ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 June 2020 www.computerfraudandsecurity.com

Featured in this issue:

The rise of telemedicine: how to mitigate potential fraud

Driven by the rapid growth in remote patient monitoring, virtual GP consultations and online prescription services, the telehealth market has enjoyed a significant boom.

However, this has created a lucrative opportunity for fraudsters. Over 1 billion patient health records can be easily accessed on the dark web and millions of additional records are being added daily. Medical records command a high value to bad actors. The future of telemedicine can only be assured if trust can be reliably established between the medical expert and the patient, says Philipp Pointer of Jumio.

Full story on page 6...

Removing a false sense of (open source) security

Software is at the heart of the 'digital transformation' as businesses rapidly transition from legacy-based models to digital business processes. And open source software (OSS) is a crucial part of this.

But there are many application security challenges that need to be understood and addressed. Security instrumentation technology gives developers current, real-time visibility into all open source components across their portfolio, so they know what needs to be secured, says Jeff Williams of Contrast Security.

Full story on page 8...

Cyber security and the remote workforce

Current world events have forced a sudden remote-working economy for which neither organisations nor their staff were prepared. This has impacted the cyber-risk profile of enterprises worldwide.

Organisations have built policies and procedures that protect individuals and the organisation's infrastructure. However, unless a significant percentage of employees had previous access to proper remote access technologies, there is a real risk of employees making bad choices. Organisations need to implement the correct tools to mitigate these threats, explains Kevin Curran of Ulster University.

Full story on page 11...

Ransomware operators now auctioning stolen data

The operators of the REvil (aka Sodinokibi) ransomware are using their dark web blog to sell to the highest bidder data stolen during attacks. This represents a new departure for ransomware operators and may even indicate a level of desperation.

While the REvil group (and others like it) are known for publishing partial sets of data as a incentive to get ransomware victims to pay up – and there is a thriving market for stolen data on cybercrime marketplaces – this is the first time that ransomware operators have threatened to

Continued on page 3...

Contents

Editorial Office: Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.computerfraudandsecurity.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Computer Fraud & Security includes 12 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/computer-fraud-and-security/1361-3723

12986
Digitally Produced by
Mayfield Press (Oxford) Ltd

Editorial

It has now been two years since the General Data Protection Regulation (GDPR) came into force, so it's reasonable to ask what kind of impact it has had. It certainly created a lot of activity among organisations scrambling to be compliant. But has it actually done any good?

Without question, the GDPR raised awareness about data privacy as an issue, both among organisations that collect and exploit such data and also within the population of people whose data it is. It's not that this was a new issue – the GDPR built upon an existing EU directive dating from 1995. But its more stringent requirements, backed up by the threat of potentially massive fines, changed data privacy from being a 'we really ought to do something about that' topic for IT departments to an urgent board-level priority.

Many organisations complained that revamping processes and implementing data-handling technologies and protocols imposed a heavy business burden. But if you're handling personal information in order to drive profits for your company, then maybe that's a burden you should expect. Besides which, the savvier organisations turned visible compliance with the GDPR into a business differentiator. The general public is becoming ever more concerned about how much personal information organisations are collecting. People are more likely to do business with a company that makes a point of treating their data with respect.

The GDPR is influencing other privacy legislation around the world. It has spurred a thriving market in data privacy tools. And there have been some headline-grabbing fines – such as the intention of the UK Information Commissioner's Office to fine Marriott International £99m and British Airways £183m for data breaches – although both companies are appealing.

However, at a fundamental level it's hard to say what has really changed. One of the notable characteristics of the GDPR is how it is not prescriptive. Aside from a few specific requirements – such as firms over a certain size needing to appoint someone to handle data privacy issues and deal with complaints – the regulation says a lot about how protective you need to be about data but not how you go about that from a practical perspective.

Experience with information security inclines one to suspect that most organisations will do the minimum – the classic 'tick box' approach. After all, there are no regular audits or spot checks. No-one is going to examine your data privacy efforts – unless, that is, you suffer an actual breach. At that point, you'll be in the position of having to prove that you took every reasonable step to prevent data falling into the wrong hands.

Again, we can draw parallels with other aspects of data security – in particular, the 'it will never happen to us' attitude that is sadly still too prevalent. In fact, it's even worse with the GDPR: even if an organisation is breached, it might feel confident that it can talk its way out of a fine because it believes its inadequate privacy protections were, in fact, up to the job. That's because of a lack of rigidly defined standards against which to compare processes and technologies.

The GDPR approach of punishing organisations that aren't sufficiently careful with data, while at the same time not bothering to spell out what adequate protection looks like, is a fundamental weakness. While the regulation has raised awareness of privacy issues to some degree, as with information security as a whole, what we really need is a privacy-first approach that is intrinsic to all relevant activities – from companies developing new business models and products, through software development to how organisations interact with the public. And the continuing stream of data breaches suggests we haven't got there yet.

– Steve Mansfield-Devine

...Continued from front page

sell on the information exfiltrated during attacks. The aim is probably to put extra pressure on victims who may fear that sensitive data could end up in the hands of rivals.

The first two batches of data have been offered for sale on the 'Happy Blog' – which has previously been used for posting samples of stolen data. The first is information including, according to the blog, "cash-flow analysis, distributor data, business insurance content, and vendor information" belonging to a US food distributor. There are more than 10,000 files that have a starting price of $100,000 and a 'blitz' (or buy it now) price of $200,000. The other is a group of more than 22,000 files, including three databases, apparently stolen from a Canadian agricultural company that, it appears, has refused to pay a ransom. The REvil group set a starting price of $50,000 and a blitz price of $100,000. Potential buyers must put up a deposit of 10% of the starting price in order to bid. The REvil group promises that this will be refunded if the buyer doesn't win the bid.

Other auctions are promised soon, with hints that data relating to Madonna and maybe Donald Trump – who were among the many people whose information was stolen by the gang in the 756GB haul of data from New York lawyers Grubman Shire Meiselas & Sack – will be among the items for sale.

There are suggestions, however, that all may not be well in the ransomware world. Since the Covid-19 pandemic started, there has been an explosion in pandemic-themed phishing, much of it carrying ransomware payloads. A significant amount of this has been directed at healthcare organisations, including hospitals, that are in a vulnerable condition.

At the same time, however, there are indications that victims – in all sectors of business – are less inclined to pay up. This might be because they are simply unable to do so, having already been severely hit by the pandemic-related economic downturn. It could also be the case that many firms have got the message about ransomware and are able to restore from back-ups. It's known that, in normal times, even firms with back-ups were paying ransoms as a 'belt and braces' approach to ensuring they could get up and running again quickly. In the current situation, that's less likely to occur. Of course, it's also possible that some ransomware victims have either gone out of business anyway or are about to, and recovering the data is the least of their worries.

The result is that ransomware groups are looking for ways of squeezing more revenue from successful attacks. Auctioning data is one approach; other groups are hitting victims twice – once by charging a fee to decrypt the data and a second time by demanding a further payment in return for permanently deleting the stolen data.

Meanwhile, it appears that some ransomware operators may be joining forces in what has been described as a 'cartel'. The Maze group was one of the first to start publishing stolen data belonging to victims who didn't pay the ransoms. Now they have begun publishing data obtained by LockBit, a ransomware-as-a-service operation. According to Bleeping Computer, which contacted the Maze group, it is also sharing resources, intelligence and experiences with LockBit and it is encouraging other ransomware groups to join. There's more information here: https://bit.ly/3eN3roB.

Finally, the DoppelPaymer group claimed to have breached the systems of Digital Management, an IT services company that counts NASA among its clients.

EasyJet suffers massive breach

The UK's largest airline, EasyJet, has suffered a breach in which attackers stole details of 9 million customers, including email addresses and full travel itineraries. Some 2,208 of the records included payment card information.

The company released some details to the London Stock Exchange, saying that it had been targeted by "a highly sophisticated source" – although that phrasing is used by pretty much every company that is breached these days. In the case of those customers who had payment card information compromised, the airline gave no indication of what was included – for example, whether CVV numbers were part of the haul.

There are some oddities about the timing of the intrusion and subsequent notifications by EasyJet. It's believed the attackers were in the airline's networks from October 2019 to January 2020. The company alerted customers about the incident in mid-May, yet those who had their payment card details compromised were told in early April. So it's unclear exactly when EasyJet discovered the breach.

However, the company did issue a statement saying: "As soon as we became aware of the attack, we took immediate steps to respond to and manage the incident and engaged leading forensic experts to investigate the issue. We also notified the National Cyber Security Centre and the ICO. We have closed off this unauthorised access."

So far, EasyJet has made no mention of offering compensation or free credit monitoring for affected customers – the latter being pretty standard these days after such breaches. Instead, it has put the onus on the customers themselves, warning them to watch out for phishing attacks, and, in particular, to be, "cautious of any communications purporting to come from EasyJet or EasyJet Holidays".

An £18bn class action lawsuit has been filed against the company by law firm PGMBM.

Like most airlines, EasyJet has been suffering badly from the Covid-19 pandemic. For several weeks it grounded all flights and has only just begun to resume some domestic routes. It is also in the middle of a major boardroom battle, with a failed attempt by founder Stelios Haji-Ioannou to oust its CEO and other key executives.

Meanwhile, in other breach news, US food delivery firm Home Chef has admitted that as many as eight million user records have been leaked. The breach came to light when hacking group Shiny Hunters offered the firm's database for sale on a dark website, with an asking price of $2,500. The stolen data includes users' emails, encrypted passwords, last four digits of their payment cards, gender, age, subscription information and more. Home Chef issued a statement two weeks after the data went on sale.

The same hacker group is also offering other stolen records for sale, including an estimated 40 million records for the popular mobile app Wishbone. In this case the data includes usernames, email addresses, mobile numbers, gender, date-of-birth, Facebook and Twitter access tokens and MD5-hashed passwords.

Report Analysis

Verizon: Data Breach Investigations Report 2020

The publication of Verizon's annual Data Breach Investigations Report (DBIR) has become something of a major event in the information security calendar. Its data is regarded as a kind of benchmark, with year-on-year figures being seen as a reliable indication of the changing (usually worsening) state of cyber security.

This is despite the fact that the data is partial. As the title suggests, the report covers only cyber incidents that have been reported and investigated. And they are high-value incidents – the type, for example, that might get the FBI involved. That said, the report does draw its information from a wide range of sources that are international in scope, including law enforcement and intelligence agencies as well as cyber security vendors.

For this year's report, the team analysed 32,002 incidents, of which 3,950 were confirmed as breaches. Of the breaches, 82% were contained within a matter of days, but more than half (52%) still resulted in the compromise of personal data. Nearly three-quarters (72%) of the breaches involved large organisations.

As is often the case with the DBIR, its figures swim against the stream somewhat in terms of not complying with current perceptions of cyber security threats. For example, there is much debate at the moment about the insider threat and you'd be forgiven for thinking that most of your security nightmares would go away if only you could stop those pesky employees from doing things they shouldn't. But according to the DBIR, 70% of breaches were perpetrated by external actors, with 55% being accounted for by organised criminal groups. Sure, that leaves 30% being committed internally, which is bad enough, but it's not quite the staff-driven cyber Armageddon you might imagine.

One conclusion you could draw from this report is that, by and large, attackers are not becoming that much more sophisticated. If we leave aside highly trained and well-resourced nation-state attackers for the moment, most (86%) of the incidents Verizon investigated were financially motivated – ie, plain old criminal activity – using the same methods we've become accustomed to over the years.

"Credential theft, social attacks (ie, phishing and business email compromise) and errors cause the majority of breaches (67% or more). These tactics prove effective for attackers, so they return to them time and again," says the report.

As Satnam Narang, staff research engineer at Tenable, explains: "While attack vectors may fluctuate over time, cyber criminals often set their sights on low-hanging fruit. Zero-days may garner most of the attention, but foundational cyber hygiene issues enable most breaches. The motivation for cyber criminals is primarily financial. As the Cyber security and Infrastructure Security Agency (CISA) recently underscored in a report about the top 10 routinely exploited vulnerabilities, cyber criminals focus their efforts on exploiting unpatched vulnerabilities. It's a cost-effective measure that provides the most bang for their buck, because they don't have to spend the capital needed to acquire zero-day vulnerabilities when there are so many unpatched systems to take advantage of. As the DBIR notes, even if a newly-discovered vulnerability wasn't patched in a network, those same systems would likely also be vulnerable to a plethora of other vulnerabilities, which signifies a lack of basic cyber hygiene."

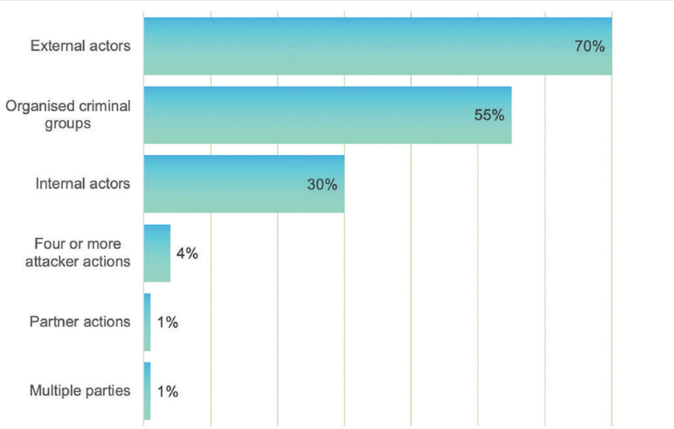
There are variations from year to year – for instance, ransomware is currently having its day in the sun. But perhaps one issue that isn't getting the attention it deserves is 'misconfiguration'. This could include bad firewall rules, a poorly maintained Active Directory instance, but more and more often it's a database or other sensitive data left in an unprotected cloud repository.

"The fact that 'misconfiguration' is in the top five action varieties for breaches is an important acknowledgment that not all incidents are the result of an exploited vulnerability," commented Tim Erlin, VP, product management and strategy at Tripwire. "Misconfigurations actually lead to more breaches than exploited systems, but organisations often don't put the same effort into assessing them as they do scanning for vulnerabilities."

The cloud is another major topic of debate in information security circles. Although cloud platforms are now extremely popular – pretty much every organisation of any size uses them, whether it knows it or not – survey after survey finds that worries about security continue to act as an impediment to wider cloud adoption. Yet the DBIR reports that 70% of attacks are against on-premise infrastructure and only 24% against cloud platforms (and a decent proportion of those are likely to involve credential theft, which is a threat that's common to any type of system). This could reflect robust security on the part of cloud service providers, or it might mean that attackers just haven't worked out how to attack these platforms yet.

Only 5% of breaches involved exploitation of a vulnerability – although that's no excuse for not patching. In fact, a key message from this year's DBIR is that basic security hygiene – such as combatting phishing with proper staff training and technical solutions, patching and ensuring that your websites are not susceptible to common attacks such as SQL injection – will go a long way to making you safe.

The report is available here: https://enterprise.verizon.com/en-gb/resources/reports/dbir/.



Who is behind data breaches? Source: Verizon.

In brief

NHS trusts fail security basics

A report by the UK's National Audit Office (NAO) reveals that only one NHS trust has reached the proper level of cyber security under the government-backed Cyber Essentials Plus scheme. The average score among the 204 trusts that have undertaken onsite assessments was 63%. This is an improvement over the 2017 score of 50%. However, full certification under the scheme – which examines areas such as vulnerability management, access controls, end-user devices, servers and network security – requires a score of 100%. "NHSX [the NHS digital services arm] and NHS Digital consider some trusts have reached an acceptable standard, even though they did not score 100% in the assessment, and note there has been a general improvement in cyber security across the NHS," the NAO says in the report. "However, while some attempts have been made to address underlying cyber security issues, and progress has been made, it remains an area of concern.' The report is here: https://bit.ly/2XvzJ1p.

IoT safety scheme

The UK Government is offering £400,000 to organisations that can come up with security certification schemes for Internet of Things (IoT) devices. The Department for Culture, Media and Sport (DCMS) anticipates that a number of schemes may need to be developed, to reflect the diversity of devices that fall under the IoT banner. The aim is to produce standards that vendors can use to promote their products through the use of logos on the products and packaging. There's more information here: https://bit.ly/2XwhuJb.

Covid-19 phishing warning

Microsoft has warned of a massive phishing campaign, using Covid-19 as a lure, which installs the NetSupport Manager remote administration tool giving complete access to the affected machine by the attackers. The emails purport to come from the John Hopkins Centre – the best known of the organisations monitoring the current pandemic – and claims to provide an update on coronavirus-related deaths in the US. An attached Excel file contains a graph and some statistics, but also has a malicious macro that downloads the NetSupport Manager from the attackers' command and control server. The hackers then have full access to the machine, including the ability to run software and commands as well as downloading further malware.

Law firms hit hard

Law firms may be among the most heavily targeted organisations when it comes to cyber attacks, according to research by security firm BlueVoyant. The investigation, detailed in the firm's report 'Sector 17 – The State of Cyber security in the Legal Sector', reveals that all the law firms the researchers studied had come under some form of attack in the first three months of 2020. Some 15% are likely to have suffered a compromise. And nearly half showed signs of suspicious activity, such as the use of malicious proxies. Attacks included ransomware, theft of financial data and personal identifiable information (PII), third-party risks, password breaches, insider leaks and hacktivism. There's more information here: https://bit.ly/2AA8ry2.

Malicious Android apps double

A review of malicious Android apps being distributed during the first quarter of 2020 showed there were twice as many as in the same period the year before. Using its Secure-D platform, security firm Upstream discovered over 29,000 malicious apps, with nine out of the 10 most popular ones being available at some point on Google's official Play store. The same goes for around 30% of the top 100. Upstream also said that the number of infected mobile devices it detected increased 7% to 11.2 million. There's more information here: https://bit.ly/2Uak45C.

Half a billion records exposed in May

The number of data records that were compromised by data breaches in May 2020 alone reached nearly half a billion, according to an analysis by IT Governance. In fact, the figure of 460 million records that the firm counted is likely to be on the low side, because it includes only those records involved in breaches that were publicly disclosed. The figure also discounts the 8.3 billion records leaked by the AIS phone network in Thailand – an issue that was quickly resolved and consisted of DNS queries and NetFlow logs, with no personal information. IT Governance said that 39 of the 105 incidents in May were due to cyber attacks, 37 to data breaches, 17 to ransomware attacks and six to insider threats or other types of incidents. There's more information here: https://bit.ly/2XBq8GJ.

Credential-stuffing attacks

Hackers are mounting 87 million credential-stuffing attacks against US targets every day, according to Atlas VPN. Using credentials leaked by previous data breaches, the attacks attempt to gain control of user accounts, with services such as PayPal, Ebay and Amazon being particularly popular targets. "Research shows that out of all possible cyber attacks, such as phishing, malware, DDoS, man-in-the-middle-attacks, and others, credential stuffing accounts for 44% of attacks on financial services – the reason being, hacking a financial institution or service would result in huge monetary gains for fraudsters," said the firm. There's more information here: https://bit.ly/3eObh19.

Non-IT data leaks

While we tend to associate data breaches with technology, new figures from the UK's Information Commissioner's Office (ICO) show that incompetence involving paper-based documents can be just as damaging. Measured in terms of incidents, the ICO said that, in the last quarter of 2019, there were 337 due to "data emailed to incorrect recipient," 265 were the result of "data posted or faxed to incorrect recipient" and 213 were due to "loss/theft of paperwork or data left in insecure location". The number of cyber-incidents were 280 as a result of phishing and 175 regarding unauthorised access. Of course, this doesn't take into account the volume of records (and therefore, potentially, the number of people) that might be compromised in a single incident. Database breaches, for example, can involve millions of records. There's more information here: https://bit.ly/3f1GCOf.

Click & Collect fraud

A significant increase in the use of 'click & collect' services, where customers order online and then collect their purchases from the retailer's premises, is leaving some smaller firms vulnerable to fraud. Many businesses have started operating such services as a result of the Covid-19 pandemic. However, according to Featurespace, a fraud-detection firm, not all of them have implemented necessary identification processes – such as demanding photo ID when customers collect their orders. This has resulted in fraudsters ordering goods, collecting them and then complaining that someone else has collected the goods. This is resulting in a large number of chargebacks via payment card issuers.

Google-branded phishing

Remote workers have been targeted by up to 65,000 Google-brand impersonation attacks, according to the most recent 'Threat Spotlight' report from Barracuda Networks. This type of spear-phishing scam uses branded sites to trick victims into sharing login credentials. Of the nearly 100,000 form-based attacks Barracuda detected in the first four months of 2020, Google file sharing and storage websites were used in 65% of attacks. This includes storage.googleapis.com (25%), docs.google.com (23%), storage.cloud.google.com (13%), and drive.google.com (4%). In comparison, Microsoft brands were targeted in 13% of attacks: onedrive.live.com (6%), sway.office.com (4%) and forms.office.com (3%). The other sites impersonated include sendgrid.net (10%), mailchimp.com (4%), and formcrafts.com (2%). All other sites made up 6% of form-based attacks. Barracuda expects these attacks to increase, not least because of the number of people working from home during the Covid-19 pandemic, and also because these attacks are proving to be highly effective. There's more information here: https://bit.ly/2zSVeR7.

The rise of telemedicine: how to mitigate potential fraud

Philipp Pointer

Philipp Pointer, Jumio

The global market for telehealth is expected to grow by $95.72bn between 2020 and 2024.[1] Driven by the rapid growth in remote patient monitoring, virtual GP consultations and online prescription services, we have already begun to see this growth take off. But these figures were estimated before the full Covid-19 pandemic ensued. With 1.5 million people in the UK now socially shielding, and with the rest of the country in lockdown for weeks, it is not surprising that there has been a surge in online medical advice and services.[2]

Before the outbreak, video appointments made up only 1% of the 340 million or so annual visits to the GP at the NHS.[3] Now, companies like Push Doctor and Docly are seeing massive increases in demand, up to 100% week on week.[4] While the UK Government insists that the NHS is open for business as usual, it's highly likely that telehealth growth rates will exceed initial estimates as people adapt to new ways of interacting with health providers, and ultimately, take telehealth into the mainstream even after the pandemic subsides.

However, this rapid rise has created a lucrative opportunity for fraudsters. Over 1 billion patient health records can be easily accessed on the dark web and millions of additional records are being added daily.[5] But what's not commonly understood is that medical records command a high value to bad actors. These medical records can be listed for up to $1,000 each, 10 times more than the average credit card data breach record because there's more personal information in health records than any other electronic database.

The emerging threat

Data breaches are, unfortunately, part of today's modern world. In March of this year alone, more than 800 million records were breached in the UK.[6] This, even at a time of global pandemic, demonstrates the dangers of operating a business that deals with personal identifiable information (PII) and sensitive data. In the healthcare sector, data breaches cost on average £5.2m a year, almost double that of the global average of £3.2m.[7]

According to research by SecurityScoreboard, the healthcare industry is the most breached industry, experiencing a 50% increase in data breaches from June 2017 to May 2019. Combine this with the growing size of the dark web, which is said to be several orders of magnitude larger than the surface web, and you can see why criminals are finding it easier and easier to prosper from obtaining PII through unscrupulous means.

> ***"Every piece of information is highly sensitive and opens an individual up to blackmail, and for the businesses, astronomical fines"***

Although, in an ideal world, all online institutions would adopt the strongest possible online security procedures, those that operate in the health industry need to be especially vigilant. They hold patients' ages, home addresses and extremely personal details around medical procedures and prescriptions. Every piece of information is highly sensitive and opens an individual up to blackmail, and – for businesses – astronomical fines with the introduction of the General Data Protection Regulations (GDPR).

One of the main issues is that we are often guilty of using the same password for multiple accounts, whether that is to log in to your GP's portal or to your Twitter account. This has seen a rise in credential stuffing, whereby would-be fraudsters purchase your email address and password on the dark web and use bots to try to access thousands of websites with these same login details, hoping to strike lucky. And most of the time, they do.

To mitigate this risk and protect their patients' valuable data, it is vitally important that all healthcare institutions reliably establish secure and accurate 'know your patient' (KYP) processes. This is particularly pertinent now that we have to factor in those who are relying on telehealth to meet their medical needs during the pandemic.

The need for KYP

The process of registering at a new doctor's surgery takes time. You need to provide proof of address, a form of government-issued identification and often you need to come into the surgery directly to provide your blood pressure so they can have it on file. Now, with the shift to telemedicine, the need to go through all the same motions might be reducing, but the importance of validating that patients are who they say they are has never been higher.

Stringent KYP procedures are the only way to be assured that the person a doctor is dealing with is who he claims to be. Last year alone, over two-thirds (67%) of UK healthcare organisations experienced some kind of cyber security incident and over the past decade, there have been over 2,550 healthcare breaches impacting more than 175 million medical records.[8,9] A sad fact is that, nowadays, there is a significant chance that the person online who claims to be a specific person is not that person at all. Therefore, online medical organisations must ensure that the person they're dispensing guidance and prescriptions to is, in fact, the patient on record. A mistake here can have huge ramifications for all those involved.

> ***"Online institutions will operate in good faith if the bad actor is able to provide date of birth, home address and even information about the person's family tree"***

For instance, if personal data is mistakenly given to a bad actor, the patient in question could fall victim to significant identity fraud. Other online institutions will operate in good faith if the bad actor is able to provide date of birth, home address and even information about the person's family tree. Imagine a criminal using a legitimate prescription to obtain addictive drugs such as morphine. This can then be sold on the black market for significant financial gain. Subsequently, the legitimate patient may also be unable to access medicines that they are in desperate need of, as the doctor's surgery will show they've already received the medicine in question. From a medical standpoint, the GP surgery that acted in good faith, but was ultimately duped by the criminal, will now be liable for retrospective fines, legal proceedings and further criminal and civil charges.

Strong processes

Although cyber criminals are becoming more sophisticated by the day, utilising machine learning and artificial intelligence to expedite the rate at which they can obtain data, there is a clear process to ensure that the power stays firmly in the hands of online medical professionals and healthcare organisations.

It starts at the new account creation stage. The medical organisation would capture an online patient's government-issued ID (eg, driver's licence, passport or ID card) via the user's smartphone or webcam, followed by a live corroborating selfie (in which a 3D face map is created) to ensure that the person behind the ID is the actual person creating the online account. Then, they would ensure that the ID document is authentic and unaltered and that the patient pictured in the selfie matches the picture on the ID.

Next comes age verification, checking the returned identity for minimum age requirements and potentially fraudulent activity through fraud detection analytics to help minimise risk and loss. From this, and depending on the results, hospitals, offices, clinics and pharmacies can now approve or deny the new online account and attempted purchases.

Lastly, after an online account has been approved, medical offices and pharmacies can approve future online prescriptions and treatment requests with biometric-based authentication. They do this by capturing a fresh 3D face map of the patient and using online identity verification technology to automatically compare it to the original 3D face map captured at enrolment to authenticate the patient.

> ***"The expedited modernisation of the healthcare industry and the dramatic shift to telemedicine will undoubtedly be a positive for the weeks, months and years ahead"***

Although this method in the UK would prevent those under the age of 16 from accessing telemedical services, it would also provide assurances to those medical organisations that minors are not obtaining powerful prescriptions accidently.

Evolving world

The weekly appreciation of the NHS in the UK is one of the few positives to come from this pandemic. More than ever, we're reminded of the vital, lifesaving work our medical professionals are doing. Likewise, the expedited modernisation of the healthcare industry and the dramatic shift to telemedicine will undoubtedly be a positive for the weeks, months and years ahead.

It's clear that the entire NHS is stretched thin and that the shift to telemedicine is going to be of vital importance moving forward and a necessary way of modernising the 70-year-old behemoth. But the future of telemedicine can only be assured if trust can be reliably established between the medical expert and the patient. Failure to do so would signal that telemedicine has only been a flash in the pan.

About the author

Philipp Pointer serves as Jumio's chief product officer (CPO) and facilitates Jumio's product strategy. Prior to joining Jumio, he was responsible for paysafecard, a prepaid solution for purchasing online. At paysafecard he played a primary role in launching the KYC-compliant mypaysafecard wallet. Before that Pointer served 10 years at e-commerce giant First Data where he took a deep dive into the classic payment industry. He graduated from the University of Applied Sciences Technikum in Vienna.

References

1. 'Telehealth Market by Product and Geography – Forecast and Analysis 2020-2024'. TechNavio, Mar 2020. Accessed May 2020. www.technavio.com/report/telehealth-market-industry-analysis.

2. Donnelly, Laura; Mendick, Robert. ‘Hundreds of thousands needing to be shielded from coronavirus have still not been contacted, investigation shows’. The Telegraph, 20 Apr 2020. Accessed May 2020. www.telegraph.co.uk/news/2020/04/20/hundreds-thousands-needing-shielded-coronavirus-have-still-not/.
3. Field, Matthew. ‘Self-isolating GPs turn to video doctor apps to see patients’. The Telegraph, 5 Apr 2020. Accessed May 2020. www.telegraph.co.uk/technology/2020/04/05/self-isolating-gps-turn-video-doctor-apps-see-patients/.
4. Mueller, Benjamin. ‘Telemedicine Arrives in the UK: “10 Years of Change in One Week”‘. The New York Times, 4 Apr 2020. Accessed May 2020. www.nytimes.com/2020/04/04/world/europe/telemedicine-uk-coronavirus.html.
5. Whittaker, Zack. ‘A billion medical images are exposed online, as doctors ignore warnings’. TechCrunch, 10 Jan 2020. Accessed May 2020. https://techcrunch.com/2020/01/10/medical-images-exposed-pacs/.
6. Irwin, Luke. ‘List of data breaches and cyber attacks in March 2020 – 832 million records breached’. IT Governance, 2 Apr 2020. Accessed May 2020. www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber attacks-in-march-2020-832-million-records-breached.
7. ‘How much would a data breach cost your business?’. IBM. Accessed May 2020. www.ibm.com/security/data-breach.
8. Scroxton, Alex. ‘Two-thirds of UK healthcare organisations breached last year’. Computer Weekly, 15 Jan 2020. Accessed May 2020. www.computerweekly.com/news/252476696/Two-thirds-of-UK-healthcare-organisations-breached-last-year.
9. Siwicki, Bill. ‘Digital identity verification is one key to fighting cyber security threats’. Healthcare IT News, 10 Sep 2019. Accessed May 2020. www.healthcareitnews.com/news/digital-identity-verification-one-key-fighting-cyber security-threats.

Removing a false sense of (open source) security

Jeff Williams, Contrast Security

Jeff Williams

Software is at the heart of the ‘digital transformation’ as businesses rapidly transition from traditional legacy-based models to more robust modern digital business processes. The rapid pace of modern software development has allowed businesses to transform the way they run – yielding superior customer experiences, greater efficiencies, faster time to market and better cost optimisation.

Software has also enabled companies to disrupt their business environments by leveraging the agility and speed of change that only software can deliver. Innovative companies realise that software innovation can drive agility, create differentiation and provide competitive advantage.

With software so predominant, it is also important to understand the positive and negative consequences of using open source software (OSS). The use of open source code has grown in popularity over the past few years and it is employed in companies of all sizes and in all industry verticals. The enticement of OSS is undeniable and the vibrant open source community has burgeoned, resulting in significant contributions to the open source movement. As a result, developers are increasingly using OSS, which has now gone mainstream.

By embracing OSS, companies realise major economic and productivity benefits and the positive impact that it provides their bottom line. Leading organisations are racing to maintain their relevance and competitive edge via the use of software. Furthermore, companies are quickly adopting and implementing agile and DevOps methodologies, allowing them to iterate, innovate and release software faster. OSS accelerates all of this by enabling organisations to move even faster by harnessing prefabricated building blocks to bootstrap the software development process. According to Gartner, OSS is so popular that it has saturated key major verticals and

Customer Experience
Operational Processes
Business Model
Investing Heavily
in Custom software
Executing with Agile,
DevOps and Cloud

Digital transformation of business via software.

it's believed that more than 95% of IT organisations are leveraging OSS assets.

Tangible benefits

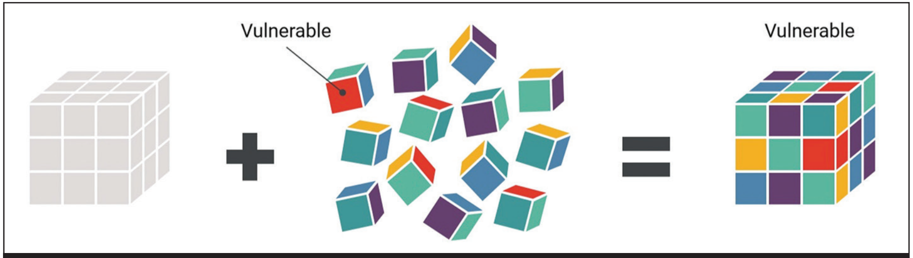
OSS is software that is distributed with source code that may be read or modified by users. It encompasses modular, pre-built and reusable components that accelerate the release and delivery of software, resulting in lower development costs and faster time to market. The use of OSS components provides critical functionality within the application – this in turn drives innovation at a much faster pace than relying on coding everything from scratch.

OSS is easy to modify, enhance and integrate, offering a collaborative approach to open source communities. Organisations use OSS as the architectural foundation for applications, operating systems, databases, development tools, cloud computing and big data. Some examples of popular OSS and associated platforms and infrastructure include Linux, Docker, .NET, Java, Eclipse, Apache, Maven, NodeJS, Drupal, GitHub and Chef, to name just a few.

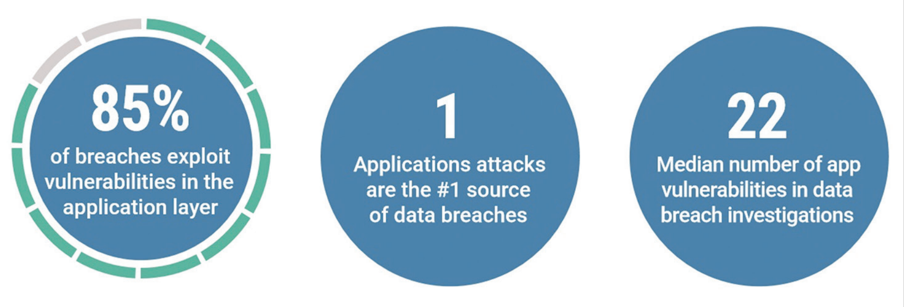
Building blocks

The amount of open source code from external sources is steadily rising and developers have become heavily reliant on it. Open source is an integral technology and business tool, requiring that security be woven into the very fabric of the code. Accordingly, there are many application security challenges that need to be understood and addressed when using open source code.

OSS security breaches are rare; however, when software is compromised it can create havoc in an organisation – hence the need to effectively identify, manage and mitigate vulnerabilities. As companies continually adopt more and more OSS assets, there is a greater emphasis on how OSS software needs to be incorporated and managed to make code more secure.



In-house and external open source software.



Application security risks.

Open source plays a pivotal role in the success and/or failure of software development teams. Most developers do not work in cultural environments where security is 'top of mind' – nor do they take the time to understand the inherent risks and implications that OSS code may contain. Additionally, OSS security practices have not kept pace with the rapid adoption of software.

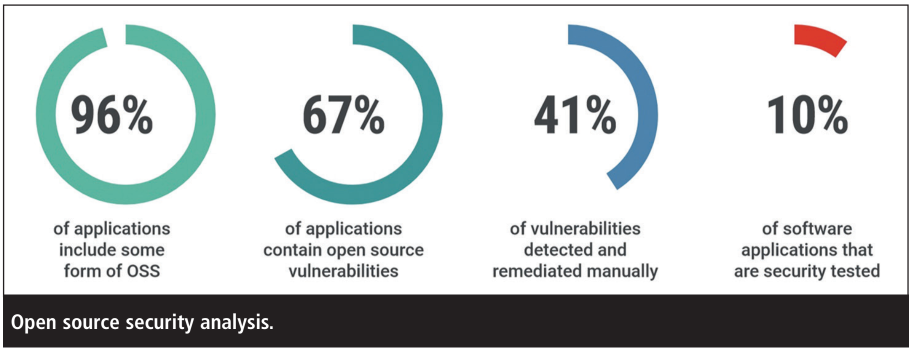
> ***"Most developers do not work in cultural environments where security is 'top of mind' – nor do they take the time to understand the inherent risks and implications that OSS code may contain"***

The fast pace of modern software development processes makes the most common vulnerabilities and risks crucial to discover and fix quickly and effectively. As software is rolled out faster, it potentially introduces additional risk for companies.

False sense of security

The benefits of OSS are generally understood by the software developer community, but not necessarily the risks. It should be fully understood by developers that OSS is not immune to potential security risks. The core security risks in using OSS are like other types of software assets. All code comes with security risks and developers have a tendency to trust OSS code, especially popular industry packages. As companies use a greater amount of open source code, it introduces vulnerabilities that expose a company to risks and possibly breaches.

Organisations are not effectively dealing with OSS security threats. Since OSS is in the public domain, hackers with malicious intentions can access the



Open source security analysis.

code base. They can identify and exploit potential failings or loopholes within the software code more easily than in-house proprietary software. Furthermore, developers may inadvertently use defective components that go undetected and get into production environments.

Applications using OSS are a primary target for cyber criminals because once exploits are developed for OSS vulnerabilities, they can be used to attack many companies. New vulnerabilities are constantly being identified in OSS, but many open source projects have no clear processes or mechanisms in place for finding and fixing them. One main issue with the use of OSS is the lack of standardised security documentation. Other issues include the use of legacy code due to compatibility, compliance and resource constraints.

Enabling developers

Traditionally, development and security teams have worked in silos, disconnected from each other. Companies need to get ahead of the curve and develop stronger protection initiatives that integrate security into their existing release methodologies. Weaving and integrating security into the development process for both the developer community (who design, write, test and release code) and security practitioners (who deploy, monitor and identify vulnerabilities and threats in production) is paramount to successful OSS implementation and management.

Both teams need to have a clear understanding of their OSS inventory that they are utilising and the potential vulnerabilities and risks that exist in using open source code.

Additionally, developers need to raise their awareness and understand the key principles and best practices of software security. OWASP provides a detailed list of the top 10 most critical web application security risks. The OWASP Top 10 has become the de facto standard to assist practitioners to adopt security within application security programmes.[1]

Security automation

Security needs to be a key component for OSS and integrated in fast-paced agile or DevOps workflow environments. Security teams need to be able to quickly and effectively respond to application security breaches in order to prioritise and remediate in real time. New innovative and automated approaches to implement and manage OSS are required – automated solutions that quickly and effectively identify, mitigate and remediate open source vulnerabilities, wherever they may reside – such as libraries, frameworks, custom code, etc.

The value of OSS is undeniable. As the pace for open source adoption continues to increase it is critical to actively pursue, manage and remediate vulnerabilities within the entire codebase quickly and effectively.

Roadmap for success

As outlined in this article, there is no denying the impact OSS has in contributing to a company's bottom line. OSS offers organisations throughout the globe greater flexibility and cost savings. However, it must be remembered that no software is completely bulletproof and OSS shares the same inherent risks as traditional software.

Organisations need to focus on security as a key component within their applications. Technology can help development and security practitioners harden their application code from the inside, which in turn helps identify, manage and eliminate application security vulnerabilities. Proper management and inventory control need to be encouraged and outlined clearly to both developers and security personnel. Organisations need to get ahead of the curve to secure their prized assets.

Software development and security practitioners need to co-ordinate and create application security programmes that are compatible with an organisation's corporate culture. This in turn will help create a more robust security posture. As a result, security-driven companies will be more successful in reducing software vulnerabilities and associated risks.

Security instrumentation technology automatically identifies and assesses all third-party libraries throughout your code base. This will instantly build a full inventory of all libraries by application and even server environment, and then contextually report the versions used and any known vulnerabilities associated with them. Further, library inventory updates continuously when running. This provides teams with a current, real-time visibility into all open source components across their portfolio, so they know what needs to be secured.

Developers and application security practitioners have access to this information with actionable details for each published CVE and insight into what is being used and where it is deployed to help prioritise remediation efforts. Additionally, developers can be alerted automatically when a newly on-boarded application utilises a library that may violate the organisation's licence or security policy, so they can take immediate action.

About the author

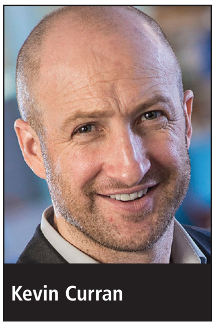
Jeff Williams has more than 20 years of security leadership experience as co-founder and chief technology officer of Contrast Security. He's very active in the DevSecOps community, recently authored the DZone DevSecOps cheat sheet, and speaks frequently on the topic at conferences. He is also a founder and major contributor to OWASP, where he served as global chairman for nine years and created the OWASP Top 10 and many other widely adopted free and open projects.

Reference

1. 'OWASP Top 10'. OWASP. Accessed May 2020. https://owasp.org/www-project-top-ten/.

Cyber security and the remote workforce

Kevin Curran, Ulster University



Kevin Curran

Current world events have forced a sudden remote-working economy that many businesses were simply not prepared for. According to a Gartner survey of 229 human resources (HR) managers, 81% or more are working remotely, and 41% are likely to do so at least some of the time even once a return to normal working is permitted. This sudden rise in remote working is not only challenging employees to work in a way they had not previously, but it has also impacted the cyber-risk profile of enterprises worldwide.

While initial concerns focused on infrastructure, equipment and bandwidth provision, it is becoming apparent that many organisations are now more vulnerable to security threats than ever before. With the reliance on personal devices (BYOD), cloud networks and remote access technology, employees now operate outside the IT safety net. This can expose private information to bad actors through common scams that are likely to increase in prevalence over the coming months.

Phishing attacks are rife

Organisations will have built policies and procedures over many years that protect individuals and the organisation's infrastructure. However, unless a significant percentage of employees had previous access to proper remote access technologies, there is a real risk of employees making bad choices.

Phishing attacks still remain a problem. In fact, many current phishing techniques are designed to be effective in these environments by targeting large numbers of employees with pandemic-related claims. These attacks use tailored techniques and dynamic websites and regularly update the methods used. The result is a series of attacks that have an alarmingly high success rate, yet a relatively low detection rate.

The increased risk, due to remote working, is that employees may be using non-standard email or messaging systems that fail to properly filter out emails that carry the threat. Employees could also be tempted to use public wifi without using a virtual private network (VPN) and this can leave them exposed to what is known as 'man in the middle attacks', which often pose as fake wifi hotspots.

Conference bombing

Conference 'bombing' has become a new challenge in cyber security, where third parties hijack video conferences. There are some protections that organisations can use on video conferencing platforms to prevent this, such as not sharing the meeting ID in public forums. In addition, users should not share a personal meeting ID (PMI) with someone else, as third parties will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.

It is best practice to create waiting rooms for attendees to prevent users from entering the meeting without first being admitted by the host. Of course, the host should be present before the meeting starts and if everyone has joined the meeting then simply lock the meeting so that nobody else can join. Organisations should also prevent participants, other than the host, from sharing their screen and ensure that they password protect meetings. It is possible to enforce stricter controls within an organisation by only allowing individuals with a given email domain to join.

It is also important to update conferencing platforms, as updates often enable meeting passwords by default, and add protection from people scanning for a meeting ID. Finally, it is important to download the conferencing platform only from the legitimate site – and not from anywhere else – as there are fake versions containing malware.

Ransomware and file sharing

One of the biggest risks is an increase in ransomware attacks, which are a serious problem in enterprises at the moment. Remote working employees may be using non-standard email or messaging systems, which fail to properly filter out emails that carry a threat.

Organisations also need to be careful when sharing files. One drawback of many file sharing options is that organisations simply do not have the necessary control over data. When employees use consumer tools to share with external entities, they are taking business information outside the company's IT scope. This means that it is also out of the IT department's control for security and integration purposes.

Some organisations have run into security breaches because employees use their personal file-sharing tools on work-issued devices and this opens up another vulnerability for point of business networks. Without visibility into business data flows, IT personnel cannot adequately track the files entering and leaving the company. This lack of transparency inhibits an organisation's ability to ensure compliance with internal policies or with external mandates and agreements.

A managed file sharing service can, however, provide detailed audit trails, as well as encrypting and compressing files in transit and at rest. What's more, it meets compliance requirements such as PCI DSS, HIPAA/HITECH, reduces the need for custom scripts and programs, single-function tools and manual processes. It also uses workflows that are easy to design and process, without the use of other tools or programming, as well as providing the ability to segment an organisation into multiple security zones.

Another effective file sharing security step is to better educate all employees about the risks of sharing files, especially in terms of using IT solutions that are not officially implemented, approved by an organisation or approved by its IT department. This type of file sharing involves using personal email accounts, free cloud storage services and other consumer file-sharing systems, as they may not meet the company's security standards and are, in many cases, outside the company's existing security controls. Companies should also implement a formal file sharing policy that provides clarity and conveys the serious nature of the risks involved in such activities. Companies' IT and security teams should evaluate the usage and security of consumer file-sharing systems to determine whether or not to allow their use and take measures to secure usage should they be allowed.

Preventative measures

VPNs are an obvious way to secure data between remote workers and core systems. In the ideal world, organisations would deploy a 'zero trust' network system. However, this can be difficult to implement, especially in response to the current pandemic, as it should ideally be rolled out in a phased manner, which entails pilot projects and tweaks in a safe environment before deployment. However, if an organisation has not yet embraced the concepts of privileged access and least privilege, or still uses shared accounts for access, then zero trust is probably not going to work.

"Some solutions can isolate sensitive personal information from privileged company information – ie, company data is never on the mobile device. This is important to the individual and company if legal issues do surface"

Organisations should ensure that employees have up-to-date security protection on any devices, such as virus checkers, firewalls and device encryption. Another fundamental for organisations to mitigate risks is to deploy mobile device management (MDM). There are some MDM options that allow multiple users who share a single device to have full control over VPN, device-wipe capabilities and configuration of enterprise data protection policies. They also allow the separation of personal and corporate data, which can be a useful feature in heavy BYOD environments. Businesses can also choose between data mining (DM) and traditional Active Directory (AD) or group policy models.

There are third-party products that can help businesses establish smaller boundaries for compliance purposes, and focus on them, rather than the whole network. For example, some solutions can isolate sensitive personal information from privileged company information – ie, company data is never on the mobile device. This is important to the individual and company if legal issues do surface. It also reduces costs and simplifies device management. Application 'whitelists' and 'blacklists' are also important.

Businesses should also use services to help control devices brought in by employees. Companies with BYOD programmes in place can let administrators do selective wipes of devices and cleaning app data without wiping the entire device. Additionally, when a full wipe is needed, the policy can now force a secure digital (SD) card wipe, along with the internal storage of the device if necessary. Admins can also set wifi configurations for every device with app policies, by letting them set it once and push to all managed devices at once.

Containerisation is another option for companies to separate corporate and personal data on an employee's device. This involves separating out the corporate mobile apps and the data associated with these into 'containers' on the mobile device, creating a clear division as to what is subject to corporate security policies such as wiping. Finally, there is also the option to build a controlled app portal from the ground up.

The future 'norm'

With the sudden rise in remote workers, as well as Gartner predicting that remote working will likely become more commonplace when people are able to go back to 'normal' working practices, cyber security has become a critical discussion point in recent weeks. The next few months will be a learning curve for many enterprises across the globe. By being aware of the current threats – whether it's phishing, conference 'bombing' or ransomware – and implementing the correct security tools to mitigate these threats and protect enterprise and employee data, then businesses will be able to put their best foot forward as they navigate this pandemic.

About the author

Kevin Curran is a senior IEEE member and professor of cyber security at Ulster University. He is an independent security expert whose research has made significant contributions to advancing the knowledge and understanding of computer networking and systems. A public-interest technologist, working at the intersection of security, technology and people, he has authored a number of books and is the recipient of various patents.

A forensic study of Tor usage on the Raspberry Pi platform using open source tools

Neerad S Vaidya

Parag H Rughani

Neerad S Vaidya and Parag H Rughani, Gujarat Forensic Sciences University

Since the invention of the first computer, scientists have striven to minimise the size – and we can see the fruits of their efforts in the form of the Raspberry Pi. This is a series of small, single-board computers developed to promote the teaching of basic computer science in schools and in developing countries. According to the Raspberry Pi Foundation, more than five million Raspberry Pi boards were sold by February 2015, making it the best-selling British computer. By November 2016 the Foundation had sold 11 million units, and by March 2017, 12.5m, which made it the third best-selling 'general purpose computer'. In July 2017, sales reached nearly 15 million and less than a year later, in March 2018, 19 million.

Several generations of Raspberry Pi models have been released. All models feature a Broadcom system on a chip (SoC) with an integrated ARM-compatible central processing unit (CPU) and on-chip graphics processing unit (GPU). Processor speeds range from 700MHz up to 1.5GHz on the latest Pi 4; on-board memory ranges from 256MB to 8GB. Secure Digital (SD) cards are used to store the operating system and program memory in either SDHC or MicroSDHC sizes. The boards have one to four USB ports. For video output, HDMI and composite video are supported, with a standard 3.5mm tip-ring-sleeve jack for audio output. Lower-level output is provided by a number of GPIO pins, which support common protocols such as I2C, SPI and UART.

The B-models have an 8P8C Ethernet port and the Pi 3, Pi 4 and Pi Zero W have on-board wifi 802.11n and Bluetooth. The Raspberry Pi 3 Model B was released in February 2016 with a 64-bit quad core processor, on-board wifi, Bluetooth and USB boot capabilities. On Pi Day 2018, the model 3B+ appeared with a faster 1.4GHz processor and a three-times faster network based on gigabit Ethernet (300Mbps) or 2.4/5GHz dual-band wifi (100Mbps). Other options are: power over Ethernet (PoE), USB boot and network boot (where an SD card is no longer required). The Pi 4 Model B was introduced in June 2019 and has full gigabit Ethernet.

The Broadcom BCM2835 SoC used in the first-generation Raspberry Pi includes a 700MHz ARM11 76JZF-S processor, VideoCore IV graphics processing unit (GPU), and RAM. It has a level 1 (L1) cache of 16KB and a level 2 (L2) cache of 128KB. The level 2 cache is used primarily by the GPU. The SoC is stacked underneath the RAM chip, so only its edge is visible. The 1176JZ(F)-S is the same CPU as used in the original iPhone, although at a higher clock rate, and mated with a much faster GPU.

The Raspberry Pi Foundation provides Raspbian, a Debian-based Linux distribution for download, as well as third-party Ubuntu, Windows 10 IoT Core, RISC OS and specialised media centre distributions. It promotes Python and Scratch as the main programming languages, with support for many other languages. The default firmware is closed source, while an unofficial open source is available. Many other operating systems can also run on the Raspberry Pi. Other third-party

Operating systems – non-Linux	Operating systems – Linux based
RISC OS Pi	Android Things
FreeBSD	Arch Linux ARM
NetBSD	Emteria OS
OpenBSD	OpenSUSE
Plan 9 from Bell Labs	Gentoo Linux
Windows 10 IoT	Lubuntu
xv16	Raspbian
Haiku	Cent OS
HelenOS	Ubuntu Mate

Table 1: Table of operating systems supported by the Raspberry Pi.

operating systems available via the official website include Ubuntu Mate, Windows 10 IoT Core, RISC OS and specialised distributions for the Kodi media centre and classroom management.

Tor

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project – The Onion Router. Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than 7,000 relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

> ***"Tor protects a user's privacy, but does not hide the fact that someone is using Tor. And some websites restrict access via Tor"***

Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to websites, online posts, instant messages and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Tor does not prevent an online service from determining when it is being accessed through Tor: Tor protects a user's privacy, but does not hide the fact that someone is using Tor. And some websites restrict access via Tor. For example, the MediaWiki TorBlock extension automatically restricts edits made through Tor, although Wikipedia allows some limited editing in exceptional circumstances.

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.

> ***"Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance"***

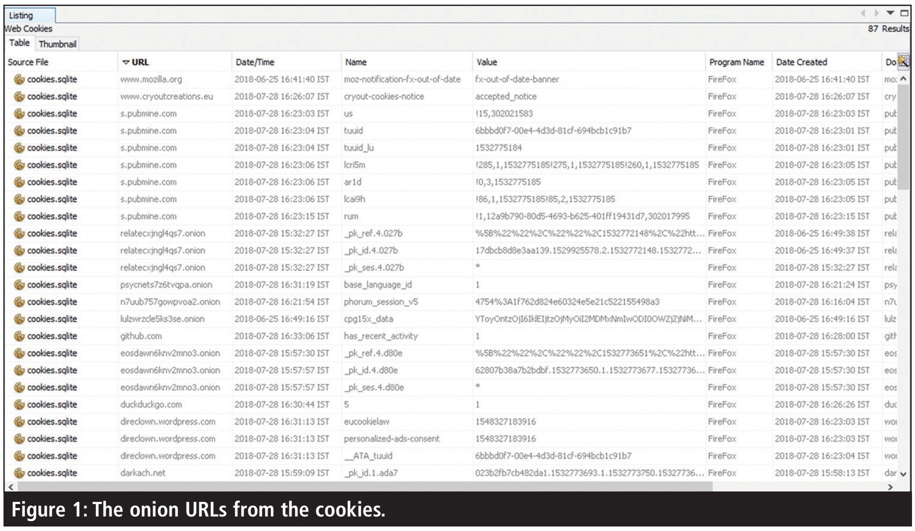
For efficiency, the Tor software uses the same circuit for connections that occur within the same 10 minutes or so. Later requests are given a new circuit, to keep people from linking earlier actions to the new ones.

Similar work

Many researchers have used Raspberry Pi in many cyber security solutions, and some of them are discussed here.

S Mahajan et al developed an intrusion detection system (IDS) using a Raspberry Pi board.[1] A Raja et al worked on an Internet of Things (IoT)-based security alert system in which they used the Raspberry Pi.[2] K Karmakar et al proposed a policy-based security architecture for software defined networks (SDNs).[3] X Feng et al published their work on cyber security investigations for Raspberry Pi devices.[4] M Williams carried out risk assessments on the Raspberry Pi using NIST standards.[5] C Lim et al developed a Raspberry Pi-based honeypot.[6] X Wang et al developed a deep learning-based classification and anomaly detection system.[7] And M Lalitha et al proposed a Raspberry Pi-based industrial control system with redundancy and intrusion detection.[8]

There has also been significant work by researchers in the investigation of Tor-based criminal activity, some of which is mentioned in this section. D McCoy et al provided a detailed understanding of how Tor works.[9] R Jansen et al discussed a sniper attack to achieve deanonymisation of Tor traffic.[10] D Dolliver worked on evaluating drug trafficking on the Tor network, especially focusing on Silk Road 2.[11] M Perry proposed a solution called Torflow for Tor network analysis.[12] A Chaabane, P Manils and M Kaafar published work related to deep analysis of the Tor network.[13]



Source File	URL	Date/Time	Name	Value	Program Name	Date Created	Do
cookies.sqlite	www.mozilla.org	2018-06-25 16:41:40 IST	moz-notification-fx-out-of-date	fx-out-of-date-banner	FireFox	2018-06-25 16:41:40 IST	mo:
cookies.sqlite	www.cryoutcreations.eu	2018-07-28 16:26:07 IST	cryout-cookies-notice	accepted_notice	FireFox	2018-07-28 16:26:07 IST	cry
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:03 IST	us	!15,302021583	FireFox	2018-07-28 16:23:03 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:04 IST	tuuid	6bbbd0f7-00e4-4d3d-81cf-694bcb1c91b7	FireFox	2018-07-28 16:23:01 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:04 IST	tuuid_lu	1532775184	FireFox	2018-07-28 16:23:01 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:06 IST	lcri5m	!285,1,1532775185!275,1,1532775185!260,1,1532775185	FireFox	2018-07-28 16:23:05 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:06 IST	ar1d	!0,3,1532775185	FireFox	2018-07-28 16:23:05 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:06 IST	lcai9h	!86,1,1532775185!85,2,1532775185	FireFox	2018-07-28 16:23:05 IST	pub
cookies.sqlite	s.pubmine.com	2018-07-28 16:23:15 IST	rum	!1,12a9b790-80d5-4693-b625-401ff19431d7,302017995	FireFox	2018-07-28 16:23:15 IST	pub
cookies.sqlite	relatecxjngl4qs7.onion	2018-07-28 15:32:27 IST	_pk_ref.4.027b	%5B%22%22%2C%22%22%2C1532772148%2C%22htt...	FireFox	2018-06-25 16:49:38 IST	rela
cookies.sqlite	relatecxjngl4qs7.onion	2018-07-28 15:32:27 IST	_pk_id.4.027b	17dbcb8d8e3aa139.1529925578.2.1532772148.1532772...	FireFox	2018-06-25 16:49:37 IST	rela
cookies.sqlite	relatecxjngl4qs7.onion	2018-07-28 15:32:27 IST	_pk_ses.4.027b	*	FireFox	2018-07-28 15:32:27 IST	rela
cookies.sqlite	psycnets7z6tvqpa.onion	2018-07-28 16:31:19 IST	base_language_id	1	FireFox	2018-07-28 16:21:24 IST	psy
cookies.sqlite	n7uub757gowpvoa2.onion	2018-07-28 16:21:54 IST	phorum_session_v5	4754%3A1f762d824e60324e5e21c522155498a3	FireFox	2018-07-28 16:16:04 IST	n7u
cookies.sqlite	lulzwrzcle5ks3se.onion	2018-06-25 16:49:16 IST	cpg15x_data	YToyOntzOjI6IklEIjtzOjMyOiI2MDMxNmIwODI0OWZjZjNiM...	FireFox	2018-06-25 16:49:16 IST	lulz
cookies.sqlite	github.com	2018-07-28 16:33:06 IST	has_recent_activity	1	FireFox	2018-07-28 16:28:00 IST	gith
cookies.sqlite	eosdawn6knv2mno3.onion	2018-07-28 15:57:30 IST	_pk_ref.4.d80e	%5B%22%22%2C%22%22%2C1532773651%2C%22htt...	FireFox	2018-07-28 15:57:30 IST	eos
cookies.sqlite	eosdawn6knv2mno3.onion	2018-07-28 15:57:57 IST	_pk_id.4.d80e	62807b38a7b2bdbf.1532773650.1.1532773677.15327736...	FireFox	2018-07-28 15:57:30 IST	eos
cookies.sqlite	eosdawn6knv2mno3.onion	2018-07-28 15:57:57 IST	_pk_ses.4.d80e	*	FireFox	2018-07-28 15:57:30 IST	eos
cookies.sqlite	duckduckgo.com	2018-07-28 16:30:44 IST	5	1	FireFox	2018-07-28 16:26:26 IST	duc
cookies.sqlite	direclown.wordpress.com	2018-07-28 16:31:13 IST	eucookielaw	1548327183916	FireFox	2018-07-28 16:23:03 IST	wor
cookies.sqlite	direclown.wordpress.com	2018-07-28 16:31:13 IST	personalized-ads-consent	1548327183916	FireFox	2018-07-28 16:23:03 IST	wor
cookies.sqlite	direclown.wordpress.com	2018-07-28 16:31:13 IST	__ATA_tuuid	6bbbd0f7-00e4-4d3d-81cf-694bcb1c91b7	FireFox	2018-07-28 16:23:04 IST	wor
cookies.sqlite	darkach.net	2018-07-28 15:59:09 IST	_pk_id.1.ada7	023b2fb7cb482da1.1532773693.1.1532773750.15327736...	FireFox	2018-07-28 15:58:13 IST	dar

Figure 1: The onion URLs from the cookies.

D Dolliver and J Kenney discussed various characteristics of drug vendors on the Tor network.[14] Similarly, R Munksgaard et al published research that evaluated drug trafficking on the Tor network.[15]

> ***"We have considered a scenario where criminals may use a combination of the Raspberry Pi and Tor in committing crimes. Since the Raspberry Pi board gives mobility and Tor provides anonymity, together they can become a powerful weapon for criminals"***

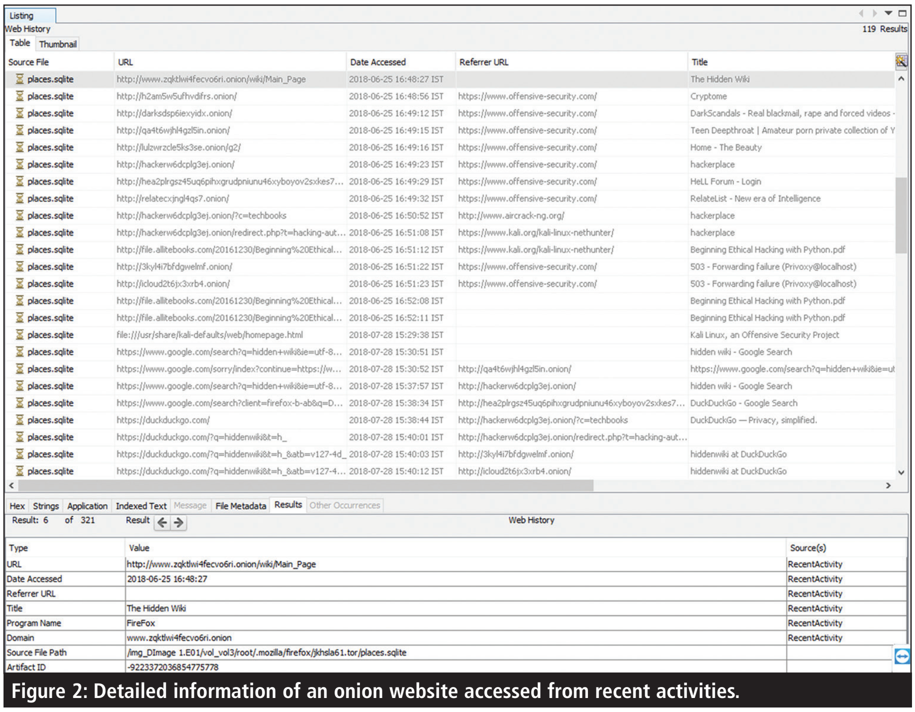
While the majority of the authors cited above have worked on Raspberry Pi and Tor separately, so far no researcher has approached both together, to discover the specific artefacts of Tor when used with the Raspberry Pi. The work proposed here touches both components to help forensic investigators in solving crimes committed using these emerging technologies. We'll now discuss the experiment carried out.

The scenario

Considering the increasing use of emerging technologies by criminals, we have considered a scenario where criminals may use a combination of the Raspberry Pi and Tor in committing crimes. Since the Raspberry Pi board gives mobility and Tor provides anonymity, together they can become a powerful weapon for criminals. As an example, a criminal selling or buying drugs from a darknet site using Tor may prefer to use a Raspberry Pi-based micro computer instead of a traditional desktop or laptop. The mobility provided by the Raspberry Pi, which has sufficient processing power and scalability, can be a better choice compared to a traditional computer. The major advantage with a Raspberry Pi is its size – a criminal would prefer to use a computer that can be destroyed or hidden easily in the case of a raid.

For experimental purposes, we considered a scenario where a criminal uses the Tor network to access the darknet using a Raspberry Pi board. The target machine was configured with the Raspberry Pi version of Kali Linux. Since there isn't a direct installer of Tor available for this distribution, we tweaked a few libraries and managed to access onion websites from the Raspberry Pi board.

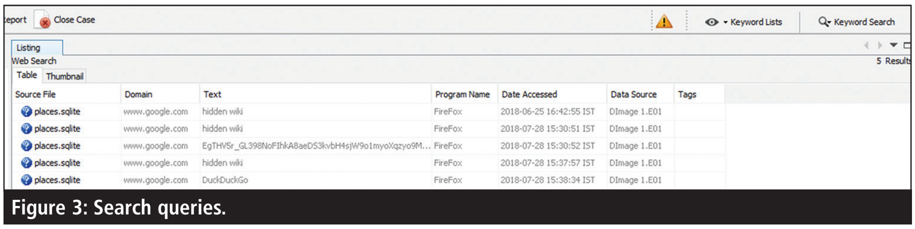
For the analysis machine, we used a Windows 10 instance, a Kali Linux instance and an Ubuntu instance as we are focusing mainly on free and



Source File	URL	Date Accessed	Referrer URL	Title
places.sqlite	http://www.zqktlwi4fecvo6ri.onion/wiki/Main_Page	2018-06-25 16:48:27 IST		The Hidden Wiki
places.sqlite	http://h2am5w5ufhvdifrs.onion/	2018-06-25 16:48:56 IST	https://www.offensive-security.com/	Cryptome
places.sqlite	http://darksdsp6iexyidx.onion/	2018-06-25 16:49:12 IST	https://www.offensive-security.com/	DarkScandals - Real blackmail, rape and forced videos -
places.sqlite	http://qa4t6wjhl4gzl5in.onion/	2018-06-25 16:49:15 IST	https://www.offensive-security.com/	Teen Deepthroat | Amateur porn private collection of Y
places.sqlite	http://lulzwrzcle5ks3se.onion/g2/	2018-06-25 16:49:16 IST	https://www.offensive-security.com/	Home - The Beauty
places.sqlite	http://hackerw6dcplg3ej.onion/	2018-06-25 16:49:23 IST	https://www.offensive-security.com/	hackerplace
places.sqlite	http://hea2plrgsz45uq6pihxgrudpniunu46xyboyov2sxkes7…	2018-06-25 16:49:29 IST	https://www.offensive-security.com/	HeLL Forum - Login
places.sqlite	http://relatecxjngl4qs7.onion/	2018-06-25 16:49:32 IST	https://www.offensive-security.com/	RelateList - New era of Intelligence
places.sqlite	http://hackerw6dcplg3ej.onion/?c=techbooks	2018-06-25 16:50:52 IST	http://www.aircrack-ng.org/	hackerplace
places.sqlite	http://hackerw6dcplg3ej.onion/redirect.php?t=hacking-aut…	2018-06-25 16:51:08 IST	https://www.kali.org/kali-linux-nethunter/	hackerplace
places.sqlite	http://file.allitebooks.com/20161230/Beginning%20Ethical…	2018-06-25 16:51:12 IST	https://www.kali.org/kali-linux-nethunter/	Beginning Ethical Hacking with Python.pdf
places.sqlite	http://3kyl4i7bfdgwelmf.onion/	2018-06-25 16:51:22 IST	https://www.offensive-security.com/	503 - Forwarding failure (Privoxy@localhost)
places.sqlite	http://icloud2t6jx3xrb4.onion/	2018-06-25 16:51:23 IST	https://www.offensive-security.com/	503 - Forwarding failure (Privoxy@localhost)
places.sqlite	http://file.allitebooks.com/20161230/Beginning%20Ethical…	2018-06-25 16:52:08 IST		Beginning Ethical Hacking with Python.pdf
places.sqlite	http://file.allitebooks.com/20161230/Beginning%20Ethical…	2018-06-25 16:52:11 IST		Beginning Ethical Hacking with Python.pdf
places.sqlite	file:///usr/share/kali-defaults/web/homepage.html	2018-07-28 15:29:38 IST		Kali Linux, an Offensive Security Project
places.sqlite	https://www.google.com/search?q=hidden+wiki&ie=utf-8…	2018-07-28 15:30:51 IST		hidden wiki - Google Search
places.sqlite	https://www.google.com/sorry/index?continue=https://w…	2018-07-28 15:30:52 IST	http://qa4t6wjhl4gzl5in.onion/	https://www.google.com/search?q=hidden+wiki&ie=ut
places.sqlite	https://www.google.com/search?q=hidden+wiki&ie=utf-8…	2018-07-28 15:37:57 IST	http://hackerw6dcplg3ej.onion/	hidden wiki - Google Search
places.sqlite	https://www.google.com/search?client=firefox-b-ab&q=D…	2018-07-28 15:38:34 IST	http://hea2plrgsz45uq6pihxgrudpniunu46xyboyov2sxkes7…	DuckDuckGo - Google Search
places.sqlite	https://duckduckgo.com/	2018-07-28 15:38:44 IST	http://hackerw6dcplg3ej.onion/?c=techbooks	DuckDuckGo — Privacy, simplified.
places.sqlite	https://duckduckgo.com/?q=hiddenwiki&t=h_	2018-07-28 15:40:01 IST	http://hackerw6dcplg3ej.onion/redirect.php?t=hacking-aut…	
places.sqlite	https://duckduckgo.com/?q=hiddenwiki&t=h_&atb=v127-4d_	2018-07-28 15:40:03 IST	http://3kyl4i7bfdgwelmf.onion/	hiddenwiki at DuckDuckGo
places.sqlite	https://duckduckgo.com/?q=hiddenwiki&t=h_&atb=v127-4…	2018-07-28 15:40:12 IST	http://icloud2t6jx3xrb4.onion/	hiddenwiki at DuckDuckGo

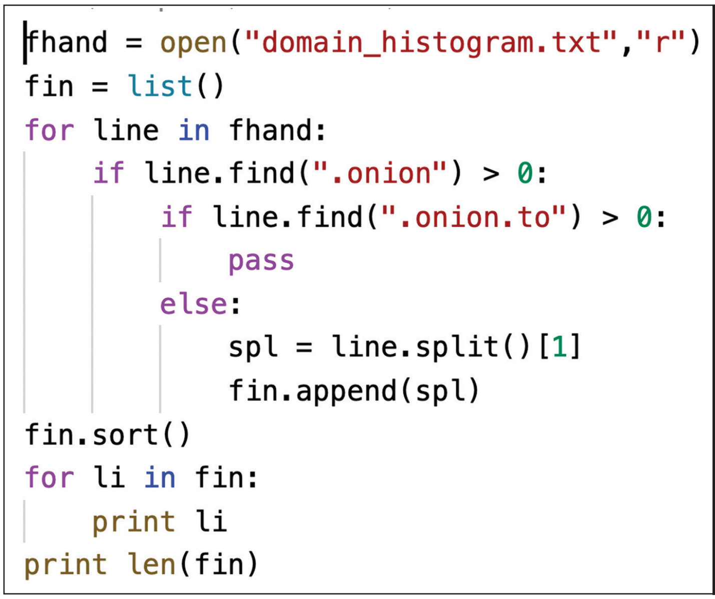
Type	Value	Source(s)
URL	http://www.zqktlwi4fecvo6ri.onion/wiki/Main_Page	RecentActivity
Date Accessed	2018-06-25 16:48:27	RecentActivity
Referrer URL		RecentActivity
Title	The Hidden Wiki	RecentActivity
Program Name	FireFox	RecentActivity
Domain	www.zqktlwi4fecvo6ri.onion	RecentActivity
Source File Path	/img_DImage 1.E01/vol_vol3/root/.mozilla/firefox/jkhsla61.tor/places.sqlite	
Artifact ID	-9223372036854775778	

Figure 2: Detailed information of an onion website accessed from recent activities.



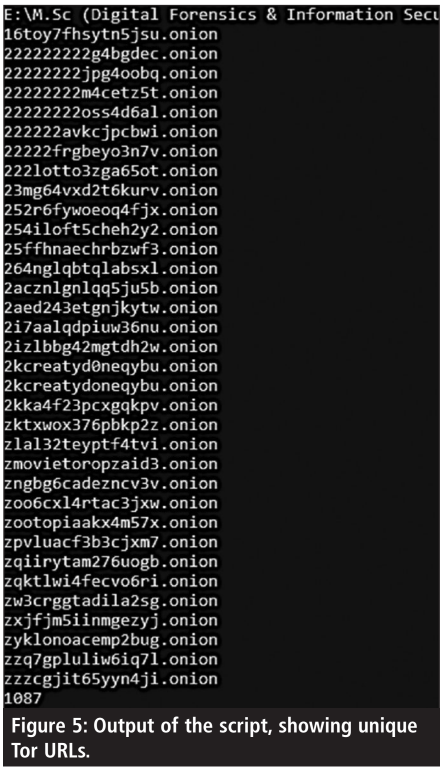
Source File	Domain	Text	Program Name	Date Accessed	Data Source	Tags
places.sqlite	www.google.com	hidden wiki	FireFox	2018-06-25 16:42:55 IST	DImage 1.E01	
places.sqlite	www.google.com	hidden wiki	FireFox	2018-07-28 15:30:51 IST	DImage 1.E01	
places.sqlite	www.google.com	EgTHV5r_GL398NoFIhkA8aeDS3kvbH4sjW9o1myoXqzyo9M…	FireFox	2018-07-28 15:30:52 IST	DImage 1.E01	
places.sqlite	www.google.com	hidden wiki	FireFox	2018-07-28 15:37:57 IST	DImage 1.E01	
places.sqlite	www.google.com	DuckDuckGo	FireFox	2018-07-28 15:38:34 IST	DImage 1.E01	

Figure 3: Search queries.



```
fhand = open("domain_histogram.txt","r")
fin = list()
for line in fhand:
    if line.find(".onion") > 0:
        if line.find(".onion.to") > 0:
            pass
        else:
            spl = line.split()[1]
            fin.append(spl)
fin.sort()
for li in fin:
    print li
print len(fin)
```

Figure 4: Custom script for parsing the domain_histogram.txt file.



```
E:\M.Sc (Digital Forensics & Information Secu
16toy7fhsytn5jsu.onion
22222222g4bgdec.onion
2222222jpg4oobq.onion
2222222m4cetz5t.onion
2222222oss4d6al.onion
222222avkcjpcbwi.onion
22222frgbeyo3n7v.onion
222lotto3zga65ot.onion
23mg64vxd2t6kurv.onion
252r6fywoeoq4fjx.onion
254iloft5cheh2y2.onion
25ffhnaechrbzwf3.onion
264nglqbtqlabsxl.onion
2acznlgnlqq5ju5b.onion
2aed243etgnjkytw.onion
2i7aalqdpiuw36nu.onion
2izlbbg42mgtdh2w.onion
2kcreatyd0neqybu.onion
2kcreatydoneqybu.onion
2kka4f23pcxgqkpv.onion
zktxwox376pbkp2z.onion
zlal32teyptf4tvi.onion
zmovietoropzaid3.onion
zngbg6cadezncv3v.onion
zoo6cxl4rtac3jxw.onion
zootopiaakx4m57x.onion
zpvluacf3b3cjxm7.onion
zqiirytam276uogb.onion
zqktlwi4fecvo6ri.onion
zw3crggtadila2sg.onion
zxjfjm5iinmgezyj.onion
zyklonoacemp2bug.onion
zzq7gpluliw6iq7l.onion
zzzcgjit65yyn4ji.onion
1087
```

Figure 5: Output of the script, showing unique Tor URLs.

open source software for our analysis. We configured the analysis machines with the necessary software, such as Sleuthkit Autopsy. Other required utilities like bulk_extractor and Foremost are bundled with Kali Linux so they required no installation and configuration.

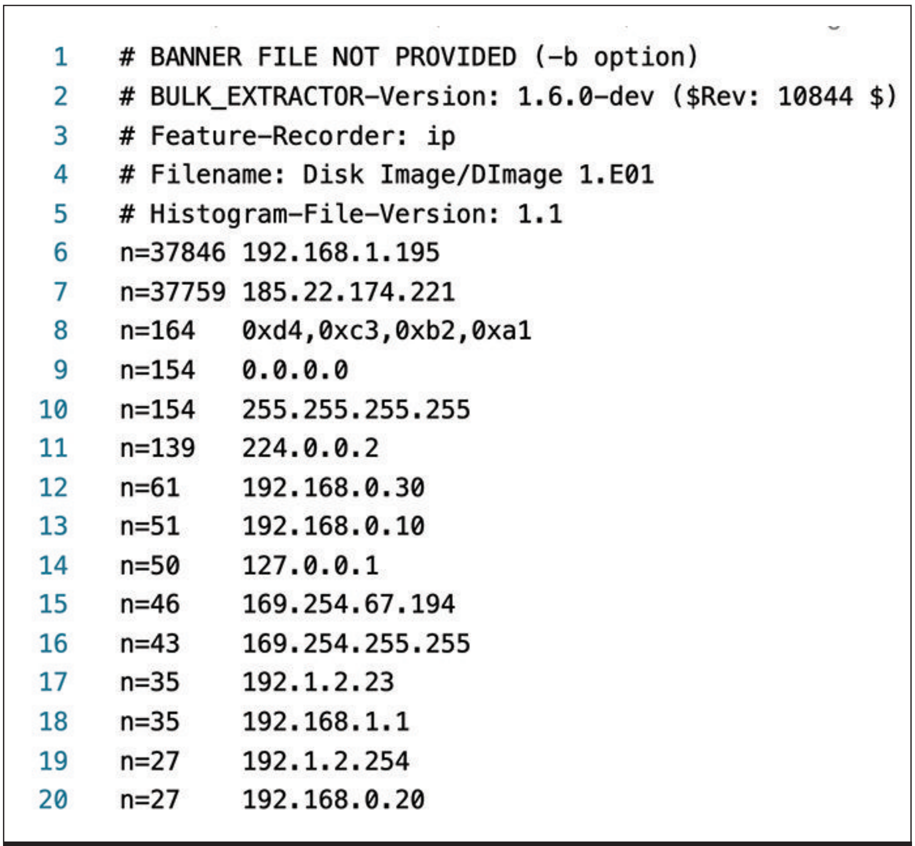
After setting up the target machine (Raspberry Pi), it was used to access darknet websites.

Observations and results

Figures 1-3 show information obtained in an analysis of secondary storage using Sleuthkit Autopsy. The information includes cookies that reveal the URLs of onion sites, specific data on such sites and data on search queries.

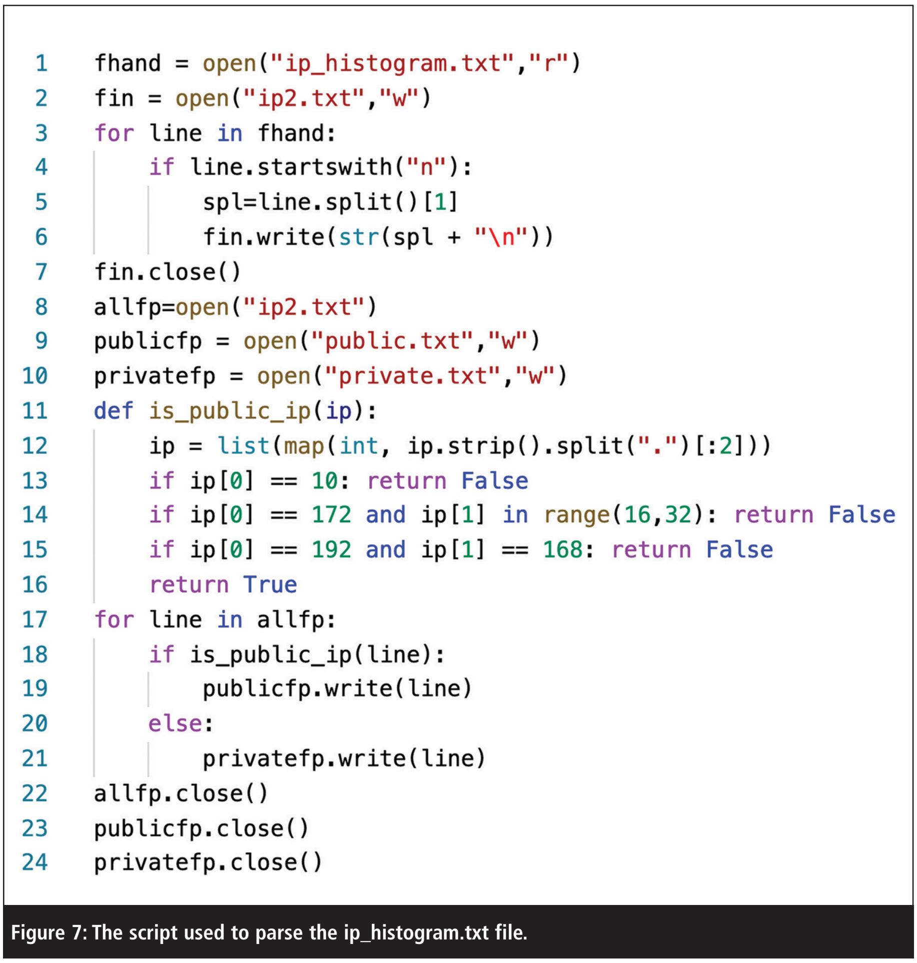
Next, bulk_extractor was used with custom scripts. The tool was employed to extract logical data out of the disk image into a structured text file. In order to extract evidence from the files, custom parsers were created in Python, and some additional open source scripts taken from GitHub were used.

Domain names that were found in an image were saved in a file called



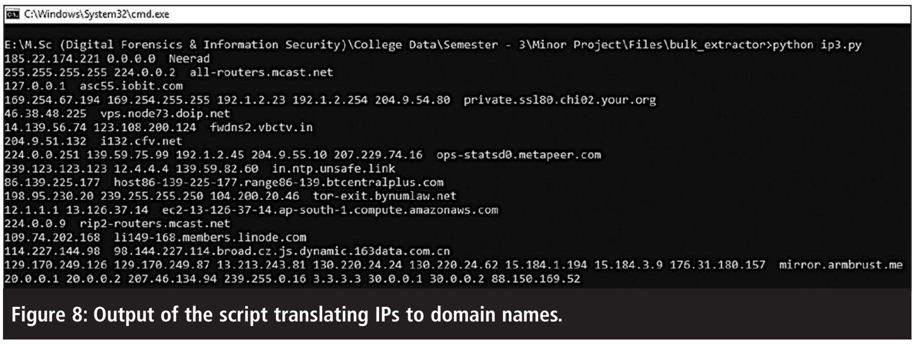
```
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
# Feature-Recorder: ip
# Filename: Disk Image/DImage 1.E01
# Histogram-File-Version: 1.1
n=37846 192.168.1.195
n=37759 185.22.174.221
n=164   0xd4,0xc3,0xb2,0xa1
n=154   0.0.0.0
n=154   255.255.255.255
n=139   224.0.0.2
n=61    192.168.0.30
n=51    192.168.0.10
n=50    127.0.0.1
n=46    169.254.67.194
n=43    169.254.255.255
n=35    192.1.2.23
n=35    192.168.1.1
n=27    192.1.2.254
n=27    192.168.0.20
```

Figure 6: A part of the ip_histogram.txt file.



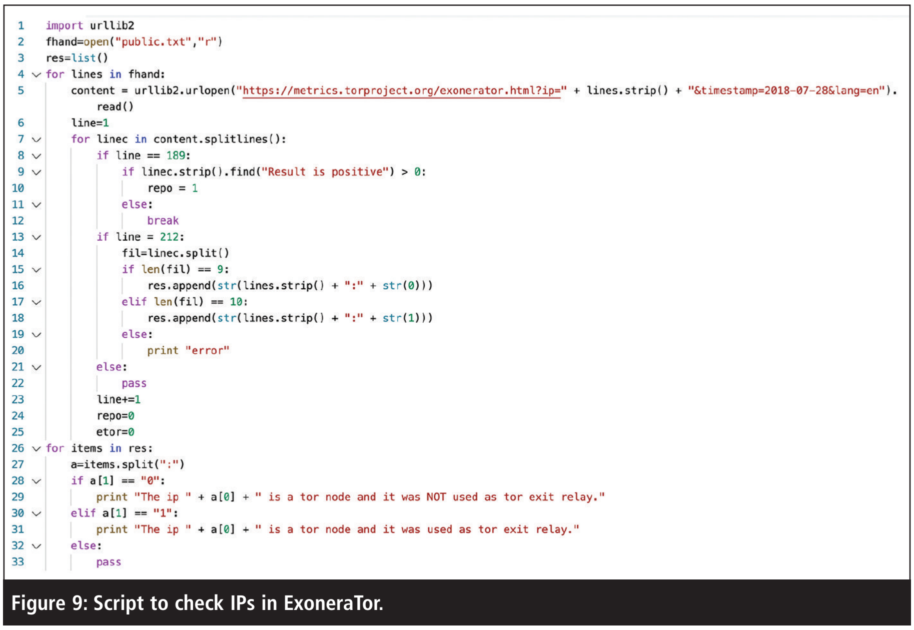
```python
fhand = open("ip_histogram.txt","r")
fin = open("ip2.txt","w")
for line in fhand:
    if line.startswith("n"):
        spl=line.split()[1]
        fin.write(str(spl + "\n"))
fin.close()
allfp=open("ip2.txt")
publicfp = open("public.txt","w")
privatefp = open("private.txt","w")
def is_public_ip(ip):
    ip = list(map(int, ip.strip().split(".")[:2]))
    if ip[0] == 10: return False
    if ip[0] == 172 and ip[1] in range(16,32): return False
    if ip[0] == 192 and ip[1] == 168: return False
    return True
for line in allfp:
    if is_public_ip(line):
        publicfp.write(line)
    else:
        privatefp.write(line)
allfp.close()
publicfp.close()
privatefp.close()
```

Figure 7: The script used to parse the ip_histogram.txt file.



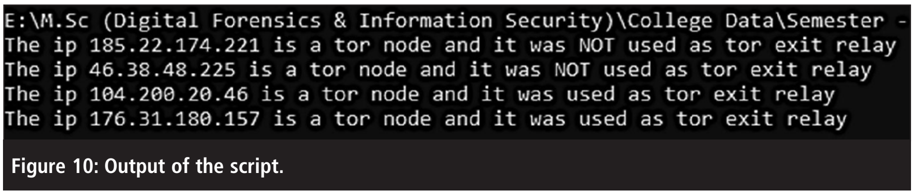
```
C:\Windows\System32\cmd.exe

E:\M.Sc (Digital Forensics & Information Security)\College Data\Semester - 3\Minor Project\Files\bulk_extractor>python ip3.py
185.22.174.221 0.0.0.0  Neerad
255.255.255.255 224.0.0.2  all-routers.mcast.net
127.0.0.1  asc55.iobit.com
169.254.67.194 169.254.255.255 192.1.2.23 192.1.2.254 204.9.54.80  private.ssl80.chi02.your.org
46.38.48.225  vps.node73.doip.net
14.139.56.74 123.108.200.124  fwdns2.vbctv.in
204.9.51.132  i132.cfv.net
224.0.0.251 139.59.75.99 192.1.2.45 204.9.55.10 207.229.74.16  ops-statsd0.metapeer.com
239.123.123.123 12.4.4.4 139.59.82.60  in.ntp.unsafe.link
86.139.225.177  host86-139-225-177.range86-139.btcentralplus.com
198.95.230.20 239.255.255.250 104.200.20.46  tor-exit.bynumlaw.net
12.1.1.1 13.126.37.14  ec2-13-126-37-14.ap-south-1.compute.amazonaws.com
224.0.0.9  rip2-routers.mcast.net
109.74.202.168  li149-168.members.linode.com
114.227.144.98  98.144.227.114.broad.cz.js.dynamic.163data.com.cn
129.170.249.126 129.170.249.87 13.213.243.81 130.220.24.24 130.220.24.62 15.184.1.194 15.184.3.9 176.31.180.157  mirror.armbrust.me
20.0.0.1 20.0.0.2 207.46.134.94 239.255.0.16 3.3.3.3 30.0.0.1 30.0.0.2 88.150.169.52
```

Figure 8: Output of the script translating IPs to domain names.



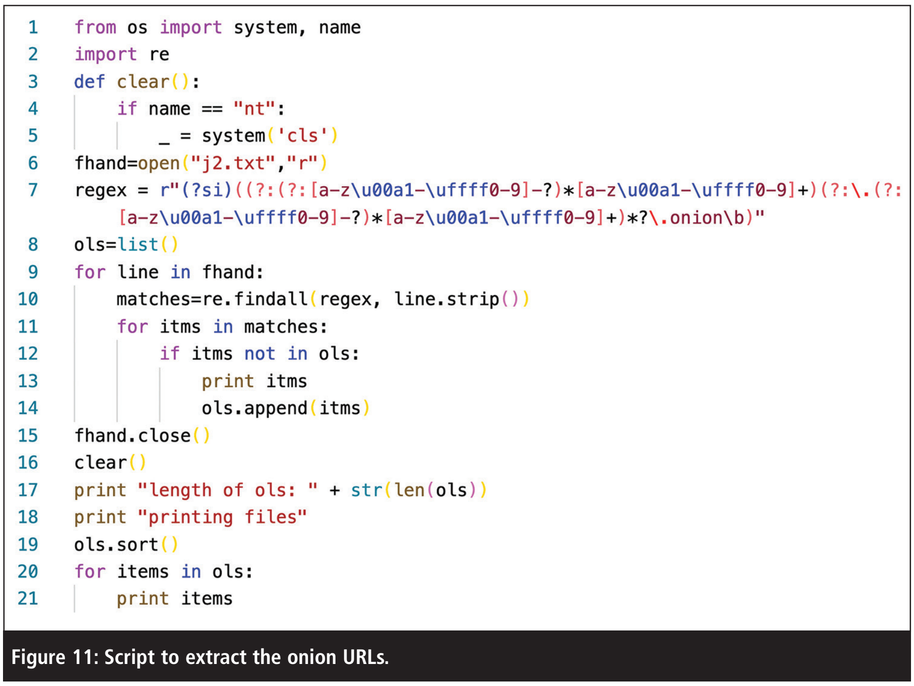
```python
import urllib2
fhand=open("public.txt","r")
res=list()
for lines in fhand:
    content = urllib2.urlopen("https://metrics.torproject.org/exonerator.html?ip=" + lines.strip() + "&timestamp=2018-07-28&lang=en").
        read()
    line=1
    for linec in content.splitlines():
        if line == 189:
            if linec.strip().find("Result is positive") > 0:
                repo = 1
            else:
                break
        if line = 212:
            fil=linec.split()
            if len(fil) == 9:
                res.append(str(lines.strip() + ":" + str(0)))
            elif len(fil) == 10:
                res.append(str(lines.strip() + ":" + str(1)))
            else:
                print "error"
        else:
            pass
        line+=1
        repo=0
        etor=0
for items in res:
    a=items.split(":")
    if a[1] == "0":
        print "The ip " + a[0] + " is a tor node and it was NOT used as tor exit relay."
    elif a[1] == "1":
        print "The ip " + a[0] + " is a tor node and it was used as tor exit relay."
    else:
        pass
```

Figure 9: Script to check IPs in ExoneraTor.



```
E:\M.Sc (Digital Forensics & Information Security)\College Data\Semester -
The ip 185.22.174.221 is a tor node and it was NOT used as tor exit relay
The ip 46.38.48.225 is a tor node and it was NOT used as tor exit relay
The ip 104.200.20.46 is a tor node and it was used as tor exit relay
The ip 176.31.180.157 is a tor node and it was used as tor exit relay
```

Figure 10: Output of the script.



```python
from os import system, name
import re
def clear():
    if name == "nt":
        _ = system('cls')
fhand=open("j2.txt","r")
regex = r"(?si)((?:(?:[a-z\u00a1-\uffff0-9]-?)*[a-z\u00a1-\uffff0-9]+)(?:\.(?:
    [a-z\u00a1-\uffff0-9]-?)*[a-z\u00a1-\uffff0-9]+)*?\.onion\b)"
ols=list()
for line in fhand:
    matches=re.findall(regex, line.strip())
    for itms in matches:
        if itms not in ols:
            print itms
            ols.append(itms)
fhand.close()
clear()
print "length of ols: " + str(len(ols))
print "printing files"
ols.sort()
for items in ols:
    print items
```

Figure 11: Script to extract the onion URLs.

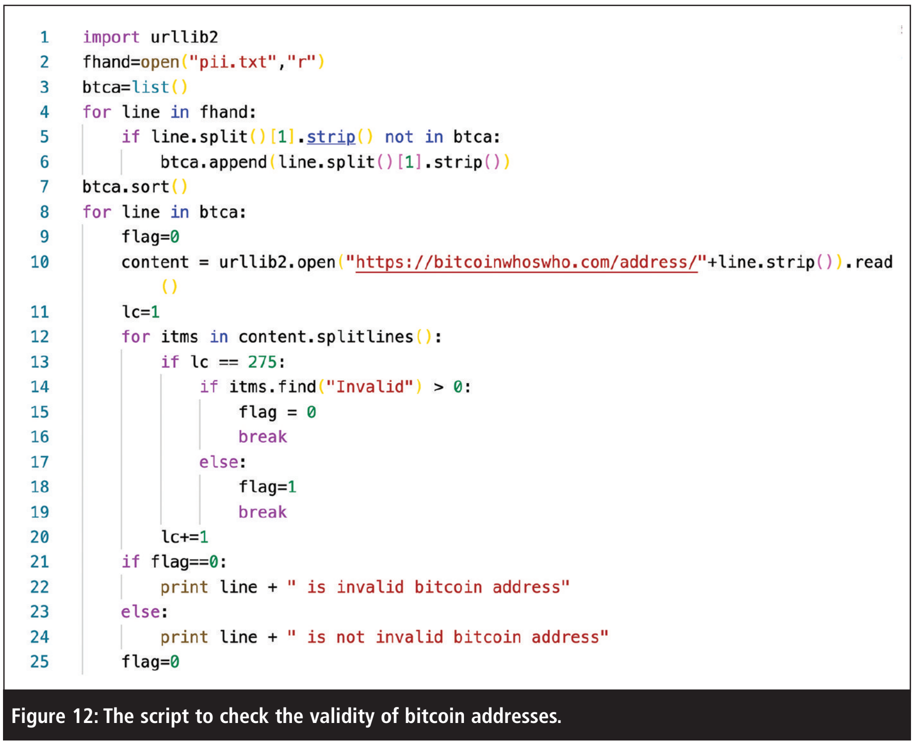
domain_histogram.txt. This list was sorted, using the script in Figure 4, in descending order, with the total number of occurrences being stored with each domain.

Similarly, IP addresses that were found in the disk image were saved in the file ip_histogram.txt file, which was sorted in descending order along with the total number of occurrences of each IP. The task was to find the IP addresses that belong to the Tor network. First we tried to separate public and private IP addresses and, after separating them, we checked to see if any IP had been used as a Tor node. As discussed earlier, a custom script written by us in combination with existing open source scripts was used to achieve the required information.

A script taken from GitHub (https://gist.github.com/DamnedFacts/5058978) was used to obtain domain names from the IP addresses. The output of the script is shown in Figure 8. As you can see above, the IP address 104.200.20.46 refers to tor-exit.bynumlaw.net.

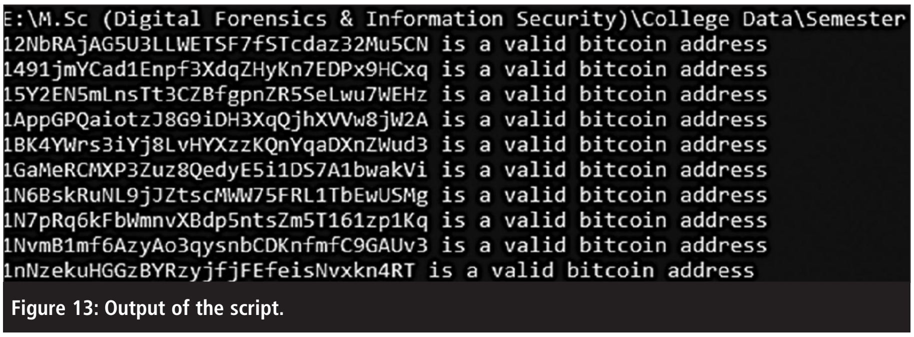
"ExoneraTor may store more than one IP address per relay if relays use a different IP address for exiting to the Internet than for registering in the Tor network, and it notes whether a relay permitted the transit of Tor traffic to the open Internet at that time"

We used another service called the ExoneraTor service, which maintains a database of IP addresses that have been part of the Tor network. It answers the question of whether there was a Tor relay running on a given IP address on a given date. ExoneraTor may store more than one IP address per relay if relays use a different IP address for exiting to the Internet than for registering in the Tor network, and it notes whether a relay permitted the transit of Tor traffic to the open Internet at that time. ExoneraTor



```
import urllib2
fhand=open("pii.txt","r")
btca=list()
for line in fhand:
    if line.split()[1].strip() not in btca:
        btca.append(line.split()[1].strip())
btca.sort()
for line in btca:
    flag=0
    content = urllib2.open("https://bitcoinwhoswho.com/address/"+line.strip()).read
    ()
    lc=1
    for itms in content.splitlines():
        if lc == 275:
            if itms.find("Invalid") > 0:
                flag = 0
                break
            else:
                flag=1
                break
        lc+=1
    if flag==0:
        print line + " is invalid bitcoin address"
    else:
        print line + " is not invalid bitcoin address"
    flag=0
```

Figure 12: The script to check the validity of bitcoin addresses.



```
E:\M.Sc (Digital Forensics & Information Security)\College Data\Semester
12NbRAjAG5U3LLWETSF7fSTcdaz32Mu5CN is a valid bitcoin address
1491jmYCad1Enpf3XdqZHyKn7EDPx9HCxq is a valid bitcoin address
15Y2EN5mLnsTt3CZBfgpnZR5SeLwu7WEHz is a valid bitcoin address
1AppGPQaiotzJ8G9iDH3XqQjhXVVw8jW2A is a valid bitcoin address
1BK4YWrs3iYj8LvHYXzzKQnYqaDXnZWud3 is a valid bitcoin address
1GaMeRCMXP3Zuz8QedyE5i1DS7A1bwakVi is a valid bitcoin address
1N6BskRuNL9jJZtscMWW75FRL1TbEwUSMg is a valid bitcoin address
1N7pRq6kFbWmnvXBdp5ntsZm5T161zp1Kq is a valid bitcoin address
1NvmB1mf6AzyAo3qysnbCDKnfmfC9GAUv3 is a valid bitcoin address
1nNzekuHGGzBYRzyjfjFEfeisNvxkn4RT is a valid bitcoin address
```

Figure 13: Output of the script.

provides a web interface to check the IP and confirms, for example, whether the IP has been used as a Tor exit relay.

To automate the task, a script was written (see Figure 9) that called the ExoneraTor API to check whether the provided IP had been used as a Tor node. The output of this script is shown in Figure 10.

A file called json.txt file was created to contain all Json objects present in the disk image. This json.txt file contained 8,327 lines. A simple script was created to filter out the lines that contained '.onion' in the string, and these were saved in a different file.

After narrowing down the lines of interest, another script was used to filter out the unique Tor website's URL. For that, the script uses a regular expression (regex) to filter out the URLs from Json objects.

"Even if a criminal uses very advanced techniques to maintain anonymity, he leaves many traces behind. Having knowledge of the techniques by which these crucial traces can be recovered can help an investigating officer in solving a crime with more confidence "

A pii.txt file was created that contained any personally identifiable information extracted from the disk image. In this case, this file contained bitcoin addresses. To extract the bitcoin addresses and check the validity of each one, we used an API call to bitcoinshossho.com. The script is shown in Figure 12 and the output in Figure 13.

Extracting images

Foremost was used to extract image files from the disk image. These images are automatically downloaded images while surfing the dark web. Foremost has recovered images that have porn content, images of real accidents, images of real autopsies, images of guns, images of drugs, images of murders, images of forged passports, images of forged driving licences etc. Some of them are shown in Figure 14.

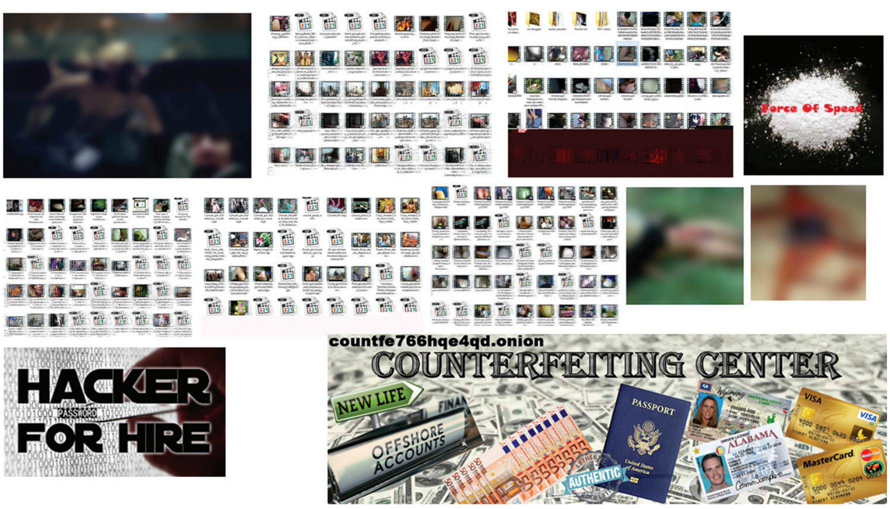


Figure 14: Examples of images extracted using Foremost.

Conclusion

The work discussed in this article clearly indicates that even if a criminal uses very advanced techniques to maintain anonymity, he leaves many traces behind. Having knowledge of the techniques by which these crucial traces can be recovered can help an investigating officer in solving a crime with more confidence. We expect that the work published in this article will be useful to investigators in handling these types of crimes more accurately and efficiently.

About the authors

Neerad Vaidya obtained a bachelor degree in computer applications from Krantigu Shyamji Krishna Verma Kachchh University, Gujarat, India. He is currently pursuing an Msc in digital forensics and information security from Gujarat Forensic Sciences University, Gandhinagar, India. His research areas of interest are cyber security, digital forensics, secure source code reviewing and vulnerability assessment and penetration testing.

Dr Parag H Rughani obtained his PhD in computer science from Saurashtra University. He is currently working as an associate professor in digital forensics at the Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar. He has more than 14 years of teaching experience and has published more than 15 research papers in reputed international journals. His areas of expertise include machine learning, digital forensics, memory forensics, malware analysis and IoT security and forensics.

References

1. Mahajan, S; Adagale, AM; Sahare, C. ‘Intrusion detection system using Raspberry Pi honeypot in network security’. International Journal of Engineering Science, 2792, 2016.
2. Raja, AA; Naveedha, R; Niranjanadevi, G; Roobini, V. ‘An Internet of Things (IoT) based security alert system using Raspberry Pi’. Asia Pacific International Journal of Engineering Science, 2(01), 37-41, 2016.
3. Karmakar, KK; Varadharajan, V; Tupakula, U; Hitchens, M. (2016, April). ‘Policy based security architecture for software defined networks’. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Apr 2016, pp.658-663.
4. Feng, X; Babatunde, O; Liu, E. ‘Cyber security investigation for Raspberry Pi devices’. International Refereed Journal of Engineering and Science, 2017.
5. Williams, M. ‘A risk assessment on Raspberry Pi using NIST standards’. International Journal of Computer Science and Network Security, vol.15, no.6, June 2015.
6. Lim, C; Marcello, M; Japar, A; Tommy, J; Kho, IE. ‘Development of Distributed Honeypot Using Raspberry Pi’. In International Conference on Information, Communication Technology and System, Sep 2014.
7. Wang, X; Zhou, Q; Harer, J; Brown, G; Qiu, S; Dou, Z; Wang, J; Hinton, A; Aguayo Gonzalez, C; Chin, P. ‘Deep learning-based classification and anomaly detection of side-channel signals’. In Cyber Sensing 2018, vol.10630, p.1063006. International Society for Optics and Photonics, 2018.
8. Lalitha, M; Meachery, N; Nair, R. ‘Raspberry Pi based cyber-defensive industrial control system with redundancy and intrusion detection’. International Journal of Pure and Applied Mathematics, 118(20), 4273-4278, 2018.
9. McCoy, D; Bauer, K; Grunwald, D; Kohno, T; Sicker, D. ‘Shining light in dark places: Understanding the Tor network’. In International Symposium on Privacy Enhancing Technologies, Jul 2008, July, pp.63-76. Springer.
10. Jansen, R; Tschorsch, F; Johnson, A; Scheuermann, B. ‘The sniper attack: Anonymously deanonymizing and disabling the Tor network’. Office of Naval Research, Arlington, VA, 2014.
11. Dolliver, DS. ‘Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel’. International Journal of Drug Policy, 26(11), 1113-1123, 2015.
12. Perry, M. ‘Torflow: Tor network analysis’. In proceedings 2nd HotPETs, 1-14, 2009.
13. Chaabane, A; Manils, P; Kaafar, MA. ‘Digging into anonymous traffic: A deep analysis of the tor anonymizing network’. In 2010 Fourth International Conference on Network and System Security, Sep 2010, pp.167-174, IEEE.
14. Dolliver, DS; Kenney, JL. ‘Characteristics of drug vendors on the Tor network: A cryptomarket comparison’. Victims & Offenders, 11(4), 600-620, 2016.
15. Munksgaard, R; Demant, J; Branwen, G. ‘A replication and methodological critique of the study “Evaluating drug trafficking on the Tor Network”‘. International Journal of Drug Policy, 35, 92-96, 2016.

The Sandbox

Are your credentials really safe?

Daniel Solís, Blueliv

With so much more activity online during the current pandemic, from home working to online shopping, the risks are multiplying and cyber criminals are looking for ways to exploit every opportunity to get their hands on key credentials.

Make no mistake – cyber criminals steal credentials to make a profit. From blackmail and ransom, through to selling sensitive information on the dark web, there's nothing hackers won't do to ensure they get a return on investment for their efforts. Tactics that cyber criminals use include malware infections, phishing, DNS hijacking, leaked databases and social engineering. What's more, the hackers that steal the credentials are usually not the same ones that use them.

Once credentials are captured, they can be used in a variety of ways, depending on their type. For example, in the retail sector, leveraging corporate account credentials allows serious intrusions into the organisation or the chance to impersonate real customers to steal goods and services by using personal emails and payment details. Unfortunately, while customers have to face the worry of where and how their data is being used, it is the corporate offering the service or goods that will usually shoulder the cost of any fraudulent transaction.

There are some key things to understand. Cyber criminals see more value in one solid corporate credential than thousands of records from unreliable leaks. Corporate credentials from VIPs or assets are the most valuable, fetching a fair price on the black market. The fresher the credential, the better. A recently compromised credential means a higher chance that the cyber criminals can achieve their financial objectives. It is even better if the credential has been compromised without alerting the affected user. And cyber criminals don't use data in real time: unless they're compromised in highly targeted attacks, hackers need time to analyse the reams of data they capture, filter out the prime credentials and sell the data that they are not going to exploit themselves.

Having access to an account of a retailer or e-commerce company normally allows the attacker to perform purchases using the stolen account balance or configured payment method. Depending on the balance and how quickly purchases are performed, the loss will have a different impact. Each retailer or e-commerce company will have its own policy in case of fraudulent transactions, but normally reporting it as soon as it happens could help to recover most of it (chargeback).

On the other hand, if the victim reports this quickly, but the purchase is already shipped, then the company will lose money, which will cause a big impact if many customers do it. This kind of attack is usually carried out by threat actors who want to get a quick win.

Professional criminals could use those accounts to transfer stolen money, or use stolen credit cards to purchase goods, shipping them to mules who will reship the goods to an anonymous postal address belonging to the bad guys. This is a way for criminals to launder their money.

Depending on the organisation, additional fraudulent activities could be performed once the attacker has access to an account, such as taking advantage of reward points or gift cards.

With so many employees working from home and an increase in online shopping, education is key to mitigating attacks. Under no circumstances should an IT security team be the only group within a company that knows how to identify potentially malicious activity. Once credential theft has occurred, it is likely that it will be all hands on deck to find the hole and plug it, fast.

EVENTS

Due to the Covid-19 pandemic, many conferences are being cancelled, postponed or converted into virtual events. The events listed here were still planned to proceed at the time of publication.

1–6 August
Black Hat USA
Virtual conference
www.blackhat.com/us-20/

6–9 August
DEF CON Safe Mode
Virtual conference
www.defcon.org

1 October 2020
ArcticCon
Anchorage, Alaska
https://arctic-con.com

6–8 October 2020
Critical Infrastructure Protection & Resilience Europe
Bucharest, Romania
www.cipre-expo.com

7–8 October 2020
International Cybersecurity & Intelligence Conference (ICSIC)
Toronto, Canada
https://www.icsicanada.org

8 October 2020
Florida Cyber Conference
Orlando, Florida, US
https://flcybercon.com

14–16 October 2020
International Conference on Digital Forensics & Cyber Crime (ICDF2C)
Boston, US
http://icdf2c.org

20–21 October 2020
600Minutes Information and Cyber Security
Stockholm, Sweden
https://bit.ly/3bNwTcr