COMMAND & CONTROL KEY FACTS

Formation and use of a Command and Control (C&C) system is an essential part of remotely-conducted cyber attacks. C&C is used to instruct compromised machines to perform malicious activity—C&C can also be used as a channel over which data can be exfiltrated. Statistics show that cyber attacks are widespread across all sectors and that preventing intrusion is difficult. A promising alternative consists of detecting and disrupting the C&C channels used by attackers: this effectively limits the damage suffered as a consequence of a successful attack (e.g., preventing sensitive data to being leaked).

C&C communication and traffic

Attackers experiment with alternative strategies to build reliable and robust C&C infrastructures and to devise stealthy communication methods. As a consequence, different C&C architectures and communication techniques have emerged. For example, attackers have used centralised architectures, based on the standard IRC and HTTP protocols. More recently, they have introduced decentralised architectures based on P2P protocols, which are more difficult to take down. Similarly, direct forms of communication have been substituted by encrypted channels, where attacker's commands and stolen information cannot be readily accessed. To make channel detection and blocking more difficult, attackers also use covert communication mechanisms that mimic regular traffic patterns. For example C&C traffic can occur through pages and images on Online Social Networks (OSNs), covert DNS traffic, and networks for anonymous communication, such as Tor.

C&C detection and disruption

A variety of techniques for the detection and disruption of C&C channels have been proposed. They typically rely on the automated monitoring and analysis of network traffic to identify indicators of compromise, malicious traffic, or anomalous communication patterns. The importance of human involvement in this activity cannot be overstated. As attackers constantly adapt their strategies, it is critical to gain a thorough understanding of the traffic flow patterns followed by manual tuning of monitoring, detection, and response infrastructure at periodic intervals.

The following is a checklist of measures that help detecting and denying C&C in your organisation. More detailed information can be found in the accompanying report.

Detect known-bad network activity

Collect and anal- yse network traffic to identify activity that is known to be caused by an active C2 channel.

- *Monitor DNS traffic* to identify internal devices that attempt to contact domains that are known to be involved in C2 activity. This measure involves collection of DNS traffic information (either through a passive DNS collector or via the name servers logs) and matching of requests against one or more blacklists of malicious domain names.
- *Monitor IP traffic* to identify internal devices that attempt to connect to endpoints that are known to be involved in C2 activity. This measure involves collection of IP traffic information (for example, enabling NetFlow and sFlow collection in routers) and matching of communications against one or more blacklists of malicious IP addresses.
- *Monitor traffic content* to identify content that matches known C2 traffic (e.g., specific network request/responses signatures). This measure involves collection of full traffic content (for example, enabling a network sniffer) and matching of the collected data against traffic signatures.

These measures enable the detection of C2 channels that are set up by known malware families, leverage known infrastructure, or employ known communication techniques.

Detect anomalous network activity

Collect and analyse network traffic to identify activity that deviates from the expected, normal traffic profile of the monitored network.

- *Establish traffic baselines* to determine the "normal" profile of the network (normal communication patterns, data exchange volumes, etc.). This measure can be implemented by determining baselines for different time windows (e.g., hour, day), internal devices, and network services.
- *Evaluate current network activity* against the established baselines to identify deviations that may be indicative of C2 activity. Pay particular attention to anomalies such as periodic beaconing, surge in the amount of exchanged traffic, suspicious network behaviours.

For example, C2 activity that relies on fast-flux techniques can be detected by searching DNS data for patterns of fast-changing associations between domain names and IP addresses; DGA-based C2 activity is revealed in DNS data by use-and-discard patterns of domain names; data exfiltration may be detected in NetFlow data by unusually large volumes of data exchanges.

These measures enable the detection of C2 channels that are set up by never-seen-before malware families and that do not re-use any known malicious infrastructure.

Deny C2 activity

Architect and operate the network in such a way that C2 activity is effectively denied or greatly impaired.

- *Segment the network* to separate devices with different trust and risk values (e.g., front-facing, publicly servers vs. internal hosts storing sensitive documents).
- *Introduce rate-limit policies* to slow down traffic directedto disreputable or untrusted endpoints.
- *Block unwanted or unused communications mechanisms* that may be used to piggy back C2 activity (e.g., anonymisation networks, P2P overlays, social networks).

Practicalities

Start small, measure, and scale up: security controls can be applied iteratively, covering first high-risks groups, identifying mechanisms that are effective, and then expanding their applications to larger portions of the organisation.