CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Conficker:

Considerations in Law and Legal Policy

Kadri Kaska

Tallinn 2012

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre) and it represents the views and interpretations of the Centre. This publication does not represent the opinions or policies of NATO and is designed to provide an independent position.

Third-party sources are quoted as appropriate and the Centre is not responsible for the content of the external sources referenced in this publication. The Centre assumes no responsibility for any loss or harm arising from the use of information contained in this publication. Copies of this publication may be distributed for non-profit and non-commercial purpose only.

Contact

NATO Cooperative Cyber Defence Centre of Excellence

Filtri tee 12, Tallinn 10132, Estonia

publications@ccdcoe.org

www.ccdcoe.org

Contents

Introduction

The first reports of the Conficker worm virus, namely the first of its five variants[1], infecting computers emerged in November 2008.[2] The following massive spread of the malware – by December 2008 Conficker infection had been detected in more than 1.5 million IP addresses in 206 countries[3] – caused serious concern, as initial attempts to contain the malware did not achieve remarkable success and Conficker appeared to have considerable potential for causing damage, all the while IT security personnel and analysts alike had little or no insight into the intended use of the botnet of the infected and thereby remotely controllable computers.

By April 2009, the total number of Conficker infections detected in unique IP's had reached 35 million.[4] The systems involved included those of businesses, governmental institutions, non-governmental organisations, and individual users; the spread and operation of the malware affected the security of the global Domain Name System.

An unprecedented initiative to tackle Conficker was taken in early 2009. What had begun as an informal collaboration to contain the malware resulted in Microsoft, ICANN and operators within the Domain Name System, together with computer security researchers and security solutions vendors, forming the Conficker Working Group in February 2009.[5] By monitoring and analysing the malware, as well as following pre-emptive domain name registration effort in collaboration with Top Level Domain registrars globally, the Working Group largely succeeded in containing the spread and upgrading of Conficker by early summer 2009.

However, the threat has not lost its actuality due to the fact that hundreds of thousands of computers are likely to have remained infected by the malware[6] and thus are potentially controllable for malicious purposes[7]. Likewise, its importance remains as a valuable example of lessons learned from a cyber threat that exceeds most others by its scale and the degree of necessity for cooperation.

---

[1] Protect yourself from the Conficker Worm virus. Microsoft Safety & Security Center, http://www.microsoft.com/security/pc-security/conficker.aspx#EWC.

[2] Protecting Yourself from the Conficker Worm. McAfee http://www.mcafee.com/us/threat-center/conficker.aspx.

[3] Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. A Foray into Conficker's Logic and Rendezvous Points. Computer Science Laboratory, SRI International. [2009] http://www.usenix.org/event/leet09/tech/full_papers/porras/porras.pdf. P. 1.

[4] Infection Distribution. Conficker Working Group, 1 Apr 2009. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution.

[5] Microsoft Collaborates With Industry to Disrupt Conficker Worm. 12 Feb 2009. http://www.microsoft.com/presspass/press/2009/feb09/02-12ConfickerPR.mspx; Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf, p. 17.

[6] In October 2009, the number of systems infected with the A+B+C variants still remained at seven million. Conficker Working Group, 16 December 2009. http://www.confickerworkinggroup.org/wiki/pmwiki.php/Calendar/20091216; Conficker Is Down But Not Out. PC Tools, 10 March 2011. http://www.pctools.com/security-news/conficker-worm/.

[7] Conficker Working Group (2011), *supra* note 5, p. 27.

While the present paper will give a short synopsis of the known facts about the spread and characteristics of Conficker, it will not explore the technical details of the infection and propagation of Conficker in depth, neither will it analyse all the countermeasures used. There is excellent research available about the Conficker malware, which we recommend to those interested in a closer acquaintance with the subject; also, the Conficker Working Group, as well as some of its individual parties, has documented the mitigation effort in detail. A list of recommended reading can be found at the end of this paper.

The focuses of this paper are the legal and legal policy implications related to the creation, distribution and operation of the Conficker malware, as well as the legal implications related to the technical, procedural and organisational mitigation measures taken in response to the incident. Given the persisting uncertainty about the identity and intent of the author of Conficker, as well as the global spread of the malware and the fact that incident response involved a number of bodies in more than a hundred countries, it is inevitable that, instead of a comprehensive legal analysis, a choice needs to be made about the issues that a paper like this can tackle. Also, there is too little factual information available to offer definite legal assessments. However, some issues raised by Conficker either appear as novel developments in cyber security, or verify a trend of a presence of legal obstacles in responding to large-scale cyber incidents. For this reason, this paper focuses on three main topics: the preparedness of substantive criminal law to address sophisticated and large-scale cyber attacks, the registration of domain names as a method of cyber defence, and private and public sector collaboration.

Like earlier NATO CCD COE legal case studies, the analysis follows the concept of a Comprehensive Legal Approach to Cyber Security, whereby different fields of cyber-relevant law, such as national security law, criminal law, and private law dealing with contractual aspects of communications service provision, are not considered as conflicting but as complementing each other to support cyber security purposes. Also, as with other legal case studies of the NATO CCD COE, the audience of the paper extends from that of the legal profession and aims to address the issues for a wider 'DIMPLE' audience involving experts in relevant fields (Diplomacy, Intelligence, Military, Policy, Law, and Economy).

Finally, this paper reflects the opinions of its author and the author is responsible for all errors and omissions. The opinions contained in this paper do not necessarily reflect the position of the NATO CCD COE or any NATO entity.

Facts of the Case

Timeline: Evolution of the Conficker Worm and of the Containment Effort

Conficker, formally **W32/Conficker.worm**,[8] is a *worm virus**,[9] i.e. a piece of computer malware*, which operates by taking advantage of a vulnerability in the Windows operating system, consequently injecting malicious code into the Windows server service.[10] The devices infected by Conficker are linked to a remote computer and thereby become part of a botnet with potential to perform under the malware author's control.[11] As a computer worm, Conficker is self-propagatory (or self-replicating): it is capable of infecting other computers across a network, via removable drives or by exploiting weak passwords, while it employs several defensive mechanisms to prevent its removal.[12] Five variants of the Conficker worm were identified between November 2008 and April 2009, each increasing in sophistication and in the capacity of the malware to avoid detection and resist countermeasures.[13]

The operating systems potentially or actually affected by Conficker include Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008.[14]

There are several aliases for the worm, most notably **Downadup** (used by e.g. Symantec, BitDefender and F-Secure), **Kido** (used by Kaspersky Lab and VirusBuster) and **Downad** (used by TrendMicro).[15]

While Microsoft patched the vulnerability almost a month before the release of the worm,[16] the common practice of delay and neglect by computer users and system managers to keep computer operating systems and antivirus software up-to-date, as well as the widespread

---

[8] Encyclopedia: Win32/Conficker. Microsoft Malware Protection Center, 8 Jan 2009, updated 17 Apr 2011. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fConficker&ThreatID=; Worm:W32/Downadup.AL. F-Secure Labs. http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml.

[9] For technical terms used in this paper and marked with an asterisk (*), an explanation is provided in the *Glossary* section at the end of the paper.

[10] Piscitello, Dave. Conficker Summary and Review. ICANN, 7 May 2010. http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf. P. 3.

[11] Conficker Working Group (2011), *supra* note 5, p. 3.

[12] Encyclopedia: Win32/Conficker (2011), *supra* note 8; Conficker Working Group (2011), *supra* note 5, p. 5.

[13] Protect yourself from the Conficker Worm virus. *Supra* note 1.

[14] Microsoft Security Bulletin MS08-067 – Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644). Microsoft Security TechCenter, 23 Oct 2008. http://technet.microsoft.com/en-us/security/bulletin/ms08-067.

[15] Encyclopedia: Win32/Conficker (2011), *supra* note 8; Encyclopedia: Worm:Win32/Conficker.E. Microsoft Malware Protection Center, 9 Apr 2009, updated 17 Apr 2011. http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.E; Worm:W32/Downadup.AL, , *supra* note 8.

[16] Microsoft Security Bulletin MS08-067 (2008), *supra* note 14.

use of counterfeit software that might not be eligible for official upgrades[17], facilitated the initial infection of systems by the Conficker worm and the later malware-initiated updates for new variants. It must be noted that the neglect or delay in applying (automated) software patches may in some cases be a conscious choice with the purpose of controlling system stability,[18] and thus not necessarily caused by user ignorance or negligence.[19]

The methods used by Conficker's author to spread the worm and counter security measures were not novel *per se*, and have been used earlier by malware authors. Conficker's uniqueness as a threat and its rapid spread was due to an efficient combination of multiple methods of distribution, multiple counter-measures, and the quick release of the malware following the publication of the vulnerability in Windows.[20]

The following is a brief chronology of the spread of Conficker and of the countermeasures employed. Both the spread and evolution of the malware and the security community's response action are displayed on a single timeline to illustrate the interaction that can take place in a cyber 'conflict' situation and the need for rapid adaptability on the side of the defence. Therefore, less emphasis is placed on an in-depth explanation of the features of the malware and the background of mitigation efforts – for those interested in a closer analysis, reference is made in the *Recommended Reading* section at the end of this paper to earlier excellent documentation and research carried out by other organisations.

Conficker variant naming in this paper follows the system used by Microsoft, while alternative names used especially by the Conficker Working Group[21] and SRI[22] are given in brackets in parallel where applicable.

[17] As noted by the Conficker Working Group Lessons Learned Report, Microsoft offers security updates also to pirated copies of Windows, but these updates are not universally available and not all users are willing to potentially identify themselves as using counterfeit copies of Windows. Conficker Working Group (2011), *supra* note 5, p. 11.

[18] Porras, Saïdi, Yegneswaran (2009), *supra* note 3, p. 1.

[19] There are several reasons why prompt or automated application of software updates may be avoided: such updates may not have consideration for existing system configuration and may conflict with certain services required by the user, also, automated system restart initiated by updates may not re-launch all required services and processes. For these reasons, prior testing of the updates at the user's system and supervised update installation is sometimes preferred.

[20] Conficker Working Group (2011), *supra* note 5, p. 5.

[21] *Ibid*.

[22] Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. An Analysis of Conficker's Logic and Rendezvous Points. SRI International Technical Report. Released 4 Feb 2009 (updated 19 Mar 2009). http://mtc.sri.com/Conficker/.

October-November 2008: Vulnerability Exposed and First Variant of the Worm

Conficker activity

Response of the cyber security community

On 23 October 2008, Microsoft releases a critical security patch for a vulnerability found in the Windows operating system, informing users that the vulnerability could allow execution of computer code from a remote location.[23]

On 21 November 2008, **Win32/Conficker.A**[24], the initial variant of the Conficker malware, is reported to Microsoft.[25]

Conficker.A was discovered as it began attempting to infect systems that had not been patched with the critical security update released by Microsoft on 23 October 2008.[26] The worm then spread further among computers connected within an intranet, meaning that one unpatched machine could quickly become a doorway leading to there being numerous infected computers within an organisation.[27]

Conficker.A involved a spreading mechanism that generated daily a list of 250 domains from five Top Level Domains (.com, .net, .org, .info and .biz) and attempted to connect to them every three hours to download new instructions.[28] To prevent identification of generated domains and subsequent registration of these domains in order to gain control of the botnet, encryption was used.[29]

As a defensive mechanism, the malware reset the System Restore Point of computers in order to avoid tracking the changes made in the Windows operating system or restoring the operating system to an earlier, uninfected state.[30]

[23] Microsoft Security Bulletin MS08-067 (2008), *supra* note 14.
[24] Encyclopedia: Worm:Win32/Conficker.A. Microsoft Malware Protection Center, published 24 Nov 2008, updated 17 Apr 2011. http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.A.
[25] Protect yourself from the Conficker Worm virus. *Supra* note 1.
[26] Conficker Working Group (2011), *supra* note 5, p. 5; Microsoft Security Bulletin MS08-067 (2008), *supra* note 14.
[27] Conficker Working Group (2011), *supra* note 5, p. 5.
[28] Encyclopedia: Win32/Conficker (2011), *supra* note 8; Conficker Working Group (2011), *supra* note 5, p. 5.
[29] Conficker Working Group (2011), *supra* note 5, p. 5.
[30] Encyclopedia: Win32/Conficker (2011), *supra* note 8.

On 29 December 2008, **Win32/Conficker.B** is reported to Microsoft.[31]. This is 38 days after the release of variant .A. Its 'payload* activation date'* – when the malware would begin attempting to connect with new domains – is set to 1 January 2009.[32]

Variant .B continued to utilise the functionality of variant .A, but used a different method of domain name generation[33] and added three additional country code top level domains (.cn, .ws and .cc for Canada, Samoa and the Cocos Islands, respectively).[34] In addition to the spreading methods employed by Conficker.A, the new variant spread via shared segments of the computer network that were not password-protected or were protected by weak passwords that could be broken by systematic automated password attempts (so-called *brute force* attacks), as well as by mapped and removable drives, such as removable USB storage devices, forcing the launch of an executable file every time a removable drive was inserted into the system.[35] The latter enabled Conficker.B to spread even to computers that were not connected to the infected network. Variant .B was more difficult to detect and remove than variant .A, in that it blocked access to many security-related websites, modified system settings and terminated certain system and security services,[36] including popular antivirus products found on the computer.[37] Interestingly, Conficker.B also avoided connecting to domains that were connected to cyber security researchers and identified honeypots*.[38]

January 2009: Spontaneous Collaborative Mitigation Efforts

In January 2009, Support Intelligence[39] launches a 'pre-emptive registration' initiative to enable monitoring of Conficker traffic, analyse the infection, identify infected hosts, and estimate the size of the botnet.[40]

The initial pre-emptive registration involved 500 domain names, which were identified by analysing the Conficker domain generation algorithm. Identified domain names were registered in order to prevent Conficker-infected hosts from communicating with command and control

[31] Protect yourself from the Conficker Worm virus. *Supra* note 1.
[32] Encyclopedia: Win32/Conficker (2011), *supra* note 8; Timeline. Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline (last modified on 26 April 2009).
[33] Encyclopedia: Win32/Conficker (2011), *ibid.*
[34] Conficker Working Group (2011), *supra* note 5, p. 6.
[35] Encyclopedia: Win32/Conficker (2011), *supra* note 8; Porras, Saïdi, Yegneswaran (2009), *supra* note 3, p. 5.
[36] Encyclopedia: Win32/Conficker (2011), *ibid*.
[37] Conficker Working Group (2011), *supra* note 5, p. 6.
[38] *Ibid.*
[39] Support Intelligence (www.support-intelligence.com) (established in 2006) is a network security company based in San Francisco, California, U.S.A. The company also participated in the Conficker Working Group.
[40] Piscitello (2010), *supra* note 10, p. 5.

(C&C) servers*and to enable directing data flow to so-called 'sinkholing hosts', under the control of security researchers and malware analysts, for further monitoring and analysis of the Conficker bot traffic.[41] (See section *Pre-emptive Domain Name Registration as a Method of Mitigation* below for a closer overview on domain name management and coordination of domain registration in mitigation) These activities, including the payment of mandatory domain registration fees, were funded by Support Intelligence from the organisation's own resources.[42]

In January 2009, organisations such as Symantec[43], Kaspersky[44], and eNom[45] begin contributing funds to assist Support Intelligence in payment of domain registration fees with the objective of containing Conficker.[46]

On 28 January 2009, a Support Intelligence researcher contacts ICANN regarding Conficker in order to obtain financial relief or reimbursement from registry fees for Conficker-affected domain names.[47]

On 31 January 2009, the pre-emptive registration initiative of Support Intelligence becomes known to Neustar[48] via informal cooperation.[49] Neustar turns to ICANN with a request to waive their mandatory registration fee on the grounds that the registration is related to protecting the security of the Domain Name System.[50]

At this stage of mitigation, operating system and security software vendors (*Microsoft, Symantec, F-Secure*), security research organisations (*Shadowserver Foundation, Team CYMRU*) and the intelligence community (*US Federal Bureau of Investigation, US Secret Service and the US Department of Defence*) had been monitoring and analysing the Conficker malware and

[41] *Ibid.*
[42] *Ibid.*
[43] Symantec (www.symantec.com) (founded 1986), a leading security, storage and systems management solutions provider. Headquarters in Mountain View, California, U.S.A.; participant in the Conficker Working Group.
[44] Kaspersky Lab (www.kaspersky.com) (founded in 1997), IT security software vendor. Headquarters in Moscow, Russia; participant in the Conficker Working Group.
[45] eNom, Inc. (www.enom.com/), ICANN-accredited domain name registrar and provider of web hosting and monitoring services. Headquarters in Kirkland, Washington, U.S.A.
[46] Piscitello (2010), *supra* note 10, p. 6.
[47] *Ibid*, p. 5.
[48] Neustar is the registry operator that manages .biz domains. Conficker Working Group (2011), *supra* note 5, p. 17.
[49] Piscitello (2010), *supra* note 10, p. 6.
[50] Conficker Working Group (2011), *supra* note 5, p. 17.

cooperated to contain the threat. F-Secure had been involved in 'sinkholing' domain names that Conficker bots were attempting to contact; Top Level Domain operators (*VeriSign, Afilias, Neustar, PIR, and WS*) and ICANN were cooperating in the pre-emptive registration effort.[51]

February 2009: Mitigation Becomes Organised

The ICANN-organised Global DNS Security, Stability and Resiliency Symposium takes place in Atlanta, Georgia, USA on 3-4 February 2009. The symposium, while arranged unrelated to Conficker, becomes a kick-off for coordinating the registration of domains, and defines the initial structure for the Conficker Working Group.[52]

As a result of the symposium, operators of affected registries volunteered their participation to block domain names, while ICANN agreed to coordinate pre-emptive registrations with Country Code Top Level Domain (CC TLDs) registrars, as well as to consider declaring the Conficker response an exceptional case qualifying for waiver of registration fees. ICANN also agreed to manage a contractual waiver to enable registries to continue pre-emptive registration activities through 1 April 2009.[53]

On 4 February 2009 (71 days after Conficker.A and 37 days after Conficker.B were detected), SRI releases the initial version of 'An Analysis Of Conficker's Logic And Rendezvous Points',[54] containing analyses of Conficker's control flow, download and validation pattern, its domain generation algorithm and propagation method. The report also provides an empirical analysis of the outbreak, outlining the temporal and geographic patterns of Conficker variants .A and .B, and touches upon potential attribution issues.

[51] Piscitello (2010), *supra* note 10, p. 7.
[52] Conficker Working Group (2011), *supra* note 5, p. 18.
[53] Piscitello (2010), *supra* note 10, p. 6.
[54] Porras, Saïdi, Yegneswaran (2009), *supra* note 22.

On 12 February 2009, Microsoft issues a press release announcing a partnership with technology industry leaders and academia to implement a coordinated global response to Conficker and offering a 250,000 USD reward for information leading to the arrest and conviction of Conficker's author.[55] This event marks the official launch of the Conficker Working Group.[56]

Organisations involved in the Conficker Working Group included Microsoft, ICANN, NeuStar, VeriSign, CNNIC, Afilias, Public Internet Registry, Global Domains International Inc. (Top Level Domain registries); M1D Global, AOL, Symantec, F-Secure, ISC (security product and service vendors); researchers from Georgia Tech, the Shadowserver Foundation, Arbor Networks (computer security research organisations); and Support Intelligence. Later, other organisations joined the Group.[57]

The Conficker Working Group was by nature an *ad hoc* organisation with a minimally defined leadership; no organisation within the group had a leading role. Each collaborating party participated according to their core competency as malware researchers, traffic analysis engineers, domain registries (with ICANN aiding in inter-registry communications), etc.[58]

Second half of February 2009: Conficker turns Peer-to-Peer

On 20 February 2009, **Win32/Conficker.C** (.B++) is reported to Microsoft,[59] 53 days after the release of .B variant.

Conficker C (.B++) was very similar to Conficker.B.[60] It used the same methods for spreading as variant .B, but added ways for downloading files to utilise peer-to-peer communications, enabling infected computers to communicate with each other without the need for a central server and thereby hampering countermeasures applied to stop the worm. Variant .C included checks to verify the authenticity/validity of content targeted for download;[61] its defined payload activation date also matched that of 1 January 2009.[62]

On 4 March 2009, 12 days after the release of .C (.B++) variant, **Win32/Conficker.D** (.C) is reported to Microsoft.[63]

[55] Microsoft Collaborates With Industry to Disrupt Conficker Worm (2009). *Supra* note 5.
[56] *Ibid.*
[57] For the full list of Conficker Working Group members, see Annex A of Conficker Working Group (2011), *supra* note 5, p. 43.
[58] Piscitello (2010), *supra* note 10, p. 10; Conficker Working Group (2011), *supra* note 5, p. 24.
[59] Protect yourself from the Conficker Worm virus. *Supra* note 1.
[60] Conficker Working Group (2011), *supra* note 5, p. 7.
[61] Encyclopedia: Win32/Conficker (2011), supra note 8.
[62] Conficker Timeline (2009), *supra* note 32.
[63] Protect yourself from the Conficker Worm virus. *Supra* note 1.

Variant .D was distributed as an update to machines that had already been infected with earlier variants (.B and .C/.B++).[64] Further spreading functionality was removed from this variant. The malware continued to expand on its file downloading capacity, generating 50,000 URLs to download files from, but utilising 'only' 500 of the generated URLs within a 24-hour period.[65] The list of Top Level Domains was increased by a number of country code Top Level Domains, making the total number of Top Level Domains involved to be more than a hundred, which considerably complicated mitigation coordination efforts.[66]

The .D (.C) variant expanded the set of measures used to hinder its removal from an affected machine by disabling a yet broader range of computer security processes, especially those designed specifically to remove Conficker. In addition, it blocked access to additional security-related websites,[67] disabled safe mode on the computers it infected, and deleted prior restore points on the computer.[68]

On 8 March 2009, SRI Conficker.C (**Win32/Conficker.D**) analysis is released, containing an overview of the new malware version, its domain generation algorithm, peer-to-peer logic, and other distinctive features. The review also includes an analysis of interactions of Conficker.C when operating live on the Internet.[69]

On 15 March 2009, a number of hosts update to **Win32/Conficker.D** (.C).[70]

April 2009: Mitigation becomes Proactive;
Increased Public Attention to both the Malware and Counter-efforts

On 26 March 2009, F-Secure publishes Conficker FAQ[71] – a public education tool to inform users about the expected events inflicted by the activation of Conficker.D (.C).

On 30 March 2009, the Honeynet Project releases 'Know Your Enemy: Containing

[64] Encyclopedia: Win32/Conficker (2011), supra note 8.
[65] *Ibid.*
[66] Conficker Working Group (2011), *supra* note 5, p. 7.
[67] Encyclopedia: Win32/Conficker (2011), supra note 8.
[68] Conficker Working Group (2011), *supra* note 5, p. 7.
[69] Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. Conficker C Analysis. SRI International Technical Report, Addendum. 8 March 2009 (last update 4 Apr 2009). http://mtc.sri.com/Conficker/addendumC/index.html.
[70] Conficker Timeline (2009), *supra* note 32.
[71] Questions and Answers: Conficker and April 1st. 26 Mar 2009. F-Secure, http://www.f-secure.com/weblog/archives/00001636.html.

Conficker', facilitating identification of Conficker.D (.C)[72] infection on computer systems.[73] Following this (from 31 March 2009), detection signatures for Conficker.A/.B/.C/.D (A/B/B++/C) are made available and included in commercial network scanners.[74]

1 April 2009 is the defined payload activation date for Conficker.E.[75]

On 3 April 2009, SRI releases a peer-to-peer detector for Conficker.D (.C), enabling the detection of the presence of Conficker-infected hosts within the boundary of a computer network (e.g. the network of an organisation or entity as a whole).[76]

On 7 April 2009, the Honeynet Project releases the revised version of 'Know your Enemy: Containing Conficker', containing updated information about the malware and tools for remedy.[77]

April 2009: Last Variant of Conficker Released;
Tools for Detecting and Removing Conficker Become Widely Available

On 8 April 2009, **Win32/Conficker.E** is reported to Microsoft[78], 33 days after the release of the previous variant, and 8 days after the release of the Honeynet Project analysis.

Conficker.E[79] again involved no spreading functionality, but updated machines previously infected with any of the earlier variants, possibly employing the Conficker peer-to-peer network

[72] Leder and Werner appear to use the same Conficker naming system as the Conficker Working Group, with their text referring to variant .C.
[73] Leder, Felix; Werner, Tillmann. Know Your Enemy: Containing Conficker. To Tame A Malware. The Honeynet Project. 30 Mar 2009 (updated 7 Apr 2009). http://www.honeynet.org/files/KYE-Conficker.pdf.
[74] Piscitello (2010), *supra* note 10, p. 9; Conficker Timeline (2009), *supra* note 32.
[75] Conficker Timeline (2009), *ibid*.
[76] Yegneswaran, Vinod. Conficker C Active P2P Scanner. Version 0.1B. Computer Science Laboratory, SRI International. http://mtc.sri.com/Conficker/contrib/scanner.html.
[77] Leder, Werner (2009), *supra* note 73; Conficker Timeline (2009), *supra* note 32.
[78] Protect yourself from the Conficker Worm virus. *Supra* note 1.
[79] Note that there is no alternative name for this variant.

for this purpose. Similarly to previously released variants, it modified system settings, terminated system and security services, and blocked access to security-related websites.[80]

The variant installed Waledac, an e-mail worm able to steal data and send spam, and SpywareProtect2009, a scareware* antivirus product that 'advised' computer users to buy fake antivirus software for an alleged malware infection.[81]

The payload was set to trigger on 1 April 2009, but to terminate itself on 3 May 2009[82] and revert to Conficker.D (.C).[83]

On 15 April 2009 Simple Conficker Scanner v2 is released by The Honeynet Project. The scanner makes detection of .E (.D) variant infection available.[84]

On 3 May 2009, self-termination of Conficker.E occurs. The malware reverts back to Conficker.D (.C).

On 2 June 2009, Symantec releases edition 2 of the 'Downadup Codex: a Comprehensive Guide to the Threat's Mechanics'.[85]

On 21 September 2009, SRI releases a Conficker.D (.C) P2P Protocol and Implementation Analysis, containing a description of the new method used by Conficker authors to include an infected machine on to the Conficker network.[86]

In October 2009, the Shadowserver Foundation estimates the number of systems infected by Conficker.A/.B/.D variants to have reached 7 million.[87] Considering that the botnet could have been retaken by its creator should the effort to block domains have waned,[88] the

[80] Encyclopedia: Win32/Conficker (2011), *supra* note 8.
[81] Conficker Working Group (2011), *supra* note 5, p. 8; Gostev, Alexander. The neverending story. 9 April 2009. http://www.securelist.com/en/weblog?weblogid=208187654; 'Watch out for fake virus alerts.' Microsoft Safety & Security Center, http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx.
[82] Encyclopedia: Win32/Conficker (2011), supra note 8.
[83] Conficker Working Group (2011), *supra* note 5, p. 8.
[84] Werner, Tillman. Simple Conficker Scanner v2. 15 Apr 2009. http://www.honeynet.org/node/397.
[85] Conficker Timeline (2009), *supra* note 32; Nahorney, Ben. The Downadup Codex, Edition 2.0. Symantec, 29 Jun 2009. http://www.symantec.com/connect/blogs/downadup-codex-edition-20
[86] Piscitello (2010), *supra* note 10, p. 9
[87] Conficker. Shadowserver Foundation [2009], http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker
[88] Conficker Working Group (2011), *supra* note 5, p. 27.

Conficker Working Group opted for a long-term approach, committing to continue with the pre-registration of domain names as long as the threat remained.[89]

While the *Conficker Working Group Lessons Learned* report does not claim this, it is highly likely that malicious usage of the Conficker botnet was prevented by the Group's efforts, in that the Conficker Working Group was too visible and too active, and thereby hindered the formation of the botnet to the desired state. It is also possible that the creator of Conficker was waiting for attractive or profitable instances to use the botnet, such as its rental to other parties, and lost the momentum in the course of the increasingly effective mitigation against the malware.

Affected Organisations

A graphic overview provided by the Conficker Working Group on the global distribution of Conficker infection shows that the spread of the malware spans all populated continents,[90] with over 6000 infected hosts[91] in 184 countries and territories, according to the Shadowserver Foundation.[92]

Due to the design of Conficker to target any vulnerable systems, and not specific systems in particular, the entities affected by Conficker include a variety of organisations from both the private (enterprises, industry, academia, etc.) and public spheres (state and local governments, military, other public administration organisations) as well as individual users. In that variants of Conficker included the capacity to replicate via USB drives, the worm spread even to secure networks when infected USB devices, such as memory sticks, were used. As detection of the malware was prevented by several methods employed by Conficker, such infection could go undetected for a significant time. However, it is important to remember that the worm affected only systems running on the Windows operating system. Systems that were for security or other reasons running on Linux, Mac OS, or others, were unaffected.[93]

Given the lack of consistent data, the following overview of affected organisations is largely indicative, but provides a better understanding of the effect of the malware than mere statistics.

Government and Public Administration

In the **USA**, the *municipal court system* in the city of Houston, Texas was severely disrupted for days due to Conficker worm infection. The police had to temporarily stop arrests for minor offences and court hearings were postponed for at least three days.[94] Likewise, the *Texas Department of Public Safety* was affected by the malware, with administrative

[89] *Ibid.*, pp. 27-28.
[90] CWG: Infection Distribution (2009). *Supra* note 4.
[91] Shadowserver lists infected hosts by Autonomous System Number (an ASN is an identifier for a collection of IP networks and routers under the control of one entity), including only ASNs with 10 or more Conficker IP's on the list. This excludes episodic incidents and only shows systems with a more severe infection.
[92] Shadowserver [2009], *supra* note 87.
[93] F-Secure, *supra* note 71.
[94] Leyden, John. Houston justice system laid low by Conficker worm. The Register, 9 Feb 2009. http://www.theregister.co.uk/2009/02/09/houston_malware_infection/

functions, such as issuing driver licences and patrol police communications, temporarily disrupted.[95]

The computer system of the *House of Commons of the Parliament* of the **United Kingdom** was infected with the Conficker malware in March 2009. Little detail is available of the effects of the malware; a memo from the Parliamentary ICT service stated that the virus caused a slow-down of the network and locked out some accounts.[96]

The UK *Ministry of Defence* reported a Conficker infection in its IT systems, including e-mail and internet access aboard its warships. The report stressed that no weaponry or navigation systems had been affected, and that no infections were detected on any networks that had sensitive information.[97] However, some systems were still unavailable two weeks after the incident occurred.[98]

An infection in the IT system of *Manchester City Council* caused a 1.5 million GBP loss as a fine processing system was taken offline.[99] As late as January 2010, *Greater Manchester Police* was disconnected from a national police database for more than three days because of an infection with the Conficker virus.[100]

Bundeswehr, the armed forces of **Germany**, reported a Conficker infection in February 2009.[101] Likewise, the **French** navy computer network, *Intramar*, was affected by Conficker, forcing their fighter planes to be grounded as a result of a network quarantine.[102]

Public Services

The **United Kingdom** *National Health Service* experienced Conficker infections in five hospitals in Sheffield and two in Scotland, requiring rescheduling of patient appointments.[103]

---

[95] Want a first-time driver's license? Not possible today, so far. Statesman.com, 15 Apr 2009. http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2009/04/15/want_a_firsttime_drivers_licen.html; Plohetski, Tony. DPS computer network hit by virus: Officials will work through the weekend to restore service. American-Statesman, 18 Apr 2009. http://www.statesman.com/news/content/news/stories/local/04/18/0418dpsworm.html

[96] Leyden, John. Leaked memo says Conficker pwns Parliament. The Register, 27 Mar 2009. http://www.theregister.co.uk/2009/03/27/conficker_parliament_infection/

[97] Wattanajantra, Asavin. Royal Navy systems hit by computer virus. IT Pro, 16 Jan 2009. http://www.itpro.co.uk/609550/royal-navy-systems-hit-by-computer-virus

[98] Page, Lewis. MoD networks still malware-plagued after two weeks. The Register, 20 Jan 2009. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/

[99] Leyden, John. Conficker left Manchester unable to issue traffic tickets. The Register, 1 Jul 2009. http://www.theregister.co.uk/2009/07/01/conficker_council_infection/

[100] Conficker virus hits Manchester Police computers. BBC News, 2 February 2010. http://news.bbc.co.uk/2/hi/uk_news/england/manchester/8492669.stm

[101] Dubsky, Daniel. Conficker-Wurm infiziert hunderte Bundeswehr-Rechner. IT Espresso.de, 16 February 2009. http://www.itespresso.de/2009/02/16/conficker-wurm-infiziert-hunderte-bundeswehr-rechner/

[102] Willsher, Kim. French fighter planes grounded by computer virus. The Telegraph, 7 Feb 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

[103] Wattanajantra, Asavin, Conficker worm hits hospital PCs in Sheffield. IT Pro, 23 Jan 2009. http://www.itpro.co.uk/609615/conficker-worm-hits-hospital-pcs-in-sheffield;

Similarly, in the **USA**, an undisclosed number of hospitals and medical institutions were affected by Conficker infections in their systems. In some cases, medically critical devices such as computers controlling magnetic resonance imaging (MRI) devices and heart monitors were involved.[104] A further complicating factor was the reported legal requirement preventing data or system modification for a 90-day period, which sustained both the infections and the exposing vulnerabilities.[105]

Other Organisations

Other Conficker-affected entities included banks,[106] educational and research institutions,[107] and a number of unspecified organisations worldwide[108].

Origin of Conficker

Despite extensive research on the worm and defensive efforts by numerous entities, including those involved in the Conficker Working Group, and the reward announced by Microsoft for information leading to the arrest and conviction of the author of Conficker,[109] the author(s) of the malware have to date not been publicly identified,[110] nor is there clarity about the intended purpose of the worm.[111]

Some particularities of the Conficker worm have led researchers to believe that the author may be of Ukrainian origin,[112] but these indications are insufficient to positively identify the

---

Heath, Nick. Downadup virus hits PCs at five Sheffield hospitals. Silicon.com, 22 Jan 2009. http://www.zdnet.co.uk/news/security-management/2009/01/22/downadup-virus-hits-pcs-at-five-sheffield-hospitals-39599480/;
Williams, Christopher. Conficker seizes city's hospital network. The Register, 20 Jan 2009. http://www.theregister.co.uk/2009/01/20/sheffield_conficker/;
Leyden, John. Scottish hospitals laid low by malware infection. The Register, 9th March 2009. http://www.theregister.co.uk/2009/03/09/scot_hostpitals_malware_infection/;
Williams, Martin. Computer virus strikes hospitals. Herald Scotland, 6 MAR 2009. http://www.heraldscotland.com/computer-virus-strikes-hospitals-1.904470

[104] Mills, Elinor. Conficker infected critical hospital equipment. CNET News, 24 Apr 2009. http://www.zdnet.com/news/conficker-infected-critical-hospital-equipment/291619

[105] Jones, Michael W. Federal rules leave medical equipment virus-infected. Tech Blorge, 3 May 2009. http://tech.blorge.com/Structure:%20/2009/05/03/federal-rules-leave-medical-equipment-virus-infected/

[106] Tindal, Suzanne. Conficker worm strikes ANZ Bank. ZDNet Australia, May 6, 2009. http://www.zdnetasia.com/conficker-worm-strikes-anz-bank-62053800.htm

[107] Weinstein, Natalie. Report: Conficker worm bites University of Utah. CNet News, 12 April 2009. http://news.cnet.com/report-conficker-worm-bites-university-of-utah/

[108] *See* ASN Charts at Conficker. Shadowserver [2009], *supra* note 87.

[109] Microsoft Collaborates With Industry to Disrupt Conficker Worm. 12 Feb 2009. http://www.microsoft.com/presspass/press/2009/feb09/02-12ConfickerPR.mspx

[110] Conficker Is Down But Not Out. PC Tools, 10 Mar 2011. http://www.pctools.com/security-news/conficker-worm/ (15 Mar 2012);
Empak, Jesse. Years-old Conficker Worm Still A Threat. 27 Jan 2011. http://www.ibtimes.com/articles/105943/20110127/conficker-worm-still-threat.htm

[111] Conficker Working Group (2011), *supra* note 5, p. 2.

[112] The original version of Conficker ran a check for a Ukrainian keyboard to avoid infecting computers using one – possibly in order to avoid violating local laws. *See* Conficker Working Group (2011), *supra* note 5, pp. 6, 9; Porras, Saïdi, Yegneswaran (2009), *supra* note 3, p. 8.

source. Also, the degree of sophistication and rapid adaptability of Conficker points to the presence of notable resources, leading some researchers to suggest the presence behind Conficker of a criminal organisation or a nation-state. However, evidence to support authorship of a nation-state behind the malware is limited.[113]

Analysts share the opinion that whoever wrote Conficker is a skilled software developer with advanced capability in cryptography and strong domain knowledge.[114] The nature and evolution of the malware also indicate at least some form of coordination behind the worm.[115]

Also, a later version of the malware (Conficker E) involved a component downloaded from a Ukrainian server. *See* Krebs, Brian. Conficker Worm Awakens, Downloads Rogue Anti-Virus Software. *Washington Post*, 10 April 2009. Available http://voices.washingtonpost.com/securityfix/2009/04/conficker_worm_awakens_downloa.html

[113] Conficker Working Group (2011), *supra* note 5, p. 9

[114] Leder, Werner (2009), *supra* note 73, p. 20

[115] *Ibid.*, pp. 20-21

Legal Considerations

Creation, Distribution and Operation of Conficker as an Object of Criminal Law

In general terms, there is no dispute that the chain of activities ranging from the creation to the distribution to the operation of malware such as Conficker falls within the scope of criminal (penal) law. What makes a specific legal 'diagnosis' difficult in Conficker's case is the lack of insight into the purpose that Conficker was designed and intended for, as well as the fact that the malware was never actively used in its perceived capacity to target (critical) information infrastructure. An additional factor that complicates the qualification – and thereby investigation – of the creation, distribution and operation of Conficker is the involvement of a large number of legal systems applicable in the countries where Conficker activities took place or where the affected entities were located and which are therefore relevant to criminal proceedings.

International harmonisation efforts in the field of cybercrime law have produced the Council of Europe Convention on Cybercrime, the only binding international treaty on the subject to have been adopted to date.[116] Currently 37 countries have brought the Treaty into effect nationally,[117] including 21 NATO nations;[118] many more have used the Treaty as a model for shaping their national cybercrime law.[119]

Due to the domestic nature of criminal law, the Convention is not directly applicable in countries that are parties to the Treaty, but is implemented by adopting its provisions into national criminal law. There are numerous factors – ranging from the nation's political choices and legal culture in general, to the level of development of information society and lessons learned from earlier cyber incidents – that ultimately define the actual application of the Treaty positions in each nation that is party to the Treaty. Also, the Convention on Cybercrime permits reservations from certain positions of the Treaty, as well as to define additional qualifying requirements for some offences. The choice of the legislator to utilise the discretion allowed by the Treaty for these reservations, or refrain from doing so, as well as the choice of a wider or a more casuistic approach will have an effect on the qualification of Conficker as a criminal offence under national criminal law. The following evaluation

[116] Council of Europe, Convention on Cybercrime. ETS No. 185. Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[117] The number of signatory nations is larger: as of September 2012, there are 47 signatories; in four nations, entry into force of the Convention is due in 2012.

[118] The following NATO Nations are parties to the Treaty and have enforced the Treaty domestically: Albania, Bulgaria, Croatia, Denmark, Estonia, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, Spain, United Kingdom and the United States of America.
The following NATO Nations are signatories to the convention, but have not brought the Treaty into effect: Belgium (entry into force due 1 Dec 2012), Czech Republic, Greece, Luxembourg, Poland, Turkey, and Canada. *See* the list of signatories of the Convention on Cybercrime, CETS No.: 185, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (status as of 28 Sept 2012)

[119] Schulman, Cristina. The global state of cybercrime legislation. Cybercrime Unit, Directorate General Human Rights and Rule of Law, Council of Europe. June 2012. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations/WS1_coe_cyber_Octopus_ws%201_6June12.pdf

therefore applies as a general assessment, where the actual domestic application of the Treaty remains a matter of national implementation.

The Convention on Cybercrime criminalises the following offences targeted against the confidentiality, integrity and availability of computer data and systems: *illegal access* to a computer system without right (Article 2); *illegal interception* of data communications (Article 3); *data interference* (Article 4); *system interference* (Article 5); and *misuse of devices* (Article 6).[120] In the case of Conficker, its defence and *modus operandi* point to the characteristics of several of these offences.

As demonstrated in the previous chapter, Conficker functions by purposefully accessing computer systems without relevant authorisation, and most likely even without the knowledge of the owner or other right holder of the computer system. By design, Conficker was created to gain access even where security measures, such as passwords, had been applied, even though infringement of security measures was not an inherent element of each individual infection (e.g. in the cases where access was gained by exploiting shared or mapped drives that were not password-protected). The technique employed by Conficker could therefore, in principle, qualify as an offence of *illegal access* (Article 2) under the Cybercrime Convention.

One of the characteristics of Conficker was to alter and damage computer data,[121] blocking the application of system updates or antivirus software. Also, Conficker (since variant .A) reset system restore points in the affected computer, disabling the option to return the system to an uninfected state, which can be viewed as an *alteration* of computer data. In that, Conficker activity damaged 'the integrity and the proper functioning or use of stored computer data or computer programs'[122] and therefore would qualify as *data interference* under Article 4 of the Cybercrime Convention.

It is also perceptible from the facts of the case that the distribution and operation of Conficker constituted the activities identified in Article 5 (inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), and by means of these activities significant and presumably intentional[123] deterioration of the functioning of computer systems took place, which would qualify as the offence of *system interference* under Article 5.

The production, sale, distribution or making available by other means and possession of malware designed primarily for the purpose of committing the offences referred to above

[120] Excerpts of the relevant articles and of the Explanatory Report are attached to this paper (see Annex).

[121] Note that the Convention view of 'computer data' encompasses both 'useful information' produced by the software as well as the actual software itself: according to Article 1 b. of the Convention, 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

[122] Explanatory Report to the Convention on Cybercrime, Council of Europe. http://conventions.coe.int/treaty/en/reports/html/185.htm. Section 60.

[123] The intent of the perpetrator as a subjective category can, insofar as the author of Conficker remains unidentified, only be a speculation. Here this view is chosen as the more likely option, based on the information available in the case; of course, the actual qualification would be dependent on due criminal proceedings.

(illegal access, data interference, and system interference) constitute a criminal offence of *misuse of devices* under Article 6 of the Cybercrime Convention, if committed intentionally and without right. As the Conficker code was created as a tool to render possible these malicious activities, but was probably only used by the author of the malware, it is doubtful whether the activities would qualify as acts of 'distribution' (which refers to the active act of forwarding data to others) or 'making available' (which refers to the placing online devices for the use of others[124]). The *production* of malware for the purpose of gaining illegal access or interfering with the confidentiality, integrity and availability of computer data and systems is also criminalised under Article 6 of the Convention, but the Treaty parties are entitled to reservations in this regard so that domestic law may not necessarily regard mere malware creation as a criminal offence.

It is worth noting that the distribution of Waledac and SpywareProtect2009 within the Conficker.E variant could additionally be regarded as an offence, where the authors of these two malware items would be responsible for the production and the author of Conficker would be responsible for actively distributing them by means of malware in his possession.

The 'Serious Harm' Clause

Both Articles 4 (data interference) and 5 (system interference) include the notion of *seriousness*. In Article 4, the Treaty permits a reservation concerning data interference in that a Treaty party may limit criminal liability to cases where the conduct results in *serious harm*. Likewise, system interference is only considered an offence if the hindering of a computer system is *serious* (i.e. seriousness of consequence).

There are several complications involved in such an approach, and these may not be reconcilable for legal (the domestic nature of criminal law) as well as political (difficulties around reaching a consensus) reasons. Firstly, in neither case does the Treaty *define what constitutes such serious harm*: the interpretation is left to domestic legislation. While the Explanatory Report of the Convention provides some indication in the form of both qualitative and quantitative examples,[125] this does not substantially minimise the risk of extensive differences in the national approaches and low transparency as to their nature. Considering the multitude of national legal regimes that are involved in the criminal proceedings of a global cyber threat such as Conficker, this ambiguity regarding the actual or potential legal restraints undermines the effectiveness of response and elevates the cost of proceedings.

Another set of complications arises from *assessing the harm*, i.e. the actual determination of the level of damage that occurred. Most of the harm caused by Conficker consisted of indirect damage, resulting from the weeks of expert labour involved in the attempt to block the further spread of the worm. If national criminal law defines damage as a monetary

[124] Explanatory Report to the Convention on Cybercrime, section 72.

[125] Some indication regarding the offence of system interference (Article 5) is provided in the Convention's Explanatory Report, by referring to the possibility to define a minimum amount of damage or an example of reference to 'form, size or frequency' of intrusion that has 'a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems'. For the data interference (Article 4) clause, some understanding of national approaches may be gained through notification requirement tied to the right of reservation (any reservations should be notified to the Secretary General of the Council of Europe). *See* sections 64 and 67 of the Explanatory Report.

category, the evaluation and verification process of damage in an event of such a scale and scope as Conficker requires resources that the criminal justice system as well as the victim organisations may not be capable of offering. Also, the involvement of confidential data, business secrets, and guarantees to their confidentiality in cross-border investigations may contribute to unwillingness on the part of the victim organisations to disclose the amount of actual damage.

Harmonisation and greater transparency with regard to the national implementation of the Convention – including the notion of serious harm that is currently extensively left to domestic legislation and can play a decisive role in the qualification of a malicious cyber act as a crime – may gain even more significance as cyber incidents grow in scope (global extent) and scale (number of countries and organisations involved or affected).

Applying Countermeasures as a Potential Act of Cybercrime

An overly broad national law approach in criminalising certain cyber activities may, conversely, complicate cyber security efforts. As noted by Rodney Joffe of Neustar[126], legislation that was enacted to combat cybercrime 'has actually blocked computer scientists and government from releasing countermeasures —the equivalent of vaccines — to disable the malicious software.'[127] Joffe argued that legislation which 'criminalises the placement and execution of computer programs on a computer without the owner's permission' forces entities dealing with cyber incident responses to resort to more neutral yet less effective mitigation measures.[128] The prevailing practice relies on making defence tools available to users and depending on user motivation to use them, but this approach is inefficient in cases of user ignorance or neglect – in fact, the failure to apply the already released system updates was the very reason for the rapid spread of Conficker malware infections.

It should be noted that the Convention on Cybercrime does not *per se* require criminalising mitigation measures – even such measures that involve access to a victimised system without the system owner's or right holder's direct consent. As referenced in previous sections, the definition of *illegal access* under Article 2 and *data interference* under Article 4 of the Convention on Cybercrime include *intentional* activities *without right*. However, potential bases for justification are not limited to owner consent; justification could arise from a legal or regulatory requirement or the legitimate interest of another party to the security and integrity of their communications devices and services. In both of these provisions, the Treaty leaves room for national adaptation to exclude mitigation measures from the scope of cybercrime.[129]

Article 5 (system interference) involves serious hindering of *the proper functioning of a computer system* as a result of the unjustified activity, with the corresponding intent to seriously hinder. It is questionable whether countermeasures to disable the malicious software would therefore qualify as system interference in accordance with the Treaty.

---

[126] Neustar is a Top Level Domain operator that took an early initiative in the Conficker mitigation process; the organisation became a founding member of the Conficker Working Group.

[127] Joffe, Rodney. The cyber crime epidemic. National Post, 23 Oct 2009. http://www.solucom.com/content/news/index.php?news=99.

[128] *Ibid.*

[129] Article 2 of the Treaty foresees that a Treaty Party may require that the offence be committed by dishonest intent; Article 4 reserves the right to require that the conduct result in serious harm.

Likewise, Article 6 of the Convention includes three elements in the offence of misuse of devices: the act of production, distribution or otherwise making available devices or software must be committed *intentionally*; it must be committed *without right;* and such devices must be *primarily designed for,* or the *actor's intent be targeted to,* committing the crimes listed in Articles 2 to 5, i.e. illegal access (Article 2), illegal interception of data communications (Article 3), data interference (Article 4), and system interference (Article 5). Section 2 of the article states explicitly that Article 6 shall not be interpreted as imposing criminal liability where the actor's purpose is not to commit an offence established in accordance with Articles 2 to 5 of the Convention. Cases involving protection of a computer system are therefore to remain outside the scope of the offence. Likewise, where the purpose of the device or software is *primarily* legitimate (even if potentially usable for malicious purposes, i.e. so-called dual-use devices), they are excluded from the scope of the offence of misuse of devices under Article 6.

Therefore, when implementing the Convention domestically, care should be taken that national criminal law provisions would involve the consideration of the specific intent of the actor regarding the purpose of the device or software.

Of course, the mere fact that certain behaviour is not criminalised will not automatically imply its legitimacy. In order for mitigation to be lawful, the desired mitigation measures must have a proper basis in substantive law, and in defining the extent and prerequisites for permissible countermeasures to cyber attacks, mitigation efficiency needs to be balanced with user rights to privacy and inviolability of property. The placement and execution of remedial programs on a device without the permission of the owner or right holder could, in principle, be considered as an appropriate measure if justified by threat level and urgency of response, or the course of action could involve disconnecting the device from the network (a measure which is currently foreseen by the EU electronic communications law[130]).

Pre-emptive Domain Name Registration as a Method of Mitigation

The pre-emptive domain registration initiative was a novel approach[131] in the toolbox of countering a botnet, and as such deserves attention from a legal perspective.

To clarify the role of domain registration as a remedy in mitigation, the mechanics of the spread of Conficker need a brief reminder. Once Conficker connected an infected computer into the botnet, the malware running on the infected machine used a domain generation algorithm to generate a number of (pseudo) random domain names from which to download updates.[132] The early variants of Conficker generated 250 domains per day from

[130] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC and Regulation 544/2009, Article 13a.

[131] Conficker mitigation was not the first occasion for the use of preventive registration, but it was the first successful occasion on a large scale. Pre-emptive registration of domains used for botnet C&C was employed in late 2008 against the Srizbi botnet by the security firm FireEye in coordination with Microsoft, Verisign, and others, with some success, but the effort could not be sustained due to lack of funding. *See* Conficker Working Group (2011), *supra* note 5, p. 15.

[132] Leder, Werner (2009), *supra* note 73, p. 9; Piscitello (2010), *supra* note 10, p. 4. For a detailed explanation, *see* Leder, Werner (2009), *supra* note 73, pp. 9-13.

five and eight Top Level Domains respectively;[133] a later upgrade[134] extended the list of domains to 50,000 per day in 116 Top Level Domains.[135] Some of the selected domains would be registered by the creator of the malware and a name resolution service set up, allowing the resolving of domain names to the IP addresses of the botnet's C&C servers[136] – i.e. enabling connection with a control server in order to receive instructions.[137]

A precondition for the pre-emptive registration was successful reverse engineering of the malware code. This enabled replication of the domain generation algorithm and identification of the target domains, which would then be referred to the appropriate Top Level Domain registries or authorities on a daily basis.[138] As part of the pre-emptive registration action, domain name servers were configured to resolve to IP addresses under the control of cyber security organisations,[139] to so-called *sinkhole servers*, which served a twofold purpose: it prevented Conficker-infected hosts from communicating with the C&C server, and enabled monitoring of Conficker traffic, analysis of the infection and identification of the infected hosts, as well as estimates of the size of the botnet.[140]

In the early phase of Conficker mitigation, organisations such as Support Intelligence took the initiative to pre-register the Conficker-generated domain names in order to prevent the malware from retrieving updates, as well as to track infected hosts.[141] After the February 2009 ICANN conference in Atlanta, DNS registration and blocking was taken on by the Conficker Working Group, which formed a subgroup dedicated to registration activities.[142] Pre-emptive registrations on Country Code Top Level Domain (ccTLD) levels were coordinated by ICANN, which was also the facilitator of communications among the participants.[143]

[133] Conficker.A .used the following TLDs: com, .net, .org, .info, .biz; Conficker.B added .cc, .cn, .ws to the list. Conficker.D used 110 TLDs with no overlap to the Conficker.A and .B TLDs except for .cn. *See* Leder, Werner (2009), *supra* note 73, p. 12.

[134] Upgrade to Conficker.D by Microsoft and SRI naming system; the Conficker Working Group identifies this variant as variant .C.

[135] Piscitello (2010), *supra* note 10, p. 8; Conficker Working Group (2011), *supra* note 5, p. 22.

[136] Piscitello (2010), *supra* note 10, p. 4.

[137] In reality, the malware only used 500 of such domains; however, the choice of domains to be used was done at random which still required the preventive registration of all 50,000.

[138] Piscitello (2010), *supra* note 10, p. 9; Conficker Working Group (2011), *supra* note 5, p. 18. The Working Group's report notes the importance of the involvement of the registries of the Top Level Domains that were affected by Conficker.A and .B (.com, .net, .org, .info, and .biz managed by VeriSign, Neustar, and Afilias), which played a key role in shaping the domain name registration model and functioning of the Conficker Working Group.

[139] Originally, such sinkhole servers were run by individual organisations. In February 2009, the Conficker Working Group decided to centralise all sinkhole data at Georgia Tech as a neutral party that enabled access control and sharing of data in accordance with relevant agreements. *See* Conficker Working Group (2011), *supra* note 5, pp. 17-18.

[140] Piscitello (2010), *supra* note 10, p. 5.

[141] Leder, Werner (2009), *supra* note 73, p. 9.

[142] Conficker Working Group (2011), *supra* note 5, pp. 18, 44.

[143] Piscitello (2010), *supra* note 10, p. 6.

Legal and Procedural Aspects of Domain Name Registration

The coordinating body for the assignment of domain names and IP addresses globally is ICANN; the right to use a domain name is delegated by ICANN-accredited *domain name registrars.* Top-level domains (TLD) are in turn maintained and serviced technically by a *registry operator** that oversees domain name allocation.

Generic Top Level Domain (gTLD) registrars[144] have a contractual relationship with ICANN, based on gTLD registry and sponsorship agreements that include common basic requirements to define functional and performance specifications, access obligations, and limitations to registration, and may include varying specific requirements.[145] Country Code Top Level Domain (ccTLD)[146] registrations are administered by national registries under national law;[147] the role of ICANN in compliance monitoring of the ccTLDs is restricted to certain technical areas and activities in order to ensure the stability and operability of the Internet, but ICANN does not have contractual or legislative authority to take compliance action against ccTLD operators.[148]

Generally, the domain name registration (both on the gTLD and ccTLD levels) follows the principle of 'first come, first served', meaning that the domain name will be registered to the applicant unless it has already been registered to someone else. Additional criteria and requirements exist to ensure that registrations are appropriate.[149] These typically include a mechanism to protect third party rights (e.g. in case of a conflict with an existing trademark, lack of legitimate interest in respect of the domain name, or use of the domain name in bad faith[150]) and the protection of public order (e.g. blocking certain domain names as defamatory, racist, or contrary to public policy[151]). Certain domain names may be blocked or reserved for technical or domain management reasons.[152] In some cases, domain eligibility requirements exist: an example of such approach is the EU residency requirement for

[144] Registrars handling the registration of generic domains such as *.com, *.net, *.org, etc.
[145] gTLD Compliance Program. ICANN. http://www.icann.org/en/resources/compliance/gtld.
[146] Country-code Top Level Domains are the two-letter combinations indicating national domain spaces, such as e.g. .cn (Canada), .de (Germany), and .ee (Estonia).
[147] Resources for Country Code Managers. http://www.icann.org/en/resources/cctlds.
[148] ccTLD Compliance Program. ICANN. http://www.icann.org/en/resources/compliance/cctld.
[149] For example, the German domain registration policy reserves a generic right to reject the registration 'if the registration would be manifestly illegal'. *See* Section III of the DENIC Domain Guidelines, http://www.denic.de/en/denic-domain-guidelines.html.
[150] ICANN Uniform Domain Name Dispute Resolution Policy. Adopted 26 August 1999, Implementation Documents approved 24 October 1999. http://www.icann.org/en/help/dndr/udrp/policy; *see* Paragraph 4(a)(iii).
[151] *See* e.g. Article 18 of Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration; section 6.1.5 of the Estonian Domain Regulation. Approved by the Estonian Internet Foundation,
Council decision of 13 April 2011. http://www.internet.ee/eng/domain-regulation/domain-regulation.
[152] *See* e.g. Article 17 of Commission Regulation (EC) No 874/2004. This includes domain names that are reserved for the operational functions of the registry (eurid.eu, registry.eu, nic.eu, dns.eu, whois.eu, etc); Estonian Domain Regulation, section 3.2.4 (includes domain names of technical nature and published in an exhaustive list of blocked domain names, such as ftp.ee; cache.ee; tld.ee; telnet.ee) .

registering a .eu domain.[153] Also, procedural reasons such as providing inaccurate data or failure to pay the registration fee may be grounds to refuse or annul a domain registration. Procedurally, refusal to register a domain or annulment of a registered domain may occur as a result of registrar activity, domain name dispute resolution procedure, or be based on a court order.

Due to the applicability of differing national regimes to ccTLD registrations, neither ICANN nor the Conficker Working Group could mandate collaboration or application of desired security measures from the ccTLDs, yet their participation was critical to the success of the containment effort. The vast majority of ccTLDs cooperated with the effort,[154] but not all TLD operators were able to uniformly and unilaterally implement certain countermeasures or pre-emptive actions without violating domestic regulations. Some ccTLDs apparently took advantage of the legal 'gray zone' where national law was unclear about the permissibility of such registrations;[155] some registry operators were legally required to obtain a court order before they could recourse to a particular countermeasure.[156]

The daily coordination and registering of tens of thousands of different domain names, across more than a hundred Top Level Domain Name registrars globally, indicated that the preparedness of the legal system to process such requests, with the necessary speed that would not void response efforts, may be critical to the success of containing a global cyber incident. Therefore, national domain registration policies deserve to be reviewed to ensure an adequate balance between the interests of a domain holder and the security of the domain name system. It is also worth considering whether the procedural burden involved in registration is proportionate to the need to ensure security of the domain name system, and whether procedural steps to respond to a threat can be taken with adequate speed.

The Conficker mitigation effort points to some measures that could contribute to more effective containment of cyber threats by means of domain name administration. One option would be to grant to the registrar the right to refuse or suspend registration if there are reasonable grounds to believe that the domain name is being used as a means to commit cyber attacks; another option would be to authorise entities responsible for network security and incident handling (national Computer Emergency Response Teams, Internet Service Providers) to request domain name suspension in such cases. Domain name dispute resolution could be subjected to a mandatory preliminary arbitration procedure at a specialised body that has better awareness of the specifics of the subject and resources for a speedier response.

Another factor that influenced the effectiveness of Conficker response was the legal arrangement for domain name registration fees. Per request of a TLD registry operator, ICANN agreed to a principal policy change to waive the registration fee in cases of threat

[153] *See,* e.g. .eu Domain Name Registration Policy, Sections 1 and 2 (v. 4.0). http://www.eurid.eu/files/Nreg_pol_EN.pdf; .eu Domain Name Registration Terms and Conditions (v. 5.0), Sections 1 and 2, http://www.eurid.eu/files/Ntrm_con_EN.pdf.
[154] Conficker Working Group (2011), *supra* note 5, p. iii.
[155] *Ibid.*, p. 21.
[156] Piscitello (2010), *supra* note 10, p. 14.

against the DNS,[157] which facilitated the Conficker domain name registration on such a scale and thereby proved a key factor in the success of the Conficker mitigation.[158]

However, reaching a speedy and working agreement in contractual negotiations, especially with a number of parties involved, is an exception rather than a rule, and in the course of determining a mitigation strategy for cyber incidents, the time and resource factor must be considered. Lack of appropriate resources can both diminish the adequateness of response and deteriorate its quality in technical, operational and legal terms.

Balancing User Rights and DNS Stability

As mentioned above, some cases of the pre-emptive registration resulted in legitimate websites being blocked, due either to human error or to the fact that the Conficker-generated domain name coincided with an existing domain name, and double-checking the site's legitimacy was (initially) unsuccessful.

The task of coordinating the daily registering and blocking of tens of thousands of different domain names across 116 Top Level Domain Name registrars under intense time pressure involved risks of oversight or error in registration, which could have caused an upgrade of the malware in more systems,[159] or on the other hand, could have resulted in legitimate domains being blocked, which in turn created the risk of damage claims against the cyber security actors involved in the mitigation effort.

As it appears from the *Conficker Working Group Lessons Learned* report, the parties involved in mitigation prioritised the 'common good' (the security and operation of the DNS and preventing a potentially serious cyber assault) over individual interests (right to unhindered access to operated domains, but more generally also the right of individual parties to conduct business or their freedom of expression). Protective measures were applied in good faith, as can be concluded from the fact that the Conficker Working Group pre-emptive domain registration included routine verification procedures and legitimate websites which were accidentally wrongfully registered were promptly restored. Yet, it is also a fact that there was no regulatory overseeing of the Conficker Working Group[160] and the rights of individual users were potentially, and in some cases actually, damaged.

The procedure for defending users' rights and interests remains vague. The same applies for potential compensation for damage, its permissibility and extent – whether compensation would involve direct damage only or also indirect damage in the form of loss of expected income – and the question of who should bear the risk that a (legitimate) domain will

[157] Piscitello (2010), supra note 10, p. 6; Conficker Working Group (2011), supra note 5, p. 17. Likewise, most registrars cooperating with the Conficker Working Group waived charges for registering Conficker domains by the Working Group.

[158] The domain name registration initiative was not entirely novel in nature. In 2008, a similar attempt had been made in relation to the Srizbi botnet, where a security solutions provider registered the domains ahead of the botnet creators in order to keep them from regaining control of the infected computers after the control servers had been taken down by the authorities. After initial success, the effort failed after two weeks due to lack of funding. *See* Conficker Working Group (2011), *supra* note 5, pp. 15, 19; Piscitello (2010), *supra* note 10, p. 5

[159] This is what happened on two occasions in March 2009. By mistake, two Conficker domain names were overlooked in registration, which resulted in more systems upgraded to Conficker.D (.C). *See* Conficker Working Group (2011), *supra* note 5, p. 22.

[160] Conficker Working Group (2011), *supra* note 5, p. 21.

become unreachable in the course of deterring a cyber threat. The Conficker Working Group did not have a direct legal authorisation for their pre-emptive domain name registering and blocking action; they simply relied on the 'first come, first served' principle in registering domains, assuming that no party had a legitimate interest to register the same domain name (insofar as using the domain as a botnet C&C server for spreading malware cannot be considered a legitimate interest).

It is problematic to delineate a preference order among the interests of different parties involved, but in finding an acceptable legal solution, the disproportionate damaging of the interests of any single party should be avoided; also, it must be kept in mind that if the risk is fully or mainly laid on the security community or Internet service provider (directing potential damage claims for wrongful domain registration at them), it is likely to have a detrimental effect both on the cost of their services and their motivation to contribute to defence. It is essential that procedural rules meant to protect legitimate users do not in themselves become a barrier to the containment of the botnet.

Private-Public Collaboration

The parties involved in the Conficker mitigation effort acknowledged that successful collaboration among the various private sector bodies in the Conficker Working Group had been among the most important outcomes of the Conficker lesson, and was regarded by some as equal in significance to the effectiveness of the containment effort itself.[161] A general assurance confirmed that 'security communities are willing and able to join forces in response to incidents that threaten the security and stability of the DNS and domain registration systems on a global scale'.[162] The Conficker Working Group has since been regarded as a model for successful collaboration.[163]

While private sector collaboration was largely deemed to have been a success, numerous participants in the Conficker Working Group expressed concern about the existence or meaningfulness of public-private collaboration in the course of containing or remedying the cyber threat. Criticism was manifold:[164]

- Lack of awareness and of participation on the part of the government as an institution towards the mitigation efforts, especially inability or unwillingness to become a formal contributor to the containment efforts;
- Lack of general understanding of possible areas for collaboration and of procedural requirements involved;
- One-sided information flow with public authorities, who would not object to receiving information but would not share information in return (apart from informal, personal contacts).

Nevertheless, some positive aspects were identified:[165]

- Informal connections through personal channels enabled developments to be followed and informal consultations to be made;

[161] Conficker Working Group (2011), *supra* note 5, p. 2.
[162] Piscitello (2010), *supra* note 10, p. 2.
[163] Conficker Working Group (2011), *supra* note 5, p. 2.
[164] *Ibid.*, pp. 19, 34, 35.
[165] *Ibid.*, p. 19, 34.

- Financial support for research (the government of the USA funded the SRI research[166] that played an important role in the mitigation process).

Legal and Regulatory Support to Private-Public Collaboration

Similarly to earlier incidents,[167] the Conficker lesson again indicated that the private sector and law enforcement still work isolated from each other when handling cyber threat, as each relies upon different frameworks to govern their procedures, and there is little common ground for both sides. Informal information-sharing is nearly the only area of cooperation that is functioning acceptably, but apart from providing the factual information of an incident having taken place, the usability of such informal information for the purposes of law enforcement or criminal proceedings is little or non-existent. Likewise, law enforcement agencies can help with advice and consultation, but that is also informal support rather than a solid, official commitment of resources to cooperate.

Both in the Conficker case and that of Estonia 2007, the problem did not lie in unwillingness or lack of interest in cooperation. As the *Conficker Working Group Lessons Learned* paper points out, both the private sector and law enforcement were open to collaboration. Yet, without a clearly expressed legal authorisation to act, and without clarity about the rules of procedure, cooperation efforts only have a very limited extent; and the situation where collaboration between public and private sectors is tolerated and possibly morally or informally supported, but not officially accepted, is becoming increasingly insufficient as threats grow more complex and a speedier and more flexible reaction is required.

On the other hand, the lessons learned also indicate that the need for a legal framework is not for one that aims to mandate or regulate collaboration, but for one to facilitate and support it. In accordance with the principle of rule of law, public authorities are limited in their activities to what is expressly authorised by law. The private sector, in contrast, enjoys freedom of activity as long as it is not restricted by the law. Each side is in need of a different legal support to its cyber security efforts, but the areas specifically pointed out by the Conficker Working Group include *public-private information-sharing, support to law enforcement, resources* and *legislative reform* to enable the cyber security community to stay ahead of impending threats.[168]

The **public sector**, i.e. government/state authorities, needs the necessary authorisation to act on both the giving and receiving end of information flow (to be able to receive information from the private sector for the purposes of law enforcement and administrative or criminal proceedings without unnecessary duplication), with the corresponding mechanism to balance individual rights and freedoms on the one hand and the needs of

---

[166] The SRI Conficker project conducted by Phillip Porras, Hassen Saïdi and Vinod Yegneswaran (2009), see *supra* note 22, and supplementary research (Conficker C Analysis. SRI International Technical Report, Addendum. 8 March 2009 (last update 4 Apr 2009). http://mtc.sri.com/Conficker/addendumC/index.html; Conficker C Active P2P Scanner. Version 0.1B. Computer Science Laboratory, SRI International. http://mtc.sri.com/Conficker/contrib/scanner.html).

[167] The case of the Estonia 2007 cyber attacks likewise indicated the ambiguity of private-public sector collaboration, demonstrating that collaboration between the two sectors is likely to rely on – and be limited to – informal communication based on personal trust. *See* Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf. P. 24.

[168] Conficker Working Group (2011), *supra* note 5, p. iii.

national security and administrative efficiency on the other. The **private sector** expects guarantees that its efforts are useful – it generally bears a lower tolerance for even perceived waste of effort or resources than the public sector – and that its commercial interests, including confidential data, are not threatened or jeopardised disproportionately to the expected benefit.

Also, such legal framework must foresee the possibility of public sector collaboration with an *ad hoc* structure with dynamically defined organisational and operational ties, and a decision-making structure run on consensus rather than a top-down hierarchy. As pointed out by a number of stakeholders in the Conficker mitigation effort, a standing organisation to handle cyber threats might not be the proper way to manage the threats,[169] and the model of collaboration developed in Conficker mitigation is already being implemented by private industry.[170]

[169] *Ibid.*, p. 30.
[170] *Ibid.*, p. 38.

Summary

The Conficker cyber threat has rightfully received widespread attention among the botnet cases of recent years. Its extent in terms of its global spread and number of systems affected, its high level of sophistication, and the relative novelty of its solution in the scale of current cyber threats posed a challenge to the established methods to deal with cyber attacks. A part of the challenge has been directed at the toolbox of measures offered by law and legal policy.

The present case study assesses three of those legal and legal policy issues: it considers the preparedness of *substantive criminal law* to address sophisticated and large-scale cyber attacks, the *registration of domain names as a method of cyber defence*, and *private and public sector collaboration*. The main conclusions of the study are briefly summarised below.

The evaluation of substantive criminal law highlights two main considerations: *harmonisation* and *balance*. The first is based on the understanding that in the context where criminal procedure is, by nature, a national sovereignty issue, while a cyber attack, by nature, a phenomenon that ignores national boundaries, it is fundamental to effective cooperation in criminal matters that nations delineate common reference points for defining cyber crime in their domestic criminal law. The Council of Europe Convention on Cybercrime may have been criticised for its relatively high burden of procedural and cooperation commitments, but it has proved a reasonable standard for defining the elements of offences against the confidentiality, integrity and availability of computer data and systems and it responds rather well to the case under study. In defining cyber crimes in national criminal law, compliance with the Treaty definitions would help to avoid significant over- and under-criminalisation and enable adequate response to cyber crime both domestically as well as in international cooperation. Furthermore, ratification of the Treaty would serve transparency objectives with regard to the national standard of addressing cyber crime.

Secondly, while the Treaty also leaves room for certain flexibility in national definitions, thus admitting national factors such as a particular nation's political preferences and legal culture, the level of development of information society, and lessons learned from earlier cyber incidents, the implementation of such reservations will require careful balancing of the interests of security of infrastructure and services on the one side and user privacy and right to inviolability of property on the other, in order not to render the Treaty provisions devoid of content. The Conficker case illustrates how a broad national law approach in criminalising cyber activities forced cyber incident responses to resort to softer mitigation measures with questionable effect. The nature of a particular cyber threat (e.g. its severity, speed of spreading, number and criticality of systems affected) and the corresponding threat to public interest, as well as the effect of the threat to other users of the infrastructure should be factors to consider in protecting the individual interest of a user. A high overall risk of a particular cyber threat may justify less intensive protection of individual interests: a practical

example brought by the Conficker case illustrates how disinfecting user systems should not be solely dependent on user consent if the user's neglect or refusal to do so would lead to the further spreading of a botnet and escalating the potential harm by allowing for the malicious software to be upgraded.

The novel approach of using registration of domain names as a method of cyber defence draws attention to the *necessity for openness to new cyber threat mitigation methods.*

Public authorities derive their mandate to act from the law, which means that the relatively static phenomenon of legislative process needs to adapt with the remarkably dynamic environment of technological progress. Therefore, it is essential that cyber threat mitigation measures be defined in a technology neutral way, i.e. based on process or activity rather than on the means or technological solutions used. Likewise, the relatively mundane understanding that prevention is a part of defence implies that the entire "food chain" which bears a role in ensuring the functioning of the Internet must also be appropriately equipped. Domain name registrars responsible for resource allocation, Internet Service providers supplying the infrastructure and handling everyday functioning of services, and computer incident/emergency response entities who react to incidents *post factum* carry different functions in ensuring cyber security, and need to be authorised to take the necessary measures if an exploit concerns their area of responsibility. The possibility for speedy and flexible action is especially important in a context where a cyber threat evolves in minutes and hours rather than days, and the attacker has no regard for legal or procedural restrictions.

As the authority to take measures to mitigate a cyber threat is delegated as near as possible to the institution managing the particular role, competent oversight needs to be involved to ensure lawfulness, and proper attention given to users' rights. Also, the potential effect of threat prevention mechanisms (such as a more rigid domain registration procedure) on technological development and the economic environment is a factor to be considered when defining measures of cyber defence, including cyber threat prevention.

And finally, the decisive factor to the success of containment of the Conficker botnet was successful *collaboration* between the entities bearing different roles in ensuring the availability and proper functioning of the Internet. The success of collaboration was in fact regarded as equal in significance to the effectiveness of the containment effort itself. This conclusion mainly applied to the various private sector bodies involved in the mitigation: Microsoft, ICANN, operators within the Domain Name System (including those managing national domain name spaces in the numerous countries affected by the malware), computer security researchers from varying countries and of varying backgrounds (academic, commercial), as well as antivirus and other computer security solutions producers; while collaboration with the public sector remained less effective. Lack of formal support from the public sector was a common criticism in the Conficker containment effort, and much of it was apparently linked to lack of awareness (including lack of procedural

understanding) rather than to the lack of willingness, especially considering the indirect and informal support of individual public sector representatives that was given.

Therefore, one of the main lessons of the Conficker containment effort is that ways for meaningful collaboration between the private and public sector in the course of containing or remedying a cyber threat need attention. Public authorities need a clearly expressed legal authorisation to act as well as clarity about the rules of procedure, so that their involvement could extend beyond toleration and moral or informal support and benefit especially the areas of public-private information-sharing, support to law enforcement, and resources. The lessons learned also indicate that instead of aiming for a legal framework that mandates and regulates collaboration, such framework should focus on facilitating and supporting it, and the legal framework to support public sector collaboration should contain enough flexibility to make room for developing and transforming threats, and reckon with flexible *ad hoc* organisation models with whom to collaborate.

A Brief Overview of the Case

INCIDENT TIME FRAME

Start 21 Nov 2008 (first reports of Conficker malware infection)

End May 2009 (end of active phase); infections may remain and infected computers are still potentially controllable

Duration 6 months

INCIDENT FACTS

Name & variants

Conficker, Downadup, Kido, Downad

Five variants identified: Conficker.A;

Conficker.B;

Conficker.C/Conficker.B++;

Conficker.D/Conficker.C;

Conficker.E

Methods

- Injecting malicious code into Windows server service by taking advantage of a vulnerability in the operating system;
- Infected devices are linked to a remote computer and thereby become part of a botnet with potential to perform under the malware author's control;
- Malware employs a self-propagation mechanism; capable of spreading across computer networks and via removable drives; capable of exploiting weak passwords;
- Defensive mechanisms are included in the malware to prevent detection and removal;
- Retrieves updates via 250 to 50,000 daily pseudo-randomly generated domain names;

Targets

- All vulnerable systems using Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008.
- Government and public administration organizations, providers of public services, financial institutions, academic organizations, etc. affected worldwide.
- 35 million unique IP's in total in at least 206 countries globally.

Origin

- Undetermined.

LEGAL LESSONS IDENTIFIED

Core of the case

- Preparedness of national substantive criminal law to address sophisticated and large-scale cyber attacks.
- Registration of domain names as a method of cyber defence.
- Private and public sector collaboration.

Summary

- Harmonisation of substantive law definitions for offences against the confidentiality, integrity and availability of computer data and systems is essential to effective criminal procedure, as cyber attacks, by nature, disregard national boundaries. The national implementation of international cybercrime legal instruments requires careful balancing of the interests of security and privacy. Disproportionate weight given to security interests may harm development and the economic environment as well as legitimate user rights; whereas over-criminalising cyber activities may render mitigation ineffective.
- As cyber threats are evolving in size and sophistication, there is a corresponding need to ensure that incident response entities, including public authorities, remain equipped with effective mitigation methods regardless of the technological solution used to carry out a cyber attack. A comprehensive approach to threat mitigation should involve all entities that have a role in ensuring the functioning of the Internet infrastructure and services. The need for speedy and flexible action requires a balancing mechanism to ensure lawfulness and respect for legitimate user rights.
- Conficker mitigation verified successful collaboration within the private sector, but the area of public-private collaboration needs improvement both in terms of awareness and of clarity regarding authority to act and procedural rules involved. The legal framework to facilitate collaboration should contain flexibility to make room for developing and transforming threats, and reckon with flexible *ad hoc* organisation models with whom to collaborate.

Recommended Reading

This paper, due to its focus on legal and legal policy issues, was only able to touch the surface of the characteristics and operation of Conficker and of the activities involved in the containment effort. For a thorough understanding of these subjects, the following materials are recommended:

I – Technical description and analysis of the Conficker malware

- Leder, Felix; Werner, Tillmann. Know Your Enemy: Containing Conficker. To Tame A Malware. The Honeynet Project. 30 Mar 2009 (updated 7 Apr 2009). http://www.honeynet.org/files/KYE-Conficker.pdf
- Porras, Phillip; Saidi, Hassen; Yegneswaran, Vinod. An Analysis of Conficker's Logic and Rendezvous Points. SRI International Technical Report. Released 4 Feb 2009 (updated 19 Mar 2009). http://mtc.sri.com/Conficker/

II – First-hand description and chronology of Conficker mitigation and containment efforts

- Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf
- Piscitello, Dave. Conficker Summary and Review. ICANN, 7 May 2010. http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf

III – Visuals and tools

- Infection distribution, tracking, timeline, malicious sites, repair tools and Conficker domain list and other synoptic tools can be found on the Conficker Working Group website at http://www.confickerworkinggroup.org/,
- Conficker. Shadowserver, http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker
- Protect yourself from the Conficker Worm virus. Microsoft Safety & Security Center, http://www.microsoft.com/security/pc-security/conficker.aspx#EWC

Glossary

Botnet

A network of computers that have been infected by *computer malware*, enabling unauthorised control of the infected computers ('zombies') to perform malicious actions, such as attacks against information systems.

Botnet command and control (C&C) server

The computer used by the botnet originator to remotely control the network of 'zombie' computers to carry out malicious actions, such as attacks against information systems.

Computer malware (malicious software)

Computer software (such as code, scripts, active content etc) designed or used to infiltrate or damage a computer system without the owner's consent. It is distributed through a variety of means (emails, computer viruses, botnets) with the intent to obtain data in a fraudulent way or to integrate the computer in a computer network destined to be used for criminal actions.

Computer worm (worm virus)

Considered a sub-class of computer viruses and bear many similarities with the latter, while bearing some functional differences:

A *computer virus* is a program or algorithm that attaches itself to a file on the computer without the user's knowledge and performs malicious actions once the program is opened or run. The capacity to attach itself enables the virus to spread across computer networks, but some level of human action (such as running an infected program) is required for spreading.

A *worm* replicates itself over a computer network by taking advantage of file or information transport features on the computer, which allows it to travel without requiring human action for spreading. Worms do not attach to other programs like computer viruses do. The replication and spreading features of the worm consume excessive amounts of system or network resourcing, causing computers or networks to stop responding.

Domain name

Alphabetic identification string for one or more IP addresses corresponding to a device connected to the Internet, which is translated into numeric IP address by the domain name server.

Domain Name System (DNS)

A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network, which resolves queries for domain names into IP addresses for the purpose of locating computer services and devices worldwide.

Honeypot

An Internet-connected server that is designed to lure potential hackers to gain access to the system, thereby enabling to identify system weaknesses and to study hacker behaviour.

IP address

Internet Protocol address, a numerical label assigned to each device on a computer network which enables identification of devices and routing of data.

Payload

The part of a computer virus which performs a malicious action, such as data destruction or mass distribution of unsolicited bulk email (spam).

Payload activation date

The time defined for the launching of the malicious activity.

Scareware

Rogue security software, which appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions.

Bibliography

.eu Domain Name Registration Policy (v. 4.0). http://www.eurid.eu/files/Nreg_pol_EN.pdf

.eu Domain Name Registration Terms and Conditions (v. 5.0). http://www.eurid.eu/files/Ntrm_con_EN.pdf

ccTLD Compliance Program. ICANN. http://www.icann.org/en/resources/compliance/cctld

Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration.
Official Journal L 162 , 30/04/2004 P. 0040 – 0050

Conficker C Active P2P Scanner. Version 0.1B. Computer Science Laboratory, SRI International. http://mtc.sri.com/Conficker/contrib/scanner.html).

Conficker C Analysis. SRI International Technical Report, Addendum. 8 March 2009 (last update 4 Apr 2009). http://mtc.sri.com/Conficker/addendumC/index.html

Conficker Is Down But Not Out. PC Tools, 10 March 2011. http://www.pctools.com/security-news/conficker-worm/

Conficker virus hits Manchester Police computers. BBC News, 2 February 2010. http://news.bbc.co.uk/2/hi/uk_news/england/manchester/8492669.stm

Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

Conficker. Shadowserver Foundation [2009], http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

Council of Europe, Convention on Cybercrime. ETS No. 185. Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

DENIC Domain Guidelines, http://www.denic.de/en/denic-domain-guidelines.html

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC and Regulation 544/2009, Article 13a. (OJ L 108, 24.04.2002, p. 33; OJ L 337, 18.12.2009, p. 37; OJ L 167, 18.6.2009, p. 12)

Domain Regulation. Approved by the Estonian Internet Foundation,
Council decision of 13 April 2011. http://www.internet.ee/eng/domain-regulation/domain-regulation

Dubsky, Daniel. Conficker-Wurm infiziert hunderte Bundeswehr-Rechner. IT Espresso.de, 16 February 2009. http://www.itespresso.de/2009/02/16/conficker-wurm-infiziert-hunderte-bundeswehr-rechner/

Empak, Jesse. Years-old Conficker Worm Still A Threat. 27 Jan 2011. http://www.ibtimes.com/articles/105943/20110127/conficker-worm-still-threat.htm

Encyclopedia: Win32/Conficker. Microsoft Malware Protection Center, 8 Jan 2009 (updated 17 Apr 2011). http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fConficker

Encyclopedia: Worm:Win32/Conficker.A. Microsoft Malware Protection Center, 24 Nov 2008 (updated 17 Apr 2011), http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.A

Encyclopedia: Worm:Win32/Conficker.E. Microsoft Malware Protection Center, 9 Apr 2009 (updated 17 Apr 2011), http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.E

Explanatory Report to the Convention on Cybercrime, Council of Europe. http://conventions.coe.int/treaty/en/reports/html/185.htm. Section 60.

Framework Directive 2002/21/EC (amended by Directive 2009/140/EC on a common regulatory framework for electronic communications networks and services) and four specific directives (with subsequent amendments)

Gostev, Alexander. The neverending story. 9 April 2009. http://www.securelist.com/en/weblog?weblogid=208187654

gTLD Compliance Program. ICANN. http://www.icann.org/en/resources/compliance/gtld

Heath, Nick. Downadup virus hits PCs at five Sheffield hospitals. Silicon.com, 22 Jan 2009. http://www.zdnet.co.uk/news/security-management/2009/01/22/downadup-virus-hits-pcs-at-five-sheffield-hospitals-39599480/;

ICANN Uniform Domain Name Dispute Resolution Policy. Adopted 26 August 1999, Implementation Documents approved 24 October 1999. http://www.icann.org/en/help/dndr/udrp/policy

Infection Distribution. Conficker Working Group, 1 Apr 2009. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution

Joffe, Rodney. The cyber crime epidemic. National Post, 23 Oct 2009. http://www.solucom.com/content/news/index.php?news=99

Jones, Michael W. Federal rules leave medical equipment virus-infected. Tech Blorge, 3 May 2009. http://tech.blorge.com/Structure:%20/2009/05/03/federal-rules-leave-medical-equipment-virus-infected/

Krebs, Brian. Conficker Worm Awakens, Downloads Rogue Anti-Virus Software. *Washington Post*, 10 April 2009. Available http://voices.washingtonpost.com/securityfix/2009/04/conficker_worm_awakens_downloa.html

Leder, Felix; Werner, Tillmann. Know Your Enemy: Containing Conficker. To Tame A Malware. The Honeynet Project. 30 Mar 2009 (updated 7 Apr 2009). http://www.honeynet.org/files/KYE-Conficker.pdf

Leyden, John. Conficker left Manchester unable to issue traffic tickets. The Register, 1 Jul 2009. http://www.theregister.co.uk/2009/07/01/conficker_council_infection/

Leyden, John. Houston justice system laid low by Conficker worm. The Register, 9 Feb 2009. http://www.theregister.co.uk/2009/02/09/houston_malware_infection/

Leyden, John. Leaked memo says Conficker pwns Parliament. The Register, 27 Mar 2009. http://www.theregister.co.uk/2009/03/27/conficker_parliament_infection/

Leyden, John. Scottish hospitals laid low by malware infection. The Register, 9th March 2009. http://www.theregister.co.uk/2009/03/09/scot_hostpitals_malware_infection/;

List of signatories of the Convention on Cybercrime, CETS No.: 185, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (status as of 28 Sept 2012)

Microsoft Collaborates With Industry to Disrupt Conficker Worm. 12 Feb 2009. http://www.microsoft.com/presspass/press/2009/feb09/02-12ConfickerPR.mspx

Microsoft Security Bulletin MS08-067 – Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644). Version: 1.0. Microsoft Security TechCenter, 23 October 2008. http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Mills, Elinor. Conficker infected critical hospital equipment. CNET News, 24 Apr 2009. http://www.zdnet.com/news/conficker-infected-critical-hospital-equipment/291619

Nahorney, Ben. The Downadup Codex, Edition 2.0. Symantec, 29 Jun 2009. http://www.symantec.com/connect/blogs/downadup-codex-edition-20

Page, Lewis. MoD networks still malware-plagued after two weeks. The Register, 20 Jan 2009. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/

Piscitello, Dave. Conficker Summary and Review. ICANN, 7 May 2010. http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf.

Plohetski, Tony. DPS computer network hit by virus: Officials will work through the weekend to restore service. American-Statesman, 18 Apr 2009. http://www.statesman.com/news/content/news/stories/local/04/18/0418dpsworm.html

Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. A Foray into Conficker's Logic and Rendezvous Points. Computer Science Laboratory, SRI International. [2009] http://www.usenix.org/event/leet09/tech/full_papers/porras/porras.pdf.

Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. An Analysis of Conficker's Logic and Rendezvous Points. SRI International Technical Report. Released 4 Feb 2009 (updated 19 Mar 2009). http://mtc.sri.com/Conficker/.

Porras, Phillip; Saïdi, Hassen; Yegneswaran, Vinod. Conficker C Analysis. SRI International Technical Report, Addendum. 8 March 2009 (last update 4 Apr 2009). http://mtc.sri.com/Conficker/addendumC/index.html

Protect yourself from the Conficker Worm virus. Microsoft Safety & Security Center, http://www.microsoft.com/security/pc-security/conficker.aspx#EWC

Protecting Yourself from the Conficker Worm. McAfee http://www.mcafee.com/us/threat-center/conficker.aspx

Questions and Answers: Conficker and April 1st. 26 Mar 2009. F-Secure, http://www.f-secure.com/weblog/archives/00001636.html

Resources for Country Code Managers. http://www.icann.org/en/resources/cctlds

Schulman, Cristina. The global state of cybercrime legislation. Cybercrime Unit, Directorate General Human Rights and Rule of Law, Council of Europe. June 2012. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations/WS1_coe_cyber_Octopus_ws%201_6June12.pdf

Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

Timeline. Conficker Working Group, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline (last modified on 26 April 2009)

Tindal, Suzanne. Conficker worm strikes ANZ Bank. ZDNet Australia, May 6, 2009. http://www.zdnetasia.com/conficker-worm-strikes-anz-bank-62053800.htm

Want a first-time driver's license? Not possible today, so far. Statesman.com, 15 Apr 2009. http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2009/04/15/want_a_firsttime_drivers_licen.html

Wattanajantra, Asavin, Conficker worm hits hospital PCs in Sheffield. IT Pro, 23 Jan 2009. http://www.itpro.co.uk/609615/conficker-worm-hits-hospital-pcs-in-sheffield;

Wattanajantra, Asavin. Royal Navy systems hit by computer virus. IT Pro, 16 Jan 2009. http://www.itpro.co.uk/609550/royal-navy-systems-hit-by-computer-virus

Weinstein, Natalie. Report: Conficker worm bites University of Utah. CNet News, 12 April 2009. http://news.cnet.com/report-conficker-worm-bites-university-of-utah/

Werner, Tillman. Simple Conficker Scanner v2. 15 Apr 2009. http://www.honeynet.org/node/397

Williams, Christopher. Conficker seizes city's hospital network. The Register, 20 Jan 2009. http://www.theregister.co.uk/2009/01/20/sheffield_conficker/;

Williams, Martin. Computer virus strikes hospitals. Herald Scotland, 6 MAR 2009. http://www.heraldscotland.com/computer-virus-strikes-hospitals-1.904470

Willsher, Kim. French fighter planes grounded by computer virus. The Telegraph, 7 Feb 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

Worm:W32/Downadup.AL. F-Secure Labs. http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml

Yegneswaran, Vinod. Conficker C Active P2P Scanner. Version 0.1B. Computer Science Laboratory, SRI International. http://mtc.sri.com/Conficker/contrib/scanner.html

Annex. Council of Europe Convention on Cybercrime. Convention on Cybercrime Explanatory Report *(Excerpt)*

Chapter II
Measures to be taken at the national level

Section 1
Substantive criminal law

Title 1
Offences against the confidentiality, integrity and availability of computer data and systems

43. The criminal offences defined under (Articles 2-6) are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

44. 'Illegal access' covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion, i.e. 'hacking', 'cracking' or 'computer trespass' should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.

46. 'Access' comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. 'Access' includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

47. The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is 'with right.'

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots' to locate and retrieve information on behalf of communication. The application of such tools per se is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it.

49. Many national legislations already contain provisions on 'hacking' offences, but the scope and constituent elements vary considerably. The broad approach of criminalisation in the first sentence of Article 2 is not undisputed. Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems. This has led in a range of countries to a narrower approach requiring additional qualifying circumstances which is also the approach adopted by Recommendation N° (89) 9 and the proposal of the OECD Working Party in 1985.

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets).

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The

offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.

52. The text of the provision has been mainly taken from the offence of 'unauthorised interception' contained in Recommendation (89) 9. In the present Convention it has been made clear that the communications involved concern 'transmissions of computer data' as well as electromagnetic radiation, under the circumstances as explained below.

53. Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation.

54. The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term 'non-public' does not per se exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute 'non-public transmissions of computer data' are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of 'computer system' may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though 'non-public', takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

57. The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision.

58. For criminal liability to attach, the illegal interception must be committed 'intentionally', and 'without right'. The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if

surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing 'cookies', is not intended to be criminalised as such, as not being an interception 'without right'. With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken 'with right'.

59. In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as 'intentionally' and 'without right'.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

61. In paragraph 1, 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

62. The above acts are only punishable if committed 'without right'. Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (e.g., software permitting access to the Internet that disables similar, previously installed programs), are with right and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain

abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime.

63. In addition, the offender must have acted 'intentionally'.

64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation, but Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

65. This is referred to in Recommendation No. (89) 9 as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.

66. The term 'hindering' refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.

67. The hindering must furthermore be 'serious' in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered 'serious.' For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as 'serious' the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

68. The hindering must be 'without right'. Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ('spamming'). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The

text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ('hacker tools') or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries. A similar approach has already been taken in the 1929 Geneva Convention on currency counterfeiting.

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in Articles 2-5 of the present Convention. 'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

73. The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted, by the last phrase of paragraph 1(b), to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent. It is up to each Party to decide the number of items required before criminal liability attaches.

76. The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'.

78. Due to different assessments of the need to apply the offence of 'Misuse of Devices' to all of the different kinds of computer offences in Articles 2 – 5, paragraph 3 allows, on the basis of a reservation (cf. Article 42), to restrict the offence in domestic law. Each Party is,

however, obliged to criminalise at least the sale, distribution or making available of a computer password or access data as described in paragraph 1 (a) 2.