ultraviolet

CONFIDENTIAL

THREAT REPORT:

Command and Control Analysis

Services Performed By:
UltraViolet Cyber
Casey Latham
(443) 351-7630
info@uvcyber.com

Published Date:
04-25-2024

Contents

1 Executive Summary

The UltraViolet Security Operations Center (SOC) monitors security events and detections 24 hours a day, 7 days a week. During our security operations, we can analyze various stages of Cyber-attacks using ingested logs, tools, threat intelligence and human intelligence. Utilizing proven methodologies such as Mitre ATT&CK and the Cyber Kill Chain, our analysts can proactively identify security threats through Threat Hunting and reactively respond to security threats through Detection and Response. A crucial part of our security operations is the Detection and Response of Command-and-Control (C2) activity. The Command-and-Control attack stage is wherein a Bad Actor has already penetrated enterprise network defenses and has established a foothold on a victim system or systems and is now pushing forward to accomplish their final malicious goal. Their goals can be achieved through Botnets, DDoS attacks or Ransomware, among many other types of malicious Cyber-attacks.[i] Understanding C2 attacks guides UltraViolet Analysts in protecting our customers against the effects of Cyber-attacks.

2 Technical Analysis

The terminology for Command and Control can be attributed, in this writer's opinion, to military tactics and is defined by National Institute of Standards and Technology (NIST) as,

> "'Command and Control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission."[ii]

This is a concept that bad actors, APT (Advanced Persistent Threat) groups and cyber criminals also use to attack enterprise networks. Once they achieve a foothold inside the enterprise, they deploy mechanisms such as remote-control software, botnets and other types of staging software/malware that will allow them to control the victim system, or systems, to advance the attack. This is their malicious Command. This is also where UltraViolet analysts are uniquely positioned to stop a Command-and-Control attack and by extension; stop the malicious attack in its tracks.

At UltraViolet, we deploy advanced detections through our customers enterprises that will find and alert our analysts about network communications, and for the sake of simplicity in explaining, that look malicious or better yet, should not be happening within our customers enterprise. These alerts are called affectionately, C2 alerts. Our analysts respond to all C2 alerts quickly and efficiently utilizing ingested log data, XDR, SIEMS and other tools of our trade. When possible malicious C2 traffic is alerted too, we analyze the traffic to confirm if the traffic was successful or blocked by security tools; we analyze the destination address utilizing Open-Source Intelligence, our own Human Intelligence and our in-house Intelligence provided by our TIDE (Threat Intelligence and Detection Engineering) team. We never limit ourselves to one source of reference when it comes to our analysis and streams of intelligence. Further analysis is completed in what can be identified as surrounding logs. Stated differently, we look at everything possible. The analysis happens and action is decided. If that action is to escalate, we communicate the Command-and-Control traffic alert to Senior personnel to review the analysis to confirm everything is “AJ Squared Away” for our customer and the escalation executes. Our escalations for C2 traffic for our customers include the malicious activity information, activity references and recommendations for remediation of the C2 attack.

It is always recommended by our UltraViolet team for customers to reach out to us if they require any further information on C2 escalations, or any escalations or communications. Our Customer Success team works closely with the Security Operations Center to meet and exceed our customer objectives and answer all questions.

In conclusion, the Command-and-Control phase of a Cyber-attack is crucial for the bad actor's success in executing their malicious plans and UltraViolet analysts are at-the-ready and standing-by to detect and respond to this activity with tools, intelligence, and a passion for Cyber Security.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Ensure that all systems and devices are transmitting logs to UltraViolet for analysis
- Establish an internal procedure for responding to Command-and-Control escalations from UltraViolet
- Reach out to UltraViolet during the remediation phase of Command-and-Control response if you require assistance or have any questions

5 References

Splunk:
Title: Command and control (C2) attacks explained
Source: Splunk. Retrieved from https://www.splunk.com/en_us/blog/learn/c2-command-and-control.html
CrowdStrike:
Title: What are command and control (C&C) attacks?
Source: CrowdStrike. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/command-and-control/
Date: 2024, February 21
CSRC Content Editor:
Title: C2 - Glossary
Source: CSRC. Retrieved from https://csrc.nist.gov/glossary/term/c2
Palo Alto Networks:
Title: What is a Command and Control Attack?
Source: Palo Alto Networks. Retrieved from
https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained

[i] CrowdStrike. (2024, February 21). What are command and control (C&C) attacks? - CrowdStrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/command-and-control/

[ii] CSRC Content Editor. (n.d.). C2 - Glossary | CSRC. https://csrc.nist.gov/glossary/term/c2