

Packet Capture Analysis Report

Task 22

UBNETDEF

April 30, 2023

Executive Summary

23:17:17 UTC on March 21st, 2022 UBNETDEF conducted analysis which revealed malicious network caused by a piece of malware called IcedID. The infected machine established connections with multiple malicious addresses and exfiltrated with data about different security policies, computer information, and domain policies. While there was no evidence in the network traffic, UBNETDEF assumes that the victim downloaded a malicious document from an email, which executed the malware.

To mitigate this incident and prevent future intrusions, UBNETDEF recommends isolating the infected machine. Firewall rules should also be implemented to block all traffic to malicious addresses. Installing and regularly updating an anti-virus program, such as Windows Defender, is also recommended to remove malicious software and prevent future installations. Additionally, training users on identifying and reporting different kinds of phishing emails can help eliminate before they enter the environment.

Contents

1	Technical Analysis	4
1.1	Indicators of Compromise	4
1.2	Malicious Activity	5
1.3	Conclusion	6
2	Mitigation Strategies	6
3	Contributing Analysts	7

1 Technical Analysis

1.1 Indicators of Compromise

UBNETDEF was given a packet capture file spanning the times 16:58:11 UTC to 23:17:17 UTC on March 21st, 2022. UBNETDEF used the tools Wireshark, Suricata, and online references like Virustotal and ThreatFox to help identify malware. The PCAP data was loaded into Suricata and there was evidence of malicious network traffic via the IcedID Request Cookie alert. See Figure 1. IcedID is also known as BokBot, and acts as a payload to deliver other viruses or download additional modules. It is usually installed via malicious document send by email.

□

Figure 1: Suricata Output of IcedID

Following the HTTP GET request associated with the IcedID traffic we see our infected machine (10.0.19.14) establish a connection with multiple malicious addresses, specifically, oceriesfornot.top, antnosience.com, and suncoastpinball.com. See Figures 2, 3, 4, and 5.



Figure 2: HTTP Packet Associated with IcedID



Figure 3: VirusTotal Results for oceriesfornot.top

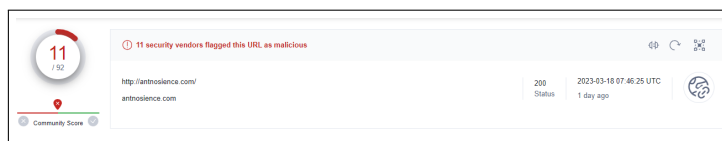


Figure 4: VirusTotal Results for antnosience.com



Figure 5: VirusTotal Results for suncoastpinball.com

1.2 Malicious Activity

After identifying the indicators of compromise, UBNETDEF looked deeper into the traffic to find out what the virus was doing. Looking at the initial indicators

of compromise do not tell us much in terms of malicious activity, however looking for file activity did. Our client made file to filebin.net. This could have been done to exfiltrate data, or bring in more malicious packages. See Figure 6.

10.0.19.14	10.0.19.9	DNS	71 Standard query 0x40ea a filebin.net
10.0.19.9	10.0.19.14	DNS	87 Standard query response 0x40ea a filebin.net A 185.47.40.36
10.0.19.14	10.0.19.9	DNS	72 Standard query 0x5095 a situla.bitbit.net
10.0.19.14	10.0.19.14	DNS	189 Standard query response 0x5095 a situla.bitbit.net A 87.238.33.8 A 87.238.33.7
10.0.19.14	10.0.19.9	DNS	72 Standard query 0x2258 a bupdater.com
10.0.19.9	10.0.19.14	DNS	88 Standard query response 0x2258 a bupdater.com A 23.227.198.203

Figure 6: Suspicious File Transfers

Another suspicious address is `bupdater.com`, which appears to be the destination our victim is making reoccurring connections to at a fixed rate. This is indicative of a command and control heartbeat, and is later confirmed via ThreatBox to be the case. See Figures 7 and 8.

[illegible]

Figure 7: Evidence of Command and Control Server








IOC ID:	439872
IOC:	 bupdater.com
IOC Type @:	domain
Threat Type @:	botnet_cc
Malware:	 Cobalt Strike
Malware alias:	Agenttemis, BEACON, CobaltStrike, cobeacon
Confidence Level @:	 Confidence level is elevated (75%)
First seen:	2022-03-22 19:19:43 UTC
Last seen:	never
UUID:	0773218f-aa15-11ec-8129-42010aa4000a
Reporter @:	 @abuse_ch
Reward @:	 10 credits from dms1899
Tags:	 Cobalt Strike
Reference:	 https://twitter.com/1zr4dh/status/1506345663990317062?%2=1

Figure 8: Evidence of Budater.com being malicious

UBNETDEF also found more suspicious behavior related to SMB. Looking at the SMB objects in WireShark there are multiple instances where the victim machine is accessing SMB files relating to group policy settings, security settings, and computer information. Afterwards it immediately calls back to antno-science.com. See Figure 9.

[illegible]

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
```

1.3 Conclusion

2 Mitigation Strategies

- Isolate the infected machine in order to prevent the spread of other malware IcedID could have installed.
- Create firewall rule to block all traffic to malicious addresses (oceries-fornot.top, antnosience.com, suncoastpinball.com, andbupdater.com).

- Install a regularly set up some kind of anti-virus. Windows Defender is a good option since its included with windows. It can remove the malicious software and prevent future malicious software from being installed.
- In the event that this breach happened as a result of phishing, train your users on identifying and reporting different kinds of phishing emails. This will help eliminate threats at your softest layer of defense.

UBNETDEF determines these actions to be productive in mitigating incidents through this attack vector again in the future.

3 Contributing Analysts

Lead Analyst: Griffin Refol