Detecting Threats in Real-time With Active C2 Information

By Takahiro Haruyama, Omar Elgebaly

Published: 2020-09-22 · Archived: 2026-04-02 12:29:20 UTC

Often security practitioners rely on the reputation of IP Addresses to determine if traffic to and from that IOC is malicious. In practice, the reputation of IOCs, IPs specifically is only updated when public repositories or tracking projects have observed the command and control server (C2) being used maliciously. This visibility can be beneficial in more commoditized attacks or campaigns, however, with targeted attacks, C2 servers are often not disclosed until well after they're no longer utilized. For several months the VMware Threat Analysis Unit™ (TAU) has been identifying and reversing different malware families that were good candidates where TAU can discover real-time C2 instances.

As an example, look at the VirusTotal result against one IP address below. At the time of this report, AV engines detected it as harmless (0/73).

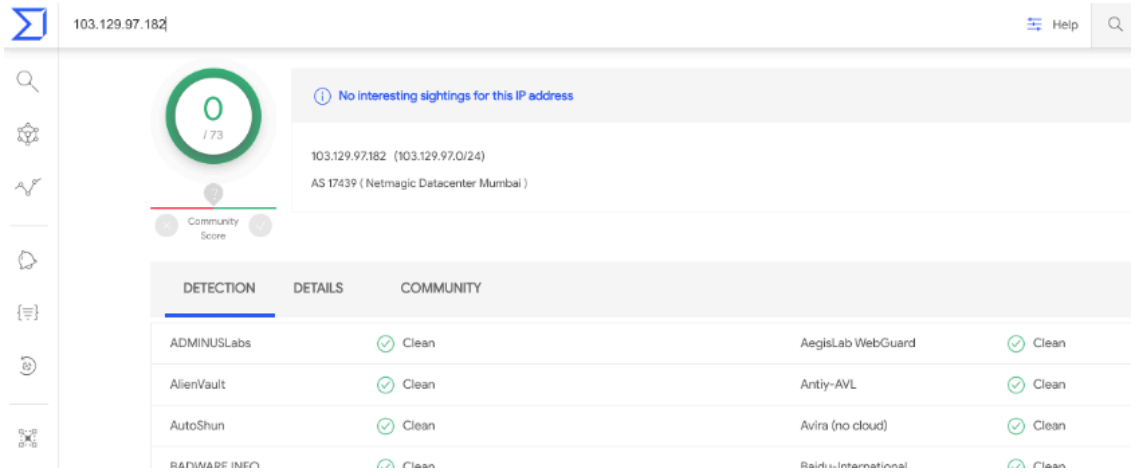

Figure 1: VT result against one IP address

However, TAU is sure it's malicious. In fact, the IP is a Winnti 4.0 C2 server. The C2 is active as of the time of this writing. How can we conclude that?

Since last year, TAU has developed a system to discover active malware C2 servers on the Internet and used this intelligence to support incident response cases. Today we are pleased to announce that this active C2 information will be available to our EDR and Enterprise EDR customers.

How to utilize the active C2 information

The information that TAU collects will be made available in the **Known IOC** Watchlist, under the **Active C2** report. It should be noted that this report will be updated on a routine basis. As we continue to discover new C2s, we will automatically add those to the report. Conversely older ones C2 IP addresses no longer being used, will be removed after 30 days of the last day they were observed. To further reiterate this point, if a C2 server is

discovered it will be added to the report when it is recompiled every Tuesday. Later when it is determined that the C2 is no longer active, the IP address will remain in the report for an additional 30 days, at which time it will be removed. This time frame allows for security practitioners ample time to identify malware samples that may still be present on endpoints that are attempting to communicate with discovered C2s.

Supported Malware families and Penetration testing tools

TAU has currently identified 6 families for which, we are actively attempting to discover C2 servers. The table below details the malware and penetration tools, where TAU is discovering the respective C2 servers. The process by which we discover these C2 servers is a snapshot in time, and it is possible that transient C2 servers can be stood up and taken down without being observed. The table also describes the protocols that we discover for each family, the date the initial discovery started, whether configuration information can be extracted as part of the process, and the current C2s observed for each family. TAU is constantly adding to the table below as new families are analyzed and deemed to be good candidates for the discovery process.

malware or tool name	supported protocols	discovery start	config extraction	accumulated total (since start date)
HYDSEVEN NetWire	TCP	Nov. 2019	no	0
Winnti 4.0	TCP/TLS/UDP/HTTP/HTTPS	Dec. 2019	no	19
Cobalt Strike	HTTP/HTTPS/DNS/ExternalC2	Feb. 2020	yes	3023
PoshC2	HTTP/HTTPS	Jun. 2020	yes	2
Dacls (aka MATA)	TLS	Aug. 2020	no	49
ComRAT v4	HTTP/HTTPS	Aug. 2020	no	1

Table 1: malware and penetration tools supported by the system

In order to discover C2 servers, the system emulates malware's customized protocols strictly. The results of the discovery process to date have not produced any significant false positives. If interested in more details, please check previous write-ups regarding HYDSEVEN NetWire and Winnti 4.0. Additionally, the system extracts configuration values by downloading/decoding samples when possible (e.g., Cobalt Strike). Note we do not circumvent any technological measure like authentication for the discovery.

TAU will continue to analyze additional malware and penetration tools and embed the C2 discovery functions into the system in order to improve our own visibility against the latest threats. By providing network-specific IOCs in combination with the native capabilities of EDR tools, customers will be able to enhance their ability to detect threats in real-time.

Known IOC Feed

Customers can review the VMware Carbon Black User Exchange post to understand where to find the Active C2 feed as well as how to subscribe to the watchlist.
