Vermilion Strike

NTT Global Threat Intelligence Center – Threat Research Report

Author: Jacob Faires, Senior Threat Research Analyst, GTIC

Contents

Our Global Threat Intelligence Center (GTIC) educates, informs and protects our clients through intelligence fusion and analytics, intelligence sharing and threat and vulnerability research. During threat research activities, the GTIC used information from a public blog to initiate a deeper dive into Vermilion Strike. Vermilion Strike is a Linux reimplementation of the Cobalt Strike Beacon, built from the ground up by threat actors.

In mid-September, Intezer released a blog detailing a reimplementation of Cobalt Strike Beacon for Linux and Windows dubbed Vermilion Strike. Our GTIC was able to pivot off the publicly released C2 IP address 160.202.163[.]100 to identify further infrastructure and narrow attribution. Using our global network visibility, we pivoted off the published address of 160.202.163[.]100 to identify a series of related IP addresses, services and tools associated with the Vermilion Strike malware.

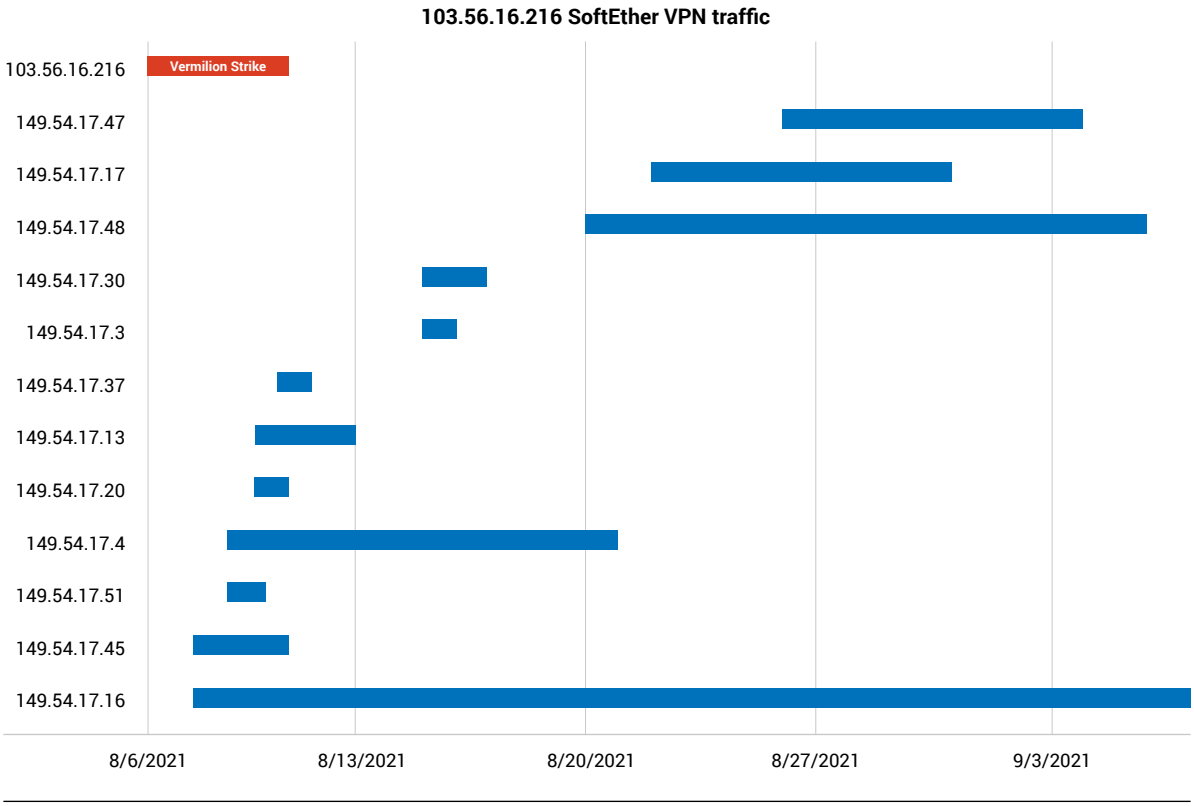
SoftEther VPN server

GTIC identified Cobalt Strike Team traffic from an Asia-based SoftEther VPN server to ports 60060 and 43968 on 160.202.163[.]100. Traffic to these ports were active until 29 August 2021. We observed concurrent connections from the VPN servers to 103.56.16[.]216 over the same control ports used by 160.202.163[.]100. Both 103.56.16[.]216 and 160.202.163[.]100 have the same self-signed SSL certificate identifying them as Cobalt Strike Team servers.

depth=0 C = Earth, ST = Cyberspace, L = Somewhere, O = cobaltstrike, OU = AdvancedPenTesting, CN = Major Cobalt Strike

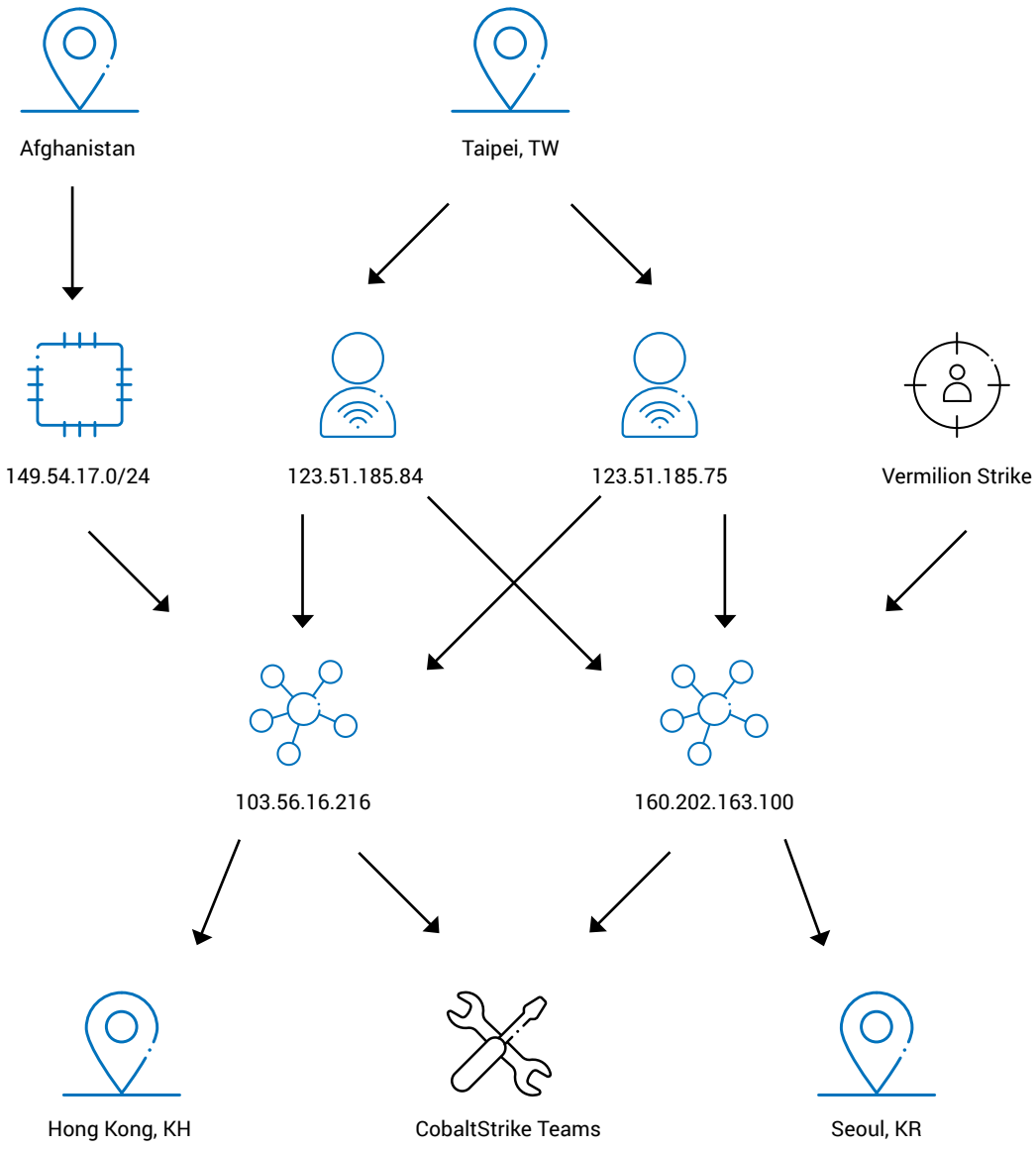
SHA256 - 2EB11CDE7B722162D7A070B1AC06A57C83A01061CF4E86CC59F42182854BBA53

Over the timeline analyzed (15 July – 15 Sept) the Cobalt Strike Server at 103.56.16[.]216 was actively controlled from 5 Aug through 10 Aug and at the time of writing was still online. GTIC discovered SoftEther VPN traffic over port 8443 coming from Afghan Telecom to the Cobalt Strike server, slowly expanding the number of hosts sending traffic.



Afghan Telecom IPs

Access to Afghan Telecom IPs started in August and continued until 7 September. Recorded Future recently released a blog detailing that multiple threat actors had targeted the mail server mail.roshan.af across the same timeframe as this attack. Analysis of our data and the C2 nodes presented by the blog corroborates the timeframe presented.



Identifying related nodes

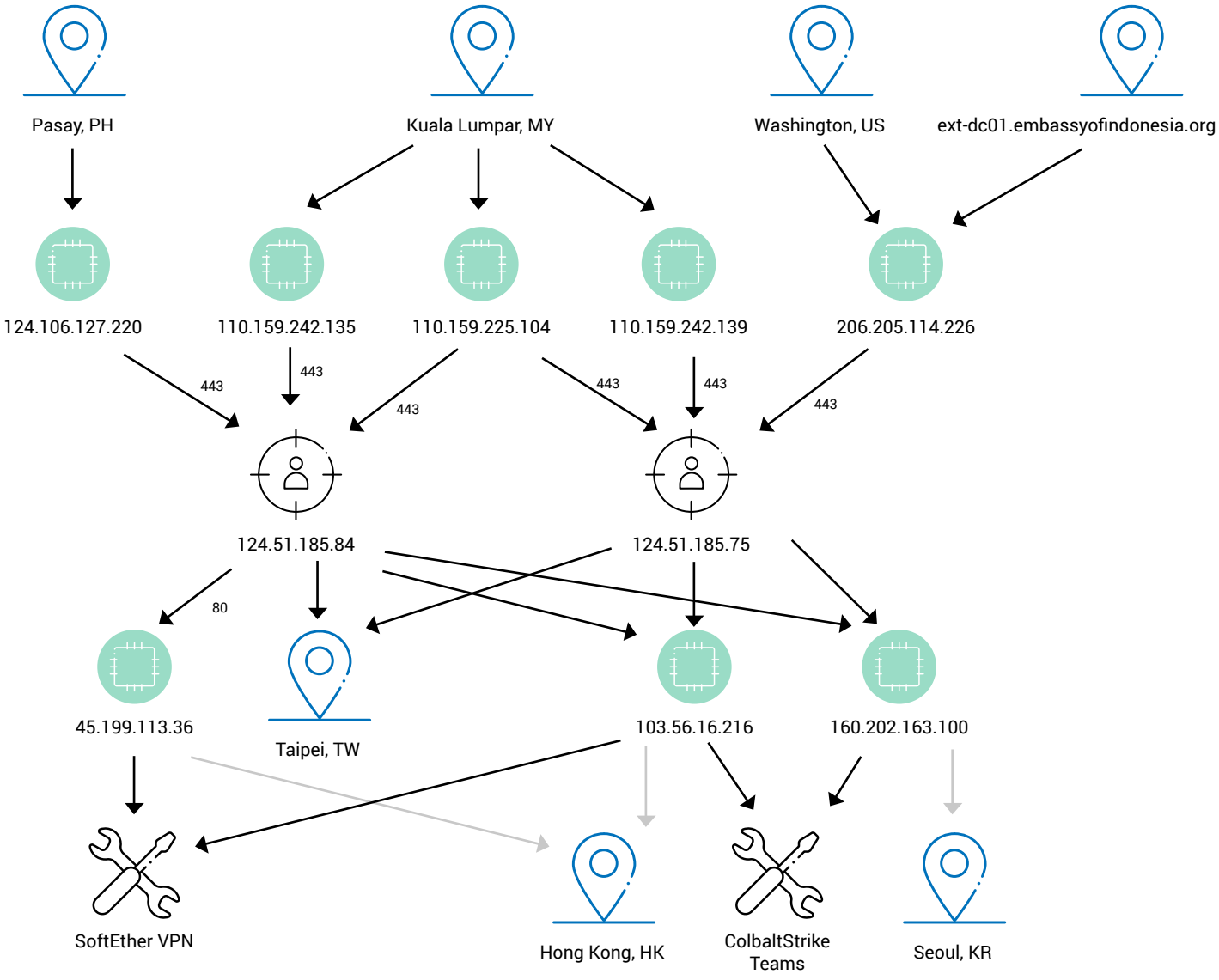
Geographically identifying traffic across the suspect VPN nodes include Malaysia, Philippines (Department of Foreign Affairs), Taiwan, Hong Kong, South Korea, and the Embassy of Indonesia. All of these are nation-state targets of interest, several of which are government oriented.

All traffic across the suspect VPN nodes, incoming and outgoing, were in Asia with the exception of the Embassy of Indonesia located in Washington DC.

- 124.106.127.202 - Philippines - Department of Foreign Affairs
- 110.159.242.139 - Malaysia - tableau.jakoa.gov.my
- 110.159.225.104 - Malaysia
- 110.159.242.135 - Malaysia
- 206.205.114.226 - Washington DC – embassyofindonesia.org
- 45.199.113.36 - Hong Kong
- 103.56.16.216 - Hong Kong
- 160.202.163.100 - South Korea
- 123.51.185.75 - Taiwan
- 123.51.185.84 - Taiwan

Multiple threat actors, including Winnti and Operation Soft Cell, have used the SoftEther VPN in previous operations. Threat actor TICK has been observed using Casper, a re-implementation of Cobalt Strike Beacon. Based on this available information, it appears that an APT is behind the development and deployment of Vermilion Strike.

We have implemented appropriate indicators of compromise into associated services and are continuing research into Vermilion Strike.



About our security capabilities

We help clients create a digital business that is secure by design. With unsurpassed threat intelligence, we help you to predict, detect and respond to cyberthreats, while supporting business innovation and managing risk. We have a global network of Security Operation Centers (SOCs), seven research and development (R&D) centers, over 2,000 security experts and handle hundreds of thousands of security incidents annually across six continents. We ensure resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology.

We partner with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace and deliver services in over 200 countries and regions. Together we enable the connected future. Visit us at our website hello.global.ntt

To find out more about our Managed Detection and Response services, please click here.


NTT