UBNETDEF Network Activity Report

Date: 2023-05-04

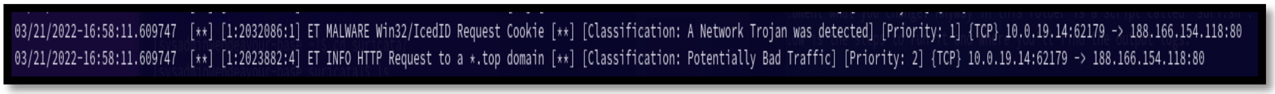
EXECUTIVE SUMMARY

On 21 March 2022, a Windows host used by "patrick.zimmerman" was infected with IcedID malware, which subsequently led to the establishment of a Cobalt Strike command and control (C2) beacon. The infected host's IP address is 10.0.19.14. This malware poses a significant threat to network security. To resolve this issue, it is crucial to remove the malware, implement stricter security measures, and prevent future infections.

CONTENTS

TECHNICAL ANALYSIS

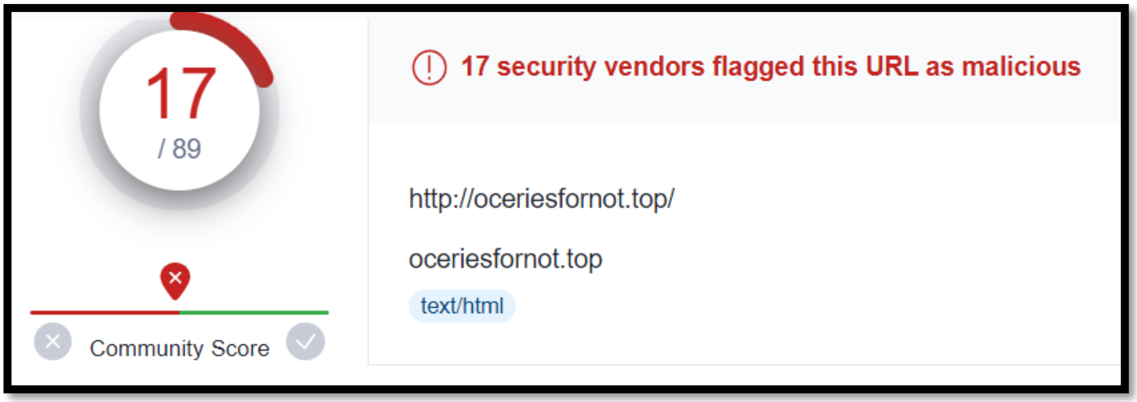
The Suricata IDS/IPS alerts indicated that the initial IcedID infection involved an HTTP GET request to a malicious domain, "oceriesfornot.top" (188.166.154.118). Further investigation revealed connections to other malicious domains, including "antnosience.com" (157.245.142.66), "seaskysafe.com" (91.193.16.181), "dilimoretast.com" (91.193.16.181), and "suncoastpinball.com" (160.153.32.99). The malware also made use of "Internet Widgits" TLS certificates, which are untrustworthy. The victim's computer connected to file-sharing websites "filebin.net" (185.47.40.36) and "situla.bitbit.net" (87.238.33.7; 87.238.33.8). Additionally, a Cobalt Strike C2 server was identified at "bupdater.com" (23.227.198.203).



```
03/21/2022-16:58:11.609747  [**] [1:2032086:1] ET MALWARE Win32/IcedID Request Cookie [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.0.19.14:62179 -> 188.166.154.118:80
03/21/2022-16:58:11.609747  [**] [1:2023882:4] ET INFO HTTP Request to a *.top domain [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 10.0.19.14:62179 -> 188.166.154.118:80
```

Figure 1

User patrick.zimmerman HTTP GET request to "oceriesfornot.top" (188.166.154.118)



17 / 89

Community Score

17 security vendors flagged this URL as malicious

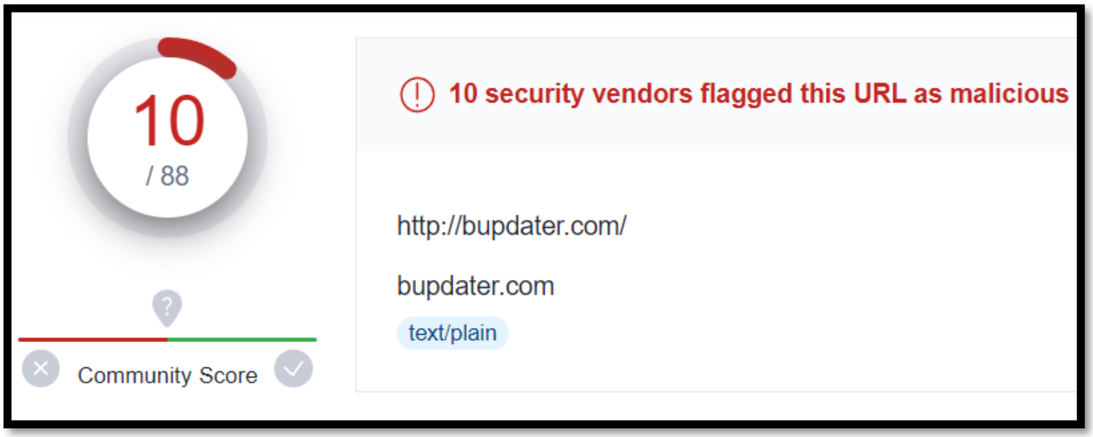
http://oceriesfornot.top/

oceriesfornot.top

text/html

Figure 2

Virustotal.com report on "oceriesfornot.top"



10 / 88

Community Score

10 security vendors flagged this URL as malicious

http://bupdater.com/

bupdater.com

text/plain

Figure 3

Virustotal.com report on the Cobalt Strike C2 server

RECOMMENDED CLEAN UP AND MITIGATION STRATEGIES

First, turn off the affected machines to prevent further infection or data exfiltration. Secondly, remove the affected machine from the network. Then, remove the IcedID malware from the infected host by identifying and deleting associated files and registry entries. Update antivirus software and ensure that it scans for IcedID malware and Cobalt Strike C2 beacons. Implement strict firewall rules to block connections to known malicious domains and IP addresses associated with IcedID and Cobalt Strike. Monitor network traffic for unusual patterns or connections, particularly those involving self-signed "Internet Widgits" TLS certificates. Educate users on safe browsing practices and the importance of not clicking on suspicious links or downloading unknown files. By following these steps, the infected host can be cleaned, and future infections can be prevented.

CONTRIBUTING ANALYSTS

Lead Analyst: Joshua Crull

Analysis Cheat Sheet:

https://www.virustotal.com/gui/home/url

https://www.digitalocean.com/community/tutorials/how-to-configure-suricata-as-an-intrusion-prevention-system-ips-on-ubuntu-20-04

https://nvd.nist.gov/