Growing Complexity

The cybersecurity threat landscape continues to grow as the attacks and evasion maneuvers of threat actors makes the task of detecting and tracking cyberattacks increasingly challenging. Threat actors rarely use single vector attacks anymore. They are combining different tactics and multiple techniques to achieve their objectives.

Tactics, Techniques and Procedures (TTPs), an essential concept in cybersecurity, describes the behavior of a threat actor or group. In cybersecurity, tactics refer to high level descriptions of behaviors threat actors are trying to accomplish. For example, initial access is a tactic a threat actor would leverage to gain a foothold in your network. Techniques are detailed descriptions about the behavior or actions that lead up to the tactic. For example, a technique to gain initial access could be phishing. Procedures are technical details or directions about how a threat actor will leverage the technique to accomplish their objective. For example, procedures about a phishing attack would include the order of operations or phases of the campaign. This could include details about the infrastructure to send malicious emails, who they are targeting, and if they use malspam that contains a link or an attachment.

By analyzing and profiling patterns, experts can understand criminal behavior and how specific attacks are orchestrated. A deeper understanding of a cybercriminal's TTPs provides insight into a threat actor's intentions to help your organizations understand how to prepare, respond and mitigate current and future threats.

MITRE ATT&CK

The MITRE ATT&CK[1] framework is an open and publicly available knowledgebase that contains adversary tactics and techniques based on real world observations. ATT&CK was developed by the MITRE Corporation[2], a nonprofit organization that manages Federally Funded Research and Development Centers (FFRDCs) supporting the United States government.

ATT&CK has become a valuable resource for organizations who wish to have a better understanding about specific threats they may face. ATT&CK tracks and profiles past and current adversary threats so organizations can understand specific TTPs.

Tactics

The MITRE ATT&CK Matrix contains 12 columns representing enterprise tactics leveraged by cybercriminals. These represent the "why" of a technique and describe what an adversary is trying to accomplish. In general, it's a tactical objective and the reason behind the action.

Techniques

The rows in the MITRE ATT&CK matrix are the techniques leveraged to perform the action for a specific tactic. In general, a technique represents how the threat actor achieves a tactical objective.

Procedures

By clicking a specific technique, the MITRE ATT&CK matrix will present the detailed information on how an adversary would implement the technique to achieve an objective. MITRE also provides examples of procedures based on past and known attacks.

---

[1] https://attack.mitre.org/
[2] https://en.wikipedia.org/wiki/Mitre_Corporation

Service Availability

When it comes to network and application security, maintaining service availability should be a top priority. If service availability is degraded, users will be impacted, resulting in reputation damage and loss of business. Full availability and maximized performance are the cornerstones of digital engagement, and cyber adversaries are continually developing ways to degrade, disrupt, or outright destroy data in transit or at rest. When transposed on the MITRE ATT&CK matrix, a majority of TTPs witnessed daily by Radware's Emergency Response Team are listed in the 'Impacts' column of the matrix.

Tactic 'Impact'[3]

The MITRE ATT&CK matrix lists impact tactics that disrupt availability or compromise integrity by manipulating business and operational processes. Some of these techniques include data destruction, data encryption, defacement, resource hijacking and data manipulation, but can also include network and application denial-of-service attacks. The purpose of a denial-of-service attack is to cause an 'impact' on the network or application resource of their target for various reasons.

Technique 'Network Denial of Service'[4]

In general, there are two different techniques for denial-of-service attacks: network-based floods and application-level attacks. Network denial-of-service attacks are designed to degrade or disrupt resources by flooding the available capacity of the network and denying access to legitimate users by blocking their internet access. Application denial-of-service attacks are designed to exhaust or remove service resources of applications, servers or network devices and impact the availability of the service.

Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
System Shutdown/Reboot
Transmitted Data Manipulation

Figure 1: Techniques of impact tactics

Procedure 'Implementation of the Attack'

The procedure for a denial-of-service attack are the steps taken by the attacker to target a victim and cause a desired impact on the network or application. In the case of a botnet-based, distributed denial-of-service network flood, this could include actions such as network reconnaissance, spreading malware in the form of IoT bots, renting an off-the-shelf attack platform such as a booter/stresser service, and more.

---

[3] https://attack.mitre.org/tactics/TA0040/
[4] https://attack.mitre.org/techniques/T1498/

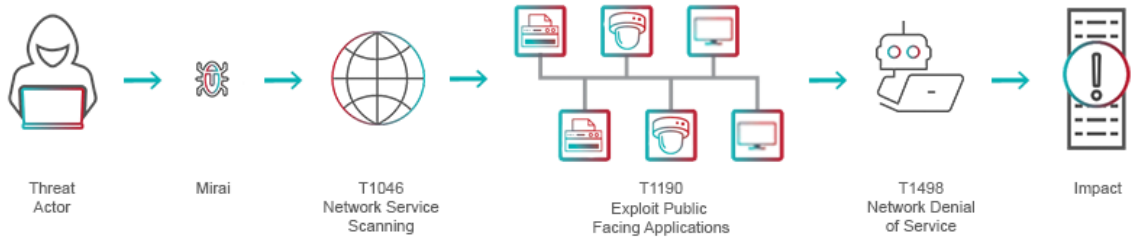

Figure 2: General procedures related to a DDoS using a botnet

Mirai

Mirai is a piece of malware that turns IoT devices running the Linux operating system into controlled 'bots' that can be used as part of a botnet in large-scale network DDoS attacks. The Mirai botnet was discovered in August 2016 and has been used in some of the largest and most disruptive distributed denial-of-service attacks. Below are the MITRE ATT&CK techniques used to create a botnet for the purpose of launching a denial-of-service attack.

Impact	Technique	ID	Description
Initial Access	Exploit Public-Facing Applications	T1190	Mirai variants take advantage of design vulnerabilities in internet facing IoT devices by exploiting SSH/Telnet
Lateral Movement	Exploitation of Remote Services	T1210	Mirai variants spread through remote code execution (RCE) vulnerabilities
Discovery	Network Service Scanning	T1046	Mirai conducts internet wide scans to discover new vulnerable IoT devices
Credential Access	Brute Force	T1110	Mirai leverages a list of hardcoded credentials to brute force IoT devices through Telnet and SSH
Execution	Exploitation for Client Execution	T1203	Demonbot was observed attempting to exploit known vulnerabilities in Hadoop
Command and Control	Domain Generation Algorithms	T1520	A Mirai variant was observed using DGA for protecting its command and control infrastructure
Defense Evasion	Connection Proxy	T1090	Botnets such as OMG, VPNFilter create anonymizing proxy networks through socks enabled bots leveraging open source software such as 3proxy. UPnP vulnerabilities in consumer routers have been abused to create port forwarding schemes that conceal malicious communications and attacks through port-hopping across multiple routers
Impact	Network Denial of Service	T1498	Mirai can conduct network denial-of-service attacks
Impact	Endpoint Denial of Service	T1499	Mirai can conduct endpoint denial-of-service attacks such as simple HTTP(S) floods

Figure 3: Examples of techniques used by DDoS IoT botnets

Corporate Insight

Effectively fighting these attacks requires specialized solutions, including behavioral technologies that can identify the threats posed by Mirai and other IoT botnets. It also requires an understanding of how to successfully mitigate the largest attacks ever seen. One of the best ways to understand the evolving threat landscape is by studying and contributing to the standardization of threat intelligence.

The MITTRE ATT&CK framework helps organizations gain knowledge about attack vectors and understand the threat landscape. This type of information allows them to focus their defenses and improve attack detection rates and analytic strategies.

Advice

The MITTRE ATT&CK matrix provides an exhaustive list of known techniques and tactics so a company can audit and better structure its defensive policies and detection methods. The MITTRE ATT&CK framework provides a common language across industries. Incorporating the structure and naming conventions used in the MITTRE ATT&CK matrix in an organization's security policy will enable a common language across the organization and the industry.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools, visit DDoSWarriors.com. Created by Radware's Emergency Response Team, it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.