Annual Report

2015/2016

CERT-UK

Working with partners across industry, government and academia to enhance the UK's cyber resilience

Contents

CERT-UK was formally launched on 31 March 2014 and is the UK National Computer Emergency Response Team. We work closely with industry, government and academia to enhance UK cyber resilience and are funded via the National Cyber Security Program (NCSP).

CERT-UK has four main responsibilities that flow from the UK's Cyber Security Strategy:

- National cyber-security incident management
- Support to critical national infrastructure companies to handle cyber security incidents
- Promoting cyber security situational awareness across industry, academia, and the public sector
- Providing the single international point of contact for co-ordination and collaboration between national CERTs

All data in this report applies to April 2015 – April 2016. Report ID: CUK-24-05-16-PD

Letter from the Director

Welcome to the second CERT-UK Annual Report which covers the period April 2015 to March 2016.

It has been a tremendously busy year with many highlights including a number of cyber exercises both nationally and internationally including Resilient Shield with US counterparts; we have launched 10 regional nodes on CiSP with the Regional Organised Crime Units; our international engagement continues across six continents; we have responded to in excess of 600 cyber incidents; and all this and more in addition to running and hosting our first annual conference late last year in Glasgow.

The Cyber-security Information Sharing Partnership (CiSP) has seen exponential growth in the last year with membership doubling to just shy of 5000 individual members and over 2000 organisations. The platform serves as an excellent device for HMG and its partners to provide advice and guidance in a dynamic environment where it simply would not otherwise be able to do so. However, the real success lies in its members and their commitment to sharing information and responding to others so a personal thank you to you all for making it the platform it is today.

As with our first Annual Report, we provide a rundown of the cyber incidents that have been reported to us this financial year as well as the malware that we have seen in the UK. We also review last year's predictions and look ahead to what we think organisations can expect to see in 2016/17.

Our Amber Annexe published on CiSP also looks back on the year's reporting including a review of how many C2 hosts we identified in the UK and how that compares to global numbers. We also provide analysis of two recent topics affecting a number of organisations: a look at the activities of the NetTraveler group, which we assess to have been responsible for attacks on the UK financial sector, as well as technical analysis of QBOT and its targeting of the health sector.

As we enter our third year of operation and as we transition into the National Cyber Security Centre (NCSC) there is too much to mention here, but as we begin work under a new moniker please remember that we are here to help make the UK more cyber-resilient and if there is anything you need, our door will always be open.

Chris Gibson
Director CERT-UK

Cyber incidents

In what has been another significant year for cyber incidents, and with growing media attention putting business' response to attacks under the spotlight, we have presented here a breakdown of incidents we have dealt with as the national CERT. Here, we present incidents broken down using the STIX incident categories, across the five most prolific sectors by amount of incidents reported to us.

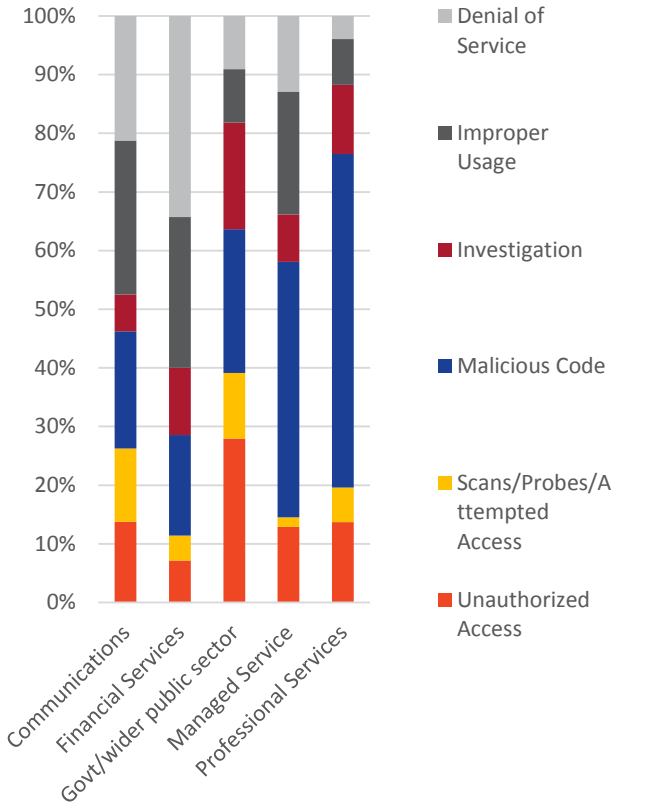


Figure 1- Incident types by top reporting sectors

Distributed denial of service (DDoS) attacks continue to increase with the financial sector again showing DDoS to be their most significant incident by percentage. DDoS has broken records during this reporting period with reported attacks reaching speeds of up to 602 Gbps. Increasingly, we see instances of DDoS used as an extortion technique, as well as more traditional blended attacks and DDoS as distraction. One of the most high profile incidents of the year, the TalkTalk data breach of unencrypted customer data, involved the DDoS as a distraction tactic.

Malware has remained at the heart of incidents affecting every sector, making up 30% of incidents reported to CERT-UK, and with the vast majority of these incidents allowing unauthorised access to a network or information held on it. **Malware remains the greatest threat to cyber-security in the UK.** Your company will receive phishing emails containing malware that could potentially lead to significant losses both financially and reputationally. You also have employees that will open those phishing emails – you may be that person. With a third of incidents occurring in this way, ask yourself what you are doing to mitigate against it.

Towards the end of this year we have seen an increase in the reported number of incidents involving ransomware, and expect this trend to continue into the next year as criminal groups increasingly see the monetary benefits and as the ever-growing **'cybercrime-as-a-service'** model makes these tools more accessible. CERT-UK's advice has been clear – do not pay ransoms. Create offline backups frequently for essential data so that if your data is ransomed you will be able to recover crucial information that might have been affected. While we recognise that the cost/benefit of paying the ransom can be a finely balanced judgement, particularly if your organisation does not have recent backups, if you pay these ransoms there is no guarantee you get your data back and the integrity of any ransomed data would be highly

If you receive a ransom attack, are the appropriate systems in place to avoid paying the ransom?

questionable. CiSP has seen much discussion in the last year about steps to take if your systems are ransomed.

We often get asked "which sector is the most targeted?" Companies understandably want to assess their risk based on metrics that apply to what they do and what they have. Certainly, there are a huge number of attacks across the finance

sector – simply put, criminals want money. But ask yourself what a criminal could do if they could access your email account? Can you authorise a payment or access sensitive information? **We are all at risk of cyber-attack**.

In the future cyber insurance policies may help to improve our security and protect assets; it will almost certainly affect how an organisation responds to a breach. But we are still far from seeing cyber insurance in parity with fire or buildings insurance – in our previous quarterly we wrote about the role insurance will have to play in security. For now however, and to answer the question, the fundamental issue is not about your sector, or the country you operate in, or even what your business does – **it is about taking the basic steps necessary and getting people thinking about cyber-security**.

By actively participating in CiSP your company can stay informed of the latest threats. Only in a community of sharing the right information at the right time, educating staff, running cyber exercises and employing services for the protection of your systems can we hope to drive down the amount of incidents reported to us. Learn about signing up here: www.cert.gov.uk/cisp/.

Phishing is the number one root cause of incidents this year

Crucially, the majority of cyber-attacks in the UK could have been prevented by taking simple steps; following the 10 Steps to Cyber-Security, attaining accreditation with the Cyber Essentials scheme and taking other preventative measures such as patching regularly and educating staff to the dangers.

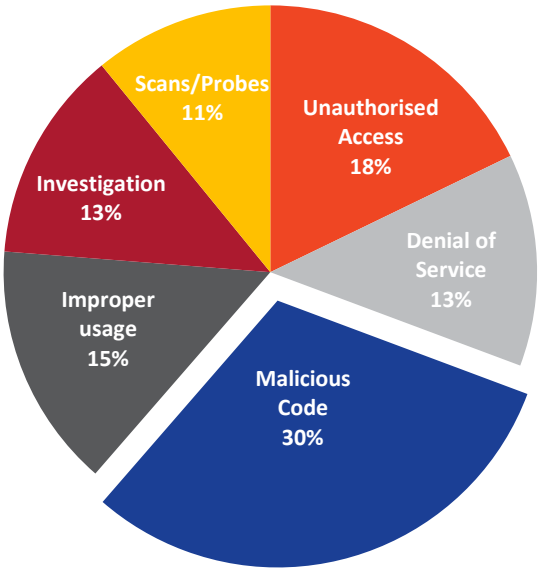


Figure 2 – Proportions of incidents reported to CERT-UK 2015/16

Malware in the UK

Accounting for roughly a third of all the incidents we observe, malware is at the heart of problems facing the businesses globally. The outlook is not good either – our malware data has once again put the same malware families in our top five list, some of which are almost a decade old and can easily be patched.

The underlying issue appears to be that too many networks are using old systems and not installing the necessary updates to counter this problem. Over the course of the last year we actually observed a small but gradual decline in the top five and this may be simply because, as time moves on, old laptops and equipment do get replaced, and suddenly the machine in your office that has stood infected for years is now offline and replaced with a clean and safer terminal (for now).

Conficker, the most prevalent malware this year, continues to remain highly active throughout the UK and could provide an indicator of the amount of machines that remain unpatched or not updated throughout the country. A patch has been available since 2008 yet we observed almost two and a half

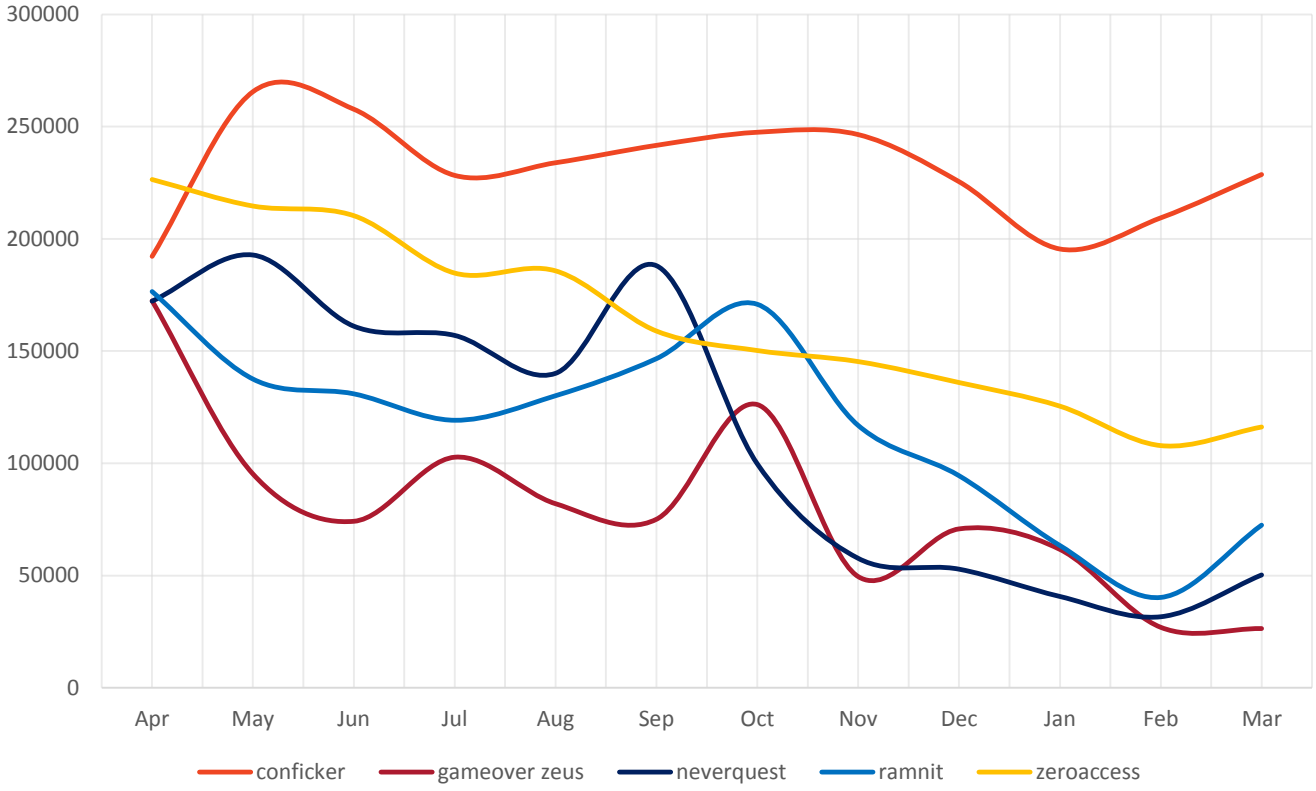


Figure 3 -Top five malware in the UK

million unique IPs active this year in the UK and infected with the bug. Microsoft provided a free tool many years ago to anyone who wanted to remove the bug and patch their systems and this is just one of hundreds of malware families we have observed this year.

Do not underestimate this problem. Some variants of Conficker, and many more additional malware types, allow criminal groups to form botnets, which are huge networks of infected machines that can be used for launching attacks, such as denial of service. So while your company may not be the victim of an attack, you may be unwittingly allowing attacks to happen, and with a cost of some £27 billion a year as a result of cyber-crime, we all need to play our part.

We know that some of the most serious malware does not lie in our top 10. Two significant malwares, Dridex and Dyre, have been plaguing the finance sector for a time now, and while observed instances were relatively low in our data, we assessed their impact to be much wider and significant.

Thankfully this year law enforcement acted to combat their infrastructure, and from November, as the graph shows, the Dyre malware volumes have dropped to nearly zero observed instances. Similarly, the banking Trojan Dridex was targeted in October. While the graph shows the significant decrease in Dridex, we have since seen a resurgence, indicated in the uptick towards the end of the year. Infrastructure associated with the Dridex malware is now being seen delivering the ransomware Locky.

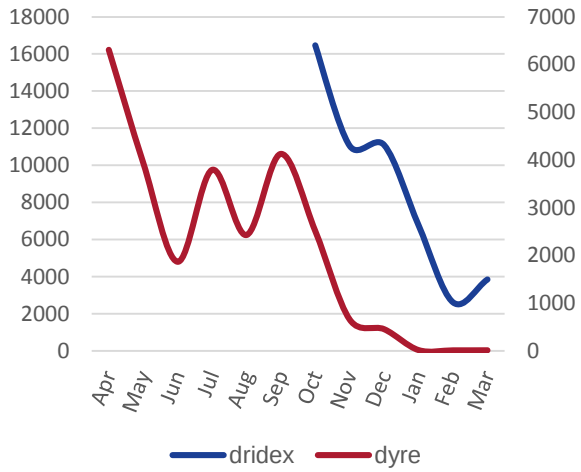


Figure 4 – Dridex and Dyre infections by month

Figure 5 lists the ten most observed malware variants in the last year. It shows the amount of unique IP addresses that have attempted communication with the sinkhole domain.

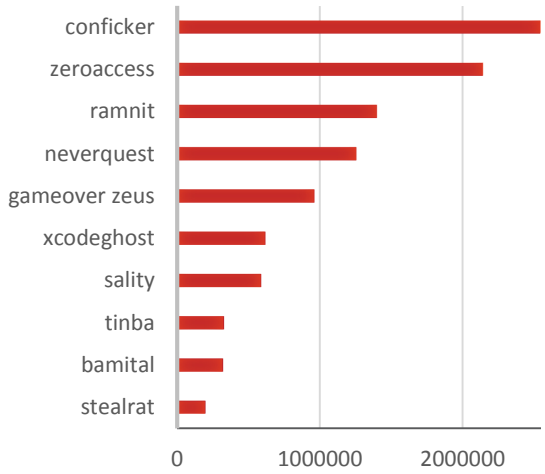


Figure 5 - Top 10 malware families observed by unique IP address observations

> With a cost of some £27 billion a year as a result of cyber-crime, everyone needs to play their part

The new wave – mobile malware

Xcodeghost hit the news in September 2015 after it was discovered in a number of apps from Apple's app store. These apps contained malicious code that made iPhones and iPads part of a botnet that stole potentially sensitive user information. Our data showed a huge spike in the latter half of 2015 which placed the malware straight into the top ten for the whole year. The shear amount of observed instances is testament to the ubiquity of mobile devices around the world and, while traditionally Android devices have been the most targeted, this shows that iOS is far from immune.

Our data also showed a significant drop off as Apple worked with developers to patch their software and rollout updates. This level of developer and customer cooperation will be more important than ever to ensure that newly discovered vulnerabilities are not exploited with malware that could rise to the levels seen in the top five.

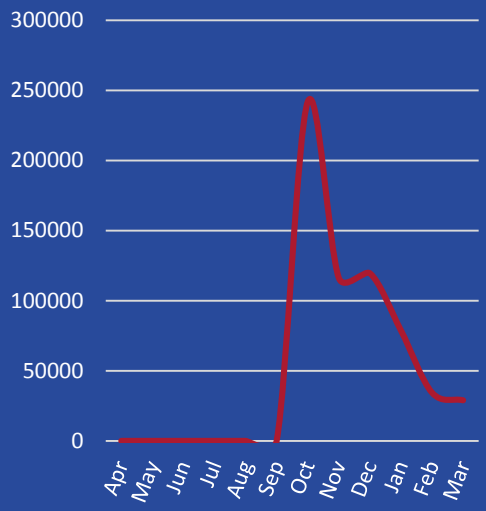


Figure 6 – Xcodeghost observations

This year, we have taken a closer look at the command and control (C2) servers, which are used to actually spread malware globally. With C2 servers observed hosted in 110 countries, over the course of the financial year CERT-UK made over 4 million C2 observations, running to over 60,000 unique IP addresses. The chart on the next page is a snapshot of the analysis we've conducted for the CiSP Members' Annexe which goes into more detail on the global distribution of this infrastructure over time. To read the full article, head to the CiSP platform.

4,649,777 C2 Observations **- 61,383** Unique C2 IP Addresses **- 17,913** Unique C2 Domains

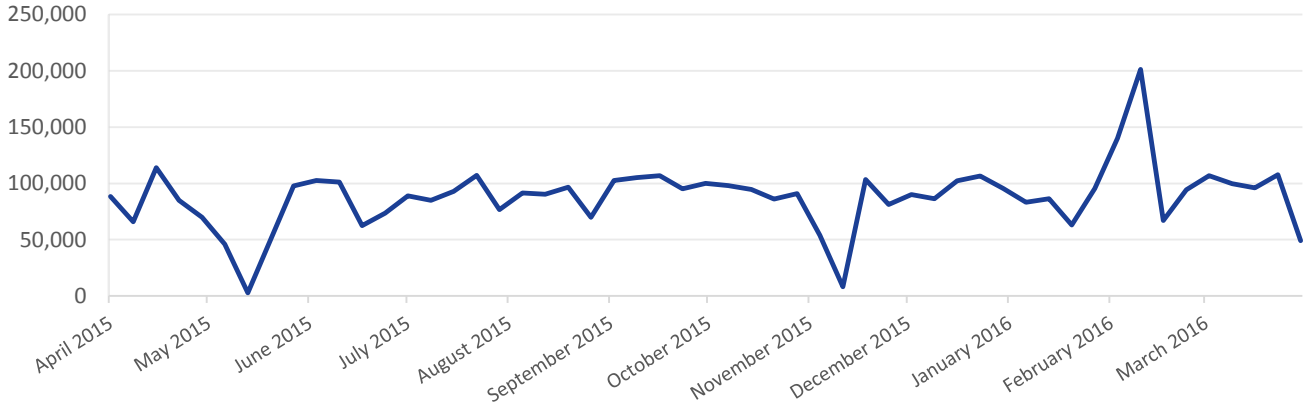


Figure 7 – Global malware C2 server observations over time

Generally, the top malware families we observe exploit vulnerabilities in older software or they sit on machines that just do not get cleaned. We have produced reports and guidance on the malware types affecting the UK, and you can find them on CiSP. However, if you take away only one point from this article, remember: educate your staff, update your software, patch regularly, and repeat.

We can all reduce the amount of infections occurring in the UK. Stop your workforce from initially infecting your networks by training them, talking regularly about the dangers of phishing and putting security at the heart of your business.

Accept however, that infections will happen. We are all human, and we can all fall victim to phishing. So accept that infections are likely but, perhaps most importantly, allow your security teams the resources and time to clean, update and patch your systems. If this requires taking systems down temporarily, then allow that to happen and build it into your schedule. If you are running software that is so old that security updates are no longer issued, replace your hardware. We do accept however that, in some cases, this advice simply is not possible, and so it is essential that your security professionals have a voice and are able communicate risk effectively.

Repeat these actions often. Upgrading computers can be expensive, but costs less than recovering from huge data loss, a denial of service attack, or even fraud.

Incidents on CiSP

We do not just report on the incidents we see as the national CERT, we reflect on the incidents that security professionals are experiencing and talking about on CiSP. Over the last 12 months, CiSP members issued reports, alerting the community to potential threats, contributing to a more robust security environment for all members. We are always looking to improve CiSP, and in the coming months we will be changing the way in which incidents are reported and absorbed by the community. More will come soon but for now, here is a reflection of what has been happening on CiSP in the last year.

Incidents reported – up 85%

Steady increase in incident reporting reflects not only the growth in membership, but also increased interaction with the platform. High profile cyber-attacks and media attention tend to result in a spike in incident reporting, as users are on high alert for any potential threats and seek community contribution. This was particularly evident in October and November of 2015 which saw an increase in incident reporting following the TalkTalk breach on October 21 2015.

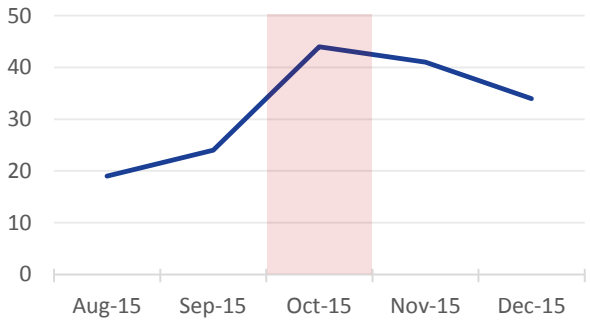


Figure 8 – Incident reports on CiSP by Month

Phishing was the most commonly discussed issue on CiSP

CERT-UK incident data has revealed that phishing emails were the number one root cause of incidents this year, therefore it is unsurprising to see phishing as the most talked about incident on CiSP, accounting for 48% of all reports. Phishing is relatively easy to identify compared with other malicious activity which perhaps contributed to the high levels of reporting. Exploit kits (12%) were the next most common incident reported, followed by DDoS (10%).

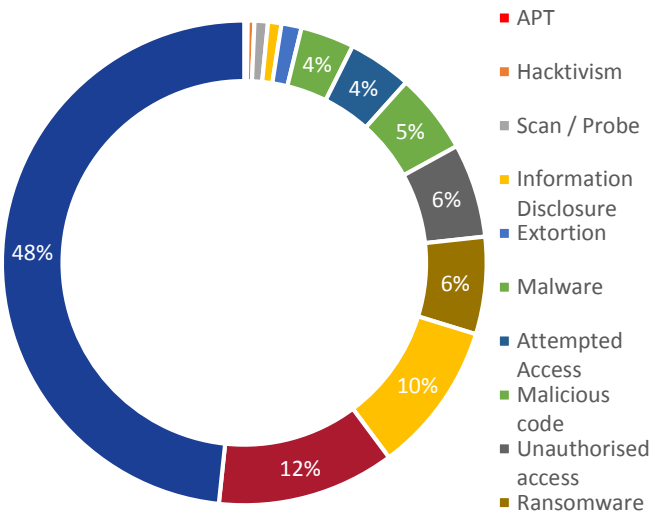


Figure 9 – Incident reports on CiSP by Type

Phishing accounts for 48% of all incidents reported on CiSP

Sharing the tactics, techniques and procedures (TTPs) and identifiers of an attack not only alerts the wider community to the threat, but may also prompt advice and mitigation used by other members of the industry. Ransomware has seen a consistently high reporting level when compared to the number of incidents seen in CERT-UK incident data. This is driven by the fact that ransomware is not only distinctly identifiable but also an emerging threat, stimulating increased reporting, contributions and discussions from members.

There has also been a considerable increase in the number of incidents reported relating to exploit kits, specifically in the finance sector. This is reflective of the high levels of reporting and engagement in the finance community on CiSP and an example of best practise on how to use the platform.

Indeed, the finance community remains the most active in reporting incidents on CiSP, accounting for 38% of all reports with defence, government and information technology the next highest reporting sectors. It is reflective of the wider community that the finance sector is a leading contributor in the community, though we increasingly see others getting better at reporting and discussing cyber incidents to the benefit of all members.

The finance sector accounted for **38%** of all CiSP reported incidents

Diverse incident reporting indicates an engaged sector

Most sectors are comfortable reporting malicious activity such as phishing, but for many this is the only incident they report. Finance, Defence, Information Technology, Academia and Communications are the most developed, reporting a wide variety of incidents which indicates higher levels of comfort and confidence in sharing information with the community in these sectors.

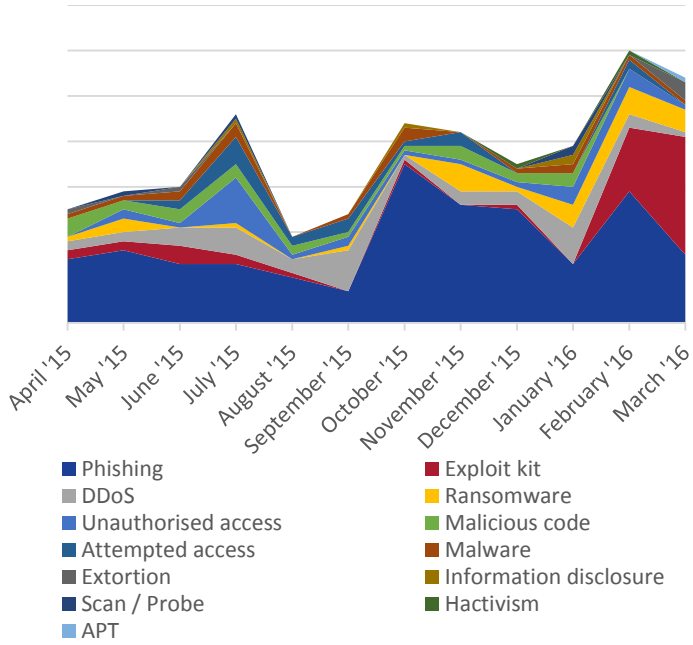
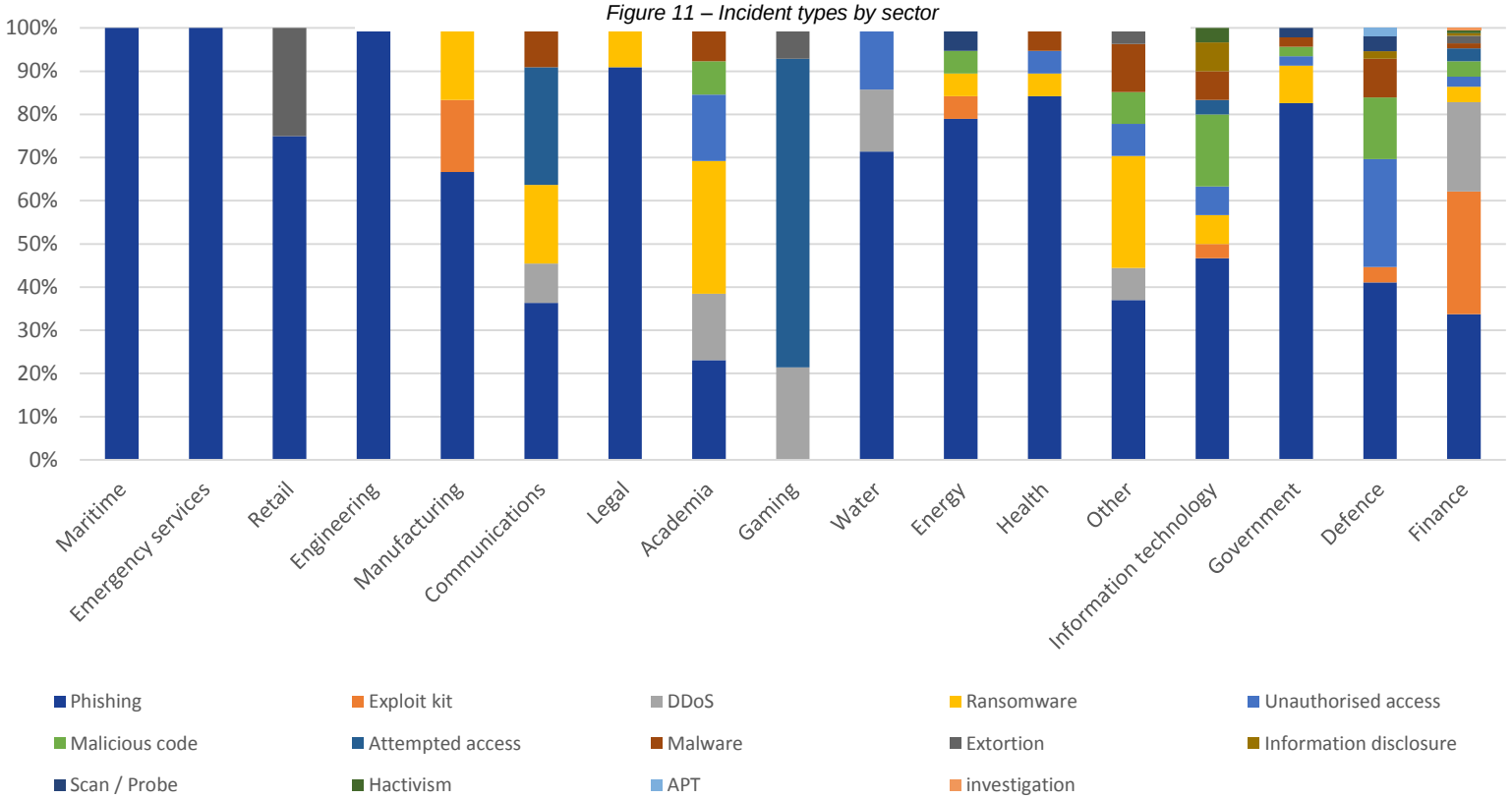


Figure 10 – Incidents by type over time

Incident sharing is a valuable function of CiSP and as such CERT-UK will be conducting a review of the incident reporting process on the platform. A more sophisticated and intuitive reporting process will be implemented in order to facilitate the threat analysis and encourage community knowledge exchange, but the fact remains that the community needs to articulate better the incidents they are experiencing, so that all can respond to the threats.

Figure 11 – Incident types by sector



Last year's six predictions – were we right?

In our previous annual report we wrote about six predictions for the year ahead. As important as it is to look forward (this year we have streamlined to five), we have taken a retrospective look at our predictions. With hindsight, we feel we identified strong themes in the development of cyber-criminal intent, the impact that vulnerabilities can have and the capabilities of both the criminal and the consumer. We hoped that businesses would identify with our predictions and they are provided here not as an exact snapshot of what we expected to happen, but as a series of things your business needs to think about over the last year, and what you need to be thinking about looking ahead. First a look back at last year:

The supply chain will be hit hard

We said that criminal groups would increasingly target the supply chain in 2015. There is evidence of breaches relating to third parties increasing over the last year, with suggestions that the proportion of breaches involving third party vendors has tripled.[1]

> The proportion of breaches involving third party vendors has tripled

A string of significant malvertising attacks occurred against the BBC and Gumtree, whereby websites were attacked by criminals using compromised credentials of legitimate businesses.[2] These attacks were successful as they exploited weaknesses in the global online advertising supply system.

CERT-UK has seen several supply chain incidents in which trust was the exploited factor in a business relationship and this has highlighted the importance of business communications and authentication methods.

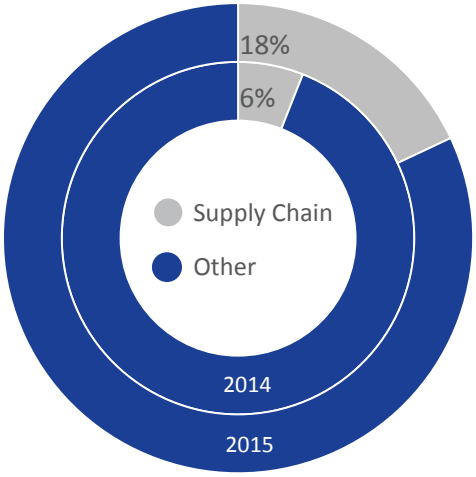


Figure 12 - % of Attacks targeting supply chain 2014

Mobile devices will be a single point of failure for business and consumers

Kaspersky recently reported that the volume of new mobile malware tripled in 2015. Furthermore, a Nokia report stated that approximately 0.3% of smartphones now exhibited signs of malware infection.

The ubiquity of mobile devices ensures that mobile based malware has the potential to be highly disruptive, though the extent of this threat is yet to materialise. As mobile devices present an increasingly attractive target, in the next twelve months, we expect to see another significant

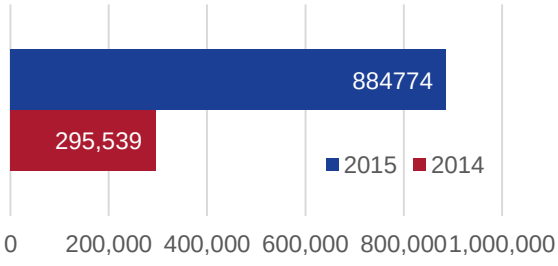


Figure 83 – Volume of mobile malware detected 2014 vs 2015

[1] https://www.beazley.com/news/news/beazley_breach_insights_2016_shows_sharp_increase_in_hacking_and_malware.html

[2] http://www.theregister.co.uk/2016/03/30/angler_malvertising_livejournal

increase in mobile-based malware, particularly mobile ransomware.

We will see another Shellshock or Heartbleed

DROWN was perhaps the most significant vulnerability of the last 12 months, potentially affecting 33% of servers by exploiting ageing elements of the internet infrastructure.[3]

Thankfully, DROWN was ultimately less damaging than Shellshock or Heartbleed largely due to mitigations put in place as a result of the swathe of vulnerabilities exposed in 2014. In 2015 only 1% of incidents reported to CERT-UK were the result of exploitation of new vulnerabilities.

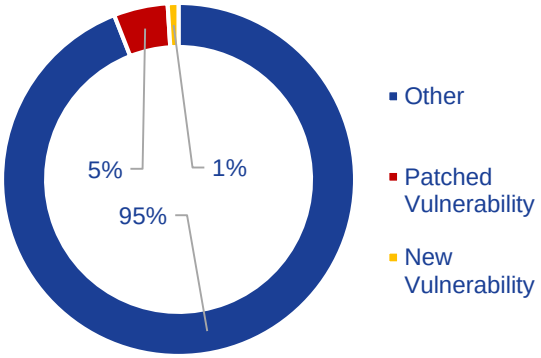


Figure 14 - % of incidents by vulnerability type

It may actually be the case that we never see an incident on the scale of Heartbleed again. Certainly, we will see vulnerabilities affecting vast numbers of computers, but the rollout of, and improved access to, patching and updates could lessen any widespread impact.

We will see the largest data breach ever

"The quantity of data stolen, or compromised, in a single operation would be the largest ever seen". What we actually saw was more breaches than any previous year, demonstrating that the frequency if not scale of breaches has increased. That said, 2015 saw three of the top twenty breaches 'of all time' and, of particular note, was the largest ever data breach suffered by US banks.[4]

We expect to see further large scale data breaches as it becomes an increasingly lucrative enterprise for criminals. But whether large or small, in data size, or quantity of records, the cost of data breaches can sometimes be immeasurable. Stolen information and pictures of children from the toy company VTech are strong examples of how data breach need not reveal financial information in order to seriously undermine consumer trust.

The cyber-criminal marketplace will become more accessible

The use of macro-based delivery for malware such as Dridex has spiked and a campaign can be easily purchased from established sellers such as Xbagging and MacroExp with prices ranging from $1 to $1000.[5] Cyber-crime-as-a-service has also increased with organisations such as the Lizard Squad offering DDoS-as-a-service for as little as $6 per month.[6] These services can allow the technically inexperienced to have an impact on even a large corporation, as was demonstrated in August 2015, when six UK teenagers were arrested for using the Lizard Stressor tool to launch DDoS attacks against Microsoft, Amazon and Sony.[7]

> Three of the top 20 incidents of all time were in 2015

Consumers will demand better security

As cyber-crime has grown, so too has the consumer's awareness of security. Customers of TalkTalk learned in the wake of the hack that their personal information had not been encrypted. This

[3] http://newdaypost.com/drown-vulnerability-hits-ssltls-no-heartbleed-0194339
[4] http://www.cnbc.com/2015/11/10/three-indicted-in-us-over-major-hacking-scheme.html
[5] http://www.itsecurityguru.org/2015/06/10/cybercrime-economics-of-malicious-macros/
[6] http://betanews.com/2015/12/28/2016-will-see-the-rise-of-ddos-as-a-service/
[7] http://www.networkworld.com/article/2977608/microsoft-subnet/6-uk-teenagers-arrested-for-allegedly-using-lizard-squads-lizard-stresser-ddos-service.html

brought to an otherwise unknowing community much media explanation of why their data should have been encrypted and of what they should actually expect from a large organisation that holds their details.

New smartphones and PCs have gone on sale this year with some increasing the default minimum password characters from four to six, the use of biometric data and even facial recognition software. The messaging app WhatsApp has now rolled out encryption of all messages, telling customers even their own company cannot read their customers' messages.

In this technology-driven age, consumers do expect not just better security of their products, but of the companies that hold their data – and you can expect them to complain if they don't get it.

Predictions for 2016/2017

Ransomware will dominate 2016

2016 has already seen an explosive growth of incidents of ransomware with TrendMicro reporting more ransomware infections in February 2016 than in the entire first half of 2015[8]. The true cost of ransomware is difficult to estimate as most demands are issued in bitcoin and anonymity is in the interest of both parties. With nearly one in every ten[9] ransomware infected emails targeting the UK, the impact on UK businesses should not be under estimated.

In 2016 we will almost certainly see ransomware diversify. Attackers will seek to exploit alternative platforms from Windows to Linux and Mac OS X – indeed Ransom32[10] has the capability to affect all three. Ransomware will move beyond computers and begin to successfully target mobile devices – early attempts of this have already been seen with the likes of SimpleLocker.

Arguably the most threatening development is the emergence of ransomware that can move through a network and even attack components and unmapped network shares, potentially crippling organisations.

The success of ransomware is driven by its victims

The success of ransomware is driven by its victims. Cyber-criminals use the profits of their extortion to improve the quality of their tools and this has led to the emergence of increasingly sophisticated variants such as TeslaCrypt, which is constantly evolving to avoid detection. The threat will continue to grow unless victims avoid paying ransoms, report incidents, and follow HMG guidance.

We will see more attacks on critical national infrastructure

Cyber-attacks on critical national infrastructure are increasingly part of the narrative of conflict and require levels of sophistication which, to date, have been the prerogative of advanced threat actors. In the last six months, high profile attacks in Ukraine and even Israel have reminded the world of the potentially devastating impact that could be achieved.

In 2016 we anticipate an escalation in the number of attacks on the country's critical national infrastructure, which will target their ICS (industrial control systems). The number of publicly disclosed

[8] http://www.trendmicro.co.uk/newsroom/pr/trend-micro-more-uk-enterprise-ransomware-infections-in-february-than-q1-and-q2-combined/

[9] http://www.techweekeurope.co.uk/security/cyberwar/bitdefender-britain-major-ransomware-target-182712#ELz7xruApfh5y0uQ.99

[10] https://securityintelligence.com/news/cross-platform-cryptoware-is-here/

vulnerabilities and off-the-shelf exploits targeting these systems has increased[11], making them potentially vulnerable to even relatively unsophisticated attacks. In particular, attacks are highly likely to focus on SCADA (Supervisory Control and Data Acquisition) systems, a subset of automated ICS, often connected to the internet with the aim of gathering real time data, but leaving them vulnerable to threat actors[12].

It is not just ICS/SCADA systems that are at risk. In the supply chain of CNI organisations it is not uncommon to see security and permissions shared, and an attacker use such organisations as a way to 'jump' onto the network of a better-protected CNI organisation. Remember, the smaller organisations with the weakest cyber-security may provide an entry route for advanced persistent threats (APTs).

Phishing campaigns will infect your corporate networks

Global and national events will create opportunities to mislead huge numbers of the public with more convincing domain names and phishing emails.

The growth of generic top level domains (gTLD) to include generic and household words (such as .coupon, .makeup, .health) means internet users are less likely to view a peculiar TLD with any alarm. Increasingly varied TLDs present new social engineering opportunities for cyber-criminals to give their malicious sites and emails the appearance of legitimate correspondence.

A malicious spam campaign could direct users towards addresses such as 'election.campaign' or 'rio.tickets' from which they can launch an attack. In the last year, Spamhaus listed the TLDs

hosting the highest percentage of SPAM domains, including innocuous examples such as .cricket[13] which spiked in line with the 20:20 Cricket World Cup. Unsuspecting cricket enthusiasts were lured onto sites which were loaded with malware. An updated version of the list can be found on the Spamhaus website.

With domain names adding an extra tool to the cybercriminal tool belt, we can expect to see an increased success rate in phishing campaigns globally. Companies will need to renew efforts in both training, particularly in awareness of phishing, as well as invest in more sophisticated defences.

We will see the biggest DDoS attack ever

2015 saw considerable growth in DDoS attacks, with an 85% increase in Q3 2015/2016[14], and attacks as large as 500 Gbps[15] observed. The 'Armada Collective' group even recently claimed that their DDoS attacks can be as powerful as one Terabit per second. Attacks are also growing in frequency, for example, DDoS attacks are increasingly commonplace, with Q4 2015 seeing a 148% increase reported on the same quarter in 2014.[16]

It is highly likely that DDoS attacks will continue to increase in both power and frequency. This is driven by the increase in automation, bandwidth and internet speeds as well as the emergence of DDoS-as-a-service, and the speed of botnets hosted on home computers[17].

The low cost and high impact that DDoS attacks bring make them increasingly an effective smoke screen for other malicious activities, such as the successful attack on TalkTalk, and the more high

[11] https://www.recordedfuture.com/ics-scada-report/
[12] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf (p.42)
[13] https://www.spamhaus.org/statistics/tlds/
[14] http://www.itproportal.com/2016/03/14/ddos-attacks-saw-85-increase-q4-2015/#ixzz42zK8xKKH
[15] Networks.https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf
[16] https://www.stateoftheinternet.com/downloads/pdfs/2015-Q4-cloud-security-report.pdf
[17] http://www.infosecurity-magazine.com/opinions/exponential-growth-of-ddos-attacks/

profile attacks such as these that are reported, the more criminal groups are learning.

Businesses will ask for cyber insurance

Transference of loss through insurance is one of the fundamental techniques of risk management. When it comes to cyber risk, however, the ability to insure has been hampered by a market which is still finding its feet. We expect cyber insurance to become a talking point for many businesses in 2016, who should make sure to understand the products and policies available and how they might be suitable for managing cyber risk.

There are a number of drivers behind this; firstly to take a cynical but pertinent viewpoint, insurance companies see huge potential to make money in the market and will make it more accessible to businesses with a larger and more tailored range of products for businesses of different sizes and industry.

Second, insurance companies are pushing to better quantify cyber risks. They have struggled to understand the risk and impact of cyber-attacks or information loss as they lacked the data on actual losses required to perform actuarial analysis. As more players move into the cyber insurance market, however, the pool of available data will grow and methods of analysis will improve. We expect that significant progress will be made in 2016 and insurers will get a much better grasp of cyber risk. The maturity of the market will increase[18] and insurers will become much keener to offer tailored cyber insurance products. Another implication of this is that there is likely to be a shakeup in the premiums charged by insurers for cyber risk coverage – particularly for larger, higher risk companies[19].

Finally awareness of cyber risk will continue to increase. We expect the trend of high-profile cyber-attacks and data breaches to continue and companies will not lose their appetite to protect themselves from potential loss.

With these in mind, we predict that the cyber insurance market will almost certainly look very different 12 months from now, and organisations which are considering taking out a policy should understand the available market and products to find one that is a good fit.

[18] http://www.darkreading.com/analytics/insurers-getting-smarter-about-assessing-cyber-insurance-policy-risks/d/d-id/1324048

[19] http://www.ajg.com/media/1698440/2016-market-conditions_cyber.pdf

The importance of automated sharing

Good network security requires a blended approach of prevention, detection and response; threat intelligence enables all of those activities. The 'operationalisation' (the acquisition, processing and deployment) of threat intelligence within an enterprise should be seen as an ongoing process and a way of working, rather than simply a service that is purchased. External feeds and products need to be combined with an organisation's strategic view of risk and technical data from its own network sensors, with that analysis and knowledge then being deployed quickly and efficiently to inform business decisions and improve network security.

> HMG does not have the monopoly on good cyber threat intelligence – if organisations do not share, these systems will never truly be effective

Threat intelligence operates at different levels, as identified by MWR and the Centre for Protection of National Infrastructure in their 2015 report[20]:

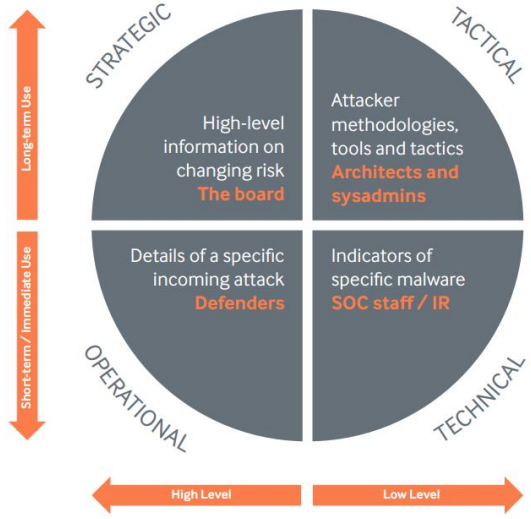


Figure 15 – Threat Intelligence Model

Looking at cyber threat intelligence across all of these levels is important because it emphasises that 'cyber' is actually just a vector through which business risk can manifest. Organisations need to be constantly evaluating their security posture in light of their business activity, and actively monitoring and defending their information systems, to prevent this manifestation[21].

Threat intelligence can be structured, unstructured or somewhere in between. Each has value. Pdf reports which are unstructured but present a compelling narrative and engaging graphics can deliver impact at board level and raise senior awareness of a threat, which helps drive investment decisions. Whereas structured data feeds characterising the indicators of an attack or the tactics, techniques and procedures (TTPs) employed by the perpetrator in a machine readable format make it far easier for analysts and network defenders to automate the processing, correlation and deployment of network signatures with as minimal human interaction required.

What is important is that information is:

- Produced in view of the intended recipient and what they are likely to want to do with the information, and/or what the producer of the information wants them to do
- Disseminated in a timely way – that might mean within weeks for strategic threat intelligence, or near real time for technical indicators
- Is designed to be as easy to consume as possible to reduce the receiving organisation's cost and enables better decisions to be made quickly
- Is shared with all of those who might reasonably need access to the information; trust remains a fundamental challenge of any meaningful threat intelligence sharing process

[20]https://www.cpni.gov.uk/Documents/Publications/2015/23-March-2015-MWR_Threat_Intelligence_whitepaper-2015.pdf

[21] The Finance Strategy and Coordination Group's Joint Working Group Initiative on Threat Intelligence published a paper on 'Cyber Intelligence in Practice' in late 2015. The paper provides a useful insight into threat intelligence at different levels, namely: board level; middle manager; network defender. It is available on CiSP.

CERT-UK's approach to threat intelligence

CERT-UK fully embraces the need to share threat intelligence and does so in three main ways:

- **CiSP** as a platform for sharing within established trust groups unstructured and semi-structured information relating to threats at a strategic all the way down to technical level

- **Through CERT-UK Network Reporting (CNR) reports**, which provide technical intelligence designed to inform network owners of suspicious events or vulnerable services affecting their infrastructure

- **To and from CERT-UK's public threat information sharing server**, currently focussed on technical and tactical intelligence but with an aspiration to share more operational threat intelligence in time; this is a Trusted Automated Exchange of Indicator Information (TAXII) node, through which CERT-UK consumes Structured Threat Information eXpression (STIX) files from its partners, and also publishes its own threat intelligence for others to consume

It is important to note that CiSP and CERT-UK's TAXII server are designed to facilitate bi- or multi-directional sharing of information. CERT-UK does not consider itself, or UK government more broadly, to have the monopoly on good cyber threat intelligence. If organisations do not choose to share, whether directly with CERT-UK, with trusted industry peers, or more broadly then these systems will never be truly effective.

What are STIX and TAXII?

Extensive studies have been written around structured threat intelligence, and of the various tools and languages which can be used[22]. Fundamentally, the principle of all structured information sharing is to make it faster, more efficient and easier to consume. STIX is one such language for articulating threat intelligence in a structured way, and TAXII is a protocol by which it can be shared[23].

> CERT-UK has adopted STIX and TAXII because they are open source and free to implement for anyone

CERT-UK has adopted STIX and TAXII because they are open source and free to implement, with a number of tools already out there; and because a number of our international counterparts and increasingly other parts of the community have chosen to do the same. A large number of vendors are also actively looking at integrating STIX data structures into their products, which should make the operational deployment of the data easier.

Originally created by MITRE, the development of STIX and TAXII as standards was recently taken on by the Organization for the Advancement of Structured Information Standards (OASIS); it is now one of their most heavily subscribed technical committees, which further demonstrates the cross-community momentum that has built up around STIX and TAXII.

[22] See for example http://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligence-augment-35692 or https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport

[23] https://stixproject.github.io/

STIX

STIX structures information by recognising the importance of the relationships between objects, as shown in the simplified diagram below. These relationships provide context; for example, an IP address on its own is simply something which exists. Where that IP address is seen being used for command and control, by a known piece of malware in a campaign against an industry sector, that information becomes far more valuable. By structuring the data an analyst can exploit the data more easily by being able to 'pivot' on any particular component of it.

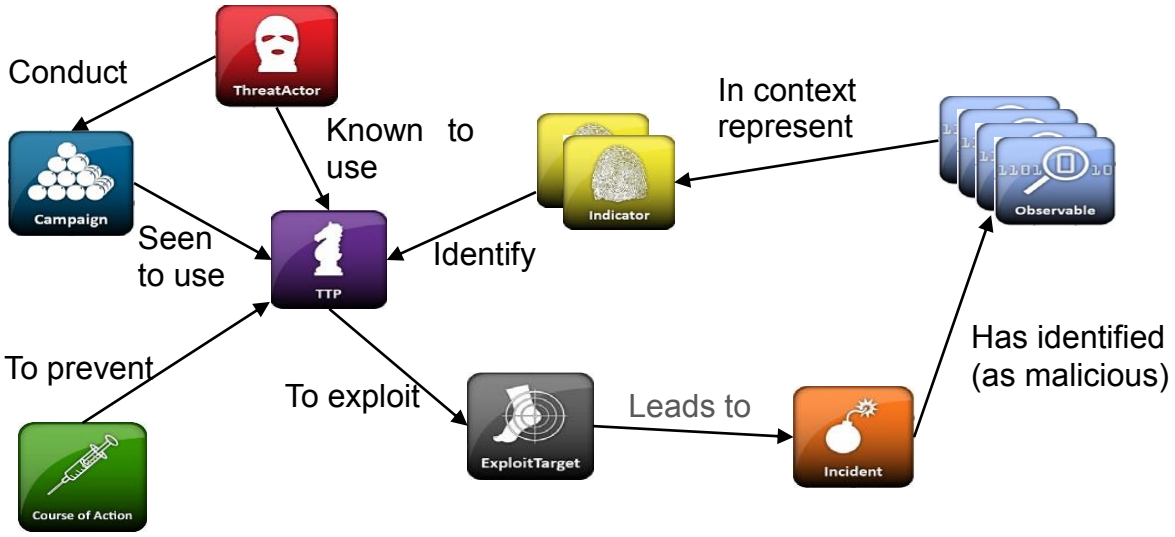
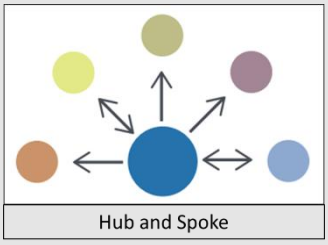
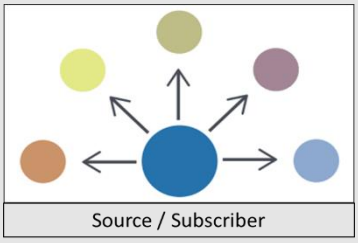


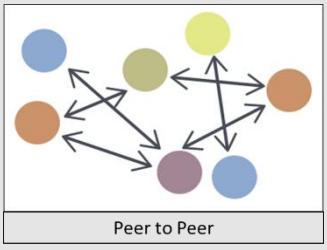
Figure 9- STIX topology

TAXII

TAXII is designed to allow high volume, secure and fast sharing of cyber threat intelligence across networks of clients and servers running TAXII. There are various different models, as with any sharing network:







CERT-UK favours a peer-to-peer model on the basis that TAXII works best when nodes are sharing with as many other nodes as possible, all of the time. CERT-UK shares data over its TAXII node using a combination of distribution groups and Traffic Light Protocol (TLP) handling conditions. Trust remains a crucial element of this approach, particularly given that in time more data will be shared faster, with less human interaction.

Organisations who are already looking at sharing threat intelligence using STIX and TAXII, have an interest in beginning to do so, or are already producing structured threat intelligence in a different format and want to discuss beginning to share with CERT-UK, should get in touch through your existing CERT-UK contact or via the website.

Our partners

www.cert.gov.uk

@CERT_UK

A CERT-UK PUBLICATION