IronRadar℠ | IronNet

WHITE PAPER

How to proactively detect **cyber attack infrastructure**

IronNet.com | info@IronNet.com | (443) 300-6761

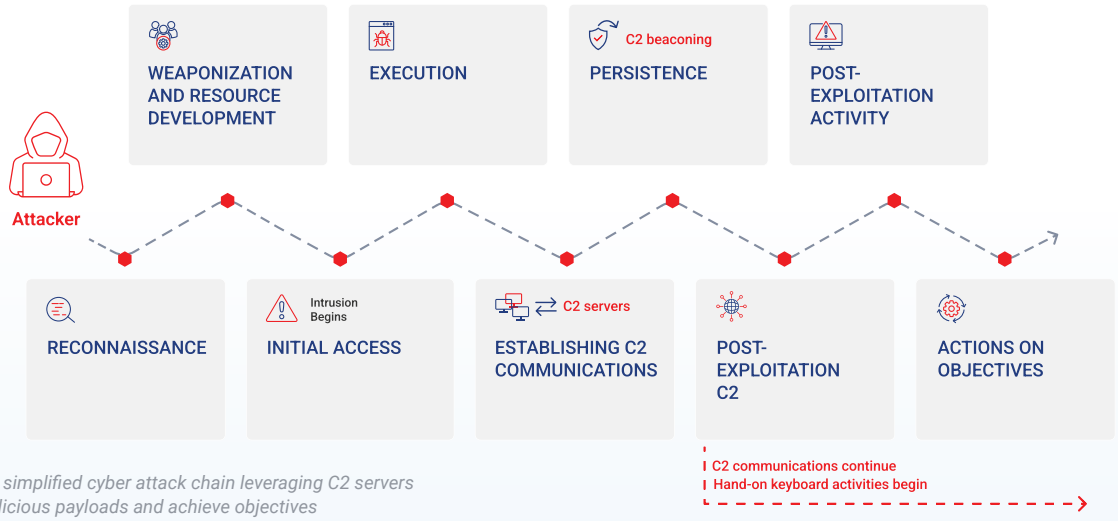
The foundation of a cyber attack

From data breaches to ransomware, all cyber attacks start with a threat actor first setting up the infrastructure – the tools, techniques, and procedures (TTPs) – necessary for the attack. This nefarious infrastructure enables them to establish and maintain a foothold in the victim's organization, conduct command-and-control (C2) communications, and drop malware payloads onto a system. An attacker's infrastructure can include many components, including redirectors or even phishing landing pages, but a cornerstone of adversarial infrastructure is a C2 server. Essentially, threat actors use C2 servers as the "brain" of the attack to maintain persistence, move laterally, drop malware, and exfiltrate data.

C2 servers: The "brains" of a malware operation

C2 servers act as command centers where a threat actor can issue commands to malware deployed in a target network and receive and store stolen data from that malware, while often blending in with normal network traffic to evade detection.

Simplified Malware Attack



Example of a simplified cyber attack chain leveraging C2 servers to deploy malicious payloads and achieve objectives

When legitimate tools become malicious C2 infrastructure

Instead of building a C2 infrastructure from scratch, adversaries often exploit legitimate and innocuous C2 infrastructure, such as existing red team tools designed for organizations to conduct penetration tests to identify security vulnerabilities. Popular platforms used by threat actors include Cobalt Strike, Covenant, Powershell Empire, and Metasploit. Among these frameworks, Cobalt Strike is the biggest go-to for threat actors; its malicious use increased by 161% from 2019 to 2020, and it was the most widely abused in 2021.

161% increase

in malicious use of Cobalt Strike from 2019 to 2020 (Proofpoint)

What is so enticing to adversaries about **Cobalt Strike** in particular?

Though developed as a pentesting/adversary simulation tool, Cobalt Strike is highly flexible and accessible (with robust documentation available), leading to its rampant abuse by threat actors, who often use cracked or leaked copies. Cobalt Strike provides a wealth of functionalities for the operator, such as keylogging, port scanning, remote screenshots, data exfiltration, credential harvesting, privilege escalation, and more.

Although Cobalt Strike is sold legitimately, it appeals to threat actors who want to acquire existing malware and related tools via underground forums; to them, it can be significantly cheaper than developing custom, in-house tools. What's more, Cobalt Strike is ideal as its wide use and commodity status make attribution much more difficult, thereby making detection of the malicious use of this C2 infrastructure even more challenging.

Why is detecting attacker infrastructure **valuable?**

The malicious use of Cobalt Strike, as well as other red team frameworks, has evolved to be used throughout the post-intrusion cyber kill chain from initial loaders to final exfiltration. For example, the ransomware group DarkSide leveraged Cobalt Strike in the infamous Colonial Pipeline ransomware attack in May 2021. SophosLabs mapped out DarkSide's toolkit as shown below:

Given C2 servers play such an integral role in executing a cyber attack, having visibility into initial C2 activity can be game-changing for defenders. Why? Because detecting activities at this stage will likely help prevent any of the subsequent downstream malicious activities that a threat actor wants to perform in your network, leading to a more serious incident (such as a data breach or ransomware attack) further down the kill chain.

Darkside Ransomware Tools

INITIAL ACCESS	EXECUTION	DEFENSE EVASION	DISCOVERY	PERSISTENCE	LATERAL MOVEMENT	EXFILTRATION	IMPACT	COMMAND & CONTROL
Phishing of credentials	Cobalt Strike	Powertool64	ADRecon	\Windows\ System32\ net.exe	PSExec	Mega.nz pCloud	wwifi.exe (ransomware executable)	Plink
External remote access (VPN, RDP)	PSExec	PCHunter	ADFind	GPO	Remote Desktop Protocol	puTTy	azure_update .exe	Anydesk
	SystemBC	GMER	NetScan	Scheduled Tasks	SSH	Rclone		Cobalt Strike
			Advanced IP Scanner			7zip		

SOPHOSlabs

USE CASE

Malicious use of Cobalt Strike

Overview

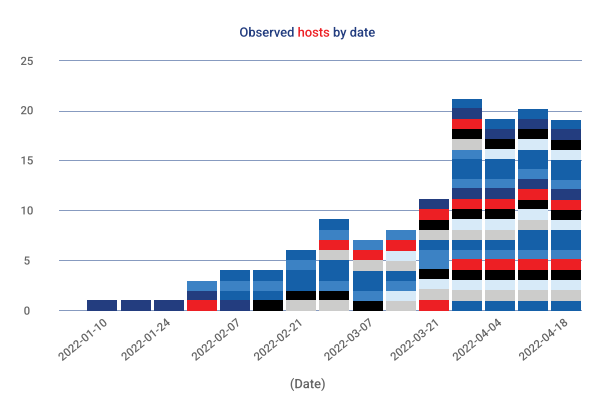
Proactive C2 detections also help add context to indicators provided by open-source reporting, such as was the case with reporting on a malicious email campaign targeting Ukrainian entities with Cobalt Strike. IronNet was able to detect the C2 servers mentioned in reporting several months prior, and we were also able to detail infrastructure features and attribute other Cobalt Strike beacon payloads to the same servers mentioned in the alert.

In April 2022, CERT-UA published alert #4490 in which they provided a list of indicators of compromise (IOCs) that are known to be Cobalt Strike C2 servers. Through scanning for malicious C2 servers, we had a longitudinal dataset of the C2 servers hosted on the IP addresses and domains referenced in the alert starting in May 2021. We were able to use this data to provide an in-depth analysis on the observed patterns of these IOCs and other indicators that may be related to those referenced in the alert.

A deeper dive into Cobalt Strike

Cobalt Strike malleable profiles allow an operator to configure the beacon communication to masquerade as benign network traffic, which is useful for obfuscating communications but can also be used as an approximate fingerprint when analyzing a Cobalt Strike C2 server. Of particular interest in this use case were two profiles observed in 2022, which overlap with Russia's invasion of Ukraine and the associated cyber attacks: a JQuery profile and a minimal defender bypass profile. JQuery is a popular choice of emulation amongst threat actors; however, the minimal defender bypass profile is something that we only noticed in the past few months leading up to CERT-UA's report and only in this campaign. The profile with the /jquery-3.3.1.min.js URI is the more common of the two profiles, both in this particular set of IOCs and in IronNet's full data set of Cobalt Strike C2 servers. The second profile, which is referred to as the minimal defender bypass profile and has the /apiv8/getStatus URI, is far more rare than the previous one. These servers were the first observations we have had of this profile. At first, we thought this was due to the relative novelty of the profile; however, further inspection indicates the profile is intended to be used behind an Nginx redirector to hide the C2 server from fingerprinting.

Apart from server configurations, there are a number of interesting relationships we observed between the infrastructure of the C2 servers mentioned in the alert. Over the course of the 15 months prior to the alert, there were three distinct clusters of activity for the IOCs provided by CERT-UA. The distribution of observations for the cluster observed in 2022 is shown in the figure below. In this cluster, 35 different domains were observed, but, as discussed above, they share many similarities such as profiles as well as watermarks.



Read the article, for more information —
Tracking Cobalt Strike Servers Used in Cyberattacks on Ukraine

The need for proactive, **actionable threat intelligence**

Before using a C2 server in a malware attack, threat actors first have to acquire it either by purchasing it legitimately, obtaining a cracked version, or obtaining a free version if it is open source. They then must take steps to stage the server, such as install software; configure the server; register SSL certificates; add files to the server; access it via SSH, RDP, or panel login; and then expose it on a port to allow for commands and exfiltration. In conducting these actions, an attacker leaves behind fingerprints. Threat intel specific to C2 can recognize these fingerprints and offer increased detection opportunities. Accordingly, the cybersecurity community has responded with detection capabilities for identifying attacker infrastructure. While these improvements in C2 detections have been significant, the majority of threat intel feeds are still reactive, meaning the intel is often shared only because someone else has experienced that attack before.

Introducing proactive threat intelligence

77% of IT security practitioners
"say threat intelligence becomes stale within minutes (54%) or within seconds (23%)"

(The Ponemon Fourth Annual Study on Exchanging Cyber Threat Intelligence, March 2021).

For that reason, there is a fundamental need to become proactive in C2 detection.

These days, the average age of a C2 (that is, the amount of time the server hosted the malicious infrastructure) is about 30 to 50 days. Detecting new C2 servers as they appear, therefore, is critical, because once the adversary has control of the compromised server, there's little time left to thwart a serious cyber attack. This is why IronNet has taken a focus on proactive threat intelligence (PTI) in addition to RTI. Proactive threat intelligence includes actively searching for threat infrastructure that has yet to be actioned and, in turn, producing intelligence before an attack occurs.

As a result, defenders rely primarily on reactive threat intelligence (RTI), which is already available information from open and paid sources, often stemming from Incident Responses (IRs), sandboxing, URL submissions, and more. While RTI is valuable for a comprehensive cybersecurity approach, it often is not the most reliable form of intelligence given that threat actors are frequently known to discard IOCs and C2 servers after use, thereby rendering the threat intel delayed and less useful in detecting emerging threats.

There is an urgent industry-wide need for proactive threat intelligence that enables organizations to block malicious C2 infrastructure immediately. Armed with such timely, relevant, and actionable attack intelligence, organizations can automatically batten the cyber hatches, so to speak, before a disruptive or destructive attack occurs.

In relation to the cyber attack kill chain of the MITRE ATT&CK® framework, PTI takes place at the resource development phase — that is, before the threat actor has gained initial access. RTI, on the other hand, is often generated at the execution or persistence phase — that is, well after the threat actor begins an intrusion into a victim network.

*Indeed, by identifying **C2 infrastructure** as it is being set up (during the early stages of the kill chain), there is an **invaluable opportunity** to be proactive.*

Proactive threat intelligence in real-life scenarios

A real-world example from the physical realm sheds light on this critical difference between RTI and PTI. In the lead up to the Ukraine-Russia War, Western allies used satellite imagery to discover and track Russian troops building up at the Ukrainian border. As a result, the West and Ukraine had the knowledge that a potential invasion might occur, as well as intelligence of the number of troops stationed, what points in the border Russia may invade, and what resources it had to supplement such an invasion. The satellite imagery and other strategic intel gleaned prior to Russia's invasion can be categorized as proactive threat intelligence in the physical world, as it was gathered as Russia was developing and staging its resources, thus allowing Ukraine and Western allies to be proactive in their defenses and set up preparations for a potential invasion.

Applying this analogy to the cyber domain shows why using proactive measures to detect adversaries' activity as they are weaponizing their resources and preparing for attack can be a much more effective mode of detection than tracking these resources after they have already been deployed. If you can see C2 as it's being set up, there is an invaluable period of time between this set-up phase and when the C2 infrastructure is actually being used in an attack. Catching malicious C2 during this in-between phase can serve as a detection "sweet spot."

A new weapon for threating cyber attacks: **IronRadar proactive threat intelligence feed**

Seeing the value in being proactive in C2 detection, IronNet's world-class threat analysts have developed a proprietary process of fingerprinting a server to determine whether it is a C2 as those servers are being stood up and even before an attack is initiated. This intelligence is provided via a threat intelligence feed called IronRadar℠ that can be directly integrated into an organization's existing security tools, thus enabling cybersecurity teams to proactively block threats and improve detection by automatically ingesting data on the latest known — as well as new and unreported — attacker infrastructure. Accordingly, IronRadar stands out as a proactive threat intelligence feed instead of a reactive one.

How does **IronRadar work?**

1 **Collect**: The first step, Collect, consists of identifying leads via an existing dataset and using a unique process to fingerprint a server to determine whether it is a malware C2 or malicious server — as those servers are being built and before an attack is initiated.

2 **Enrich:** After fingerprinting, we then enrich the data with context into purpose-built intelligence updates for proactively blocking the C2/ adversary infrastructure.

3 **Inform:** These intelligence updates are delivered via a REST API integrated directly into an organization's existing security stack, such as Firewalls, SIEMs, SOARs, EDRs, and other tools that accept third party feeds. This intelligence feed is easily accessible and can be deployed in minutes to offer protection across any network. IronRadar's ability to integrate with security tools that can consume standard threat intelligence data, as well as block or query for IOCs to correlate with other threat alerts, enables threat hunting and provides situational awareness for hunt operations or information on IronRadar integrations is available on our GitHub page.

Benefits of IronRadar

There are four characteristics that make attack intelligence actionable:

1. **Accuracy rate, unique IOCs, and high fidelity indicators.** Proven 98% accuracy over 6 months of testing with 97% unique data (addresses and domains) over 30 days compared to a leading threat feed.

2. **Attribution capabilities.** By collaborating on threat intelligence from industry partners, we are able to attribute detected C2 servers to known threat actors and identify clusters of infrastructure mapped to a specific adversary.

3. **Trend reports.** All IronRadar customers will receive a monthly C2 trends report with collated data from IronRadar detections over the past month. These reports will include analyst comments on trends observed in C2 infrastructure on a month-to-month basis, as well as details into any new IronRadar features, and unique IronRadar detections attributed to known threat actors.

4. **Benefits for both large and small SOCs.** Proactive threat intelligence produced by IronRadar provides benefits to SOCs of all sizes and levels of resources. By integrating IronRadar directly into their firewall, smaller SOCs will have a hands-off feed that can proactively block C2 servers without any interaction from analysts. Larger SOCs, however, can integrate IronRadar with their EDR and/or TIPs and contextualize the data they are receiving to facilitate hunt operations and incident response processes.

IronRadar℠ | IronNet

If you're ready to start identifying and blocking C2 servers as they are built – *before an attack* – **IronRadar is available to purchase through the AWS Marketplace, via your local channel partner, or directly from IronNet.**

Learn more **Free 14-day trial of IronRadar**

IronNet.com | info@IronNet.com | (443) 300-6761