virus BULLETIN Covering the global threat landscape

ON THE BEAT

Kevin Williams
TC-UK Internet Security, UK

I read with interest *VB*'s recent *Throwback Thursday* article detailing the process which led, in 1996, to the conviction of self-confessed virus writer Christopher Pile, the first person in the UK to be given a custodial sentence for writing and distributing computer viruses [1]. Having recently left UK law enforcement after 25 years of service, I am pleased to report that there have been many more successful cybercrime prosecutions since then.

In October 2008, I helped set up the Police Central eCrime Unit (PCeU) in the Metropolitan Police Service, building on the success of the Computer Crime Unit. We were able to create a unique national response to the growing cybercrime problem. From February 2012, the PCeU had a presence outside London, with regional hubs created in the North West, North East and the East Midlands. Ultimately, this grew to representation at a regional level across the whole of the UK, and in 2013, the National Cyber Crime Unit (NCCU) of the National Crime Agency was set up. Through central government funding via the National Cyber Crime Programme, the NCCU established a head count of 200 cybercrime specialists, resulting in a much improved and coordinated regional response.

Thanks to the support of senior police officers including Sue Wilkinson and Janet Williams, and the dogged determination of Charlie McMurdie and Terry Wilson, the PCeU was able to demonstrate its success in a report entitled 'Police Central e-Crime Unit Financial Harm and Reduction Report', published in September 2013.

The report highlighted successes such as:

- £1.01 billion financial harm reduction: a £58 financial saving to the UK economy for every £1 invested in the PCeU.
- 255 persons arrested, 126 persons charged, 143 persons brought to justice, 89 persons cautioned, 26 organized crime networks disrupted.

The operational activity of the PCeU covered several ground-breaking investigations.

Operation Pagode

In September 2010, it was reported that, as part of Operation Pagode, the PCeU had arrested 19 people in London in connection with the theft of millions of pounds from online bank accounts [2]. Thousands of PCs belonging to UK citizens were believed to have been infected with malware, enabling an organized criminal network to capture users' log-on details and subsequently use the information to fraudulently access bank accounts and transfer funds to mule and drop accounts.

Several major international banks suffered losses, with around £6 million thought to have been stolen in just a three-month period.

Operation Pagode – harm saved

In October 2011, it was reported that Operation Pagode had resulted in £84 million worth of harm saved [3].

Following an 11-month investigation, five defendants were jailed for a total of 15.5 years. Detectives uncovered evidence that the defendants had been directly involved in a global forum which promoted and facilitated the electronic theft of personal information. Detectives also uncovered evidence that the defendants had been involved in credit and debit card fraud; the buying and selling of personal information (including passwords and PINs); the creation and exchange of malware; the establishment and maintenance of botnets; and tutorials offering advice on how to commit such offences.

Operation Dynamaphone

In October 2011, it was reported that Operation Dynamaphone had resulted in £5.5 million worth of harm saved [3].

Three men were jailed for 13.5 years for their part in a sophisticated attack on UK and international banking systems. The defendants had used phishing techniques to obtain large volumes of personal information, including online bank account passwords and credit card numbers, and subsequently used that information to steal money from the accounts, and to use the credit card details fraudulently. In all, the defendants were believed to have compromised over 900 bank accounts and 10,000 credit cards.

Operation Allandale

Reported in September 2013, Operation Allandale was an investigation into offences of conspiracy to defraud UK and international banks [4].

Several UK banks were targeted during a sophisticated phishing campaign that had been instigated by a highly organized criminal network. Actual financial losses to the UK banking industry stood at over £300,000, with further potential losses of £53m.

A Nigerian national residing in Birmingham headed the UK part of the network and performed the roles of organiser, coordinator and treasurer. He was convicted of offences relating to the Conspiracy to Defraud and Proceeds of Crime Acts, receiving a term of eight years imprisonment.

This was the longest custodial sentence secured by the PCeU for a criminal of this type, and illustrates the increasing level of understanding within the judicial process of the serious nature of cyber offences. (Two other defendants, who were Romanian nationals, received sentences of five years and seven months imprisonment, and seven years and two months imprisonment.)

Cybercrime gang behind major bank fraud jailed

In April 2014, it was reported that the cybercrime gang behind a major bank fraud had been jailed [5].

The gang had stolen more than £1.25 million by remotely controlling bank accounts, using a KVM switch to access and control *Barclays* and *Santander* bank accounts remotely on three occasions.

Nine members of the gang were sentenced to a total of 24 years and nine months imprisonment.

INTERNATIONAL OPERATIONS

During my time at the NCCU, we also looked to respond to the threats caused by those criminals who were beyond the jurisdiction of the UK, by taking down their infrastructure in order to cripple their activities. This required the expertise and cooperation of law enforcement globally, but also close collaboration with industry and academia. This was best demonstrated in the operations to combat the GameOver Zeus and Shylock banking trojans.

Operation Tovar

In June 2014, it was reported that, as part of an international law enforcement operation (also involving security firms and academic researchers), the GameOver Zeus botnet had been taken down [6].

Operation Tovar was a collaborative effort involving investigators at the National Crime Agency, the FBI and Europol; security firms including *CrowdStrike*, *Dell SecureWorks*, *Symantec*, *Trend Micro* and *McAfee*; and researchers at VU University Amsterdam and Saarland University in Germany.

The GameOver Zeus botnet was estimated to consist of between 500,000 and 1 million compromised systems globally, with infected PCs both being harvested for sensitive financial and personal data, and being rented out to hackers for use in other attacks.

Law enforcement and industry collaborate to combat Shylock malware

July 2014 saw an international collaboration between law enforcement and industry to combat the Shylock banking trojan [7].

The National Crime Agency brought together investigators and researchers from the FBI, Europol, GCHQ, the German Federal Police (BKA), *BAE Systems Applied Intelligence*, *Dell SecureWorks* and *Kaspersky Lab*, to jointly address the Shylock trojan.

Law enforcement agencies took action to disrupt the system on which Shylock depended to operate effectively. This involved seizing the servers which formed the trojan's command-and-control system, as well as taking control of the domains Shylock used for communication between infected computers. The action was conducted from the operational centre at the European Cybercrime Centre (EC3) at Europol in The Hague. Investigators from the NCA, FBI, the Netherlands, Turkey and Italy gathered to coordinate action in their respective countries, in tandem with counterparts in Germany, Poland and France.

CURRENT THREATS

Having moved from law enforcement to the private sector, I have gained an even greater understanding of the current threats to the UK and Europe. I see the greatest threats as APTs, driven by state-sponsored attacks, stealing and destroying the intellectual property and sensitive data of companies and governments. I also see the continued escalation of the threat from denial of service attacks, in some cases with associated ransom demands.

For the individual, the most devastating attacks are those that deliver ransomware or banking trojans. Often, it is not just the loss that impacts the individual, but also the feeling of helplessness through a lack of understanding of how to protect oneself online.

I believe that we can never do enough to educate users on how to protect themselves online – which is why I now work for an organization whose mission is to 'save and improve human lives'. I also commend those who try to help with delivering the public message, such as *Get Safe Online* [8]. Additionally, I wholly support the work of the Cyber Security Challenge in looking to find young people with information security skills, and encouraging them, through online and real-world competitions, to hone their skills and consider a role in cybersecurity.

Who knows where we will all be in another 25 years' time!

REFERENCES

[1] Throwback Thursday: Regina v Christopher Pile: The Inside Story & Off with his Head! Virus Bulletin. https://www.virusbtn.com/blog/2015/04_30a.xml.

[2] PCeU arrests 19 over multi-million pound online banking raids. Finextra. http://www.finextra.com/news/fullstory.aspx?newsitemid=21838.

[3] E-Crime Unit saves UK economy £140m in six months. http://content.met.police.uk/News/ECrime-Unit-saves-UK-economy-140m-in-six-months/1400003449724/1257246745756.

[4] Police Central e-Crime Unit Financial Harm and Reduction Report. http://content.met.police.uk/cs/Satellite?blobcol=urldata&blobheadername1=Content-Type&blobheadername2=Content-Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22694%2F43%2FCO624-11harmreductionreport2013.pdf%22&blobkey=id&blobtable=MungoBlobs&blobwhere=1283654366819&ssbinary=true.

[5] Cyber crime gang behind major bank fraud jailed. http://content.met.police.uk/News/Cyber-crime-gang-behind-major-bank-fraud-jailed/1400023721922/1257246745756.

[6] ‘Operation Tovar’ Targets ‘Gameover’ ZeuS Botnet, CryptoLocker Scourge. Krebs on Security. http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.

[7] Law enforcement and industry collaborate to combat Shylock malware. NCA. http://www.nationalcrimeagency.gov.uk/news/news-listings/408-law-enforcement-industry-collaborate-to-combat-shylock-malware.

[8] Get Safe Online. https://www.getsafeonline.org/.

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

© 2015 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England.

Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com

Web: http://www.virusbtn.com/