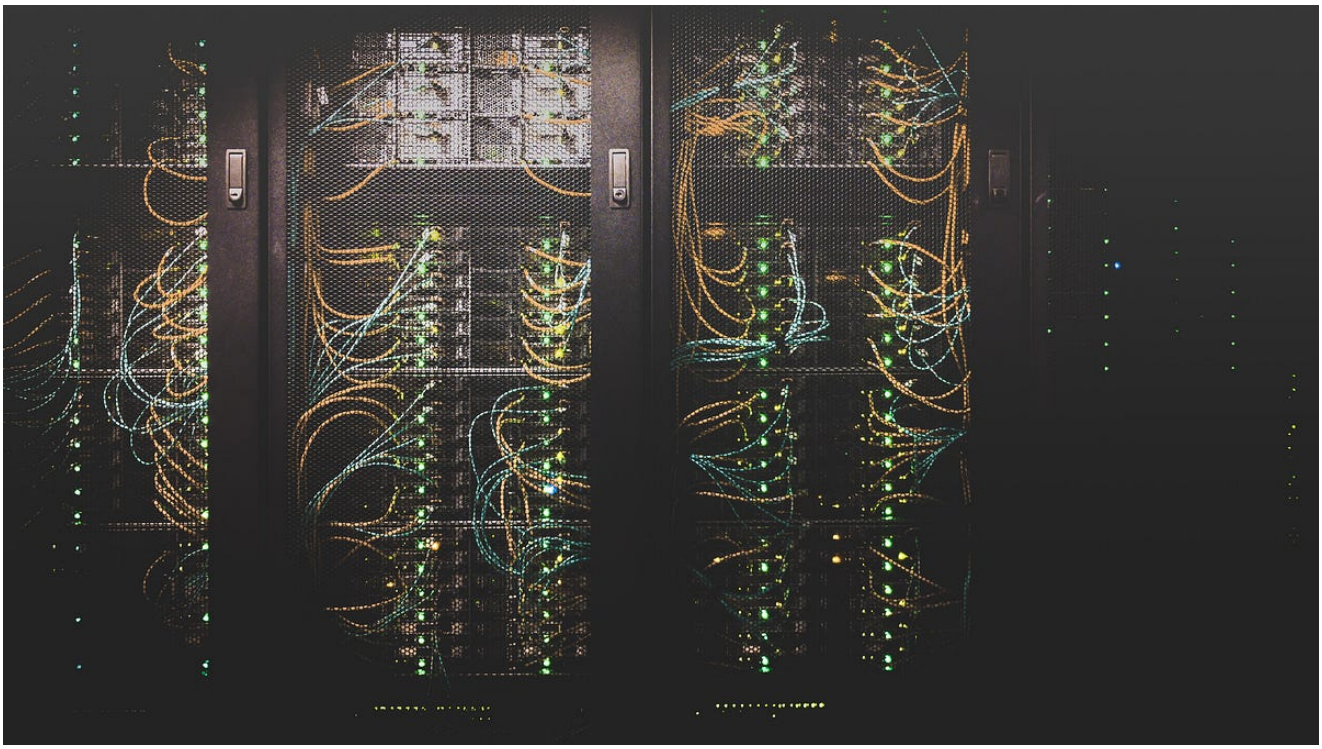
Reporting on Volt Typhoon's "JDY" Botnet Administration Via Tor Sparks Questions

medium.com/@DCSO_CyTec/reporting-on-volt-typhoons-jdy-botnet-administration-via-tor-sparks-questions-c4c5f4afcae5

DCSO CyTec Blog January 30, 2024



DCSO CyTec Blog

--

Both legitimate and criminal internet users have a long-standing demand for privacy beyond the mere usage of commercially available VPN providers, and numerous articles, discussions, and research projects revolve around the (in)feasibility of being anonymous on the internet.

The Tor network is frequently cited as the most popular and best performing anonymization network today. However, when investigating Tor usage by malicious actors, a noteworthy consideration is that not all Tor nodes (also called "relays") are created equal, with the difference between various Tor use-cases and their utility to threat actors presenting challenges but also possible opportunities for researchers.

Photo by on

In this blog post, we seek to take this consideration into account as we attempt to dig further into interesting research findings published on January 11, 2024 by SecurityScorecard concerning activity linked to China-nexus threat actor Volt Typhoon, which detailed increased exploitation activity against vulnerable SOHO devices directly exposed to the internet with the apparent target objective of expanding a botnet named “JDY” believed to be used by the threat actor for scanning/reconnaissance activity.

Blog post authored by .

Remote hands, different for once

Of particular interest to DCSO is the C2 structure (and management thereof) when investigating botnets. In SecurityScorecard’s detailed write-up, the following paragraph is noteworthy:

> Additional activity involving 45.63.60[.]39 may further reflect behavior associated with Volt Typhoon. It and 67.205.139[.]175, a Tor exit node, communicated twenty-five times between December 28 and December 30. Previous reports have noted that Volt Typhoon has used Tor for its C2 communications, so this traffic may reflect C2 communications between different Volt Typhoon-controlled resources (one routing traffic through Tor and the other hosted at 45.63.60[.]39).

According to a tool named ExoneraTor, however, which is provided by The Tor Project for enumerating if a certain IP address was in use by a Tor relay at a certain date, 67.205.139[.]175 was not configured as a Tor exit relay between December 28, 2023 and December 30, 2023. ExoneraTor also reveals that the IP address was running a Tor relay with the fingerprint of C899F20DC8005037C86B0E447857383D95FC7422, which in turn permits the retrieval of further details on its configuration via the “relay search” interface of the Tor Metrics portal.

Interestingly, Tor Metrics reports at the time of writing that a Tor relay with the fingerprint C899F20DC8005037C86B0E447857383D95FC7422 was first seen on January 10, 2024, significantly later than the timeframe highlighted in SecurityScorecard’s report. DCSO is currently under the assumption that this may be caused by a bug in the Tor Metrics interface, since ExoneraTor has reported a live Tor relay with the same fingerprint at the same IP address in December 2023, and checking the traffic history graphs for the past 6, 12, and 60 months at the Tor metrics page shows long-standing activity that suggests C899F20DC8005037C86B0E447857383D95FC7422 has been live since as early as August 31, 2022.

However, it does not appear to have been configured to be a Tor exit relay at any point in time. This means that vanilla Tor clients would not have tried to use C899F20DC8005037C86B0E447857383D95FC7422 for routing traffic from the Tor network

back to the “normal” internet. Even if they had done so, C899F20DC8005037C86B0E447857383D95FC7422 appears to be configured to reject any such connections, as indicated by the “reject 1–65535” exit policy (which rejects connection attempts to all possible destination ports). An analysis of the raw Tor network consensus data carried out by DCSO appears to confirm this, seeming to rule out the possibility of a bug in ExoneraTor.

If this observation that 67.205.139[.]175 does not appear to have hosted a Tor exit node during the relevant timeframe is correct, it could be surmised that Volt Typhoon may not have leveraged Tor’s capability to connect to normal destinations on the internet (i.e. establishing connections to a FQDN or bare IP address via Tor, thereby using a Tor exit relay on principle) for obfuscating their source IP address while conducting administrative tasks. The exact implications of such a finding, however, remain unclear; a number of possible hypotheses are posited and explored below.

Hypothesis A: 45.63.60[.]39 is running or connecting to a Hidden Service

DCSO’s first potential explanation for the network communication observed between 45.63.60[.]39 and 67.205.139[.]175 is that the former is either running a so-called Hidden Service (also referred to as “Onion Service”), or frequently connects to such a Hidden Service. In this scenario, 67.205.139[.]175 could have been one of 45.63.60[.]39’s “Entry Guards.”

Tor relays must fulfill several requirements to become eligible for use by Tor clients as an Entry Guard: relays must be stable, must provide a certain amount of bandwidth, and must have been online for a while.

C899F20DC8005037C86B0E447857383D95FC7422 fulfills all these requirements, reflected in its receipt of the “Guard” flag, a signal to Tor clients that they can use it as an Entry Guard. According to Tor Metrics, the probability of C899F20DC8005037C86B0E447857383D95FC7422 being chosen as an Entry Guard by an arbitrary Tor client was between 0.08% and 0.1% in December 2023. It is worth noting that Entry Guards are used by a Tor client regardless whether it hosts a Hidden Service or not.

If DCSO’s Hypothesis A holds correct, Volt Typhoon would appear to carry out at least a certain fraction of C2 management by connecting to a C2 system through its Tor Hidden Service, or having a Tier 1 C2 server connect to a Tier 2 counterpart hosted by a Hidden Service. The latter is in line with previous reporting on this threat actor.

From the perspective of an APT, using Hidden Services carries the benefit that the traffic never leaves the Tor network, thus leaving comparatively fewer traces on an application level that can be intercepted. It also makes attacks against the application used significantly

harder — for example, the Terrapin attack against SSH cannot be conducted if SSH is used in conjunction with Tor Hidden Services, since no AitM scenario in which the attacker can observe the application traffic is feasible.

Hypothesis B: Volt Typhoon is running Tor relays as a disguise

However, Tor Hidden Services have several downsides, such as less bandwidth, higher latency, and dependence on the reliability of all Tor relays used for a connection (the "circuit" in Tor jargon). For interactive applications such as SSH, the high latency can make usage tedious.

Superficial investigations may disregard network communication involving Tor relays for further analysis, as such connections are highly likely (but not guaranteed) to stem from Tor (exit) traffic, thus being resistant to further tracing attempts.

The Tor Project's FAQ contains an interesting entry suggesting that running your own Tor relay may increase resilience against some traffic correlation attacks since an adversary has no trivial way of determining whether a connection originated from the Tor relay (on behalf of other users) or from a Tor user connecting from the same IP address as the relay:

> Yes, you do get better anonymity against some attacks. The simplest example is an attacker who owns a small number of Tor relays. They will see a connection from you, but they won't be able to know whether the connection originated at your computer or was relayed from somebody else. […] It is an open research question whether the benefits outweigh the risks. A lot of that depends on the attacks you are most worried about. For most users, we think it's a smart move.

Similarly to such a scenario, routing non-Tor traffic through a Tor relay might allow a threat actor to evade closer investigations. However, this works best for Tor exit relays, and is not impermeable to investigators with access to all netflow and/or traffic volume data involving the IP addresses used as Tor relays and proxies for non-Tor traffic simultaneously.

Conclusion

Based on the ExoneraTor results and the Tor network consensus data analyzed, the possibility that 67.205.139[.]175 was not used by Volt Typhoon as a Tor exit relay to obfuscate the origin of connections to the C2 server located at 45.63.60[.]39 appears to emerge.

Even if this initial assessment is correct, however, without further information on the communication between 45.63.60[.]39 and 67.205.139[.]175, such as the port numbers used and whether or not the traffic metadata matches typical Tor client communication, it is impossible to conclusively assess whether hypotheses A or B hold true.

As further research continues into Volt Typhoon's activity in general, and its botnet administration and higher-tier C2 infrastructure in particular, the further analysis of forensic artifacts of Tor usage is likely to constitute a more useful source of insights to investigators than a first glance at such digital traces might suggest.