The Supply Chain Problem - Whitepaper

Jonathan Davies, CTO Pervade Software

Background

On April 3rd 2016 the first of 11.5 million documents, amounting to over 2.5 terabytes of data, began to be published by journalists around the world. The documents, leaked by an anonymous hacker to a German journalist, contained personal financial information about wealthy individuals and public officials including presidents, prime ministers, and royalty from around the world as well as offshore financial records for over 200,000 of the largest companies in the world.

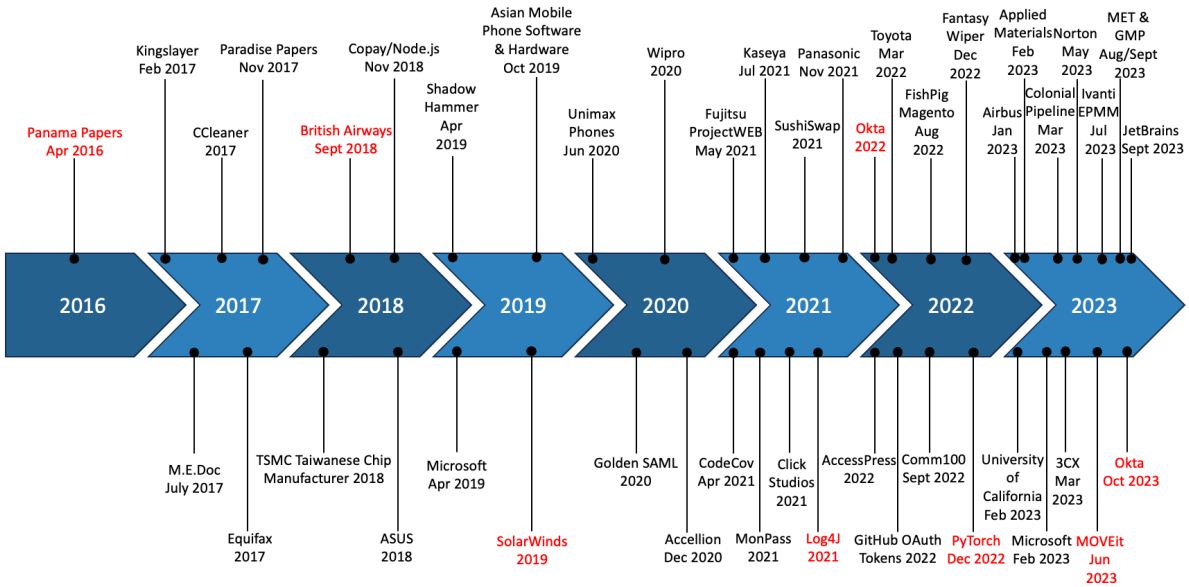
Two days before the publication started a small law firm in Panama named Mossack Fonseca, who specialised in the creation and management of offshore companies, notified their clients that they had been hacked. This list of clients included former UK prime minister David Cameron, former Argentinian president Mauricio Macri, former Sudanese president Ahmed al-Mirghani, President Khalifa bin Zayed Al Nahyan of the United Arab Emirates and King Salman of Saudi Arabia as well as the children and immediate relatives of China's paramount leader Xi Jinping, former prime minister of Pakistan Nawaz Sharif, former South African president Jacob Zuma, former United Nations Secretary-General Kofi Annan and the former UK prime minister Margaret Thatcher.

The data leaked detailed offshore shell companies that had been set up by Mossack Fonseca for their clients to serve a range of purposes, some legal and some not. These included fraud, tax evasion and evading international sanctions.

Mossack Fonseca explained to their customers that they had fallen victim to an email-based attack. However, in the immediate aftermath of the attack, information security experts from around the world began to comment on the law firm's very poor cyber security. Simply by running scans of the firm's Internet facing systems these experts were able to identify that the firm was running a very out-dated version of Drupal on an even more outdated Apache web server and on April 12th 2016 a grey-hat hacker announced that they had been able to access customer data because the company was vulnerable to SQL Injection, a very well-known web server vulnerability.

The data leaked by the anonymous hacker impacted some of the most influential individuals and companies in the world, people and organisations that pay vast sums of money to ensure their data is private. Whether intentional or not, this hacker identified and widely publicised something that would change the face of digital crime forever - no matter how large and well protected your target, the people they trust their information to may not be as well protected.

Immediately following this 2016 hack which became known as "The Panama Papers" many law firms around the world became the focus of sophisticated cyber-attacks targeting the data of clients they serve. Whilst supply chain attacks were not invented in 2016 it was clear this attack sparked a new trend that would last. This trend has continued and appears to still be accelerating with more and more organisations falling victim to supply chain attacks every year since 2016.



This chart shows some of the more notable supply chain cyber attacks to have occurred since 2016, with the most severe attacks shown in red.

It is not just the rate of supply-chain attacks that is increasing, but also the severity. The SolarWinds attack in 2020 broke new ground when attackers hacked into the Texas-based software company and injected malicious code into it's popular Orion product. The malicious code was pushed down to over 18,000 of it's customers including Cisco, Department of Defence,

Deloitte, Intel, Microsoft, Department of Energy, Department of Health and the Department of Homeland Security as a legitimate patch. SolarWinds Orion is an IT network monitoring/management software, this meant that attackers not only gained control of the servers running this software but also gained access to the servers being monitored and managed by this software. This attack, since attributed to a Russian Advanced Persistent Threat (APT) hacking group known as CozyBear (APT29), is regarded to be the largest single compromise of western government organisations in history.

Not all of these cyber supply-chain attacks have been strictly IT related however, for example, in 2023 both the London Metropolitan Police and the Greater Manchester Police announced data leaks whereby hackers had obtained the personal information of civilian staff and police officers in their employ. Both forces have dedicated information security professionals and have deployed market leading cyber security software to stop attackers getting in. Unfortunately, the hackers had found that the companies that print the physical ID access cards for the forces did not have the same level of sophisticated cyber protections in place and therefore made far easier targets.

The Problem

Larger organisations, whether public or private, have responsibility to protect their IT networks and customer data, whether motivated by the risk of the commercial impact of a cyber event or by regulatory requirements. This leads to those organisations employing teams of dedicated experts and purchasing the latest cyber security technologies to protect themselves against cyber threat actors.

The UK's National Cyber Security Centre (NCSC) posits that organisations can protect themselves against 80% of cyber attacks by implementing very simple cyber security controls such as properly installing and configuring a firewall, installing Anti-Virus software, using strong passwords and ensuring that users don't use privileged accounts for their normal day-to-day work. The vast majority of malicious hacking techniques look for organisations that have not properly implemented these basic controls as low-hanging fruit. Large organisations will implement these basic controls and then further controls to combat more sophisticated cyber attacks, the top 20%.

The cyber threat landscape is not a single attack surface, it is multiple surfaces that are both inside and outside the organisation. Organisations have both internal and external users that have varying levels of access to IT resources and data, to effectively defend an organisation against cyber-attacks, users are grouped and assigned different levels of access and trust based on the risk they pose to the organisation.

For example, external users of the company website are typically provided with the minimum level of access and trust, they are permitted to use a single protocol to access a single application that can only read data. At the other end of the scale, an IT administrator will be given maximum privileges to access equipment and data to help other users when they have problems. If an external website user is infected with malware when they access the company website it is very unlikely to have any affect, however if an IT administrator's laptop becomes infected with malware (such as ransomware) it is likely to be able to infect every device in the company in minutes. These example users pose a very different risks and large organisations have different policies controlling the level of trust and therefore the level of access they are given. Similarly, these users will have different expectations placed upon them to protect the organisation, for example an external website user will have no expectations and it should be assumed their device may be infected with malware, however an IT administrator will be expected to only access the IT network using company equipment which is running the latest anti-malware software, will be expected to use multi-factor authentication to prove their identity and will be expected to have a high level of IT maturity, for example not to fall for obvious phishing email scams.

The two examples given so far are clear-cut and easy to manage, but issues arise as the examples get more complex. For example, somebody in accounts that cannot be relied upon to be IT savvy but who has access to extremely sensitive information, or a consultant to the IT team who works from their own laptop device to help implement a project. Most of an organisation's supply chain fall into these grey areas and it is very common for suppliers to be given access to high risk equipment and data. Some examples of this may include:-

- Providing personal information of all staff to an accountant
- Putting commercially sensitive information about products as well as personal information about customers into a cloud-based CRM system
- Providing the most sensitive of information to a law firm
- Allowing an IT managed service provider to maintain a direct connection to corporate IT network in order to provide their service
- Providing administrator level access to contract IT support staff

Every company on the FTSE 100 index, large organisation and every government department have suppliers, contractors and consultants that they allow to access their confidential information and IT systems. Unfortunately, auditing the cyber security protections in place at every supplier individually can prove costly and enforcing the use of large industry standards such as ISO-27001 is not feasible given the high volume of SME suppliers.

A recent government report shows that in 2023 the UK has just over 8,000 businesses that are classified as large (250+ employees) and over 5.5 million businesses that are small and medium (SME) sized, meaning that 99% of business are SMEs and they account for over 90% of all trade, many of the SMEs are the supply chain of the large companies.

Small organisations, who cannot afford dedicated cyber security staff or the latest cyber security technologies, rarely have any expectation of cyber defence placed upon them. The organisational structure of micro companies (less than 10 staff) for example means that it is very common for everyone in the organisation to have privileged access to most if not all data/equipment and their flat network structure mean that if one staff member gets infected with malware it is very likely that the whole company can become infected quickly.

With smaller organisations being less likely to have implemented even basic cyber security controls they are a far easier target for malicious hackers. Hackers target them not to attack the small organisations, but to use them to compromise larger organisations, either in a direct supply-chain attack or by using them in large "botnets", army's of small compromised computer devices used in coordinated attacks without their knowledge such as the Distributed Denial of Service (DDoS) attack against the BBC in February 2020 which set the record for the largest ever DDoS attack at over 2.3Tbps.

The trend of increasing frequency and sophistication of supply chain attacks poses an important risk for large organisations, who must not only protect their own IT infrastructure but must ensure the organisations that they share data with, or that they provide IT network access to, take the same care to protect any data and privilege shared with them. Larger organisations need to be confident that they can trust their suppliers and properly assess their associated risk. In order to secure the top 1% of UK companies, government departments and Critical National Infrastructure (CNI), as a nation we must sure up the security of the bottom 99% because they form critical links in the supply chain.

The Response

Fortunately for citizens, companies and government organisations of the UK, the government, the NCSC and the Police have all launched schemes to help small organisations become more cyber aware and cyber secure. These schemes provide quantitative measurements to larger organisations to help them better manage their supply-chain risk.

The UK's NCSC's offers a number of quality free tools, particularly to government organisations, in addition to their revolutionary Cyber Essentials scheme. Run by The IASME Consortium on behalf of NCSC, the scheme will be celebrating it's 10th anniversary in 2024. Organisations complete either an online assessment, or an on-site audit in the "Plus" version, to attest that they have essential cyber protections (detailed in the questions) in place and they receive a certificate if they do. This simple idea provides businesses of all sizes with an easy-to-use and low-cost introduction to and assessment of the cyber protections and allows larger organisations to insist that their supply chain have this certification as a minimum standard.

Organisations who have passed Cyber Essentials are said to have protected themselves against the 80% of cyber-attack methods, just by ensuring the basics are done properly. Additionally, in their 2023 annual review NCSC state that "80% fewer cyber insurance claims are made when Cyber Essentials is in place", this is because most cyber-attacks target simple misconfigurations and errors that the Cyber Essentials controls protect against.

The UK Police run a service aimed at UK businesses and government bodies which is free to use and complimentary to the NCSC services. Police CyberAlarm is a technical solution that provides gateway security monitoring and vulnerability scanning to any organisation that wants it. This service, funded by the Home Office and managed by the National Police Chief's Council (NPCC), provides visibility of cyber-attacks and potential vulnerabilities to organisations that would not ordinarily have access to these tools or information.

The goal of the service being to make small companies aware of cyber and give them the information they need to protect themselves against attackers on the Internet. With thousands of UK organisations already signed up, the scheme is growing rapidly year-on-year. In addition to helping the organisations that sign up to protect themselves, the scheme also helps UK Police to get a near-real-time insight into how UK organisations are being attacked which in turn helps the Police cyber experts to issue more relevant and helpful advice to the public.

These government backed services are deliberately targeted at small and medium enterprises that would not normally pay attention to their cyber security, they promote awareness of cyber security and give these organisations the tools needed to protect themselves better at a free or low-cost price point. By helping the smallest 99% of companies to protect themselves against over 80% of cyber-attacks these schemes greatly reduce the risk of the top 1% of companies as well as the government organisations and critical national infrastructure that rely on them in their supply chain.

The tangible benefits of these schemes can be seen by those that have embraced them. In the case of Police CyberAlarm the Department for Education (DfE) made registration for the scheme mandatory for organisations to qualify for it's Risk Protection Assurance (RPA), since then thousands of live critical vulnerabilities have been detected and resolved, multiple

cyber attacks have been prevented and where attacks have happened Police have had data to investigate which is not normally the case when small organisations are attacked. Cyber Essentials, which has been made a requirement under the tender purchasing processes of many large companies and government departments has clearly demonstrated it's effectiveness in both improving the security of small organisations and in allowing large organisations to better quantify their risk by ensuring their whole supply chain is protecting itself against 80% of cyber attacks.

Conclusion

In order to help mitigate their own risks large enterprises should actively promote these free and low-cost government schemes to help their supply chain become more cyber aware and cyber secure. Large organisations could educate their suppliers that the schemes exist, provide links to their websites, and even require enrolment in the schemes as part of supplier agreements where data security is a priority.

Government departments should be setting an example for enterprise and enhancing the effectiveness of these schemes to maximise the investment being made by other areas of government. Using the work already done by the DfE as a case study, other departments should require GP Surgeries, Job Centres, Ambulance Services, Train Operating Companies, Councils, Port Authorities, and other small operating units to register for participation in these and other free government-backed services. Much like schools these small organisations, though part of larger departments, typically operate with a degree of autonomy that means they cannot afford to deploy dedicated cyber security specific technologies or staff. Requiring enrolment in these schemes will cost little to nothing, will actively improve the cyber security of the organisations and will benefit the government departments running the schemes.

In addition to enrolling small government organisations in these schemes, all government departments should recommend and, in some cases, require enrolment in these schemes to their supply chain. Government departments can quantifiably reduce the risk their supply chains represent in an easy, inexpensive way that is achievable for SMEs and can be rolled out with minimal effort.

If large companies and government organisations work together, it is possible to raise the cyber bar of the smallest 99% of companies in the UK that make up the supply chain to the top 1%. The resources required to do this are already available, low cost and proven to be effective.

The UK government, NCSC and Police are all leading the world in creating schemes specifically designed to address the issue of poor cyber security among SMEs in the supply chain, made viable by the benefits that they bring to the departments funding them. Making better use of these schemes in a coordinated effort to raise the minimum level of cyber security throughout UK organisations is the fastest, cheapest and most effective way to lower the overall risk of cyber attacks on the UK.

Appendix A – List of Cyber Supply Chain Attacks

2016	
April 2016	Panama Paper
2017	
February 2017	Kingslayer
July 2017	M.E.Doc
November 2017	Paradise Papers
2017	CCleaner
2017	Equifax
2018	
September 2018	British Airways
November 2018	Copay/Node.js
2018	TSMC Taiwanese Chip Manufacturer
2018	ASUS
2019	
April 2019	Shadow Hammer
April 2019	Microsoft
October 2019	Asian Mobile Phone Software & Hardware
2019	SolarWinds
2020	
June 2020	Unifax Phones
December 2020	Accellion
2020	Wipro
2020	Golden SAML
2021	
April 2021	CodeCov
May 2021	Fujitsu ProjectWEB
July	Kaseya
November 2021	Panasonic
2021	MonPass
2021	SushiSwap
2021	Click Studios
2021	Log4J
2022	
March 2022	Toyota
August 2022	FishPig Magento
September 2022	Comm100
December 2022	Fantasy Wiper
December 2022	PyTorch
2022	Okta
2022	AccessPress
2022	GitHub OAuth Tokens
2023	
January 2023	Airbus
February 2023	University of California
February 2023	Applied Materials
February 2023	Microsoft
March 2023	Colonial Pipeline
March 2023	3CX
May 2023	Norton
June 2023	MOVEit
July 2023	Ivanti EPMM
August/September 2023	MET/GMP
September 2023	JetBrains
October 2023	Okta

Appendix B – Useful Links

Police CyberAlarm
https://www.cyberalarm.police.uk/

Cyber Essentials
https://www.ncsc.gov.uk/cyberessentials/overview

IASME Consortium
https://iasme.co.uk/

NCSC
https://www.ncsc.gov.uk/

Panama Papers - 2016
https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

https://www.bbc.co.uk/news/world-35954224

British Airways – 2018

https://www.bbc.co.uk/news/technology-54568784

https://www.ncsc.gov.uk/guidance/ncsc-advice-british-airways-customers

SolarWinds – 2019

https://www.fortinet.com/uk/resources/cyberglossary/solarwinds-cyber-attack

https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery/

Log4J - 2021

https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

https://thehackernews.com/2021/12/extremely-critical-log4j-vulnerability.html

Okta – 2022

https://www.okta.com/uk/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/

https://www.bleepingcomputer.com/news/security/oktas-source-code-stolen-after-github-repositories-hacked/

PyTorch – 2022

https://www.bleepingcomputer.com/news/security/pytorch-discloses-malicious-dependency-chain-compromise-over-holidays/

https://www.securityweek.com/malware-delivered-pytorch-users-supply-chain-attack/

MOVEit – 2023

https://www.ncsc.gov.uk/information/moveit-vulnerability

https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability

https://www.bbc.co.uk/news/technology-65965453

Okta – 2023

https://thehackernews.com/2023/11/okta-discloses-additional-data-breach.html

https://www.theregister.com/2023/11/02/okta_staff_personal_data/