Editorial Preface

"Just when you Thought it was Safe to go Back Online" – Flame: A New Type of Virus that has Changed the Face of Malware Forever

Kevin Curran, University of Ulster, UK

The Tech world awoke in June 2012 to a new type of super virus – Flame. Flame is correctly being classified as the most impressive piece of malware discovered to date. The word 'discovered' is important as we do not really know how many 'hybrids' of Flame are also out there. If one could write a wish list for a clever intrusive secretive information gathering piece of malware - then Flame would cover all aspects. The fact that it can gather personal files, remotely change settings on computers, turn on PC microphones to record conversations, take screen shots, log instant messaging chats and cover its own tracks so neatly makes it very impressive. All these vulnerabilities have been known for some time. In fact professionals such as me place black tape over the webcam when we are not using it. We have known about intrusive webcam hacks and of course the other separate information gathering tools in flame however no malware to date has so expertly compiled all of these attack vectors into such a single system with such success.

It poses enormous threats. It can be distributed via removable networks and local area networks. It can snoop on a network, detecting network resources, and collecting lists of vulnerable passwords as they pass by over that network. It can capture the contents of any fields filled out, even when obscured by asterisks or dots (e.g., password fields). It can scan disks of an infected system seeking specific content. It can perform screen captures of the infected machine when specific programs are running and it can activate a microphone and record over a long period of time any sounds in the environment. It can overcome the security of Skype calls by such a process. That is significant and all of the data captured is saved in a local database which it is able to transfer back to control servers - encrypted... It bypasses all known antivirus detection, antimalware and other security software. That is one big threat.

There are some indicators which point to government involvement including the fact that Flame has the ability to replicate over a local network using several methods, including the same printer vulnerability and USB infection method exploited by Stuxnet. Stuxnet of course is the well-known computer worm which included a highly specialized malware payload designed to target only supervisory control and data acquisition (SCADA) systems that

are configured to control and monitor specific industrial processes. These SCADA systems were used in Iran's uranium enrichment program. Recently, what has long been suspected has come to light - that the U.S. and Israel crafted the Stuxnet computer worm to attack Iran's uranium enrichment program. There are similar traits in the flame malware but many agree that there are also too many differences in this sophisticated software to make a direct link between the makers of Stuxnet and Flame.

The sophistication of many aspects of it could be said to point to state involvement but it is a little early to tell. This software is 20MB whereas Stuxnet was only about 0.5MB. It really is has its own complete database architecture. The actual name Flame comes from one of the attack modules located at various places in the malware code. This malware is a platform which is capable of receiving and installing various modules for different goals. In fact not one of the 40+ tested antiviruses could detect any of the malicious components. That again points to an incredible sophisticated system which could not have been developed by a small group of individuals.

The prevalence of cyberespionage is starting to suddenly become visible. 2012 may become the year of cyberespionage. To date, we could only speculate but last week with the US government admitting involvement in previous malware brings it to the fore. Now companies know that it is not a matter of if but when rogue nations come looking for their data or to wreak havoc in their systems. The US government has admitted to working on offensive and defensive cyber war systems but they have also strived to say that they place the emphasis on defensive but who is to argue otherwise. It is also incredibly difficult to estimate which countries are heavily conducting research into cyber war as it is not as simple as perhaps counting the size of their armies or weaponry. What we can say is that the beauty of the pervasiveness of the Internet is also its weakness. Once a computer is connected to the Internet, it for all intents and purposes is a potential target. There is no such thing as a secure network. It you wish to remain secure then do not own a computer...

It is difficult to predict how these new types of super malware will evolve. The clever ones in the future will probably exhibit behaviour we simply had not predicted. One thing we can it that they will most likely continue to 'phone home.' That is, all these sophisticated malware systems tend to encrypt their 'calls out' to secret servers where they upload their data but they disguise the IP addresses of the master and command servers very well with sophisticated algorithms so by peeking into the code , it is not obvious where they send that data to. They will basically dynamically generate domain names on the fly. At specific times in the future, the bad guys register new domains so that they can allow these systems to send the data out. They will also continue to use anonymising proxies which hide the data trail to shove their data over. This makes it very hard for the authorities to trace.

Other possible futuristic scenarios are cyber-attacks that destroy critical data such as a crucial database for the government like Social Security. Terrorists could also penetrate a hospital database, causing fatal medical errors when a patient takes prescription drugs. It is also possible that terrorists could hack airline systems such as the weights and measures which control plane fuel and payload measurements. Ultimately, this type of cyber-attack (whether government funded or not) can do extreme damage to cyberspace. Increasingly the Internet will become the defacto platform for commerce. It is also so difficult to detect destructive malware when you do not know it is even present. Even the behavioural analysis engines of the leading anti-malware engines did not detect this. We now know it has been in the 'wild' for about 5 years. No system saw this malware messing with system OS files. It is really clever. It changes dates and file names and covers its tracks very carefully. These systems are like nothing seen to date.

Countries will unfortunately increasingly use cyberspace to cause disruption. Countries have always fought against governments for

their cause, and they use every means possible to get what they want. Cyber-attacks generally come in two forms; one against data, the other control systems. Theft and corruption of data leads to servicing being sabotaged and this is the most common form of internet and computer attacks. Attacks which focus on control systems are used to disable or manipulate physical infrastructure. For example, the provision of electrical networks, railroads or water supplies could be infiltrated to have wide negative impact on particular geographical areas. This is done by using the internet to send data or by penetrating security systems. Countries are beginning to set up cyberspace network operations centres which include internet service providers and computer hardware and software developers. Their task is to develop secure technology such as intelligence analysis software which will be capable of sifting through and analysing existing data, both public and private, in order to uncover suspicious activity. The have found that they cannot continue to rely on smaller commercial organisations to do this on their own.

To some degree, governments do not choose to use malware as 'weapons' but rather as surveillance tools akin to spy planes. This can result in increased intelligence in the long run rather than short term damage. We can expect to see retaliation from states in the future. The problem with any cyber-attack is that once it is discovered (and inevitably we can expect this to be the case) - the other side will be able to analyse the code and repurpose it for reverse attacks. In fact, it seems that the success of Flame is due to its modular nature. It is entirely possible that Flame was initially released as a smaller focused virus to do a single task, then as this was deemed a success, more features may have been added until we reach the state of the virus as we see it today. This was a well-executed plan. However, what is to stop future states from expanding it with additional modules?

In summary, Cyber espionage by governments is using increasingly clever methods and tools to attack systems and governments. Issues of national and worldwide safety are at risk here. The reason this risk exists is that the Internet offers little or no regulation, potentially huge audiences, anonymity of communication and a fast flow of information. Enjoy this MindTrek special issue.

Kevin Curran
Editor-in-Chief
IJACI

Kevin Curran, BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA, is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr. Curran has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 700 published works. He is perhaps most well-known for his work on location positioning within indoor environments, pervasive computing and internet security. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to BBC Radio & TV news in the UK and is currently the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Technical Expert for Internet/Security matters. He is listed in the Dictionary of International Biography, Marquis Who's Who in Science and Engineering and in Who's Who in the World. Dr. Curran was awarded the Certificate of Excellence for Research in 2004 by Science Publications and was named Irish Digital Media Newcomer of the Year Award in 2006. Dr. Curran has performed external panel duties for various Irish Higher Education Institutions. He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computing Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE) and a fellow of the higher education academy (FHEA). Dr. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He is the Editor-in-Chief of the International Journal of Ambient Computing and Intelligence *and is also a member of 15 journal editorial committees and numerous international conference organising committees. He has authored a number of books and is the recipient of various patents. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies.*