CYBER SECURITY – TURNING THE TABLES ON OUR ADVERSARIES

Mr. Nick Hopkinson, Director of Cyber security, CSC

Cyber Security is now recognised as an issue of strategic importance and one of the top risks to national security. It is also a unique threat comprising a multitude of different adversaries and affecting many different facets of national life through cybercrime, damage to our economic prosperity, and potentially disruptive attacks on our national infrastructure. This recognition poses some serious questions. How well are we protected as a nation against our cyber adversaries? Are we winning the battle in cyber space?

ABOUT THE AUTHOR

Nick Hopkinson is Director of Cyber security at CSC, the world's leading independent systems integrator. Prior to joining CSC, Nick was Director General for Information, Security & Assurance at the Government's intelligence and security organisation GCHQ, where he worked for 27 years.

ABOUT CSC

With over 50 years of information security experience, CSC provides security transformation services across commercial sectors and government, supporting some of the world's most security-conscious enterprises. CSC's established collaborative partnerships with leading security product and service providers, including RSA and Symantec, enables clients to rely on CSC to deliver levels of information security that allow them to benefit from new cost saving approaches to differentiate their businesses, including cloud computing services.

At the moment the attackers appear to have the upper hand. The recent DDOS attacks on organisations such as Paypal, Visa and Amazon, in support of the Wikileaks cause, demonstrate the damage that can be inflicted by ad hoc groups using basic attack tools, and highlights the damage that could be caused by well organised, well funded groups using more sophisticated attack techniques. Much of the damage inflicted by such attacks is never revealed as it impacts on the heart of national security, and the competitiveness and brand reputation of our major companies.
Are we doomed to fighting a reactive, defensive battle which can only limit the damage as our most dangerous adversaries - typically those backed by state organisations or criminal groups - remain one or two steps ahead?
If we are to transform this situation we need to consider new strategies which turn the tables on the attacker and harness the full power and resources of the community of organisations which are interested in developing cyber space as a safe environment.
"By playing to our strengths there is much more that can be done to tilt the playing field in our favor and make it more difficult for the attacker to operate on the internet"

CIRCUMSTANCES FAVOUR THE ATTACKER

Currently, attackers are able to exploit all the advantages of operating on the internet, including operational agility, massive force multiplication (through use of botnets for example),and the rapid development of attacks to exploit newly discovered vulnerabilities. They use the internet to minimise the risk of discovery, shift the command and control of their exploits to different servers in new locations; user friendly attack tools are freely available enabling organisations to develop relatively sophisticated attacks very quickly. The asymmetric advantages of cyber attack have made it a very attractive option for all types of groups and organisations.
Much of the attention, energy and resource in Nations cyber security communities are focussed on two types of threat: the politically embarrassing losses and leaks whether through loss of media or laptops, or through exploitation of personal email, social networking sites; and, the equally dramatic but strategically more important scenario of a Pearl Harbour style attack on defence or CNI networks. The potential for the latter has now been vividly demonstrated by the Stuxnet attack on Iranian nuclear facilities which not only accessed an air-gapped network but inflicted significant physical damage on a key industrial process (the centrifuge systems for refining nuclear fuel). While the latter is clearly significant and is rightly the subject of strategic planning, it can induce a cold war approach to the problem with long planning and delivery cycles. The nature of the adversaries – utilising all the agility, speed and power of the internet – demonstrates that such an approach is not tenable.

MEANWHILE THE STRATEGIC DAMAGE TO NATIONS IS POTENTIALLY SEVERE

Another powerful reason for urgent action is that significant strategic damage, some of it irreversible, is already being inflicted some Nations like the UK, and on partners and allies, through the ongoing and systematic theft of intellectual property and commercial intelligence. Some key figures in the US have now recognised this and highlighted the strategic significance.

Last year, U.S. Deputy Secretary of Defense William Lynn spoke about the targeting of intellectual property as one of the "least discussed" of the cyber threats facing the United States (see *Reference 1)*. He referred to the exfiltration of "key parts of Google's source code" that were part of a larger "sophisticated operation that also targeted dozens of other companies"; he noted that the U.S. defense industry "has similarly been targeted," and that "designs for key weapons systems have been stolen." He concluded that "the threat to intellectual property is less dramatic than a cyber attack on our infrastructure. But it may over the long term be the most significant cyber threat our nation faces." Such an assessment almost certainly applies to the NL and other allies. The long term consequences for national security could be severe with major impacts on our technological advantage and economic competitiveness.

TOWARDS A NEW STRATEGY

Clearly, more can be done and needs to be done to improve our defences. Modern layered defensive architectures based around sound design of information systems and networks, using assured products and services, with modern protective monitoring systems built to the latest standards can provide effective defences against the majority of attacks. A number of organisations claim to have solutions which can detect the presence of the most sophisticated malware (the

APT – Advanced Persistent Threats), and as these become more mature and are deployed more widely they will provide further assurance. Finally, we need to become smarter at sharing intelligence on threats and vulnerabilities – this information is often slow to circulate due to concerns over source, commercial or legal sensitivities – this is an area where both Government and industry can take a lead and cut through many of these issues by a bold initiative which would immediately improve our defences. The longer we delay the more damage is being done.

While all these initiatives are important, they are essentially defensive. Our adversaries still enjoy all the fundamental advantages of free use of the internet and all its resources to support their operations. We need to think radically about new approaches which can deny or disrupt their access to internet resources. There are a number of new ideas out there which offer the prospect of being able to move on to the offensive in the battle for cyber space:

- Many attacks, including sophisticated APTs, use command and control software hosted on third party platforms to manage and control their malicious code. A collaborative initiative to identify, pool and disseminate information on the web sites and IP addresses used for C2 would allow organisations to block outbound traffic going to these sites and thus deny the attackers the results of their attack.
- The same information could be used to encourage, or direct ISPs to close down IP addresses used by attackers for C2 or data exfiltration. This would need to be enforced internationally otherwise attackers would simply move their internet operations to a more benign environment.
- This, in turn, could be part of a larger effort to improve the current norms of behavior between ISP's that help maintain order in the Internet. Among other things, this could reduce malicious activity by the ISP's customers by enforcing their contractual terms of use, blocking uncooperative ISP's, and developing a system of white listing cooperative ISP's.

These measures play to the strengths of Governments and large corporations who have the powers to legislate, mandate and encourage compliance and cooperation by those bodies providing the internet services on which attackers depend. Concerted action would deny them easy access to these resources. All this requires a much greater degree of collaboration between Government bodies and the private sector, nationally and internationally. Collaboration in this field is not instinctive due to sensitivities over intelligence sources, or leakage of information which might damage brand reputation or shareholder value. Hence, leadership from the top in both Government and industry is vital to:

- Recognise the urgency of the problem and insist on a common strategy – a bureaucratic pace of response is no longer tenable given the damage that is already being incurred.
- Overcome the inhibitions to a more radical sharing of information.
- Achieve a common response and adherence to agreed standards and mechanisms.

By playing to our strengths there is much more that can be done to tilt the playing field in our favour and make it more difficult for the attacker to operate on the internet but resolute action is needed now if cyber space is to become an economic and security asset rather than a major vulnerability.

REFERENCES:

William Lynn, Remarks at the Stratcom Cyber Symposium, May 26, 2010. http://www.defense.gov/speeches/speech.aspx?speechid=1477.

For more information please visit www.csc.com/cybersecurity, or contact us on cyber@csc.com