Research Paper

Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179

A Proposed Study of Advance Persistent Threats – Survey

Computer Science

KEYWORDS : SMB, Large, Enterprises and Govt Agencies

Ms. Komal Saxena Phd scholar Singhania university.

Dr. Anurag Awasthi Research Guide Singhania university

ABSTRACT

With the evolution of technology, there is also an increase in the cyber crime activities. For the past couple of years cyber security is of prime concern to various organisations. Large data stored in databases need to get highly encrypted so as to overcome the cyber crime threats. One such threat that has created a buzz these days in SMB, Large, Enterprises and Govt Agencies is the Advance Persistent Threats (APTs).

This paper gives an insights of APT risks, provides prevention and detection methods on how enterprises can protect themselves and overcome the threats to continue smooth operations in a healthy environment.

I. INTRODUCTION

1.1Advance Persistent Threats (APTs)

Hackers who employ APTs (advanced persistent threats) are a different breed[1].There is a buzz these days all around in SMB, Large, Enterprises and Govt Agencies about APTs. APT is the technique used by cyber criminals that steal data from businesses for financial gain. Many organizations both large and small have been affected with it.. A real and constant threat to the world's companies and networks, APT hackers tend to be well organized, working together as part of a professional team. Their goal, typically, is to steal valuable intellectual property, such as confidential project descriptions, contracts, and patent information.[1]

1.2Data Analysis on Awareness of APT :

The survey results reveal that 25.1 percent of respondents are very familiar with APTs, with a total of 96.2 percent expressing that they are at least somewhat familiar[1.1]

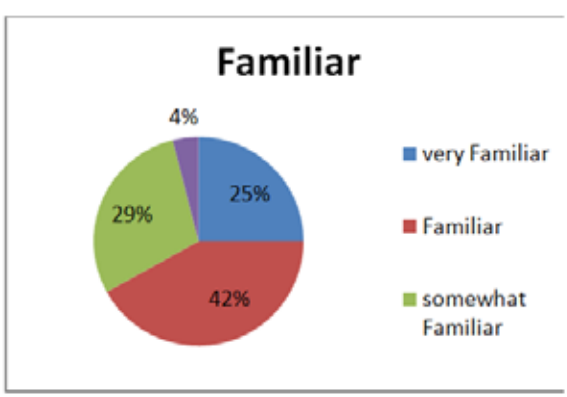

Figure1.

1.2.1APTs targets

APTs can target any business or organization to steal specific data.

1.2.2The APT process

1.2.2(i)**Phase 1 :-Inspection, Starts, and finally infect.**

The attacker always do inspection identifies vulnerabilities, then start the attack, and finally infect hosts.

1.2.2(ii)**Phase 2**

Manage, Update, Determine, and Persist.

The attacker manage infected host, updates code, spread to other Legacy systems and collects target data. The tools used to gain more control are standard network tools such as gsecdump, cabel & Abel (to crack passwords), SSH, RDP

1.2.2(iii)**Phase 3**

Extract and take various Actions The attacker extracts data from the target network and takes action(Like sells data, Public disclosure, share or sell attack method)

Phase 1

Inspection, Starts, and Finally infect

Phase 2

Manage, Update, Determine, and Persist

Phase 3

Extract and take various Actions.

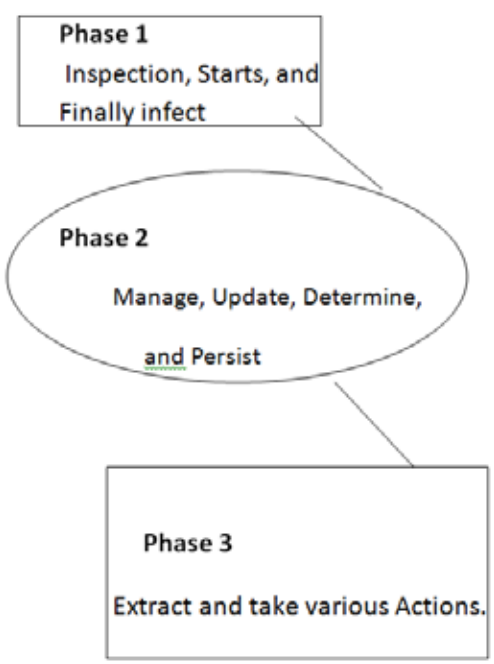

Figure 1.2[2]

2.REASONS SMB, LARGE, ENTERPRISES AND GOVT AGENCIES ARE TARGETED[2]

2.1 Data is more valuable than you imagine

Data is so valuable and important that an SMB knows better

than any other. There is some information that most businesses want to keep it surreptitious. It can be employees' personal data, clients' information, products and services strategies, accounts data, list of customers, credit card data, and many more. Often it is seen that Companies doing business with their partners often interact via computer systems. This interaction is in the form of valuable information, supply chain management and access to confidential data. Though you are not targeted directly but it can be a valuable target for APTs. It might not be your data they're after but can be a pivot point in APTs environment.

2.2 Low risk and high returns for APTs

Progressed malware regularly dwells in infected systems for a longer period of time, even months, before normal security software identifies it and cleans up. In some cases attackers fetch the data, quietly clean and exit themselves without being noticed by the administrator. Those enterprises that are not performing well in the market and are facing stiff competition from SMB/ large enterprises often outsource the APTs to help them stealing the confidential data to take an edge over their competitors.

Doing such thing APTs get huge incentives with just a code entering into the computer and infecting or stealing the information smoothly to earn huge profits.

2.3 An easier and least challenging approach of targeting

Talking about the SMB, these businesses are easily affected by APTs. The reason is they have reasonable budget to deal with it. They don't have IT security offers, Chief Information officer and IT director to wear the threats. They lack in security features which lead them to fatal consequences. As a result it becomes easier for APTs to attack the system and reside till it discovers and capture the target data. You are an easier target to them. Not only SMBs but Large Enterprises and Govt Agencies are also now easier to get hacked by APTs. Highly effective and efficient lines of code break the layer of security to various levels making it easier to enter Large Enterprises and Govt Agencies system. Similarly, numerous organizations need solid security methods and strategies. Just 36 percent of organisations have information security approaches, as indicated by a September 2013 review supported by Bank of the West [1]. Most APT takes after the easy way out. By and large, this implies focusing on the SMB that can slightest bear to be hit but not leaving large and government organisations.

2.4 Outdated least effective security tools

Today, large organizations whether small or big use outdated and least effective security tools. This gives a good chance to APTs attack the system easier and convenient. They are no match to these attacks. Firewalls, Intrusion Prevention Systems, gateways, security software are ineffective stopping APTs. These all rely on approaches like signatures and URLs. These approaches are least effective to stop APTs as a result SMB, Large, Enterprises and Govt Agencies are targeted easily.

2.5. Organisations operating under false security myth

Various organisations operate under myth that their data is protected and safe. But actually they are unaware of the fact that APTs have already entered their system without getting noticed by the administrator. Despite the rise of APTs, 77% companies believe that they are safe from cyber crime activities. Giving chances to attackers steal their confidential data.

3. APTs DETECTION METHODS [2]

3.1 A Increase in log-ons late at night

APTs quickly rise from single PC to the entire environment. They start by entering in the database, stealing data and sending it to the source. They realize which client (or administration) records have raised benefits and authorizations, and then steal those records to trade off resources. Frequently, this happens around evening time in light of the fact that the attackers on the opposite side of the world. If you suddenly find that there is an increase in the log-ons at night, then this is the serious thing to worry.

3.2 Finding backdoor Trojans

APT attackers install backdoor Trojans to infected computers. They do this to make it sure that even if the login credentials changes they can easily enter the computer without causing any trouble. You won't be able to notice how quickly and safely they install Trojan at your computer. Today, most companies systems are infected by Trojans. They are common is such types of environments.

3.3. Unforeseen information flows

Look for large unforeseen data from one computer to another or from one server to another. In order to detect the APTs you have to monitor the flow of data from source to the destination.

3.4Discover unforeseen data bundles

APTs often cumulate stolen data to an internal place before moving it outside. Look for large chunk (in GB) data appearing in places where the data should not be present. It may be in the compressed form detect them and take the action quickly.

4. APTs PREVENTION METHODS [3]

4.1Multi layered Antivirus

Today, APTs are so strong that they are ineffective to normal antivirus. They break the code and enter the system quickly residing for longer duration to fetch information. This is why it is important to use multilayer antivirus to protect your PC.

4.2 Patch Management and Leverage Configuration

Software vulnerabilities grows with time daily you have new challenges to deal with these vulnerabilities making it difficult for network manager to look for security patches. Patch Management and Leverage Configuration systems help enterprises to tackle with APTs. It has the ability to monitor and manage policy based configuration security which include mobile devices, servers and endpoints, and cross platform systems. It supports operating system and offers reporting and support.

4.3 Device management

Any device such as mobile phone, tablet or PC connected to the enterprise can subject to data theft. To control each and every device in the enterprise a data prevention system ne to be established so that the data is encrypted and its access is controlled.

4.4 Deploy Memory/Data Injection Prevention Technologies:

Sometimes a code is being injected via APTs in the database input form, which forces the data base to return information to the source. To protect such activities of APTs there is a need to Deploy Memory/Data Injection Prevention Technologies. For example Desktop OSes and Windows Server offer local memory security controls, such as ASLR and DEP.

5. CONCLUSION

This paper analyzed the ATPs faced by various small to big organisations. Most security specialists concur that the term "Advanced Persistent Threat" was initially instituted by the U.S. Aviation based armed forces, around 2006, to portray complex digital assaults against particular targets. Today it is the incorporate comparative assaults did by cybercriminals taking information from organizations for benefit. In order to protect you business data, follow the detection and prevention method, and implement strategies accordingly to protect your data from APTs. The paper will help you in understanding the insights of APTs and how to tackle the ATPs.

Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179

REFERENCE

[1]www.trendmicro.com/apt | | [1.1]www.Isaca.org/cybersecurity | | [1.2}.2(i) A Websense White Paper "Advanced Persistent Threats and Other Advanced Attacks". | [2]. Harris Interactive "Fighting Fraud: Small Business Owner Attitudes about Fraud Prevention and Security." September 2013 | [3]. This story, "5 signs you've been hit with an advanced persistent threat," was originally published at InfoWorld.com. | [4]. The website www.techrepublic.com, article "Proven tactics for preventing advanced persistent threat incursions" | [5]. A Websense White Paper "Advanced Persistent Threats and Other Advanced Attacks". | [6]. A Fire Eye White paper "Big threats of small business".