Grim Spider

NTT Global Threat Intelligence Center – Threat Research Report

NTT's 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 reviewed a DFIR Report titled 'Bazar Drops the Anchor.'

The report detailed an IP address, 23[.]94[.]51[.]80, which accessed a honey document during an incident response engagement. During the incident, attackers initially deployed bazarloader and later deployed Ryuk ransomware as the final stage of the attack.

The GTIC determined that the IP address and attack activity is associated with the group Grim Spider (also known as FIN6 or UNC1878). Grim Spider is part of the Wizard Spider group, which is notorious for operating the Trickbot banking Trojan and is also known for its deployment of Ryuk ransomware onto targeted systems as the last stage of infection. Wizard Spider is one of the most nefarious cybercriminal groups; it maintains a high tempo of operations and carries out targeted ransomware campaigns against high-value targets.

Using our global network visibility, we pivoted off 23[.]94[.]51[.]80 to discover the threat actor's working environment. By analysing the operations of a single Grim Spider node, the GTIC was able to:

- identify sites the group uses for log resale and bot affiliate program access
- identify the tools the operators used to monetize their activities
- determine how the malicious actors accomplished operational security
- observe how they carried out their daily tasks

Contents

Black market sites

We found that the IP address 23[.]94[.]51[.]80 frequents websites for log resale to monetize access to compromised machines. The IP accessed the following sites frequently and with large amounts of traffic during the last three weeks of March 2021.

Genesis Marketplace

23[.]94[.]51[.]80 frequently visited 89[.]44[.]9[.]110, the IP address associated with various domains within the Genesis Marketplace. Genesis is a black-market site specializing in the sale of cybercriminal access and information. Threat actors can purchase digital fingerprints on the market and bots which have accounts associated with target sites. These bots can mimic devices associated with previous transactions on the relevant target sites.

HYIPLogs

HYIPLogs, hyiplogs[.]com, is a site dedicated to tracking high yield investment programs (HYIPs). The site was registered on 6 March 2017, and it promises to provide a search and analysis of various HYIPs. High yield investment programs are a type of Ponzi scheme promising unsustainably high returns on investment.

RNJLogs

RNJLogs, rnjlogs[.]com, is a fairly new site, having been registered on 11 January 2021, and is used to buy and sell log files. The primary commodity available on the site is banking logs with information on users, accounts and login credentials. Since performing this threat research, RNJLogs has either moved or been taken down.

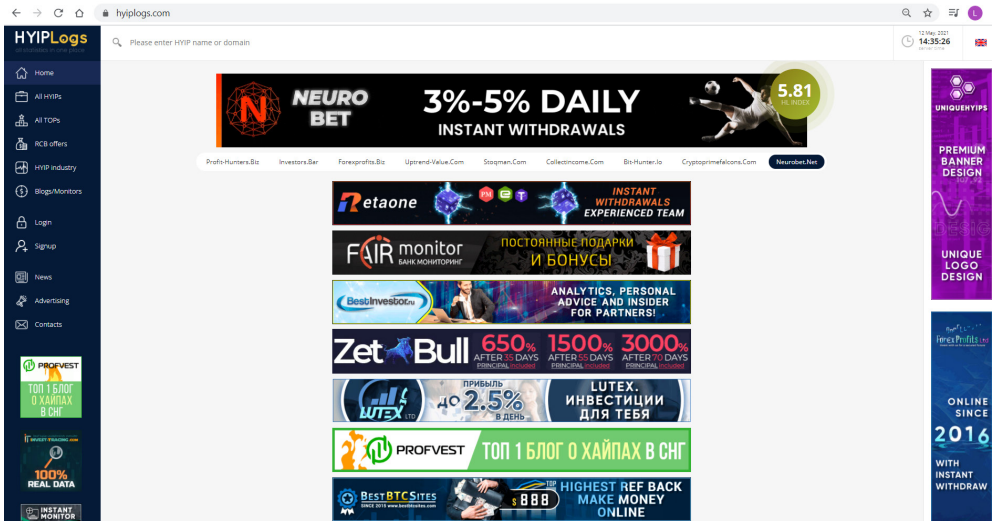
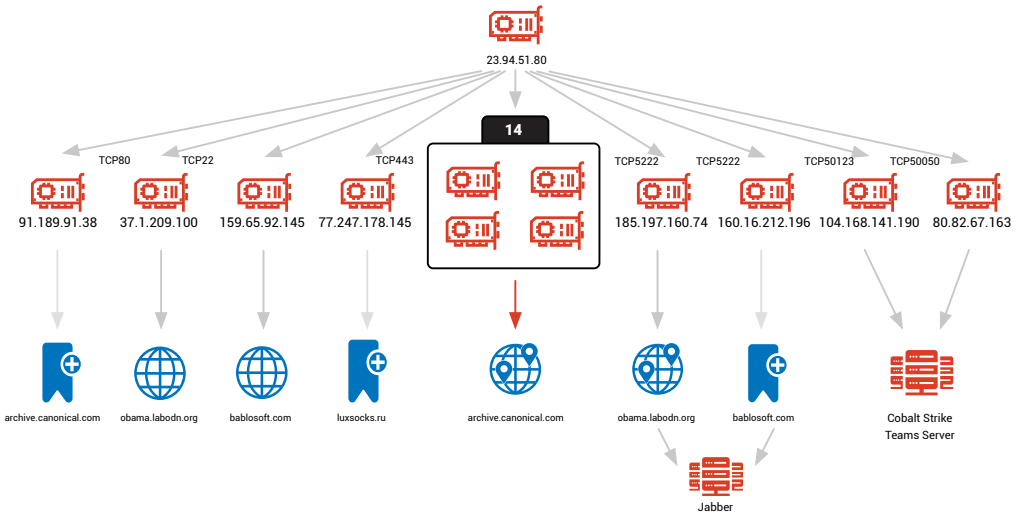


Figure 1: HYIPLogs, hyiplogs[.]com landing page

Tools

By further pivoting off the IP Address 23[.]94[.]51[.]80, we discovered a variety of tools and software associated with this Grim Spider node. The tools and software include proxy services, attack tools, cloud infrastructure and communication technologies.



Cobalt Strike

Our GTIC team discovered the pivot IP accessing a management port of 50050 for a Cobalt Strike server. Cobalt Strike is divided into client and server components; the server is referred to as the team server. The team server functions as the control point for the beacon payload and the host for Cobalt Strike's social engineering features. The server also manages logging and stores data collected by the Cobalt Strike client.

Other tools

Aside from Cobalt Strike, we discovered the pivot IP address is associated with the following:

- Luxsocks[.]ru – a proxy service that provides residential SOCKS5 proxies.
- Che Browser – a desktop application which allows for the substitution of browser and hardware fingerprints. Grim Spider likely uses the browser to leverage fingerprints acquired from Genesis Marketplace.
- Bablosoft Browser Automation Studio – a suite to automate tasks in the Chrome browser.
- MEGA – a cloud storage and file hosting service.
- Tor – an open-source software for enabling anonymous communication over the internet. GTIC identified access to several Tor exit nodes.
- Tox – a peer-to-peer instant messaging and video calling protocol that offers end-to-end encryption.
- XMPP – an open communication protocol designed for instant messaging, presence information and contact list maintenance.
- Linux – frequent access to Canonical's repositories suggests the actors use Ubuntu.

The team server functions as the **control point for the beacon payload and the host** for Cobalt Strike's social engineering features.

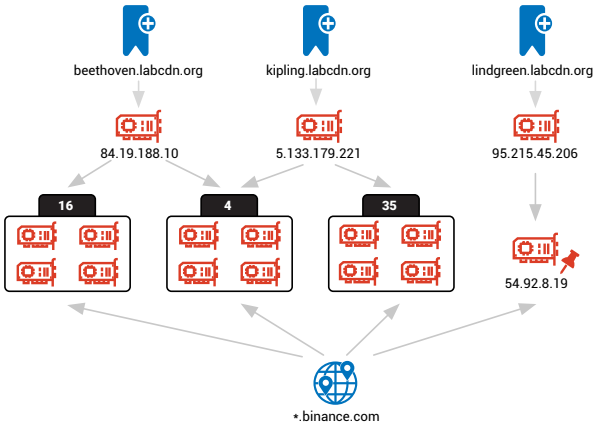
Labcdn[.]org

We discovered the most active identified connection from the pivot IP address was with the address 37[.]1[.]209[.]100. This IP address resolves to obama[.]labcdn[.]org; this site's parent domain, labcdn[.]org, has 13 subdomains located around the world. We believe Grim Spider users this network for managing their cryptocurrency. After identifying obama[.]labcdn[.]org, GTIC further researched labcdn[.]org, detailed in the following paragraphs.

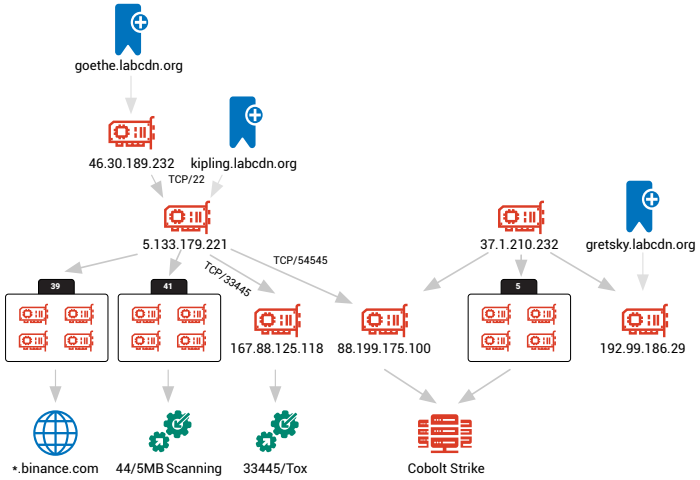
Cryptocurrency association

We discovered numerous connections from the beethoven and kipling labcdn[.]org subdomains to Binance streams (Binance is a cryptocurrency exchange). We identified similar connections from IP sources located in Russia connecting to obama[.]labcdn[.]org. The purpose of these systems appears to be solely for interaction with Binance. Additionally, the lindgren domain accessed Binance, cryptonight-hub[.]miningpool[.]com,and several Monero miners, using the Tox protocol for communication.

Over the course of the research, we found kipling[.]labcdn[.]org accessed 88[.]119[.]175[.]100 over its Cobalt Strike Team server via port 54545. Though most traffic on kipling is to Binance WebSocket streams and daily SMB scans, there are cases of direct access to Grim Spider's Cobalt Strike infrastructure.



GTIC found lindgren[.]labcdn[.]org accessed 88[.]119[.]174[.]118 via Remote Desktop Protocol. This IP is used as a Cobalt Strike Beacon command-and-control (C2) and is a known Ryuk indicator of compromise (IOC). These connections reinforce the attribution of the pivot IP to Grim Spider.



Recommendations

We've found the MITRE ATT&CK framework to be robust and provide excellent information to help organizations address cybersecurity threats and mitigate risk. Our following mitigation suggestions align with this framework:

Mitigation	MITRE ATT&CK ID	Description
User training	M1017	Grim Spider gains initial access to systems through phishing campaigns and the use of malicious attachments. Organizations can mitigate attacks by training users to only open emails, download software, open attachments and follow links from trusted sources.
Antivirus/antimalware	M1049	Use heuristic-based malware detection which has updated virus/malware definitions and create custom signatures as needed.
Filter network traffic	M1037	Use network appliances to block traffic entering or leaving a network; configure endpoints to filter network traffic; create blacklists from IP addresses known to be associated with Grim Spider.
Data backup	M1053	Take and store data backups in hardened storage systems separate from the corporate network.
Network segmentation	M1030	Architect the corporate network to isolate critical systems, functions and resources and limit their exposure to any ransomware incident.

About Security and NTT Ltd.

Security is a division of NTT Ltd., a global technology services company. The Security division helps clients create a digital business that's secure by design. With unsurpassed threat intelligence, we help you to predict, detect and respond to cyberthreats, while supporting business innovation and managing risk. Security has a global network of SOCs, seven R&D centers, over 2,000 security experts and handles hundreds of thousands of security incidents annually across six continents. Security ensures that 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 new website hello.global.ntt

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

Together we do great things