How Advanced Persistent Threats Exploit Humans

Mercy Bere[1], Fungai Bhunu-Shava[2], Attlee Gamundani[3], Isaac Nhamu[4]

[1, 2, 3, 4] Computer Science Department, Polytechnic of Namibia, Windhoek Namibia

Abstract

Advanced Persistent Threats (APT) are a fast growing security concern for ICT users in homes, governments and other organisations. Initial delivery of APT in computer systems is achieved by social engineering people within the organisations. This research employed a preliminary desktop review of how APTs are delivered in organisations' computer systems and discovered that spear phishing is the leader in social engineering techniques used in APTs to compromise industrial control systems security. A description on how APTs operate and how spear phishing and click jacking are used as tools to successfully exploit organisational security is presented. In addition the paper briefly describes implications of successful APT attacks in organisations. Further the paper proposes use of the APT awareness stages in order for organisations to improve their security posture through user security awareness

Keywords: *Advanced Persistent Threats; Industrial Control Systems, social engineering; security awareness; organisational security*

1. Introduction

Advanced Persistent Threats (APT) are a rapidly growing information security threat to businesses and government organisations [1]. The 2014 State of Endpoint Risk report states that out of 676 organisations surveyed APTs were ranked as the third most risky security threat to organisations. First being the use of mobile platforms and the second being use of cloud computing. It is speculated but never been proved that APTs are nation sponsored attacks because of their sophistication and also because originally they targeted military and government agencies [2, 3]. This trend has changed as APTS target any businesses and government agencies as well [4]. In many instances we find that the goal of the APT is to steal intellectual data.

Of interest is the fact that most APT success is attributed to the manipulation of or in some cases wilful participation of an organisation's employees to gain access to the business IT networks. The authors did a document review to find out human related methods used by APTs to penetrate IT networks. Most of the APTs considered were those APTs that attack industrial control systems. The reason for mainly analysing these APTs is that, the main objective of the research being undertaken is to design a networking security model for securing industrial control systems from APTs.

The following sections of the paper are organised as follows. The next section will outline APT and the APT lifecycle. Section 3 and 4 will discuss the social engineering methods used by APTs to attack IP networks. Section 5 will give a brief overview of the implications of successful APT attack. Section 6 will show some of the security aspects organisations need to beef up on, in order to increase user security awareness. Section 7 will be the conclusion.

2. Advanced Persistent Threats

Advanced Persistent Threats are sophisticated multistep cyberattacks which are designed in such a way that they only attack specific targets [5]. In order to successfully infiltrate a network APTs usually follow the following attack stages [2, 5, 6]:

- Choosing a victim
- Reconnaissance
- Delivery
- Exploitation
- Operation
- Data collection and exfiltration

2.1 Choosing a victim

At this stage the attacker chooses which organization they want to attack. The attacker also decides what they want to achieve out of the attack. Maybe the attacker wants to steal data source code, confidential information, trade secrets or they want to sabotage operations [2].

2.2 Reconnaissance

This is the stage attackers seek information about their target. They use network scanning and mapping mechanisms to gather information [2, 6]. They also use social engineering techniques, employee profiling, social networks and phone directories to get information [2]. This investigation is used to find pathways into the system.

2.3 Delivery

Using the information gathered in the reconnaissance stage the attackers develop malicious code that exploits the identified vulnerabilities and this code is attached to pdfs, docs, ppts, ready for delivery to attacker's victim [7]. Several ways can then be used to penetrate the network to infect the target's systems. The graph below highlights some of the methods used to initiate APT attacks [2].

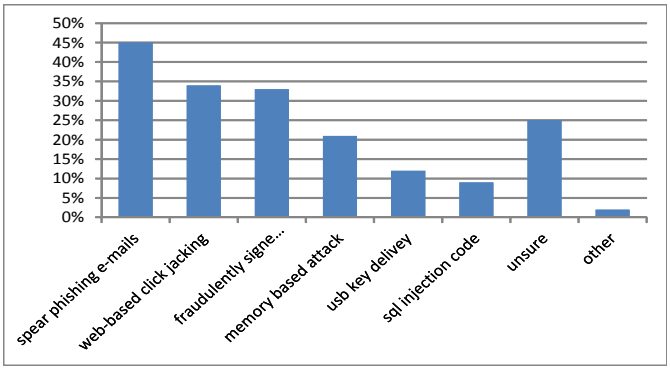

Fig 1. Methods Used by APTS to Penetrate Networks [1]

2.4 Exploitation

This stage is executed when the malware is now in the system. At this point the malware uses vulnerabilities to execute its payload [7]. In addition, the malware makes contact with its command and control centre. When a secure connection is established with command and control centre information about the victim's computer is collected and sent to the command and control centre [6].

2.5 Operation

When the attacker has gained a base in the system they persistently maintain presence in the network over a long time. If it is necessary the attacker moves laterally in the network to find strategic positions such as servers with sensitive information [6]. They might just move in the network to have access to other devices in the network which are consequently also compromised [2].

2.6 Data Collection and Exfiltration

Using access gained from previous stages data is gathered, segmented and encrypted. It is kept in temporary servers in the internal system while attacker establishes redundant command and control channels that can be used in case of changes in security configurations. Finally data gathered is sent over encrypted channels to multiple external servers. This is done to hide the final data destination [6].

3. APTs Exploiting Humans

As shown above the APT stages of reconnaissance and delivery are successful to a great extend because they manipulate the human. By looking at Fig 1, we see that spear phishing email, click jacking and USB key delivery which are some of the methods used to deliver an APT in a network are successful only by human interaction. The table below highlights some APT examples and how they were initially delivered to target systems.

APT	Target	Initial attack method	Purpose	Wilful participation
Stuxnet	Iranian Natanz Nuclear Enrichment Facility	Infected removable drive	Disrupt nuclear plant operations	yes
Duqu	Several organisation in Sudan, middle east, and Europe	Infected MS Word file sent to victim	Extract information	no
Flame	Iranian educational institutions	Impersonation of windows update server	Extract information	no
Red October	Research organisations	Spear phishing mails infected word and excel documents	Extract information	no
Miniduke	23 countries Government bodies	Pdf mail attachments	Extract information	no
Operation Aurora	Google network	Infected website	Extract information	no
Operation Shady rat	71 companies all over the world	Spear phishing mails with MS word, Excel, PowerPoint and pdf attachments	Extract information	no
RSA attack	RSA network	Spear phishing mails infected excel documents	Extract information	no

Table 1: APT attack examples

It can be seen from the table that most initial infection is done through tricking people into opening files with malicious extensions or tricking them to visiting infected websites. Therefore we can conclude that humans are social engineered by the attackers. Social engineering is not a new weapon of attack but has been used from ancient times. The next section will look at the social engineering mechanisms most used in APT attack

4. Social engineering as an APT tool

"Generally social engineering attacks are security exploits that prey on the vulnerable attributes of humans rather than technology" [8]. SRI International defines social engineering as: "deceptive practices to obtain information from people using social, business or technical discourse" [9]. From these various definitions, it could be noted that, social engineering mainly operates at the entry point for APT attacks

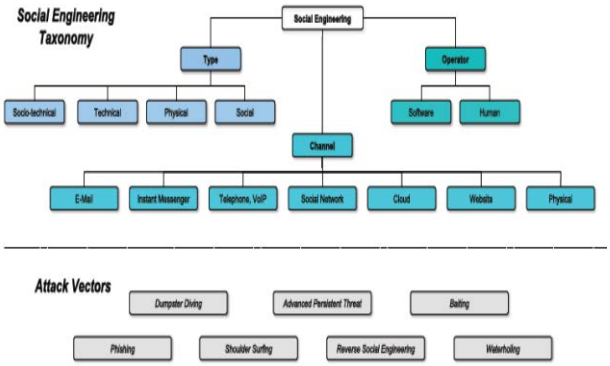

Fig 2: Social Engineering taxonomy [10]

The social engineering taxonomy presented by [10] Fig 2, is detailed enough to portray an overview of what constitute social engineering at an advanced level and will be adopted for the purposes of shading light on social engineering for this paper.

The taxonomy above hints on four crucial aspects to consider when discussing social engineering attacks namely: channel, type, operator and attack vectors. The ever growing communication media like e-mail, instant messaging, Skype, Dropbox, LinkedIn, Lync, etc create new attack vectors for social engineering attacks [10], as depicted in Fig 2 above.

In general, [11], outlines that social engineering methods target some human behaviour attributes such as trust, the desire to be helpful, wishing to get something for nothing, curiosity, fear of the unknown or losing something (as when responding to popup windows), ignorance and carelessness. In APT attacks social engineering attacks are aimed at manipulating humans or software into divulging confidential information about the targeted network. This means that humans trust the 'perceived' sender and the email subject and in their curiosity and need to be helpful they download the attachment.

To gain initial information attackers may use physical means such as dumpster diving, theft or exhortation. Dumpster diving is identified as a component of the careless attack vectors by [12] in his Four Vectors of Psychology Based social engineering. Dumpster diving is presented by [13], as searching through the organisation's trash to build personalised profiles about the victims. Attackers might also search for information about organisations and/or employees on social web pages to gain more information.

After obtaining initial information they can send targeted emails also termed spear phishing [10]. Spear phishing capitalises on e-mail attachments as discovered by [14]'s research. McAfee [15] point out that spear-phishing is a popular way to bait targeted users into downloading initial APT delivery malware. Most of the downloads are attached to the email and the most common spear-phishing attachments are shown in Fig 3.

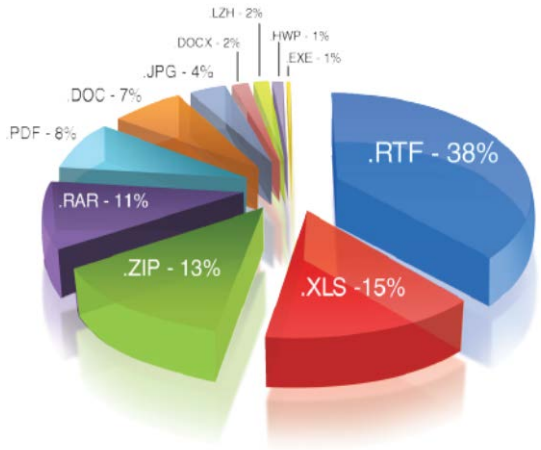

Fig 3: Top spear phishing e-mail attachment file types [14]

As affirmed by [16], reverse social engineering makes use of sabotage, advertising and assisting to gain access to desired information. Considering [17], a usb drive containing a trojan horse can be used by the attacker, they then advertise to have effective antivirus, in the process of assisting they gain access to the victim's password [10] in the name of assisting or offer certain software installations.

Another common attack used in APT initial attacks is click jacking. Click jacking is also known as UI-redressing. Chaitanya et al, 2012 say that click jack attackers con users into believing they have clicked on genuine buttons when they have actually clicked invisible targets. In this manner attackers use the hijacked mouse click to do tasks that will achieve their goals [18].

Broadly social engineering attacks have taken different advanced dimensions and technical solutions may not harness such approaches. APTS are capitalising on the social engineering route as it is proving to be effective

5. Implications of successful APT attack

Successful APT attacks have consequences. ICS which consist of among others, power grids, water, and oil distribution systems are also being attacked by APTs. Attacks in ICS will result in endangering people's health and safety [19]. In other computer systems successful attacks might result in damage to infrastructure and in most instances there will be a financial losses as a result [19].

Because there is an increase in the number of attacks on organisations IT budgets are being strained [1]. This is because organisations need to fork out more to address the possible security breaches. This might be taken to mean that most of the IT budget is spent on trying to secure systems instead of on upgrading or improving them.

As revealed by the Trend research, the most targeted industry for APT attacks via spear phishing are government with a 65% attack rate which is almost double the second target industry classified as Activists with a 35% attack rate [14]. As stated by [2] most APTs are being created by governments because of the complexity, time, sophistication and resources needed to create an APT. If this is the case then if countries are spying on each to improve the weaponry or just to find out what the other nation is doing in their governments and armies. Who knows how the nations being spied on will react on discovering their data is being stolen? Will this be the breeding ground for a nations cyber war? Even if the war starts in cyberspace, who knows how and where it might end up and the impacts and implications of such a war

6. What can be done to improve awareness or better security use?

Based on literature studies, APTs are gaining access to ICS due to enabling user behaviour. In order for the security officers to address this problem, there is need to address the root cause of the APT success by doing risk assessment, policy and control implementation, awareness campaign and monitoring and evaluation. However, this paper recommends focus on awareness campaign because it sensitises humans on APT initial infection symptoms as there is no one solution to APT security breaches.

Users fall under the operations/ human resources domain of the ISO27002 standard. To address the human aspect of security, policies should be designed and implemented. However policies are as effective to the extent determined by the usage. If there is consistent correct usage then policies are effective, otherwise they are fruitless. Social engineering hinges on poor policy implementation practices. Based on this it is important to address APT awareness, as it is the basis of correct usage and it impacts on behaviour change. Security conscious decision making and behaviour is enhanced by awareness campaigns as they increase the user's security related knowledge [20].

SANS security awareness model begins from non-existence of an awareness program, then compliance focused, promoting user awareness & change long term sustainment and metrics [21]. A complementary model was designed by [22] for awareness program cycle which focuses on reducing the phishing threat by influencing behaviour through awareness. In this paper we will focus on promoting user awareness and change as follow up to the compliance focused stage (where standards and policies relevant to the ICS security domain should be implemented). Promoting awareness and changes focus on positively influencing behaviour and reducing security threat [21]. Fig 4 presents stages of APT awareness based on [21, 23].

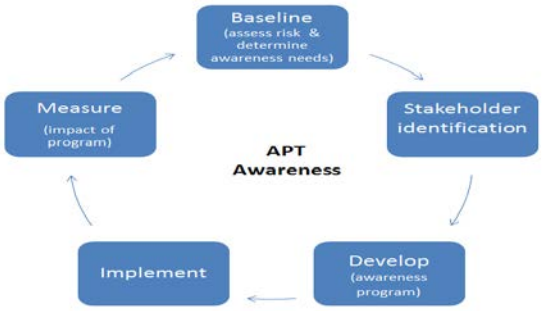

Fig 4: APT awareness lifecycle based on [21, 23]

Stage 1 of the APT awareness cycle is the determination of the level of risk the ICS are exposed when it comes to APT attacks and assign them levels of criticality to aid prioritisation. This can be done through surveys to gauge the APT and general security awareness levels before planning for the improvement. We need to identify the topics to address in the awareness program and these are depicted in fig 5. The user need to be aware of what APTs are, the APT attack vectors, the impact of successful APT attacks and best practices in mitigating them. Stage 2 involves identifying the stakeholders in the successful execution of the program. Once the stakeholders have been identified we then move on to develop the program. Stage 3 involves selection of awareness strategies for identified stakeholders, area of focus, material to distribute and an implementation plan. Awareness strategies include posters, blogs, newsletters, websites, briefings, bulletins and tutorials [20, 23, 24]. Stage 4 is the execution of the program and finally the stakeholders are re-evaluated to check on progress. The latest evaluation then serves as the baseline for future evaluation.

Fig 5: User awareness of APT

7. Conclusion

From the way APTs are getting initial access to networks it can be seen that humans are a very weak link. From the examples given in Table 1 it can be seen that all the APTs gained access by human means. The most common way of gaining initial entry in networks is by delivering spear phishing emails to individuals within organisations in the hope that they will download the email attachments. Literature shows that the attackers hope becomes reality as user download the attachments and thus the first stages of the APT are achieved.

The consequences of a successful APT attack in organisation could be detrimental to the operation and finances of an organisation. Hence we suggest that organisations must improve their user awareness programs. We suggest following APT awareness stages so that in promoting awareness we realise changes on positive security behaviour and thus reducing security threats

It can be noted from this paper that the human aspect of APTs is very complex and needs to be addressed from behavioural perspective as well the theories of reasoned action behaviour. Thus future research will focus on developing a technical model to address technical APT attack vectors.

References

[1] Ponemon Institute, 2014, 2014 State of Endpoint Risk. https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf.

[2] Fortinet, 2013, Solutions Brief: Threats on the Horizon - The Rise of the Advanced Persistent Threat, http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-the-horizon-rise-of-advanced-persistent-threats.pdf,

[3] Lumension, 2012, Preventing Weaponized Malware Payloads in Advanced Persistent Threats. https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Lumension_2013-Febl_wp_Preventing_Weaponized_Malwa.aspx.

[4] FireEye, 2013, Fireeye Advanced Threat Report, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf.

[5] N. Virvilis, D. Gritzalis and T. Apostolopoulos, "Trusted Computing vs. Advanced Persistent Threats: Can a Defender Win This Game?", in 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), 2013, pp. 396-403.

[6] P. Giura, and W Wang, "A Context-Based Detection Framework for Advanced Persistent Threats", in International Conference on Cyber Security (CyberSecurity), 2012, pp. 69-74.

[7] P Bhatt, E. Toshiro Yano, and P. M. Gustavsson, "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks", in 8th International Symposium on Service Oriented System Engineering (SOSE), 2014, pp390-395

[8] L. P. James, L. B. Janet, and F.C. James, (2009) A personality based model for determining susceptibility to phishing attacks. www.swdsi.org/swdsi2009/papers/9J05.pdf

[9] S. Cobb, The NCSA Guide to PC and LAN Security, McGraw-Hill .pp 230, 1996.

[10] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", Journal of Information Security and applications, 2014, doi 10.1016/j.jisa.2014.09.005

[11] R. Gulati, 2003, The Threat of Social Engineering and Your Defense Against It. SANS Institute, http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232.

[12] E.C. Lively, 2004, Psychological Based Social Engineering. SANS Institute http://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780.

[13] S. Granger, 2001.Social engineering fundamentals, Part1: Hacker Tactics. Security Focus.

[14] Trend Micro Incorporated, 2012. Spear-phishing Email: Most favoured APT attack bait, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

[15] McAfee, 2011, Combating Advanced persistent Threats, How to prevent, detect and remediate APTS, www.mcafee.com.

[16] K. Mitnick, and W. Simon, The art of Deception: Controlling the human element of security Wiley. 978-0-7645-4280-0, 2002.

[17] S. Stabiukonis, 2006, Social Engineering: the USB way, http://www.darkreading.com/security/perimeter/showarticle.jhtml?article ID=208803634.

[18] K. T. Chaitanya, H. Ponnapili, D. Herts, and J.Pablo, "Analysis and Detection of Modern Spam Techniques on Social Networking Sites" in 3rd International conference on Services in Emerging Markets (ICSEM), 2012, pp 147-152.)

[19] D. Hadziosmanovic, D. Bolzoni, S. Etalle, and P. Hartel, "Challenges and opportunities in securing industrial control systems", in Complexity in Engineering (COMPENG),2012, pp 1-6.

[20] M. Kajzer, J. C. R. D'Arcy*, and D. Van Bruggen, "An exploratory investigation of message person congruence in information security awareness campaigns." Computers & Security Vol 43, 2014, pp 64 -76.

[21] L. Spitzner, 2012, Next generation security awareness programs: securing the human SANS, www.securingthehuman.org/blog,

[22] N. A. G. Arachchilage, and L. Steve, "Security awareness of computer users: A phishing threat avoidance perspective." Computers in Human Behavior, Vol 38, 2014, pp 304–312.

[23] L. Lindholm, 2006, What is security awareness. FISSEA.

[24]L. Spitzner, 2012. Security awareness maturity model promoting change. SANS. http://www.securingthehuman.org/blog/2012/05/29/security-awareness-maturity-model-promoting-change