Cyber Security Predictions for 2017

Huntsman®
Defence-Grade Security Platform

Ransomware attacks will continue to escalate and will include new attack vectors, such as distributed denial of service attacks on Internet retail services, social media platforms and cloud service providers. IoT devices will also come under increased scrutiny from threat actors as they vie for access to otherwise protected networks.

A NEW WORLD ORDER

The final months of 2016 saw a significant shift in the cyber threat landscape, when what has been a lingering international concern around the security of IoT devices turned into a sobering reality when DNS service provider, DYN, suffered a blistering Distributed Denial of Service (DDoS) attack. The Huntsman Security team continues to monitor this escalation, especially in attacks that incorporate so-called Internet of Things (IoT) devices in the weaponised botnet.

IoT devices remain a growing cybersecurity challenge and are key target for threat actors since they are often so easy to hijack. Most have limited internal cyber security defences and some even ship with default security weaknesses that remain unpatched even when they are demonstrably insecure. Furthermore, IoT devices are a wonderful source of intelligence for attackers, who regularly attack these peripheral devices to glean metadata that helps to further profile corporate, enterprise or home networks.

Huntsman Security believes that IoT manufacturers will continue to produce devices that ignore good cybersecurity practices - and pay little attention to the security development lifecycle that enterprises have adopted over the past decade. The lessons in this arena will take some time to learn and even longer for standards and labelling systems to emerge across the sectors to provide greater protection and cyber awareness for users of IoT devices. Vehicle safety test and appliance environmental ratings are user information regimes that come to mind; although scale is another thing all together!

CASE STUDY – DYN ATTACK – OCTOBER 21ST 2016

On Friday 21st October 2016, DNS provider, DYN, suffered a prolonged DDoS attack on its core DNS service infrastructure, resulting in widespread disruption across the whole of North America and crippling some of the world's most established online brands, such as Airbnb, Amazon, Visa and Twitter. Hacktivist organisations, Anonymous and New World Hackers, claimed responsibility, but culpability remains unsubstantiated. Reports have emerged suggesting that the hijacked devices used to launch the attack comprised mainly IoT devices, such as CCTV cameras, residential Internet routers, and infant monitors, all infected with the Mirai malware.

RANSOMWARE

Ransomware is the most common online threat affecting today's Internet users. From the smallest retail outlets to the most classified government agencies, ransomware is relentless in its pursuit of targets and does not discriminate in who gets targeted. However, the mode of attack is changing, as end users get wiser to some of the techniques used by cyber criminals. Nevertheless, ransom-style attacks are here to stay. Whether the offence relates to a traditional encryption-based attack, or a more recent sustained DDoS attack on your online presence, you will need to plan for an escalation in ransomware attacks in 2017. Monetised attacks may also extend to IoT devices including, concerningly, medical devices where patients' lives could be put at risk.

INCREASING POLITICAL AND MEDIA INFLUENCE (AND UPHEAVAL)

2016 saw a number of major political events where cyber security, government processes and the role of the wider media started to converge — often in a negative way.

In the UK's Brexit vote, the role of social media in influencing opinion before, as well as the rise of hate-related content afterwards, is clear. Just recently the "US government" — the White House's view could pivot dramatically on 20 Jan — instigated an enquiry into cyber interference during the US election process and social media networks have introduced fact checking of hosted news. Traditional roles are being juxtaposed as cyber capabilities and hosted news services were successfully used to swing public opinion and even effect political change while traditional media outlets, sometimes targets themselves, were left to report the outcome.

CYBER SITUATIONAL AWARENESS

Security operations centres (SOCs) are seeking ways to increase their cyber situational awareness and make better use the investments they have made in people, processes and technology. Security intelligence centres (SICs) have been hailed as the future of security operations since this incorporates gathering, analysing and disseminating actionable intelligence to the business for earlier intervention on the cyber kill chain. What is clear, however, is that whether you call it a security operations centre or a security intelligence centre, the ability to automate routine threat investigation, verification and response processes can deliver material benefits. Up 80% and more of analysts' time can be freed up to focus on proactive threat hunting and investigation and shorten the time at risk.

Through the close integration of machine based analysis and workflow automation, skilled and insightful analysts will deliver a hybrid process that reengineers the threat management to meet the speed, accuracy and scale required of today's organisations. Throughout 2017, we expect to see security operations teams, investing in new products that will push the envelope to deliver operational and business benefits through automated threat verification, machine learning and behavioural analyses.

THREAT INTELLIGENCE SHARING

Cyber defenders need to get better at collaborating and sharing indicators of compromise if they are ever to get inside the decision loops of the attackers. Vendors sometimes hamper best intentions and intelligence sharing by using threat intelligence services as a differentiator in the marketplace. Evidence suggests that collaboration of vendors and users delivers better awareness for better security outcomes. Huntsman Security believes that broader sharing of standards based STIX and TAXII feeds across vendor platforms helps organisations get on the front foot ahead of cybercriminals and nation-state actors. Increasing collaboration between vendors will build interoperability between security solutions to deliver better threat intelligence and generate improved actionable and contextual intelligence for their customers.

SOCIAL MEDIA IN THE BUSINESS WORLD

Businesses will continue to struggle with how to best leverage social media and how it can impact their business models. As the past few years have shown, the most popular platforms are here to stay and are affecting businesses whether they like it or not. Cybercriminals are increasingly targeting companies through their social media accounts, where massive reputational damage is possible even with a relatively low-tech and inexpensive attack.

Throughout 2017, corporate social media platforms will become more persistent as they become a legitimate part of the corporate DNA and even begin to displace communications media, like email. It is essential that cybersecurity strategists grasp the nuances of these new vectors and start modelling attacks that include using social media platforms to gain access to sensitive systems.

PRIVACY AND DATA BREACH NOTIFICATION

Mandatory breach notification is fast becoming a reality for most countries that take their sovereign data security posture seriously. As these laws pass, governments and businesses are investing in the protections they need to detect, deter and disrupt the attacks that yield significant data breaches. Through 2017, we will see an increasing demand on cyber security resources as more businesses embrace the digital economy.

In the EU and UK the GDPR regulation changes the way privacy and consumer rights need to be considered in terms of the notification requirements around breaches. The sizes of fines (up to 4% global turnover), the scope of liability (including data processing supply chains) and the scope of what personal data actually is (including network addresses) will certainly make this a front-of-mind issue for 2017.

INSIDER THREAT

With the focus of the past few years being on external attacks from cybercriminals and nation states, there is a perception that the insider threat has been somewhat ignored. Insider risks have not abated and 2017 will see a renewed focus on the malicious insider activity. Technology, processes and managed security service providers will start providing insider threat protection to complement more traditional perimeter controls and external attack vectors.

For 2017 we can expect ongoing volatility in the threat landscape from familiar threat vectors, although as we've discussed above, these will be punctuated with the emergence of easily accessible but harmful threats. The attacks of 2016 have confirmed the reality that good cyber governance is a key enabler for successfully operating in the digital economy. So as we develop strategies for vigilance against the emerging and repurposed threats for tomorrow; right now we need to remember to maintain a level of effective cyber hygiene that permits a manageable threat environment for the future.

Visit us online at **huntsmansecurity.com**

Author: Peter Woollacott
Co-Founder and CEO, Huntsman Security

Peter Woollacott is the co founder and CEO of Tier-3 Pty Ltd (now trading as Huntsman Security), the software company that holds the patent for Behavioural Anomaly Detection and developed Huntsman® Intelligent Security.

He has 25 years' experience in operational and risk management with companies like Lend Lease, CBA, AXA, EDS, PWC and Bain International. Peter holds Masters Degrees in Applied Finance and in Business Administration, and lectures in executive post graduate education at Macquarie and Sydney Universities.

Peter may be contacted at
pwoollacott@huntsmansecurity.com

Please visit the Huntsman Resources page at **www.huntsmansecurity.com/resources** for White Papers, Compliance Guides, Solution Briefs and more resources by this author.

Huntsman | Tier-3 Pty Ltd

Asia Pacific
t: +61 2 9419 3200
e: info@huntsmansecurity.com
Level 2, 11 Help Street
Chatswood NSW 2067

EMEA
t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com
10 Greycoat Place
London SW1 1SB

North Asia
t: +81 3 5809 3188
e: info@huntsmansecurity.com
TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas
toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com
Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com
linkedin.com/company/tier-3-pty-ltd
twitter.com/Tier3huntsman

© 2015. All rights reserved. Huntsman is a registered Trademark of Tier-3 Pty Ltd