribution and waste collection systems, oil and gas pipelines, railway transportation control or, in the case of Stuxnet, nuclear facilities.

Stuxnet's particular target within the SCADA system was the programmable logic controllers (PLC). PLCs are small computers that control functions performed by electrical hardware such as switches, relays and timers/counters (Tsang, 2010). The PLC that Stuxnet looked for were those controlling centrifuges used in enriching uranium.

Stuxnet found and analysed

In May 2010, Virusblokada, an anti-virus company in Minsk Belarus, reported the finding of Stuxnet (named RootkitTmphider) and that it used a previously unknown LNK vulnerability in the Microsoft Windows operating system (commonly known as a zero-day vulnerability) (Falliere, Murchu & Chien, 2011). This came to the company's attention when it was engaged to investigate a computer in Iran that had started continuously to reboot itself for no apparent reason. Virusblokada staff examined the troubled computer remotely over the internet and confirmed that they had found something they had never seen before: a worm of surprising size and complexity. Virusblokada issued a worldwide alert on Stuxnet and began an international effort to track down the worm's source. The release of the worm saw

robust international cooperation from IT experts and anti-virus vendors. Kaspersky Labs in Moscow were working with Microsoft in Redmond, Washington, US to uncover the vulnerabilities in Windows that the worm was exploiting. To date, the most in-depth study and research conducted on Stuxnet was performed by Symantec. Liam Murchu and his international team worked solidly for three months on the worm. This work mostly took place in Symantec's malware lab, which is basically similar to a biological containment facility (Weinberger, 2011).

In September 2010 the Bushehr nuclear power plant was believed to be infected by Stuxnet. This speculation came about from the delayed start-up of the Russian-built facility (Clayton, 2011). Ali Akbar Salehi, the head of the Iranian Atomic Energy Organisation, stated that the plant was no longer being "affected" by Stuxnet and the delay was due to "hot weather" (BBC, 2010, para 7). To increase the chance of success for the worm, the authors bestowed a plethora of abilities such as four zero-day exploits, anti-malware evasion, a Windows root-kit, a command and control (C&C) interface, network infection routines/hooking, malicious code injection techniques, and the first ever PLC root-kit (Falliere et al., 2011). Stuxnet does not actually attack SCADA systems, but uses them to gain access to and control PLCs. Researchers for Symantec state that there were up to 9000 new infections a day from Stuxnet (Garber, 2010). Once inside the nuclear control systems, the worm would cause the centrifuges in the uranium enrichment process to spin out of control, thereby destroying them. It is still in debate as to how exactly Stuxnet infected ICSs in Iran and around the world. While the majority of analysis indicates that the worm must have propagated through a USB or other similar device, Byres, Ginter and Langill (2011) suggest that it is quite possible that the worm infected ICSs by moving silently through computer networks. What is apparent is that the worm could take whatever path it needed to reach its intended victims, as the authors endowed the worm with several different propagation techniques. Stuxnet could not only spread through USB drives, but also the devices that supported them, such as printers and scanners. The worm also showed restraint when the initial infection took place, by only infecting three additional computers after attacking the primary system. This was likely done to reduce the probability of the worm being noticed and is indicative of the professionalism of the malware writers; this type of code writing is not the standard for the typical hacker or cyber criminal (Willems, 2011).

ICSs function on special code that run on embedded systems such as PLCs; these PLCs are usually managed from computers running Windows which are not connected to the internet or even an internal network. In a best practice setting, an ICS would not be connected to the internet (Falliere et al., 2011). Unfortunately, modern ICS and SCADA systems are increasingly interconnected and interdependent, offering multiple pathways from the outside world to PLCs. To assume there is an 'air-gap' between ICSs and corporate networks is unrealistic. Information exchanges between these networks are essential for facility and corporate operations to function effectively (Byres et al., 2011).

When infection occurs, the worm will seek and infect any additional systems containing Windows; after this it becomes more selective about which PLC it wants to control. Its preferred targets were PLCs from Siemens, which would be attached to an infected Windows PC via an ethernet, process field bus (Profibus) or Siemens own communication link called multi point interface (MPI). Stuxnet would then perform a verification process to make sure it was the right controller for manipulation. This involved the checking of serial numbers, configurations, and the sampling of

programming code to ensure it had the correct target. The worm achieved this by exploiting the host's dynamic-link library (DLL, which facilitates communication between SIMATIC S7 (PLC control software) and the PLCs. Once a perfect match was found, Stuxnet's dropper loaded rogue code onto the PLC (Langner, 2011).

In a US Senate hearing on Stuxnet (US Senate, 2010) it was reported that at least 10,000 person-hours went into its production, and the worm's authors would have been experts in both Microsoft's operating systems and in the much more intricate systems and computer language that manage ICSs. Stuxnet has some 4000 functions compared to the basic email server which has about 2000 functions.

In their specialised lab, the Symantec investigation team was able to analyse the worm by allowing it to attack a computer network within a controlled environment. Here they could safely watch the worm in action without the risk of it infecting the outside world. The first thing the team noticed was the size of the worm; at around 15,000 lines of code, it was larger than anything they had previously witnessed (Weinberger, 2011). The code used not one (as is sometimes the case in new malware) but four zero-day vulnerabilities. It also included two stolen authentication certificates from Realtek and JMicro signing its components. Table 1 summarises some of the differences seen in Stuxnet compared to earlier malware.

Implications for cyber security and critical infrastructure

Stuxnet has challenged assumptions about environments not connected to the internet and the belief that network defences will protect facilities from vulnerabilities in software applications. Stuxnet has also shown that SCADA/ICS personnel can no longer rely upon the fact that their systems are so obscure that it is impossible for attackers to identify, analyse and exploit vulnerabilities. Stuxnet demonstrated that the attackers knew more about the hardware and software than the system owners (Hewlett-Packard, 2011).

Stuxnet is not the last worm that the SCADA/ICS industry will face. Stuxnet has exposed ICS security deficiencies, providing people around the world with a model on how to structure their own malware and carry out similar attacks (Byres et al., 2011). The importance of cyber crime in the evolvement of malware is a key element in Stuxnet's creation. Farwell and Rohozinski (2011) propose that Stuxnet is more of a 'Frankenstein' worm, patched together by best practice, code and expertise sourced from the global cyber-crime community. The integration of these individual components in Stuxnet was something that had never been done before (Byres et al., 2011).

The ramifications of Stuxnet present an urgent necessity for the SCADA/ICS industry to accept changes in the cyber-security landscape. The most critical threats

Table 1. Differences between Stuxnet and other malicious software

Function	Stuxnet	Other malware
Targeting	Extremely selective	Indiscriminate
Type of target	SCADA/ICSs	Computers/PCs
Size	500 Kbytes	Less than 500 Kbytes
Exploits	Four zero-days	Possibly one zero-day
Authentication	Valid certificates (stolen)	Forged

are no longer DDoS attacks, but stealthy, resilient malware that are complex and expertly engineered. Stuxnet has shown there needs to be a greater emphasis on application control, rather than trying to block every single point of entry into a system. There are a myriad of packages designed to block available entry points and Stuxnet has proved that this protection is ineffective (Davies, 2011).

While Stuxnet focused on specific products like Siemens SIMATIC/Step 7 projects, a modified version or copy of the worm could have a more indiscriminate attack strategy, resulting in components from other vendors being compromised as well (Rossel, 2011). US Senator Susan Collins (US Senate, 2010) stated that, if an attack like Stuxnet were to be executed on a large transformer within the US power grid, the impact could cascade and leave much of the nation without power, shutting down the economy and undermining national security. Stuxnet has opened the possibility for an intelligent attacker to exploit a common vulnerability across multiple critical infrastructure sectors simultaneously, providing the attacker the benefits of anonymity and distance. At the least, Stuxnet should be viewed as a wake-up call to governments and businesses, especially those reliant upon internet-based ICSs (Gross, 2010).

For the first time a computer worm, through malicious manipulation, caused physical destruction in the real world. The Stuxnet worm was a malware program so complex that it could stealthily move from system to system, replicating itself and effectively reprogram critical systems while hiding the modified code from human controllers. Stuxnet only performed repairable damage to the Iranian nuclear facilities, most likely because it was programmed to do so. This was, however, the intention of the writers of Stuxnet rather than a limitation of the technology; such restraint may well not be the aim of future malware.

Conclusions

Amongst others, Israel has focused on its computing sector to strengthen its ability to confront cyber attacks. Yuval Elovici, an Israeli computer scientist, has been working closely with the Israeli government on cyber security. Elovici has been warning the cyber security and critical infrastructure industry for years about emerging cyber threats against SCADA and ICSs, even before the discovery of Stuxnet. He has warned the threats are credible and underestimated, stating that a full blown 'Stuxnet-like' attack against critical infrastructure would have a greater impact than several atomic bombs being released on a major city (Gross, 2010).

The fears of cyber warfare were raised with the Estonia/Georgia cases in 2007–2008. These cases dealt with DDoS, which is a brute force attack that only hampered information infrastructures. Stuxnet, on the other hand, was stealthy, resilient and highly intelligent. After the Stuxnet attack, Iran accused NATO and the US of being involved, which they strenuously denied. Some have also suspected Israel's Unit 8200 security agency. The UK, China and the Russian Federation are all believed to be developing their own cyber warfare capabilities in a new cyber arms race. The US has already established Cyber Command (USCYBERCOM) at Fort Meade in Maryland to defend military networks (Chen & Abu-Nimeh, 2011).

Eric Knapp, Director of Critical Infrastructure Markets for NitroSecurity, states that, in the end, Stuxnet is a weapon. He argues that the worm is concrete evidence that governments will develop malware to sabotage their opponent's IT systems and critical infrastructure; proving that hostile organisations can now attack SCADA

systems on which a nation's essential services depend (Davies, 2011). Since the end of World War Two, military powers have commonly used technology to hinder the productive capabilities of their enemies without creating an act of war (Grier, 2010). Michael Assante, President and CEO at the National Board of Information Security, says:

> I view Stuxnet as a weapons delivery system, like the B-2 bomber. It's clear to me that the resources available to the authors of the worm were substantial. They designed it with high confidence that the warhead would do exactly what it was designed to do (Hulme, 2011, p. 40).

Langner (2011) suggests the attack on Iran's uranium facilities has set back their nuclear programme by at least two years. In Langer's opinion the worm was more successful than a kinetic military strike, as it avoided casualties and averted a full scale war. In January 2011, Meir Dagan (then serving Israeli intelligence chief) stated that Iran will not reach nuclear capability until 2015 due to the measures deployed against them (Nicoll & Delaney, 2011).

More importantly are the implications the worm has generated within political and strategic contexts. The most important aspect is the convergence between cyber crime and state action; this is where the state benefits from technology development driven by cyber crime. Even if the state does not have the capability to utilise this technology, there is always the possibility of contracting third parties to conduct cyber attacks. Most of the Arab states and the US seek to end Iran's nuclear programme. A full scale military strike from either party to limit Iran's nuclear capability would generate more problems than it would solve. Whatever the cost to create Stuxnet, it was far less than the cost of a traditional military attack. It is highly plausible that the US, in collaboration with Israel or other Arab states, conceived Stuxnet as a means of delaying Iran's nuclear capability. At present, cyber attacks that cause repairable damage but do not injure humans are not classified as use of force or armed attack. This is the present stance held by the US, which has had countless probes and penetrations to its Department of Defense. It must be remembered that cyber weapons are not like conventional ones; compared to other weapon systems, cyber weapons used in the future can be captured, analysed, modified and turned against their creators with relative ease (Farwell & Rohozinski, 2011).

Cyber warfare is open to a number of aggressors, not just nation states. Nations around the world should be deeply concerned with the possibility that hackers, organised crime networks or terrorists may wish to harness cyber warfare with a weapon such as Stuxnet. PLCs are found across the broad spectrum of critical infrastructures, and Stuxnet is possibly the first of many such attacks yet to come (Chen & Abu-Nimeh, 2011). Cyber-based espionage and nation state backed hacking are increasing in occurrence. Taking out a power plant with a computer was once the domain of Hollywood films; now the line between fantasy and reality has become increasingly blurred. Stuxnet may be the catalyst for a new arms race (Riley, 2011).

Herbert Lin, Chief Scientist for the Computer Science and Telecommunications Board (US National Research Council), suggests that cyber tools can be used as instruments for government security as well as weapons for the military and intelligence agencies. Many nations already possess sophisticated hacking and intrusion capabilities, and actively participate in 'cyber offensives' during times of

peace; testing their capabilities in a way that cannot be attributed to them. Whereas nation states are selective of their targets and mindful of the possible outcomes of using cyber attacks, terrorists are less cautious, trying to cause as much destruction and chaos as possible. These types of attacks are very attractive to terror groups as they provide anonymity because they are difficult to trace (Greengard, 2010).

Nevertheless, Stuxnet has proved that cyber terrorism is now a credible threat to nation states. The threat of terrorism has moved beyond conventional surface targets to critical infrastructures that are heavily dependent upon computer systems and networks. These targets now relate to power, finance, military and transport as well as other essential human services. Wilson argues that links have already been made between conventional terrorist attacks and cyber crime, and believes that current computer vulnerabilities make critical infrastructure an attractive target (Puran, 2003). Currently, terrorist groups do not have the technical ability to develop a Stuxnet-type worm. However, there is much open source information on Stuxnet and so much of the development work has already been done (Fidler, 2011).

On a technical level, Stuxnet has raised the standard of malware, something many groups and individuals will try to surpass. While some in the security community say that the threat of cyber warfare is over-exaggerated, concocted by security vendors and the government to forward their own aims, this claim has not been made in regards to Stuxnet. The post-Stuxnet behaviour by nation states indicates an endeavour to create political and legal space for the legitimate use of cyber operations, in a bid to exceed the boundaries in a post-Stuxnet world (Kerr, Rollins & Theohary, 2010).

With Stuxnet, the real risk is not the worm itself, but the availability of its code for reproduction or modification. It also provides a proof of concept for future cyber weapons targeting SCADA systems. The new malicious software that Stuxnet spawns will invariably be smarter, stronger and more resilient. Future versions of Stuxnet may be used by nation states, terrorist groups, hacktivists and cyber criminals to achieve their own goals. In the future, cyber weapons may not be as restrained as Stuxnet. This malware has started a new arms race and has created serious implications for the security of critical infrastructure worldwide.

References

Abrams, M., & Weiss, J. (2008, July 23). Malicious control system cyber security attack case study. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

BBC. (2010). Start-up of Iran's Bushehr nuclear power plant delayed. *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-middle-east-11445126

Berghel, H. (2001). The Code Red worm. *Communications of the ACM*, *44*, 15–19. doi: 10.1145/501317.501328

Byres, E., Ginter, A., & Langill, J. (2011, February 22). How Stuxnet spreads: A study of infection paths in best practice systems. Retrieved from http://abterra.ca/papers/How-Stuxnet-Spreads.pdf

Chen, T.M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*: 91–93. doi: 10.1109/MC.2011.115

Clayton, M. (2010, September 21). Stuxnet malware is 'weapon' out to destroy … Iran's Bushehr nuclear power plant? Retrieved from http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

Conficker Working Group. (2010). *Lessons learned*. 2–3.

Davies, S. (2011). Out of control. *Engineering and Technology Magazine*, 60–62. Retrieved from http://eandt.theiet.org/magazine/2011/06/out-of-control.cfm

Denning, D. (1999). *Information warfare and security*. New York, NY: ACM Press (Addison-Wesley).

Falliere, N., Murchu, L., & Chien, E. (2011, February). Symantec Security Response. W32.Stuxnet Dossier, Version 1.4. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Farwell, J.P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival – Global Politics and Strategy*, *53*, 23–40. doi: 10.1080/00396338.2011.555586

Fidler, D.P. (2011). Was Stuxnet an act of war? Decoding a cyberattack. *IEEE Security & Privacy*, *9*, 56–59. doi: 10.1109/MSP.2011.96

Garber, L. (2010). Worm targets industrial-plant operations. *Computer*, *43*, 15–18. doi: 10.1109/MC.2010.333

Greengard, S. (2010). The new face of war. *Communications of the ACM*, *53*, 20–22. doi: 10.1145/1859204.1859212

Grier, D.A. (2010). Sabotage! *Computer*, *43*, 6–8. doi: 10.1109/MC.2010.323

Gross, G. (2010, November 17). Stuxnet changed cybersecurity. *Networkworld*. Retrieved from http://www.networkworld.com/news/2010/111710-experts-stuxnet-changed-the-cybersecurity.html

Hafner, K., & Markoff, J. (1991). *Cyberpunk: Outlaws and hackers on the computer frontier*. New York, NY: Simon & Schuster.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*, 49–60. doi: 10.5038/1944-0472.4.2.3

Hewlett-Packard. (2011, August). How Stuxnet demonstrates how software assurance = mission assurance (HP Enterprise Security Business Whitepaper). Retrieved from https://www.fortify.com/downloads2/user/StuxnetWhitepaper_SoftwareAssuranceEqualsMissionAssurance.pdf

Hulme, G.V. (2011). SCADA insecurity: Stuxnet put in the spotlight on critical infrastructure protection, but will efforts to improve it come too late? *Information Security Magazine*, *13*, 40–41.

Karresand, M. (2003, June). Separating Trojan horses, viruses, and worms – a proposed taxonomy of software weapons. Paper presented at Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society.

Kerr, P.K., Rollins, J., & Theohary, C.A. (2010). *The Stuxnet computer worm: Harbinger of an emerging warfare capability* (CRS Report for Congress No. R41524). Washington, DC: Congressional Research Service.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*, 49–51. doi: 10.1109/MSP.2011.67

McCombie, S., & Warren, M. (2000). *A profile of an information warfare attack*. Geelong, Australia: Deakin University, School of Computing and Mathematics.

Moteff, J., & Parfomak, P. (2004). *Critical infrastructure and key assets: Definition and identification* (CRS Report for Congress No. RL32631). Washington, DC: Congressional Research Service.

Nicoll, A., & Delaney, J. (Eds.) (2011). Stuxnet: Targeting Iran's nuclear programme. *Strategic Comments*, *17*, 1. Retrieved from http://irannuc.ir/fa/images/stories/Stuxnet_-_targeting_Irans_nuclear_programme1.pdf

Poulsen, K. (2003). Slammer worm crashed Ohio nuke plant network. Retrieved from http://www.securityfocus.com/news/6767

Power, R. (2000). *Tangled web: Tales of digital crime from the shadows of cyberspace*. Indianapolis, IN: Que Publishing.

Puran, R.C. (2003, February 28). Beyond conventional terrorism: The cyber assault. SANS Institute. Retrieved http://www.sans.org/reading_room/whitepapers/threats/conventional-terrorismthe-cyber-assault_931

Rossel, T. (2011). *Post-Stuxnet industrial security: Zero-day discovery and risk containment of industrial malware*. Berlin: Innominate Security Technologies AG. Retrieved from http://www.innominate.com/data/downloads/white_papers/post_stuxnet_industrial_security_en.pdf

Schwartau, W. (1996). Information warfare: Cyberterrorism – protecting your personal security in the electronic age. New York, NY and Emeryville, CA, Thunder's Mouth Press.

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.M., & Vihul, L. (2008). *Cyber attacks against Georgia: Legal lessons identified.* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence.

Tsang, R. (2010). *Cyberthreats, vulnerabilities and attacks on SCADA networks* (Working Paper). Berkeley, CA: University of California, Goldman School of Public Policy. Retrieved from http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

US Senate. (2010). *Securing critical infrastructure in the age of Stuxnet*. Washington, DC: US Senate on Homeland Security and Government Affairs. Retrieved from http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet

Vatis, M. (2001). *Cyber attacks during the war on terrorism*. Hanover, NH: Institute for Security Technology Studies at Dartmouth College.

Verton, D. (2003). *Black ice: The invisible threat of cyber-terrorism*. New York, NY: McGraw-Hill/Osborne.

Weinberger, S. (2011). Is this the start of cyberwarfare? *Nature*, *474*, 142–143. doi:10.1038/474142a

Willems, E. (2011). Cyber-terrorism in the process industry. *Computer Fraud & Security*, *3* 16–19. doi: 10.1016/S1361-3723(11)70032-X