Araali Whitepaper

Threat Brief for your cluster / environment

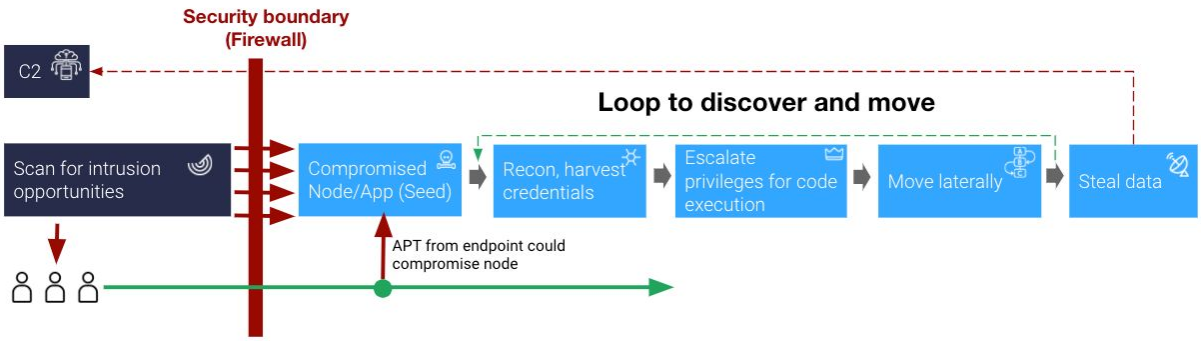
Content

Entry Point/ Getting In

Enterprises spend a lot of time and energy guarding what comes in. But adversaries have become sophisticated and are programmatically scanning and looking for opportunities to get into your environment. Any mistake, however small, they get in.

Once an adversary gets in, they have access to a broader privilege network. They programmatically scan the internal network (reconnaissance), harvest credentials, and move to the next asset. They keep repeating this loop till they get to your crown jewel, data. Sometime during the loop, they get lucky and are able to escalate privileges to a root user in the process. They are generally programmed to wipe logs and clean up their traces which makes it hard to capture these threats, sometimes also called APTs (Advanced Persistent Threats).

Some common ways adversaries get in:



1. **Public-Facing Application**

   Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands to cause unintended or unanticipated behavior. The flaw in the system can be a bug, a glitch, or a design vulnerability. If an application is hosted on cloud-based infrastructure, then exploiting it may lead to a compromise of the underlying instance. This can allow an adversary to access the cloud APIs or take advantage of weak identity and access management policies.

   Example:

   - A front end app is running struts framework, which has vulnerabilities that are exploited (**Equifax**)
   - A front end app has a WAF service, which has a vulnerability that is exploited (**CapitalOne**)
   - Blue Mockingbird gained initial access by exploiting CVE-2019-18935, a vulnerability within Telerik UI for ASP.NET AJAX

- Rocke exploited Apache Struts, Oracle WebLogic (CVE-2017-10271), and Adobe ColdFusion (CVE-2017-3066) vulnerabilities to deliver malware

2. **External Remote Service**
   Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.

   Access to Valid Accounts to use the service is often a requirement, which could be obtained through credential pharming or by obtaining users' credentials after compromising the enterprise network. Access to remote services may be used as a redundant or persistent access mechanism during an operation.

   Example:
   - Linux Rabbit attempts to gain access to the server via **SSH**
   - APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment service

3. **Trusted Relationships**
   Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through a trusted third-party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

   Examples:
   - Organizations often grant elevated access to second or third-party external providers to allow them to manage internal systems as well as cloud-based environments. **Home Depot**
   - IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security) - **Target breach**
   - The third-party provider's access may be intended to be limited to the infrastructure being maintained but may exist on the same network as the rest of the enterprise. Valid Accounts used by the other party for access to internal network systems may be compromised and used.

4. **Misconfiguration - Exposed endpoints**

   Cloud endpoint (e.g., a test VM) left publicly accessible, allowing adversaries to scan and attack it.

   Example

- Member of your dev team/test team creates a cloud instance.
- They configure security group in a way that they allow access from 0.0.0.0/0 on multiple or all ports.
- Any adversary can interact with the instance

Anecdotes

- VMs running spark clusters had a specific port open. Adversaries were able to get in, pivot, and wget script from their servers to compromise the machine and establish an entry point.

5. **Employee route - compromised endpoint/malware**

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior, such as acquiring an Application Access Token.

Example:

- A user visits a website that is used to host the adversary controlled content.
- The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
- Upon finding a vulnerable version, exploit code is delivered to the browser.
- If exploitation is successful, it will give the adversary code execution on the user's system unless other protections are in place.

Adversaries may also use compromised websites to deliver a user to a malicious application designed to Steal Application Access Tokens, like OAuth tokens, to access protected applications and information. These malicious applications have been delivered through popups on legitimate websites. This event might also happen on another personal device and laterally move to victim’s office laptop and from there to enterprise environments.

6. **Employee route - phished users**

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials, or other actionable information. Phishing for information is different from Phishing in that the objective is gathering data from the victim rather than executing malicious code.

Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

7. **Employee route - rogue behavior**

   3 types of rogue employees might undermine your application/infra security.

   A. **Ambitious and resourceful Employees** are driven to get the job done in some way or the other. They might circumvent rules to make things work. In the process, they might do something that put your organization security posture at risk
   B. **Disgruntled Employees** - This set of employees might compromise your security posture or try to steal or leak proprietary information.
   C. **Negligent Employees** - These employees disobey protocols because they are incapable or negligent. They leave/share login ids. They use office laptops to browse high-risk sites, and they probably aren't trying to harm your business and just don't know how dangerous their behavior is.

8. **Employee Route - Removable Media**

   Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes.

   Example:

   - An employee found a USB drive and inserted it into an endpoint - server or laptop.

9. **Supply chain compromise - manipulated software**

   Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

   Supply chain compromise can take place at any stage of the supply chain including:

   - Manipulation of development tools
   - Manipulation of a development environment
   - Manipulation of source code repositories (public or private)
   - Manipulation of source code in open-source dependencies
   - Manipulation of software update/distribution mechanisms
   - Compromised/infected system images (multiple cases of removable media infected at the factory)
   - Replacement of legitimate software with modified versions
   - Sales of modified/counterfeit products to legitimate distributors

10. **Hardware Additions**

Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open-source products are leveraged with capabilities such as passive network tapping, man-in-the middle encryption breaking, keystroke injection, adding new wireless access to an existing network, and others.

Example:

- There are hardware keyloggers that can be connected to victims machine to collect information
- The adversary can use Bash Bunny, Raspberry Pi, netbooks, or inexpensive laptops to connect to the company's local network

Detection and Prevention

Once an adversary gets in, it still has to programmatically move around (reconnaissance) to figure out network topology, get on other hosts, till it gets to your crown jewels, your data. It takes time and effort to map internal networking and get to the data tier. The adversary programmatically cleans up its logs/ traces in the process. That's the reason why a lot of APTs remain in the environment for months before even getting detected.

Araali enables you to turn the tables on your adversaries by disrupting their kill chain at every app/node boundary. The adversary has to successfully execute the full kill chain to take your data. Araali gives you the ability to break the kill chain at multiple points and increases your probability to win this game. Araali calls it the "Winners Approach"

Following are some of the broad class of events that happens after adversaries get in. Araali can detect, alert, and prevent these events.

11. Exfiltrations - C2 channels

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

12. Exfiltration - over web services

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of coverage due to the likelihood that hosts within a network are already communicating with them prior to the compromise. Firewall rules may also already exist to permit traffic to these services.

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

13. Exfiltration - transfer data to cloud accounts

Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service. This strategy is adopted to avoid typical file transfers/downloads and network-based exfiltration detection.
A defender monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider APIs and the cloud provider's internal address space to blend into regular traffic or avoid data transfers over external network interfaces.

14. Lateral Movement

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their goal usually involves pivoting through multiple systems and accounts to gain.

Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

15. Command Control

The adversary is trying to communicate with compromised systems to control them.

Command and Control consist of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic regular, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth, depending on the victim's network structure and defenses.

About Araali Networks

Araali Networks enables enterprises to easily protect their VM and Kubernetes cluster on app boundaries with a single click and without any performance penalty. It is easy to install and run and ensures that compromises are limited to an app without putting the whole cluster/infrastructure at risk.

Want to learn more about Araali? Contact us at support@araalinetworks.com.