# *Malware Traffic Analysis – Incident Report*

# *Nikhil Babu Jakkam*

# *Id# 3023266*

# *The University of Tampa*

# Executive Summary:

On November 7, 2018, an aggressive malware attack targeted Carlos Danger. Detailed network traffic analysis using tools such as Wireshark and Brim pinpointed alarming signs of system compromise. An intruding host (IP: 10.22.15.2) was identified engaging in active network surveillance and mapping. The cyber adversaries employed methods like EPMapper, smb\_mapping, and kerberoasting, successfully breaching the network's Domain controller.

Subsequently, they executed a DNS poisoning strategy, redirecting users to their harmful website. The system labeled Danger\_Win\_PC (with specifications 10.22.115.119 & 00:18:8b:f7:20:6a) was notably compromised, downloading a Trojan from shumbildac.com. Notably, this site used a self-signed SSL certificate and had an IP address of 46.29.160.132.

After its successful infiltration, the malware laid its groundwork on the affected machine and initiated a connection to the attackers' Command & Control (CnC) hub at 192.162.244.171. Investigations revealed this malware to be the notorious "Ursnif" variant. It then signaled the attackers' CnC hub. Culminating their attack, the adversaries, believed to be of Russian origin, accessed the compromised machine, leading it to their website, from where a set of malicious files were downloaded, including an image and a txt file sourced from http://dhsiwyqdlskwsqo.com.

# Analysis Report:

While examining the pcapng file, the initial phase of the investigation was directed towards the identification and enumeration of hosts present within the network traffic. Utilizing Wireshark's statistical tools, essential data about IP addresses, domain name resolutions, and MAC addresses of various hosts were collected.

From this, a recurring IP address was identified: 10.22.15.119. By evaluating the conversation patterns, it was inferred that this IP address could be the primary target of any potential malicious activity. To further corroborate this, an examination of NetBios packets pointed to a user by the name of Carlos Danger associated with this IP.

The subsequent phase involved leveraging Brim for a deeper dive into the network landscape. One of the first anomalies spotted was unusual traffic patterns between the Domain Controller, known as geeographic-dc, and Danger\_Win\_PC. The domain controller, with an IP of 10.22.15.2, was engaged in activities such as EPMapper and SMB mapping. This led to a hypothesis that this domain controller might have been compromised, potentially through tactics like kerberoasting. The eventual poisoning of the DNS table seemed to affirm this, with traffic being redirected in a malicious manner.

The malware traffic analysis unveiled that Carlos' PC was lured to a potentially harmful website: shumbildac.com (46.29.160.132). This visit, flagged due to its self-signed SSL certificate, resulted in the download of a suspicious file named ngul5.xap. Validation of this file's hash on VirusTotal confirmed its malicious nature, pointing towards a Trojan malware. The likelihood is that this Trojan acted as a precursor or a gateway for subsequent malware intrusions.

Deepening the investigation with Brim showed that post the aforementioned download, the victim's machine started communicating with a Command and Control (C2) server based in Russia (192.162.244.171). This communication led to additional downloads from suspicious domains, one of which was

*“http://dhsiwyqdlskwsqo.com/images/UIL\_2BVxj\_2FFv/cAgM9ZivBfYRBhzmpmqE8/gTexqC1Lh\_2F0iW2/AATDXP0c4G4qcxV/\_2FXAAoF8eHHNZ8c43/RrSntOi0N/4VTdgqIWbPwlUsd3uIxL/BZP\_2Bzh085fEx639Yq/B1kvRr\_2FOEM0k57tlZ1QS/8lw2Htym.avi”*

Moreover, another malware identified was Ursnif. Recognized as a banking Trojan, this provided a clear insight into the probable intention behind this entire operation, suggesting a financial motivation on the attacker's end.

**Recommended Actions:**

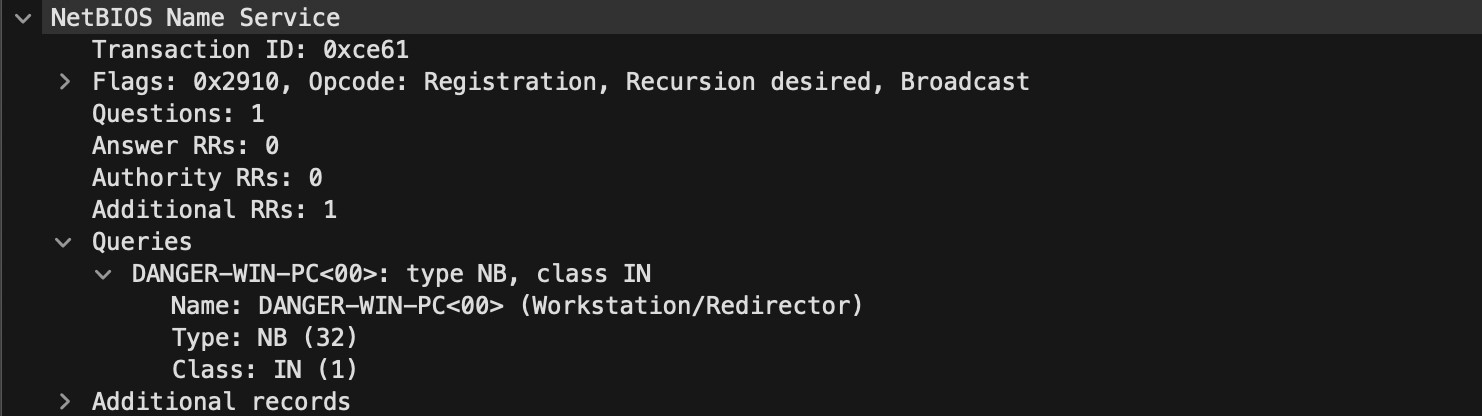
To combat such threats in the future:

* Deployment of a robust network intrusion detection/prevention system is crucial to detect and halt C2 traffic.
* Enhance domain controller security with regular updates, restricted network access, and backup DNS solutions.
* On individual endpoints like Carlos Danger’s PC, install comprehensive anti-virus/firewall solutions to vet downloads for harmful signatures.
* This incident underscores the paramount importance of adopting a multi-layered defense strategy to thwart elaborate cyberattacks.

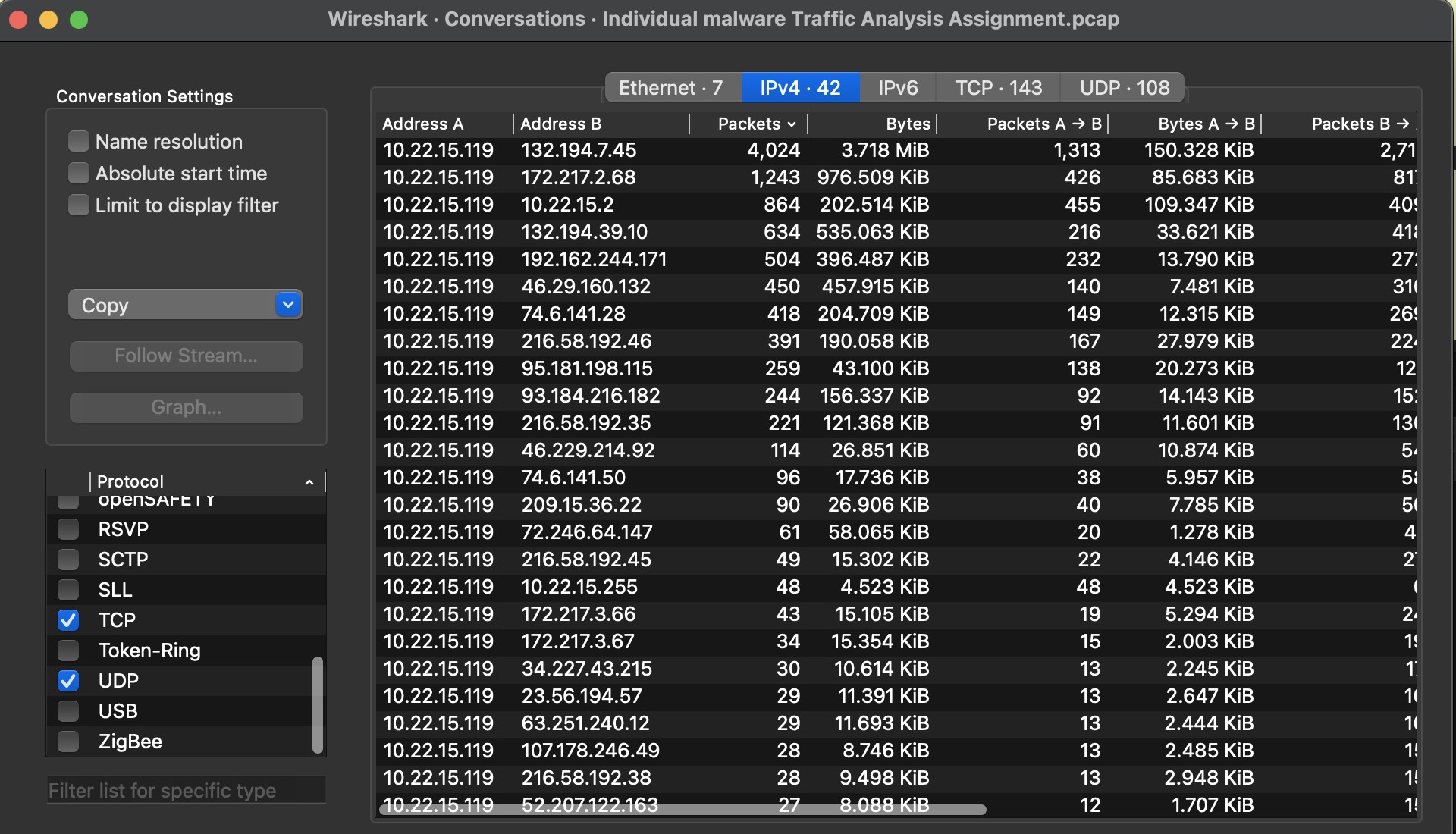
# Appendices (Indicators of Compromise):

## Victim:

Hostname: Danger\_Win\_PC (NetBios Name service packet filter -> See registration packets -> multiple names are registered -> final name registered is the hostname)



IP address: 10.22.15.119



* (Statistics-> Conversations -> IPv4 -> Most common address) MAC address: 00:18:8b:f7:20:6a



* (Statistics-> Conversations -> Ethernet -> Name Resolution -> Find most active MAC address)

Windows user account name: carlos.danger (Kerberos -> CName String)



**Attackers:**

IP address:

* (Malicious domain controller) 10.22.15.2 (Analyze conversations -> notice a variety of unusual packet types from this address to our victim IP -> discover this IP address)



* (Malicious website) 46.29.160.132
* (Malicious Command and Control Server) 192.162.244.171

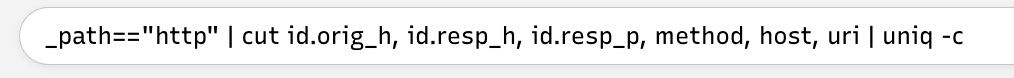
MAC address: 00:11:2f:d1:6e:52 (From IP address above -> Look at ethernet data within packet

-> find this MAC address (ASUSTek)



**Ngul5.xap Malware:**

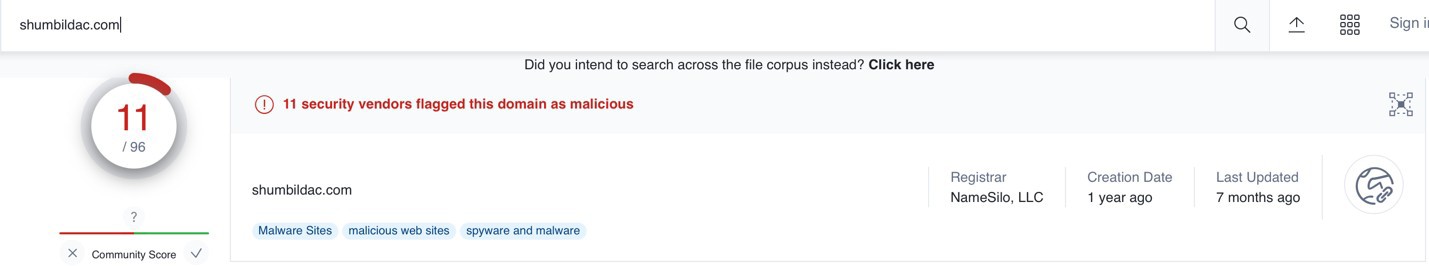
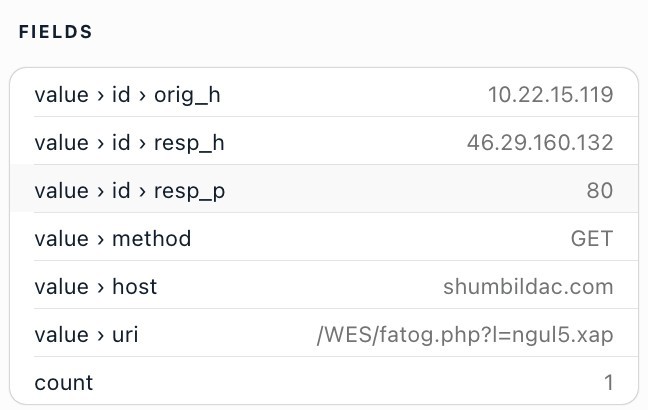
Filtering Brim for malicious traffic/files



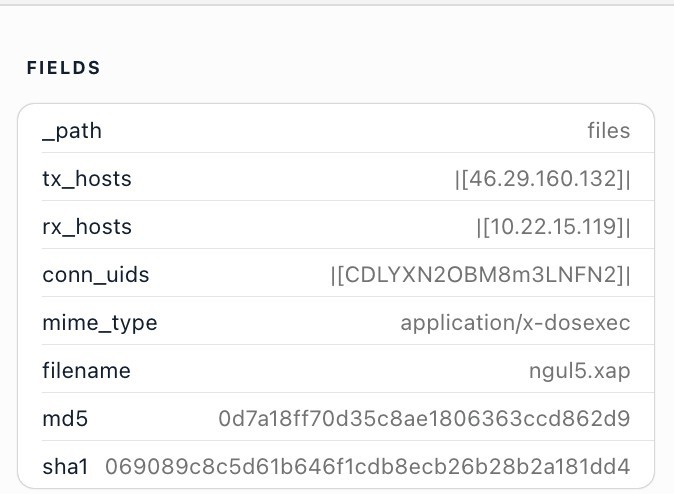
Brim identifies the file *ngul5.xap* as a malicious file.



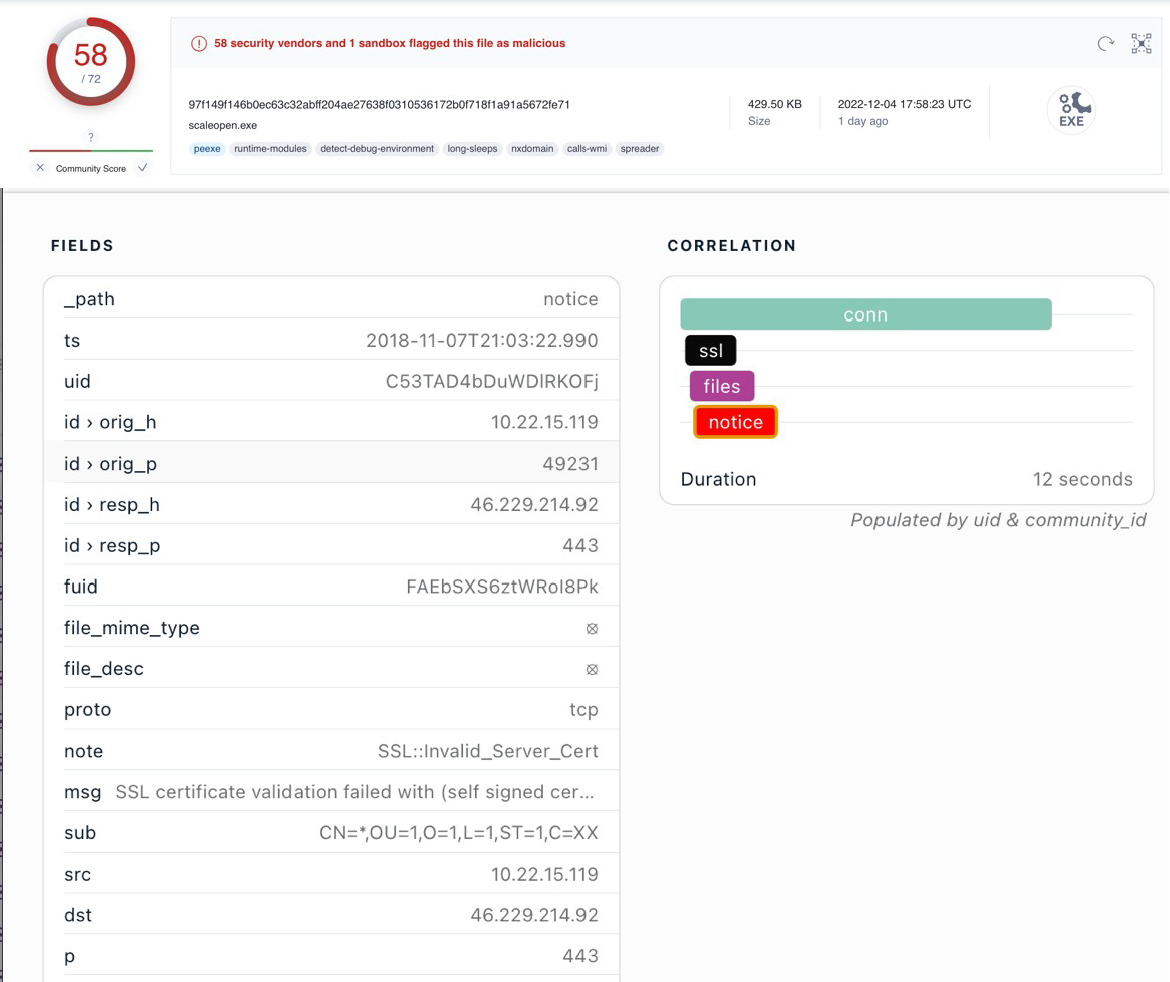
Digging further into the source, we find the HTTP “GET” request from a malicious website.



Brim enables us to retrieve the file hashes.

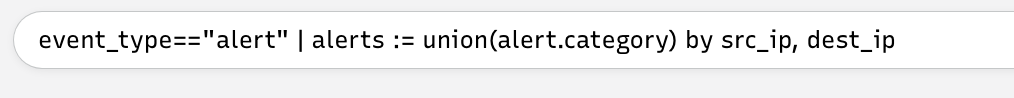


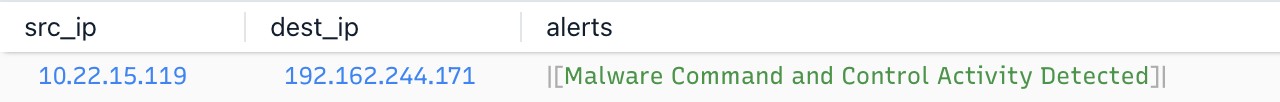
Virus Total confirms this file-hash is malicious. The file is a Trojan malware.



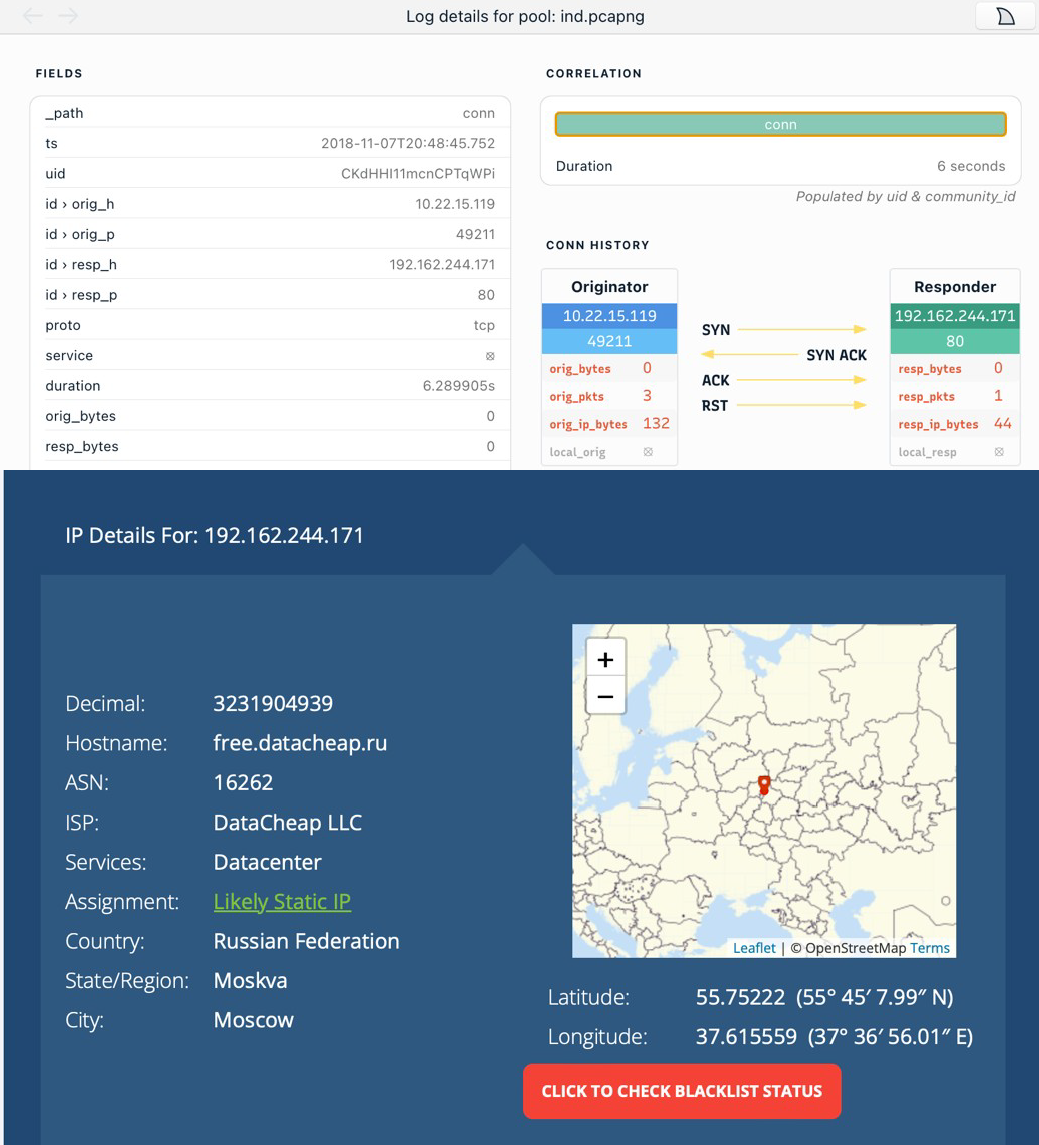
**Command and Control:**

Filtering Brim for for command & control traffic

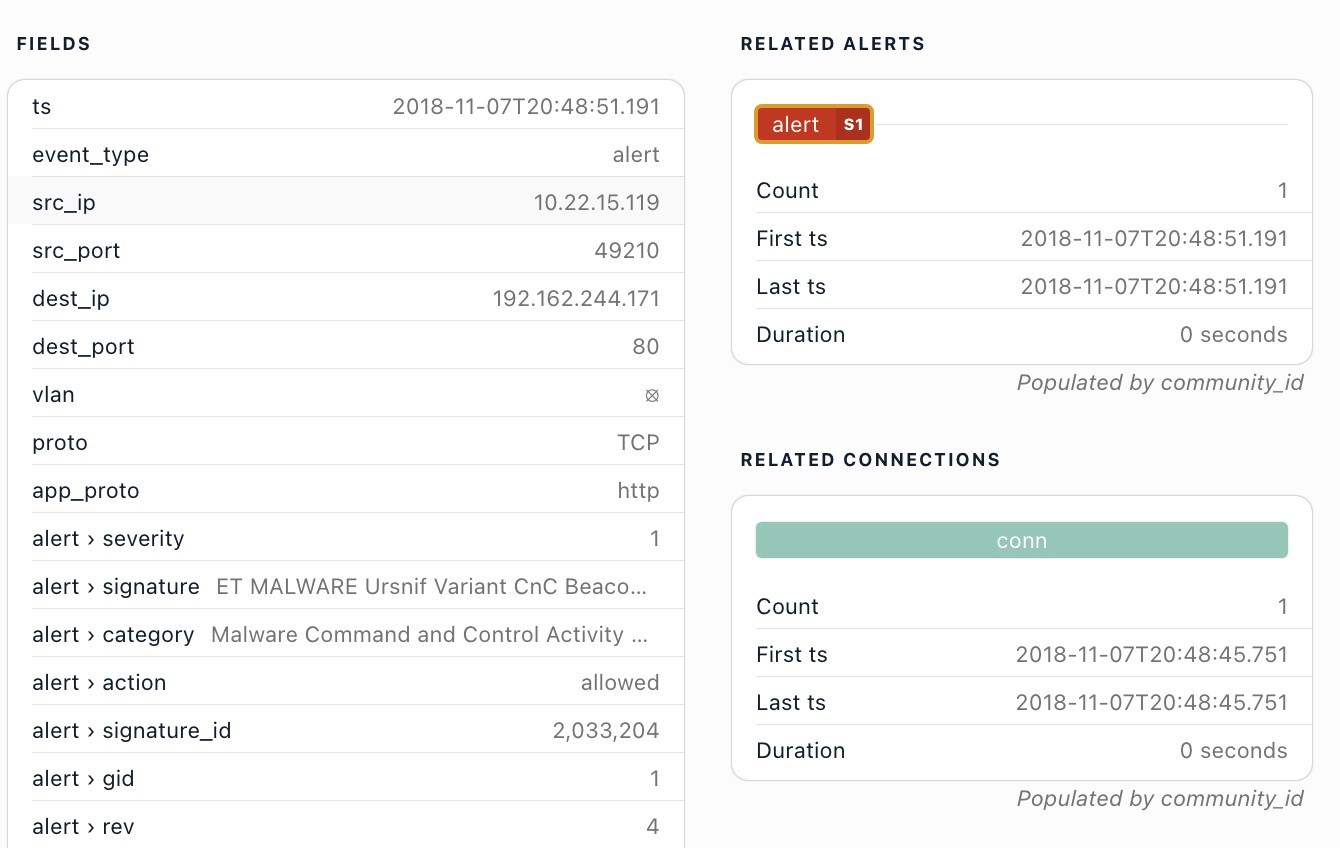




Inspecting the packet location reveals that there is a Command & Control (CC) server originating from Russia communicating with the victim client.



The Malware variant is determined to be “Ursnif”



The CnC server retrieves a malicious file from the attacker’s website.

