Twitter Threat Detection Report - 16164571

Part 1: Why should we perform threat modeling for Big Data Solutions?

1 - What is threat modelling?

Threat Modelling involves the analysing of a ICT system to find its weak points which may be exposed to potential attacks and vulnerabilities. These models can be used as input into the definition and evaluation of risk metrics. A threat model can help companies decide on enterprise architecture and general security measures. It is always better to understand what threat risks are in your system

2 - Why should we perform threat modeling for Big Data?

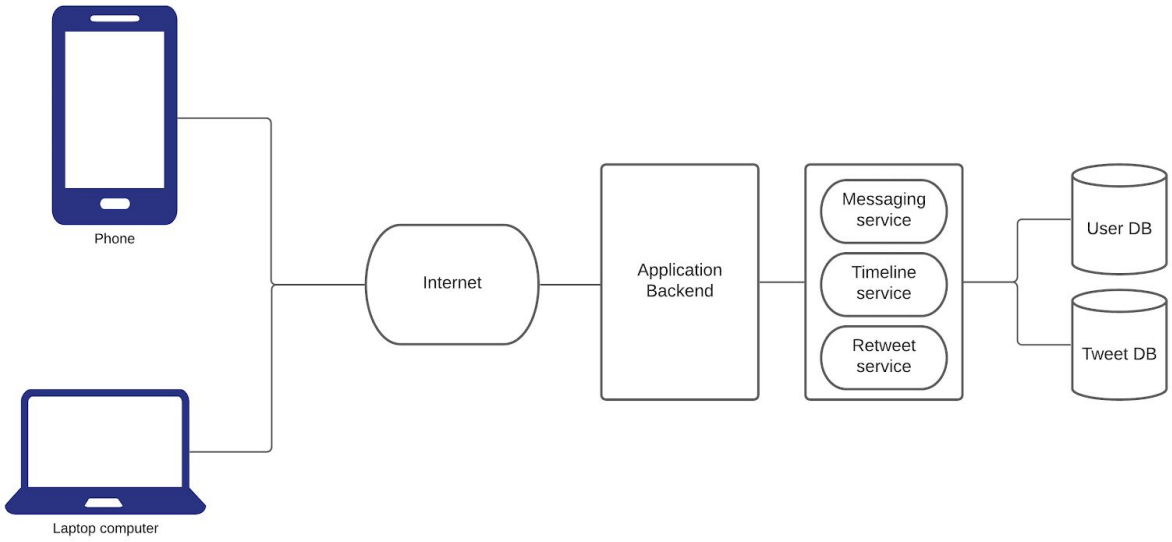
Big data involves a large flow of information being shared among many parts of a system. It is important to make sure that when threat modelling for these big data systems that you know where all the data is going. This includes looking at who the data interacts with along its path, is there places it interacts with which can leak the data or where the data can get exposed. The more data components that a big data system contains the more opportunities there are for a hacker to intercept this data and gain access to it. As a lot of big data systems contain sensitive and private information it is very important to perform threat modelling to keep this information safe from hackers

3 - How is Big Data security different from conventional database systems security?

Traditional Database vulnerabilities include SQL Injection attacks, human error and denial of service attack (DDoS). All these vulnerabilities each have their own way of being secured.

BigData vulnerabilities include Endpoints, Distributed frameworks and when using BigData management tools such as Hadoop.
Ways to overcome these vulnerabilities is by using tools and services. A common solution is to provide access control for the Data storage. This will restrict access for users based upon their authorization level; the higher the level the more access and permissions they are granted. Encryption is also a very good security measure to take on for both standard and big data bases. This encrypted data is of no use to the adversary if they do not have their key to unlock it.

4 - System Design



Part 2: Threat Intelligence

1) Fin5 is a threat group that has financial motivation. They have targeted personally identifiable information and payment card information. This adversary is important to identify as Twitter business ads accounts can contain sensitive information for businesses who want to advertise on Twitter. Ad accounts must have a payment method selected such as Visa or American Express. Twitter would need to be aware of techniques used to stop this sensitive data been accessed

Techniques used:

Brute Force: This technique involves adversaries using brute force to gain access to accounts when their passwords are unknown. It can also be used when they obtain hashed passwords. The adversary will guess the password using a repetitive mechanism. This brute-forcing of passwords can occur with a service that will check the validity of the password or offline against obtained credential data such as hashed passwords

External Remote Services: This technique involves adversaries using external-facing remote services to their advantage to access a network. An example of these services might be a VPN. These services, when connected to, can allow users to access internal enterprise networks. To access these services, the adversary will have to have a valid account. These accounts can be obtained via credential pharming or by using compromised user credentials. The adversary might not use malware in conjunction with this technique as since they have legitimate credentials, it will make it harder to detect their presence in the compromised system.

Tools used:

PsExec: This is a free tool which is made by Microsoft. This tool can be used to access and run programs on Windows PCs remotely. This tool can be used in a variety of ways by adversaries. Files can be uploaded and downloaded between two computers which are remotely connected via this tool. Programs can also be written to the ADMIN$ network share which would allow the adversary to execute system commands on the system they are attacking.

2) Wizard Spider is a financially motivated criminal group that specialises in ransomware campaigns. They are a new group and active since 2018. This group can knock out a high tech system such as Twitter and wait until a ransom is paid to them in bitcoin.

Techniques used:

Create or Modify System Process: Windows Service: This technique allows the adversary to create or modify a Windows Service in order to execute malicious payloads and software. These services are booted up when windows are started and run in the background unknowingly to the user.
They can use a technique known as Masquerading, which uses a current service name or they modify existing services to make detection harder for security analysts.

Service Stop: This is a technique used to stop or disable systems services. Stopping services which are critical can help inhibit the response of a company to an attack by an adversary. This can allow the adversary to continue their malicious attack.
Stopping high importance services may be used to bring down systems such as Twitter and stop their users from being able to render the system.
The stopping of this service can also allow for data stores to be stopped allowing the utilisation of techniques such as data destruction.

Tools used:

TrickBot: This is a tool which is commonly used by Wizard Spider. Trickbot is a Trojan spyware that has been used for the targeting of banks in locations around the world, including Ireland. This software is usually installed from phishing campaigns that contain links or malicious emails. It can also be placed using create or modify system process techniques. Once the link has been downloaded, it copies a random 12 character .exe file to the windows systems where when ran can allow for many malicious activities such as the development of Ryuk ransomware and credential harvesting.

3) Numbered Panda: This group has targeted a wide variety of high profile victims. An example of this is their target on organisations during the Fukushima Reactor Incident.

Techniques used:

Web Service: Bidirectional Communication: Twitter is a powerful existing web service which millions of users use today. This technique allows adversaries to leverage their existing web services and send commands to and receive output from a compromised system. The infected systems can be sent commands(C2). The output of these commands can be received in various ways such as the compromised system posting on a form or sending a tweet which was not initially authenticated by the compromised system in the first place. Using these familiar media sources allow for the adversary to hide and become undetected easily, especially with SSL encryption.

Exploitation for Client Execution: This involves the exploit of software vulnerabilities in client applications to execute code. Files are shared, which can only be opened by applications that are commonly used to do work, such as PDF or excel sheets. Files can be shared in offices which once opened allow for an exploit to run on the system without the user's knowledge. Users can also have their systems compromised if they are routed through certain endpoints while web browsing. These files and links to endpoints can be found on Twitter.

Tools used:

HTRAN: This tool allows for a user to hide their true geographical location by proxying connections through intermediate hops. This allows the adversary to hide their location so they can not be tracked by the victim's network if they are discovered. A "listener" program is hacked stealthily onto an unsuspecting host anywhere on the Internet. It redirects the returning information to the hacker's server when it receives signals from the actual target system. This tool is used to pass communication from unauthorised ports via ports whitelisted in firewalls.

4) Inception is a cyber espionage group. They have attacked many locations, including Europe. They specialise in leveraging the cloud and IoT to make their detection harder. They are also known as Cloud Atlas

Techniques used:

Application Layer Protocol: Web Protocols involves the adversary using application layer protocols associated with web traffic to communicate with systems they are attempting to compromise. The use of this method allows them to avoid detection by blending in with existing traffic. The commands which an adversary is trying to send will be blended in an embedded within the protocol traffic, so they do not stand out. As HTTP packets have a lot of associated fields and headers, it is easy for these commands and responses to be communicated between an infected system. This technique is also used for C2 communication, as seen in a previous references technique.

Credentials from Password Stores: Credentials from Web Browsers: Web browsers are now equipped with services that allow the saving of credentials for sites that the user visits. An example of one of these sites may be Twitter. These credentials are stored in an encrypted format within an area known as a credential store. However, these adversaries have methods to extract this data from the web browser in plain text, exposing the credentials for a user's Twitter account. They can read the chrome user database file, perform a SQL query on it and then use a Windows API function, CryptUnprotectData, which uses a user's cached logon credentials as the decryption key.

Tools used:

LaZagne: This is an open-source tool which is publicly available on Github. It is marketed as a tool to recover stored passwords on a system but has been used to recover infected systems passwords. Once these passwords are recovered the same credentials can be run over many sites in the hope of people using the same credentials on many sites. Each software stores its passwords using different techniques.An example of these are plaintext, APIs, databases and custom algorithms.This tool has been developed for the purpose of finding these passwords for the most commonly-used software.

Part 3: Detection and Analytics

Brute Force: A data source for this technique is authentication logs. These logs display information about authentication events that occur when a user tries to access a network or its resources which have been controlled and access is monitored by an Authentication Policy. These authentication logs can be used to identify suspicious activity such as this Brute Force. These logs can be used to also check and help with troubleshooting user authentication permissions and help the admin to adjust the authentication policy.

Service Stop: A data source for this technique is Process Monitoring. Process monitoring is a provided tool in windows which allows the user to view the currently running process/thread activity. It can be used to detect any running process including malware, but it can also be used by adversaries to stop a service which may be essential to the running of a system. Process Monitor can be used to detect failed attempts to read and write registry keys. This tool is also used for the monitoring of CPU utilisation, memory utilisation and CPU temperature.

Credentials from Password Stores: System calls let a computer request a service from the kernel of the operating system. These system calls use APIs. An example of an API used for gaining password stores is the CryptUnprotectData Windows API. All programs needing resources must use system calls. These System calls can provide file access and networking to the adversary, which are essential for grabbing their credentials.

The detection of Brute Force involves the monitoring of the authentication logs. The logs must be monitored for system and application login failures for accounts which are valid in the system. If there is a high amount of authentication failures on these accounts, then this may be a sign of a brute force attempt on a system. One way to prevent brute force attacks which are usually automated is to enable CAPTCHA as most automated systems cannot get by these measures. It is important to monitor and look out for a high amount of failed login cases with one successful login, where the same IP is exceeding a high amount of reject or invalid login returns and monitoring the number of attempts over a period of time.

Part 4: Adversary Emulation and Assessments

1. Summary of one atomic test

One atomic test that I looked into was T1110.1; this is a sub technique of Brute Force hacking and is known as password guessing. Brute Forcing credentials involves the adversary creating two files, one containing usernames and the other with matching passwords. The adversary then attempts to brute force their way into the systems they are trying to access via a remote host. If one of the guesses is correct, then they gain access to the system, but there is also the risk of being locked out from accounts due to the use of Authentication Policies. Single sign-on(SSO) and SSH are two services targeted by this method. Fin5 is an example of an adversary who has used this technique.

2. ATT&CK Metric

Below we can see the ATT&Ck Metric for the group, Fin5. Please zoom in to fully read the text. When we compare this to the techniques in the Adversary Analysis in part 2 , we can see that our information and techniques used are the same. The techniques marked in red are all the techniques used by this adversary, blue are the sub techniques of any and green is Brute Force.