Command and Control

Command and Control is the 11th stage of the MITRE ATT&CK framework. Command and Control consist of techniques and methods adversaries use to communicate with systems they have compromised on the targets networks. Adversaries use various methods of command and control and will use commonly used protocols and ports to blend in with normal traffic, making malicious traffic harder to identify. At the time of writing there are a total of 16 techniques for Command and Control. **We will be looking at the following:**

- Application Layer Protocol
- Web Service
- Non-standard Port

MITRE Technique T1071

Adversaries commonly use application layer protocols to blend in with standard traffic and to assist in avoiding detection as a method of command and control (C2). Adversaries utilise numerous different protocols including HTTP, HTTPS, DNS and others that are associated with standard web browsing or email usage. Looking at the sub-techniques for Application Layer Protocol we can see the methods commonly used for C2.

Sub-techniques (4)

ID	Name
T1071.001	Web Protocols
T1071.002	File Transfer Protocols
T1071.003	Mail Protocols
T1071.004	DNS

Cobalt Strike is a popular attack platform for both penetration testers and malicious actors, and allows communication between internal systems encapsulated in SMB. Once the traffic comes back to the host that is beaconing out to the command-and-control IP address it will send information back to the attacker. Dragonfly 2.0 have also been observed using SMB as a C2 method, and Duqu uses a custom C2 protocol which is encapsulated in application layer controls such as HTTPS, DNS, and others.

Procedure Examples

Name	Description
Cobalt Strike	Cobalt Strike conducts peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.[1]
Dragonfly 2.0	Dragonfly 2.0 used SMB for C2.[4]
Duqu	Duqu uses a custom command and control protocol that communicates over commonly used ports, and is frequently encapsulated by application layer protocols.[2]

The best mitigation for preventing the use of this technique is to use Network Intrusion Detection and Prevention Systems (NIDS/NIPS) to alert on suspected C2 activity or to take automated actions to block the connection and effectively remove the adversary from the network (but beware, the actor may have multiple methods of C2 communication).

There are numerous detection methods that can be used for this. The utilisation of an IDS system such as Suricata, Snort or Zeek can greatly assist in this. Zeek contains a log type by default named x509.log, which extracts certificate information seen over the wire. By default, C2 servers may use the same default certificates, on your SIEM tool you can run queries against this and alert based on a blacklist of known 'bad' certificates. Continue utilising your SIEM tool by looking for ports that machines may be listening on, with an unknown service, that may not be normal to that host.

Another detection method is to analyse network data for any uncommon data flows, such as a client sending huge

amounts of data out to an external IP address. Ask the following questions:

- **Should my client be communicating directly out the network?**
- **How much data has it sent?**
- **Has there been other unusual traffic on this host?**

Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.

Detection

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.[7]

MITRE Technique T1102

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

There are some really interesting examples for this technique where adversaries have utilised legitimate services to communicate with infected systems within a network. FIN6 have previously used Pastebin to host content related to cyber operations, Gamaredon Group hosts malicious code on GitHub which is then downloaded to an infected system by their .NET executable on a target system. Inception has utilised a large number of cloud service providers into the C2 infrastructure to provide resiliency and ensure that they can continue to operate even if one method is taken down.

Procedure Examples

Name	Description
FIN6	FIN6 has used Pastebin to host content for the operation.[1]
Gamaredon Group	Gamaredon Group has used GitHub repositories for downloaders which will be obtained by the group's .NET executable on the compromised system.[6]
Inception	Inception has incorporated at least five different cloud service providers into their C2 infrastructure including CloudMe.[2][3]
Rocke	Rocke has used Pastebin, Gitee, and GitLab for Command and Control.[4][5]

To mitigate malicious communications using web services, same with application layer protocol C2, organisations should deploy Network Intrusion Detection and Prevention Systems (NIDS/NIPS). Detection systems can generate alerts when suspicious activity is detected which will be investigated by security analysts, while Prevention systems can take automated actions to block or reset connections and inform the security team. Organisations should also be using a web proxy to filter incoming and outgoing web traffic, which allows for the ability to blacklist domains to prevent outgoing connections. Depending on the business operations of the company, it may be possible to block sites such as GitHub or Pastebin to prevent them being used for command-and-control or data exfiltration purposes.

To detect unusual activity regarding web services we should monitor for uncommon data flows, such as a client sending a lot more data to a web resource than is being returned, a typical indicator of an upload occurring. Timestamps should also be monitored, as an employee working 9AM – 5PM logging in at 4 AM on a Sunday and visiting GitHub is pretty unusual, and needs to be investigated immediately.

Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.
Restrict Web-Based Content	Web proxies can be used to enforce external network communication policy that prevents use of unauthorized external services.

Detection

Host data that can relate unknown or suspicious process activity using a network connection is important to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure or the presence of strong encryption. Packet capture analysis will require SSL/TLS inspection if data is encrypted. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). User behavior monitoring may help to detect abnormal patterns of activity.[7]

MITRE Technique T1571

Adversaries may communicate using a protocol and port that are typically not associated. For example, HTTPS over

Adversaries may communicate using a protocol and port that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

A couple of examples include APT33 using HTTP over 808 and 880 instead of 80, and BADCALL malware uses ports 443 and 8000 using FakeTLS (Read the CISA malware analysis report here, and CTRL+F "fake" to learn about FakeTLS!).

Procedure Examples

Name	Description
APT-C-36	APT-C-36 has used port 4050 for C2 communications.[24]
APT32	An APT32 backdoor can use HTTP over a non-standard TCP port (e.g 14146) which is specified in the backdoor configuration.[22]
APT33	APT33 has used HTTP over TCP ports 808 and 880 for command and control.[1]
BADCALL	BADCALL communicates on ports 443 and 8000 with a FakeTLS method.[18]

As which the other two techniques above NIDS/NIPS should be used within the environment to alert or take actions against suspicious or malicious network traffic. Proper segmentation should be implemented using firewalls and VLANs to limit which systems can communicate directly with each other. Perimeter firewalls and proxies should also have restrictions on what ports are being used for outbound connections, such as only allowing TCP 80 for HTTP and 443 for HTTPS.

Packet inspection would be the best way to identify unexpected behaviour in network traffic so that it can be flagged for inspection or dropped to prevent it leaving the organisation. Tools such as Snort and Bro/Zeek offer this functionality using free and community rules.

Mitigations

Mitigation	Description
Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level.
Network Segmentation	Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports for that particular network segment.

Detection

Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.[29]

Previous Topic

Mark Complete

Next Topic

Back to Lesson