SUCCESSES AND FAILURES APPREHENDING MALWARE AUTHORS

Raymond A. Pompon
HCL CapitalStream

Email ray.pompon@hcl.in

ABSTRACT

This paper walks through the Donttrip malware case, a successful malware investigation prosecution, from the initial infection to the concluding sentencing. Along the way, the paper will point out and examine significant issues while reviewing other relevant malware cases. The paper will include commentary from law enforcement personnel as well as victims on the key problems and methods used to investigate and prosecute malware criminals. Two interesting findings resulted from this analysis. Although malware criminals are difficult to apprehend, once caught nearly all of them admit guilt. Also, the lack of victim reporting of malware crimes not only severely limits the apprehension of malware criminals but degrades the overall effort of law enforcement to predict and punish malware authors.

1. INITIAL INFECTION

The Donttrip malware infection began, as it usually does, with a call to the help desk: 'Is the network down? I'm having problems getting my email.' It was the first weekend of the new year and hangovers of the holiday season were just wearing off. The tech support team began to investigate when a second call came in. Then a third. That's when the techs realized this was a serious problem. For a normal business, a network outage is bad news. But this was Northwest Hospital, a large medical facility in Seattle that served thousands of people. And on 9 January 2005, a botnet invasion would threaten to shut them down.

A surge of malware scans for fresh victims quickly overwhelmed the medical centre's network. Patient financial systems froze. Pagers remained silent. Laboratory services clogged up. Diagnostic imaging systems failed to transmit data. Terminals in the Intensive Care Unit disconnected. Since the doors to the operating room were computer controlled, they locked down as well. The hospital staff rose to the occasion and implemented workarounds. Nurses were stationed to manually operate the operating room doors. Patients were rescheduled for surgery. Secondary processes designed for disaster recovery were brought online. Switching to backup systems to contain the compromise saved the hospital from total meltdown and no lives were lost. Arguably, patient care may have been compromised and the operations network remained unusable. Technicians would disconnect a machine from the network and clean it. As soon as a clean machine was put back online, it became reinfected. The techs didn't have the people or the technology to fix things fast enough. They were in over their heads and they knew it [1].

Incident response

A man who responded to many malware incidents is retired Supervisory Special Agent Michael Levin, formerly the Deputy Director of the National Cyber Security Division at the Department of Homeland Security. In his years working on the US Secret Service Electronic Crimes Task Force, Levin responded to many organizations lost in the chaos of a malware outbreak. 'There needs to be a plan in place,' commented Levin. 'Many were not ready to deal with the issues that come with a law enforcement investigation.' Smaller organizations were the worst, Levin notes, '… as they are resource constrained and often hit hardest.' [2]

The typical small organization, characterized by 15 to 50 employees with an annual budget of just a few million dollars, is often completely shut down by a malware outbreak. Smaller organizations often lack internal security personnel to triage and eradicate the infection. Often organizational leadership brings in contractors with instructions to wipe the machines clean and restore functionality. In most of these cases, law enforcement is never made aware of the event or the damages. The organization simply shoulders the burden and limps on as best it can [3].

2. CALL FOR HELP

Losing ground to the botnet, Northwest Hospital called a security integrator who had helped them with some network devices in the past. That's when my phone rang. I realized they were experiencing what Dr Peter Tippett calls a 'virus disaster', where more than 25 machines were infected and the prognosis was days of downtime, possibly weeks [4]. As we began to discuss remediation, I asked them if they'd called the FBI. They didn't quite understand why the FBI would care, but I convinced them it was the best thing to do. I gave them the name and the direct phone number of a colleague inside the Seattle Field Office. Hospital employees probably shared the thought running through my head – someone is going to pay for this. The men and women of the United States Department of Justice were going to find that someone.

Critical infrastructure

NW Hospital made two decisions that would result in the apprehension of the guilty parties. The first was to call in outside help. Few smaller organizations have technical staff properly trained in incident response and investigation. The second good decision that NW Hospital made was to call the FBI. Public health organizations, like hospitals, are classified by the Federal government as critical infrastructure under Presidential Decision Directive 63. In 1997, President Clinton published PDD-63, which required the FBI to play an active role in protecting critical systems such as the electrical grid, the telephone network, and the financial system [5]. A hospital with downtime because of a malware attack meant the FBI was going to make a high priority response.

Victim reluctance to report

By calling the FBI to report the malware incident, NW Hospital did something that was actually very unusual. Throughout the

interviews conducted with law enforcement officers, one critical problem was brought up repeatedly: malware victims rarely call the police. The Field Office of the Seattle FBI receives fewer than two dozen malware complaints a year [6]. Contrast this with Seattle being ranked as one of the top ten cities for cybercrime year after year [7].

One reason that malware is underreported is that some victims of malware attacks misattribute their experiences to something else. This is a common enough problem that the National White Collar Crime Center felt their numbers regarding malware do not accurately reflect what is going on [8].

Misattribution is certainly a problem, especially as malware becomes silent and invisible. However, there are other reasons why victims choose to not report. Law enforcement officials often talk about the 'push pull' relationship organizations have with pursuing justice versus the potential of bad publicity [9]. In interviews with business victims of malware, fear of bad publicity is the primary cited reason why there is a hesitation to call the police [10].

In recent years, American breach disclosure laws have required organizations to inform victims of breaches of confidentiality. One of the ways to forestall disclosure is to have an active police investigation underway. Unfortunately, breach disclosure laws only force reporting of verified leaks of customer data. Organizations afraid of bad publicity may be tempted to assume a malware infection only caused denial of service or resource hijacking, but not theft of data. In those cases, victims would not report any potentially embarrassing breaches [9].

For whatever the reason, the lack of reporting malware infections is a huge blow to law enforcement efforts. Often even the smallest malware cases are kept on file and cross-referenced against other pending investigations. When perpetrators are finally identified, investigators can use these files to gather additional victims to build a stronger case and ensure stiffer penalties. The main US website for reporting cybercrimes, called the Internet Crime Complaint Center (IC3), is run by the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance [11]. When the IC3 collects enough cybercrime complaints that appear to be related, they bundle them up and the FBI will open a case. Even if a case isn't investigated, the intelligence data provided from a report helps enforcement officials justify additional resources [6].

Law enforcement outreach programs

The US Department of Justice publishes a training booklet called 'Prosecuting Cybercrimes' which urges Federal prosecutors to 'build relationships before an intrusion' because 'Many companies, universities, and other victims are reluctant to report cybercrime incidents to law enforcement because they are fearful that law enforcement will conduct an investigation in a manner harmful to their operational interests…' [12].

One of the key ways in which the FBI tries to build relationships is through InfraGard, a civilian outreach program. Each FBI field office runs a local chapter of the all-volunteer organization [13]. Because of my InfraGard membership, I was able to give NW Hospital a personal contact within the FBI cyber squad.

How does one measure a good relationship with law enforcement? Levin succinctly defines it as 'Good enough to ask hypothetical questions.' [2].

3. THE FBI RESPONDS

When NW Hospital called, the FBI cyber squad sent their best man. Although a younger agent with relatively little field experience, Special Agent David Farquhar was unique. He'd walked away from a lucrative job in the tech industry to serve his country. At that time, a typical FBI agent's expertise was heavy with traditional police investigations, accounting and law. David's rich computer and network skills were a rare asset for the FBI in 2005. He had already proved his mettle in the Blaster case two years before. Now the Bureau was looking to him for another big win. He would not disappoint them [6].

Cyber cops

Clearly, SA Farquhar's skills and promptness were critical success factors in this case. In 2005, the Federal government had a shortage of agents and prosecutors with cybercrime skills. Since then, the FBI has added over a thousand computer crime investigators divided amongst technical specialties. There are reverse engineers, honeypot experts, Computer Analysis and Response Teams (CART), and liaisons. Liaisons are especially important as they work with civilians to bring external expertise into investigations. Often liaison-supplied help can be the key to cracking a large cyber investigation. For example, liaisons can draw technical experts from InfraGard, academia and software manufacturers [6].

The cybercrime enforcement system is still far from ideal. For over-burdened field agents, computer evidence can be shipped back to FBI headquarters to be analysed. This creates delays in the investigative process, prompting some FBI field offices to build up their local cyber forensic labs and attempt to recruit additional experts. However, there is a shortage of cyber security experts in general. With government pay lagging behind the private sector, law enforcement finds it very difficult to hire sufficient qualified investigators to meet their needs [6].

What can a victim organization do if the investigator assigned to their case isn't up to speed technically? Levin offers this advice: 'Do your forensics before the cops get there and vault the evidence.' Specifically, he means that as soon as any crime is suspected, local techs should get the infected drive offline and lock the drive away to protect its chain of custody. All analysis should be done against an image carefully copied from the original drive [2]. The reason this should be done beforehand is that Federal investigators cannot give any investigative direction to victims once a case is opened. If they do, the victims could be construed by the court as acting as an agent of law enforcement and be subject to subpoena and cross-examination by the defence [9].

Victims should also prepare a timeline of events related to the crime and clearly document their financial losses. This means that organizations in general should already have been logging computer events before the crime occurred. Victims can request that certain proprietary data be redacted from police reports if

the case goes to trial so that corporate secrets remain undisclosed. In some situations, organizations may have to dedicate internal resources to provide technical assistance to law enforcement as the investigation proceeds [2].

4. ON THE SCENE

SA Farquhar was on the scene the same day he was called. Usually the FBI has to extract a sample from a forensic image at a crime scene and then try to reconstruct the behaviour in a virtual sandbox environment. But because the botnet was still loose, he was able to observe an infected workstation live. He found that there seemed to be two files, 'dust.exe' and 'msams.exe', that were causing the most trouble. So far, over 150 computers at NW Hospital had this infection. The scan time on the malware was set to zero minutes, so they were scanning relentlessly for fresh machines to infect. In fact, this was probably a bug that caused the malware to be noticed too soon. If the malware had been stealthier, the botnet might have survived. The malware was using *Microsoft Windows* vulnerabilities LSASS (MS04-11) and RPC/DCOM (MS04-12) to break into fresh machines. SA Farquhar passed this information on to the NW Hospital techs so they could target their clean-up efforts [1].

SA Farquhar saw that the malware was using Internet Relay Chat over TCP port 30108 to talk to a botnet controller at the IP address 54.39.20.81. This IRC server was owned by *DNS Made Easy* and seemed to have nearly half a million other bots under its command. SA Farquhar contacted *DNS Made Easy* and subpoenaed the records for that particular site. They returned to him the IP address of the machine that opened the account and the email address donttrip31337@cashette.com. Donttrip. Now he had a hacker name. It was a start [1].

Online versus offline response

The DOJ team that prosecuted the Donttrip case attributes a big part of their success to having a qualified agent onsite while things were still happening. For FBI investigators, there are two kinds of malware response: online and offline, referring to the state of the malware. Offline means the malware is contained and the drives are available for forensics. If the malware is online, then active captures must be obtained without hampering the victim's mitigation efforts [6].

Case – malware insider at a bank

Many cases never get off the launch pad because of a late response or spoiled evidence. Consider the case of the malware at a medium-sized bank. An intrusion detection system rang an alert after detecting a library file associated with malware on a workstation. The security team performed a hasty remote investigation and determined that a user had installed hacker tools on a computer. The security team contacted the internal audit and the user's manager. Within hours, the user was interviewed, processed, terminated, and escorted from the building. Before any forensic data could be captured, the IT help desk reloaded the hard drive with the corporate image. Because the entire incident unfolded in under a day, many critical data preservation and analysis steps were skipped. Without clean forensic data on the malware, no future legal actions could be supported and no further investigation into the nature of the malware could be performed [14].

5. INVESTIGATION PROGRESSES

The originating IP address that SA Farquhar got from *DNS Made Easy* traced to *NetZero*, a free dialup ISP. He subpoenaed their records and examined the results. Two patterns of usage emerged, tracing back to two telephone numbers, one in California and one in Texas. This was good but he needed more to ensure a solid conviction.

SA Farquhar continued to monitor the *DNS Made Easy* records. There he saw a new botnet controller come online on a hacked system in Kansas. SA Farquhar contacted the owner of the hacked box and got permission to monitor the botnet command and control network. Now the FBI could watch the bot-masters at work.

The monitoring began on 9 February 2005 and continued until 25 February. In all, SA Farquhar collected 2,672 data files, each holding over 16 megabytes of controller traffic. Analysis revealed 355,497 compromised systems from 104 different countries. This was a respectable-sized botnet.

Watching the traffic, SA Farquhar noted that a common botnet command issued was for all the bots to go to the 'www.top48hours.com' site and vote for a website called 'www.donttrip.org'. The site was hosted by *California Regional Internet*, *CARI.net*, in San Diego. SA Farquhar subpoenaed their records and found that the site was paid for with a *PayPal* account registered to the email address 'chrismax85@yahoo.com'. *CARI.net* also provided logs of the IP addresses that connected to their site. The IPs traced to a phone number in California. The same phone number that was using *NetZero* to access *DNS Made Easy*. He was getting closer [1].

Identifying perpetrators

Although the FBI had the home phone numbers of the Donttrip authors, they still couldn't make any arrests. For a US court, a phone number or an IP address isn't sufficient evidence. Prosecutors need to prove 'whose hands were on the keyboard' at the time the crime was committed. But even to uncover IP addresses and email addresses can be a difficult and sometimes fruitless pursuit [6].

Recently, investigators are finding that nearly 75% of the domains used by botnets are anonymized and require extensive court orders to uncover. Some Internet companies now are providing anonymization services coupled with extensive sub-contracting of parts of their business. For example, an investigator will submit a subpoena for DNS records. Two weeks later, the response will be that the particular domains in question have been subcontracted to a different company. The investigator will then resubmit his subpoena to the new company. Then this process could repeat again, if enough slices of the business have been resold and distributed. Since financial records require a different subpoena, the investigator will submit again back at the first company. In many cases, payment services are also subcontracted, requiring more subpoenas and

time. Investigators are now finding that it's taking months and, on average, six subpoenas to trace a single attack. Couple this with log retention and records management issues and by the time the correct corporation is contacted, the data may have been deleted. An investigator will have to sort through thousands of changing domains and dozens of servers to trace back to a single criminal group [6].

American laws, such as the Communications Assistance for Law Enforcement Act (CALEA), require telecommunication providers to provide access to police investigators for wiretaps and tracing. However, there are no specific requirements for log retention. Industry-wide, the typical log retention for an organization is around 90 days. Investigators lament that if a service provider can't identify the bad guys, then their hands are tied. This is why the FBI has been urging Congress to draft legislation requiring that Internet service providers retain two years' worth of log data [15].

Overseas investigations

In many malware cases, an FBI investigation leads out of the United States. For these investigations, the FBI must rely on their Legal Attachés or 'legats', who coordinate with other countries' law enforcement officials. In countries where the police cooperate with the US authorities and are competent, the FBI is very open to allowing a local prosecution of a criminal [6].

Case – Zotob

A rare success would be the Zotob trojan case, where *Microsoft* and the FBI provided technical assistance to Moroccan authorities. Malware author Farid Essebar was convicted and sentenced to two years in a Moroccan prison while his cohort, Achial Bahoul, was given one year. However, in general, FBI investigators report that overseas cases are tougher and take longer often because of technical and legal deficiencies in some countries [16].

6. MORE VICTIMS

As SA Farquhar continued his investigation, other victims began to surface. As early as October 2004 the DoD Global Information Grid had been tracking and analysing a new botnet. It had already hit DoD systems in Mannheim Germany and it had spread to over 400 machines and caused more than $100,000 in damages. Their incident response team assigned eight investigators to find the hacker who they knew only as 'Don't Trip.'

And on Valentine's Day, 2005, Colton School District in California experienced a replay of what happened to Northwest Hospital. Machines flooded with pop-ups and ads. Entire classrooms of computers were going down, with techs having to re-image the boxes from scratch to get them back up only to have them reinfect. At one point, there were five technicians assigned full-time to the clean up and containment of the malware. After weeks of outbreaks, Colton School District traced the malware back to its command and control server. It was mid-April when *DNS Made Easy* passed on their abuse complaint to SA Farquhar. The FBI shared their insights into how the malware spread, which the School district was able to use in their containment efforts. Both the DoD and the School District would publicly allow themselves to be identified as victims [1].

Long investigations

What could Northwest Hospital be thinking at this point in time? They had a huge malware infestation that nearly crippled them. They called the FBI, who swooped in, did a bunch of analysis and left. Now months had passed and they had heard nothing. They couldn't be faulted for wondering why they bothered. Over the past decade, the length of time from the point at which a malware crime is committed to the actual sentencing of a convicted criminal is about two and a half years. This means that after a malware victim calls law enforcement, it will be on average 14 months before an arrest is made. Then it will be another nine months before trial and then about six months before sentencing (see Table 1). For this reason, successful malware prosecutions depend on organizations to commit to a protracted investigation without any feedback. The Donttrip case ran a bit faster: ten months from initial call to arrest, six months to trial, and three months to sentencing [1].

One reason for this is that cyber cases are larger and are complex, like organized crime cases. Malware cases can take years to investigate, as opposed to most fraud cases, which finish in under a year. Several FBI personnel have commented that victims often call back asking to know a case's status. Because of the confidential nature of investigations, they cannot be told much more than 'we're working on it'. For some victims, this isn't enough. They ask what techniques the FBI is using and how close the agents are to an arrest. Unfortunately, they have to wait patiently. For some victims, the wait is forever.

Case – Blaster-B

In 2003, SA Farquhar and Levin swiftly identified the authors of the Blaster variant B worm [17]. When asked why the case was so successful, Levin replied, 'We moved fast because time is of the essence in these kinds of cases.' When asked why they moved fast, he said, 'We had the commitment of the victim and we had the commitment of law enforcement,' adding that the primary victim, *Microsoft*, 'Helped point them in the right direction.' When asked to define law enforcement commitment he explained that the FBI and US Secret Service worked together and 'We had teams ready to fly at a moment's notice.' Finally, when asked how to get law enforcement commitment, he replied that it all depended on the 'significance of the case' [2].

7. PAYPAL

The last piece of the puzzle for SA Farquhar was the money. He started by subpoenaing *PayPal* about the account Chrismax85@yahoo.com. In there was nearly $100,000 in adware earnings. Between July 2004 and May 2005, over $15,000 was moved to a *Wells Fargo* savings account. And in the same time period, over $30,000 flowed in from adware businesses. Then there was another $6,000 from *Toolbar* cash in payment for installing their software on customers' machines. Of course, these weren't willing customers, but victims of the

botnet. With the financial records, he was able to confirm the names and addresses of the perpetrators. Two were juveniles and one was 20 years old. His name was Christopher Maxwell of Vacaville, California. SA Farquhar and Assistant US Attorney Kathryn Warma put together an indictment [1].

Following the money

Investigators will examine malware and identify the signature of a particular virus author by the packers they use and the strings they embed. However, this won't provide solid proof of the identity of the perpetrator. Investigators crack almost all malware cases by following the money trail. Not only does monetary gain 'put hands on the keyboard', but it is the key factor in making the case that this wasn't some joyriding kid. Now that botnets and malware are large money-making criminal enterprises, this is the best path to follow [6].

At the time of the NW Hospital infection, malware authors primarily monetized their botnets by subverting the pay-per-install advertising market. Internet marketing companies pay independent software manufacturers to install adware-enabled programs. Malware authors would exploit this by simply embedding the adware directly into infected computers. This is the primary way that Christopher Maxwell and his conspirators were making money from their malware [1].

The secondary method by which the Donttrip malware made money was click-fraud. In this case, the malware causes the infected computer to click on web advertisements on sites owned by the malware author, thus creating the illusion that the site is heavily visited. The more popular a site is, the more advertising revenue it is worth [1].

Malware authors now are more aggressive and using hidden spyware to steal banking credentials or credit card numbers from victims. These newer types of malware are harder to detect, as no annoying advertising messages give away the presence of the malware.

Case – the 'Unix Terrorist'

There are cases where the money trail leads only to an organization but not to specific members. A good example is Stephen Watt, the 'Unix Terrorist'. Watt was prosecuted as a member of the *TJ Max* breach conspiracy led by his friend Albert Gonzalez [18]. For no direct payment, Watt wrote the malware that Gonzalez used to steal hundreds of millions of credit cards from dozens of large corporations. However, Gonzalez did invite Watt to lavish parties paid for with the proceeds of his crime. Watt was convicted and sentenced to two years in prison because of his willingness to cause malicious damage and his indirect gains [19].

8. ARREST & TRIAL

In November 2005, FBI agents served search warrants simultaneously at all three residences, two in Texas and one in California. The two suspects in Texas were juveniles, so their names and details have never been made public. Christopher Maxwell of Vacaville California was charged with violating Federal law 18 USC 1030, fraud and related activity in connection with computers. When interviewed by the FBI, Maxwell was shocked to discover that his botnet had disrupted a medical facility.

In May 2006, Assistant US Attorney Kathryn Warma prosecuted 'United States versus Christopher Maxwell' in the District Court in the Western District of Washington. The evidence presented against Christopher Maxwell included the logs and network captures from NW Hospital as well as data from the DoD and Colton School District. Damages were calculated to exceed $250,000. Christopher Maxwell ended up pleading guilty to one count of conspiracy to intentionally cause damage to a protected computer and to commit computer fraud, and two counts of intentionally causing and attempting to cause damage to a protected computer [1].

To an outsider, this case could be considered a success. But in reality, the battle was only half won. The real challenge lay ahead.

Making a malware case

It was no surprise that Christopher Maxwell pleaded guilty. Malware defendants make plea agreements and admit guilt in 94% of the cases that go to trial. More recently, FBI cyber investigators have taken a page from organized crime investigations. They will arrest a low-level member of the conspiracy on a lesser crime, like software piracy or possession of child pornography. The low-level member is then offered a '5K letter', which certifies that a defendant has cooperated substantially in a prosecution or investigation of another person. These letters, which refer to section 5K1.1 of the US Sentencing Guidelines, are used to reduce a defendant's sentence in Federal court [6].

One of the reasons why investigators spend enough time to gather extensive evidence is that judges and juries have a difficult time with technical cases. In addition, there are also venue challenges because victims are often spread across the world and the question of where a defendant should be tried can be difficult to resolve. Finding applicable laws can also come into play when a venue is being decided. And lastly, the technical nature of the evidence means the defence attorneys often require additional time before trial to prepare [9].

Case – ILOVEYOU

In most failed malware cases, the causes can be attributed to immature laws. For example, in the Philippines, defendants Onel de Guzman and Reomel Ramones were arrested for the ILOVEYOU virus but were quickly released because they had violated no Filipino law [20].

9. SENTENCING

Now convicted, Christopher Maxwell would face sentencing in August 2006. Since only three victims had come forward publicly, the judge could only consider their damages. Assistant US Attorney Warma, in arguing for a six-year sentence, said to the judge, 'The importance of deterrence in this case is profound. There is a hacker community. They will know immediately what sentence you impose.' In his defence,

Maxwell pleaded for mercy, 'I am a 21-year-old boy with a good heart and I made a mistake, I never realized how dangerous a computer could be. I thank God no one was hurt.' US Attorney Warma pointed out to the judge that hackers who create these kinds of malicious tools are fully aware of their indiscriminate destructive nature. She also presented letters from the computer community stressing the serious threat botnets pose to the Internet and society in general. The judge ruled for a 37-month prison sentence and that he make restitution of $252,000–$136,000 to the DoD and $114,000 to Northwest Hospital [21].

Sentencing of malware criminals

A strong punishment comes from explicit damages claimed by a large number of victims. Since victim damage is such a huge factor in a sentence hearing, investigators work hard to collect this information long before a case goes to trial. Investigators and prosecutors will also collect as much data on a particular crime from multiple complaint sources, such as the Internet Crime Complaint Center, the Federal Trade Commission, the Federal Communications Commission, the Attorney General and the FBI [6].

The danger is that without sufficient damages, judges can perceive the defendant as a 'troubled smart kid' and let them off with a light sentence. Sentences with high restitution also serve to punish the criminal and help defray the damages that victims suffer. In malware cases, prison terms average 17 months and restitution repayments average $100,000 (see Table 1).

Cases – Digerati and Resili3nt

A good example of how damages determine sentencing is the 2008 botnet case involving Ryan Brett Goldstein, aka Digerati. Goldstein created a botnet and used it for a denial of service attack against a university. The damages were a comparatively low $6,000 [22]. For this he was given only three months incarceration, a $30,000 fine and was ordered to make restitution. Contrast that with Resili3nt or Jeanson James Ancheta. Ancheta ended up pleading guilty to creating a botnet of half a million computers. In 2006, he was sentenced to five years and was required to pay $72,000 in damages and asset forfeiture [23].

10. FINAL THOUGHTS

Overall, NW Hospital's actions can be seen as a positive model for their speed, willingness to report, and commit to a lengthy prosecution. They were able to compensate for the lack of awareness of law enforcement resources by the hiring of outside security contractors who did have partnership resources. Organizations in general should be encouraged to seek out local law enforcement resources before a cybercrime occurs and be prepared to provide useful and timely information in the event of an incident.

Since the Donttrip case, there have been two more malware cases involving hospitals. In October 2006, James Brewer of Texas created a botnet for spam that accidentally infected a hospital in Chicago causing similar denial of service damage to that which NW Hospital suffered. He was sentenced to 36 months in prison and must make $270,000 restitution [24]. In April of 2009, Jesse William McGraw was in the process of using malware to threaten a hospital in Texas where he worked. In mid-May of 2010, he pleaded guilty and is expected to be sentenced in September [25].

In general, the FBI is diligently working more malware cases than ever. Although no one in the US Department of Justice can comment on an on-going investigation, one only needs to look at the newspaper to guess the complexity and magnitude of the investigation for malware such as Storm, Conficker and Zeus. The FBI has confided that they are striving to become more threat-focused, as opposed to incident-response focused. This means they will be more aggressive in using more technical and human means of gathering intelligence. Overall, the law enforcement community has realized that malware and the proliferation of botnets represents a clear and present danger to global e-commerce and the infrastructure that supports our modern society. To win this war, they will need more specialists, international coordination, and better cooperation from victims [6].

ACKNOWLEDGEMENTS

Thank you to Mike Simon for technical editing and fact checking. Special thank you to the agents and support staff of the United States Department of Justice – because of your dedication, the world is much safer.

REFERENCES

[1] Federal Court Case: USA v. Christopher Maxwell – 2:06-CR-00042-MJP.

[2] Interview, Michael Levin, US Secret Service (Retired) and former Deputy Director of National Cyber Security of Department of Homeland Security.

[3] Interview, Security Consultant, Conjungi Networks.

[4] Beer, S. Virus attacks continue to escalate says survey. IT Wire. http://www.itwire.com/it-industry-news/development/1130-virus-attacks-continue-to-escalate-says-survey.

[5] Presidential Decision Directive 63. http://www.justice.gov/criminal/cybercrime/factsh.htm.

[6] Interviews, Federal Bureau of Information, Seattle Field Office, Cybecrime Squad. Not for attribution.

[7] The Norton Top 10 Riskiest Online Cities Report Reveals Who's Most Vulnerable to Cybercrime. http://norton.newslinevine.com/Riskiest_Online_Cities_Press_Release.pdf.

[8] E-mail interview, John Kane, Research Manager, National White Collar Crime Center.

[9] Interview, Assistant US Attorney Kathryn Warma, United States Attorney's Office – Western District of Washington.

[10] Interviews, Directors of IT, Financial Institution, eCommerce site, Services Organization.

[11] Internet Crime Complaint Center website. http://www.ic3.gov.

[12] United States DOJ, Prosecuting Computer Crimes. http://www.justice.gov/criminal/cybercrime/ccmanual/index.html.

[13] InfraGard website. http://www.infragard.net/.

[14] Interview, Network Security Engineer, Washington-based Financial Institution.

[15] McCullagh, D. FBI, politicos renew push for ISP data retention laws. http://news.cnet.com/8301-13578_3-9926803-38.html.

[16] FBI press release. http://www.fbi.gov/pressrel/pressrel06/zotobcertificates092506.htm.

[17] Federal Court Case: USA v. Jeffrey Lee Parson – 03-cr-00379.

[18] Federal Court Case: USA v. Albert Gonzalez – s 08-CR-10223-PBS, 09-cr-102262-pbs, 09-cr-10382-dpw.

[19] Federal Court Case: USA v. Stephen Watt – 1:08-cr-10318-ng.

[20] ILOVEYOU virus. http://en.wikipedia.org/wiki/ILOVEYOU.

[21] Barber, M. Hacker faces prison for PC attacks; Northwest Hospital among targets. Seattle Post-Intelligencer. http://www.seattlepi.com/local/282561_botnet25.html.

[22] Federal Court Case: USA v. Ryan Goldstein – 2:07-cr-00680-mmb.

[23] FBI press release. Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers. http://www.justice.gov/criminal/cybercrime/anchetaArrest.htm.

[24] Federal Court Case: USA v. James C. Brewer – 07-cr-00379.

[25] Federal Court Case: USA v. Jesse William McGraw – 3:09-CR-00210-B.

Case	**Perpetrator**	**National origin**	**When crime**	**When indict/ arrest**	**When trial**	**Plead guilty?**	**When sent.**	**Prison (months)**	**Fines & restit. ($)**
Morris worm	Robert Morris	USA	Nov-88	Jul-89	Jan-90	N	May-90	0	$10,000
MBDF	David Blumenthal, Randall Swanson, Mark Pilgrim	USA	Dec-91	Sep-92	Sep-92	y	Oct-92	0	$2,500
Pathogen	Christopher Pile	UK	Apr-94		May-95	y	Nov-95	18	$0
Melissa	David Smith	USA	Mar-99	Apr-99	Dec-99	y	May-02	20	$5,100
Love bug	Onel de Guzman	Philippines	May-00	May-00					
Anna Kourikouva	Jan de Wit	Dutch	Feb-01	Feb-01	Sep-01	y	Sep-01	0	$0
Thr34krew	Andrew Harvey	UK	Dec-01	Feb-03	May-05	y	Oct-05	6	$0
Thr34krew	Jordan Bradley	UK	Dec-01	Feb-03	May-05	y	Oct-05	3	$0
Thr34krew	Raymond Steigerwalt	USA	Oct-02	Jun-03	Jan-05	y	May-05	21	$12,000
WebTV-911	David Jeansonne	USA	Jul-02	Feb-04	Feb-05	y	Mar-05	6	$27,000
AgoBot	Axel Gembe	Germany	Nov-03	May-04	Nov-06	y	Oct-08	0	$0
AgoBot	Jay Saad Eschoaufini	Morocco	Nov-03	Aug-04					
AgoBot	Lee Graham Walker	UK	Nov-03	Dec-07	Oct-08				

Table 1: Overview of malware cases.

Case	Perpetrator	National origin	When crime	When indict/ arrest	When trial	Plead guilty?	When sent.	Prison (months)	Fines & restit. ($)
Gobo	Simon Vallor	Wales	Dec-01	Feb-02	Dec-02	y	Jan-03	24	$0
BlasterB	Jeffery Lee Parson	USA	Aug-03	Aug-03	Aug-04	y	Jan-05	18	$498,622
Volkam	Anthony Scott Clark	USA	Jul-03	Dec-05	Dec-05	y	Jan-08	15	$30,800
Nessun	Jason Michael Downey	USA	Jun-04	May-07	Jun-07	y	Oct-07	12	$21,110
Sasser	Sven Jaschan	Germany	Apr-04	May-04	Jul-05	y	Jul-05	0	$0
JJ Ancheta	Jeanson James Ancheta	USA	Jun-04	Nov-05	Jan-06	y	May-06	60	$57,000
JJ Ancheta	BDH – Juvenile	USA	Jun-04	Nov-05		y	Feb-08	12	
SecConsultant	John Kenneth Schiefer	USA	Jan-06		Nov-07	y	Mar-09	48	$22
Zotob	Farid Essebar	Morocco	Jul-05	Aug-05	Aug-05		Sep-06	24	
Zotob	Achial Bahoul	Morocco	Jul-05	Aug-05	Aug-05		Sep-06	12	
Zotob	Atilla Ekici	Turkey	Jul-05	Aug-05					
Donttrip	Chris Maxwell	USA	Jan-05	Nov-05	May-06	y	Aug-06	37	$252,000
Silenz	Gregory King	USA	Oct-04	Sep-07	Jun-08	y	Oct-08	24	$69,000
Brewer	James Brewer	USA	Oct-06	Jun-07	Apr-08	y	Sep-08	36	$270,000
Bots for hire	Adam Sweaney	USA	May-06	Jun-07	Sep-07	y	Feb-09	0	$0
Akill	Owen Thor Walker	New Zealand	Feb-06	May-07	Mar-08	y	May-08	0	$10,000
BigLevel	Christopher Kennedy	USA	Feb-09	Feb-10	May-10	y			
SpamKing	Robert Alan Soloway	USA	Jun-04	May-07	Oct-07	y	Jul-08	47	$773,000
Digerati	Ryan Brett Goldstein	USA	Feb-06	Nov-07	Mar-08	y	Aug-08	0	$36,000
Bentley	Robert Mathew Bentley	USA	Feb-06	Nov-07	Mar-08	y	Jun-08	4	$65,000
BofA Trojan	Aleksey Volynskiy, Alexander Bobnev	USA	Sep-06	Dec-08	Aug-09	y	Apr-10	37	$30,000
BofA Trojan	Alexey Mineev	USA	Jul-07	Nov-08	Jun-09	y	Nov-09	18	
Nugache	Jason Michael Milmont	USA	Mar-07	Jun-08	Jun-08	y	Apr-09	0	$36,859
Shadow	Leni de Abreu Neto	Brazil	May-08	Jul-08					

Table 1: Overview of malware cases (contd.).

Case	Perpetrator	National origin	When crime	When indict/ arrest	When trial	Plead guilty?	When sent.	Prison (months)	Fines & restit. ($)
Shadow	Nordin Nasiri	Netherlands	May-08	Jul-08					
Gonzalez	Stephen Watt	USA	Dec-05	Oct-08	Dec-09	y	Mar-10	24	$171,500,000 (shared)
DevilsArmy	Jesse William McGraw	USA	Apr-09	Jul-09	Feb-10	y			
Caverly	Rodney Reed Caverly	USA	Mar-09	Apr-10	Apr-10	y			
	Mitchell Frost	USA	Aug-06		May-10	y	Aug-10		
Alltaple	Artur Boiko	Estonia	Mar-07	Sep-08	Mar-10	N	Mar-10	31	$580,000

Table 1: Overview of malware cases (contd.).