

# Packet Capture Analysis Report

## PCAP 4

UBNETDEF

May 12, 2023

## Executive Summary

On March 14th, 2021 UBNETDEF conducted analysis which revealed the computer DESKTOP-F3P7XLU owned by Samantha Reed was infected malware called Dridex, which is used to steal system information and credentials. The system was infected due to Samantha downloading an Microsoft excel file that contained malicious code that was executed upon opening. The malicious software was able to exfiltrate with system information and files from Samantha's computer.

To mitigate this incident and prevent future intrusions, UBNETDEF recommends isolating the infected machine and removing any malicious software, installing and regularly updating an anti-virus program, such as Windows Defender, and implementing an intrusion detection system, such as Suricata. Additionally, it can be reasonably assumed the source of this attack was due to poor cybersecurity practices on the end-user's part, so training users safe cybersecurity practices would be effective in preventing future attacks.

## Contents

<b>1</b>	<b>Technical Analysis</b>	<b>4</b>
1.1	Indicators of Compromise . . . . .	4
<b>2</b>	<b>Malicious Activity</b>	<b>6</b>
<b>3</b>	<b>Mitigation</b>	<b>7</b>
<b>4</b>	<b>Contributing Analysts</b>	<b>8</b>

## 1 Technical Analysis

UBNETDEF was given a packet capture file spanning the times 16:30 UTC to 20:47 UTC on July 14th, 2021. UBNETDEF used the tools Wireshark, Virus-Total, and Suricata to identify indicators of compromise. The first action was establishing the clients involved in this packet capture which could be compromised, for which UBETNDEF found:

Client Name	IP	MAC	Owner
DESKTOP-F3P7XLU	172.16.1.239	00:13:D4:10:05:25	Samantha Reed

## 1.1 Indicators of Compromise

Inputting the traffic into an IDS like Suricata shows the following:

[illegible]

Figure 1: Suricata Fast.log

Suricata notified that there's traffic between the host buyer-remindment.com (185.21.216.153) and our client, DESKTOP-F3P7XLU (172.16.1.239) where a Microsoft office document (likely excel) that contains embedded Visual Basic Application (VBA) code was downloaded over HTTP. Looking up this hostname in VirusTotal shows the following:

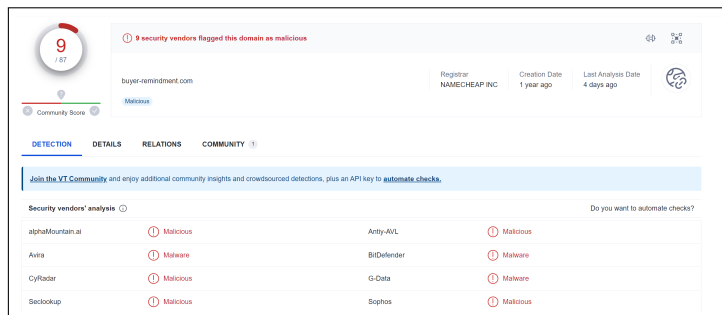


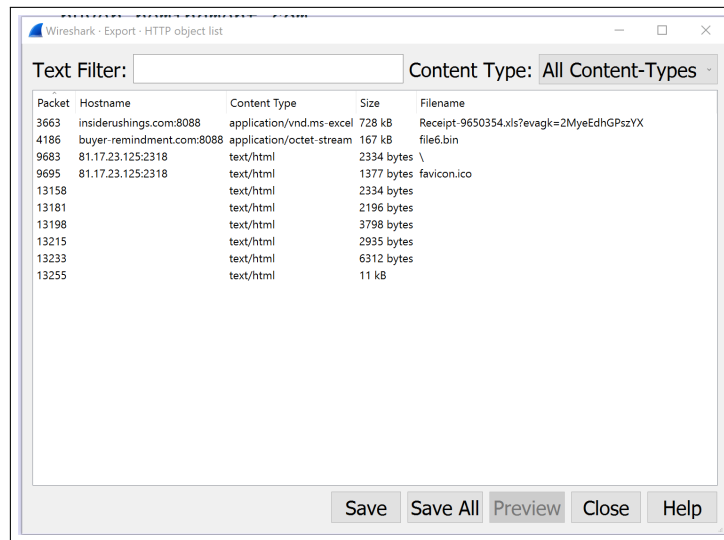
Figure 2: VirusTotal for buyer-remindment.com

In addition to the communicated files, which are all malicious Microsoft excel spreadsheets:

Scanned	Detections	Type	Name
2021-11-30	34 / 60	MS Excel Spreadsheet	Receipt-9650354.xls
2021-07-30	37 / 62	MS Excel Spreadsheet	zbtcheckin_tracker_invoice%2081806%20from%20Quickbooks.%20LLC.xls
2021-11-30	33 / 60	MS Excel Spreadsheet	Receipt-9650354.xls
2021-11-30	33 / 60	MS Excel Spreadsheet	Receipt-9650354.xls
2021-09-13	37 / 61	MS Excel Spreadsheet	13a0c59d32aba7c7b98f7ef413e91cb707a603404821a78a15067f1d00994da.bin
2021-09-13	29 / 61	MS Excel Spreadsheet	Receipt-40481256.xls
2022-02-16	32 / 62	MS Excel Spreadsheet	Receipt-9650354 - Copy.xls
2021-01-09	35 / 62	MS Excel Spreadsheet	accounts.xls
2021-10-10	38 / 59	MS Excel Spreadsheet	246.mai
2023-05-07	40 / 60	MS Excel Spreadsheet	Receipt-9650354.xls

Figure 3: buyer-remindment.com Files

Finally, UBNETDEF looked at the files associated with buyer-remindment.com in the HTTP export list from Wireshark, UBNETDEF found files that closely resemble the commonly named malicious files hosted on buyer-remindment.com.



Packet	Hostname	Content Type	Size	Filename
3663	insiderushings.com:8088	application/vnd.ms-excel	728 kB	Receipt-9650354.xls?evagk=2MyeEdhGPszYX
4186	buyer-remindment.com:8088	application/octet-stream	167 kB	file6.bin
9683	81.17.23.125:2318	text/html	2334 bytes	\
9695	81.17.23.125:2318	text/html	1377 bytes	favicon.ico
13158		text/html	2334 bytes	
13181		text/html	2196 bytes	
13198		text/html	3798 bytes	
13215		text/html	2935 bytes	
13233		text/html	6312 bytes	
13255		text/html	11 kB	

Figure 4

Analyzing these files using VirusTotal outputs the following in Figures 5 and 6:

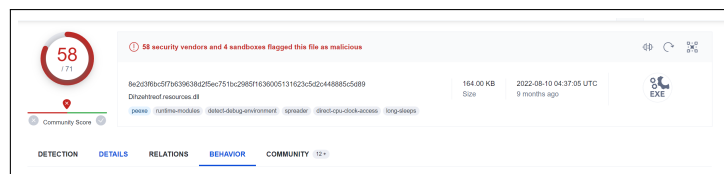


Figure 5: file6 VirusTotal



Figure 6: Receipt VirusTotal

Based off these findings, UBNETDEF can confirm with reasonable certainty that Samantha Reed downloaded malware and therefore must be met with an incident response.

## 2 Malicious Activity

UBNETDEF responded by reviewing the documented behavior of the malware and determining whether or not Samantha Reed's client is experiencing the same behavior. One of the behaviors the malicious excel file will do is make a GET request to `http://buyer-remindment.com:8088/templates/file6.bin`, which tracks due to the fact that we see `file6.bin` as a downloaded object in HTTP Exports, and that we traffic of `file6.bin` being downloaded in Wireshark:

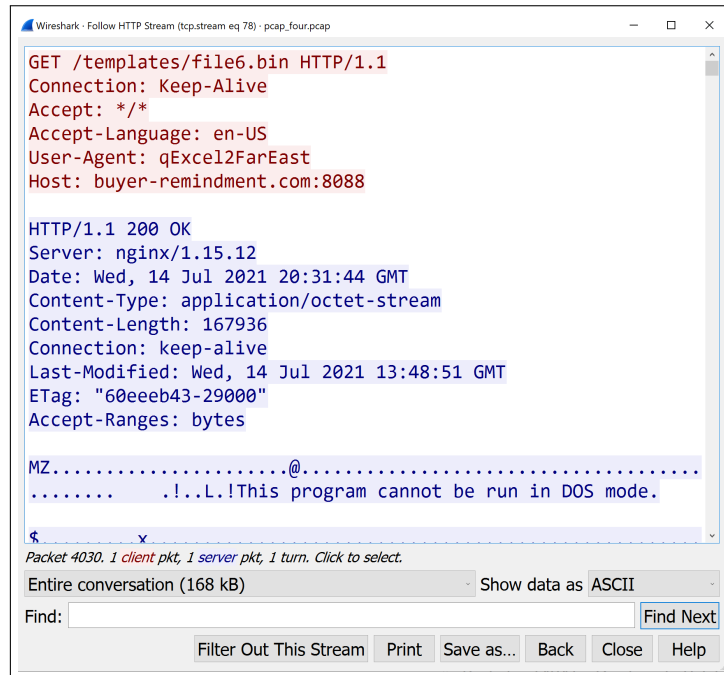


Figure 7: Evidence of `file6.bin` being Downloaded

`file6.bin` is reported to be Dridex, a windows-focused banking trojan designed to steal information and credentials. Looking back at Figure 4, we notice a couple files grabbed from IP: 81.17.23.125. Analyzing the text in Figure 8, UBNETDEF sees it is HTML code that appears to be related to Samantha's computers C: D: and Z: drives and uploading files. This kind of behavior is indicative on a reverse shell.



Figure 8: HTML File

Reviewing the traffic between 81.17.23.125 and Samantha's computer further reveals evidence that there's a reverse shell in place extracting system information. See Figure 9.

[illegible]

Figure 9: Reverse Shell Evidence

Based off this evidence, UBNETDEF can conclude that Samanatha downloaded a malicious excel file which in turn downloaded a Dridex virus, which begin to ex filtrate system information via a reverse shell.

### 3 Mitigation

UBNETDEF has a set of recommended activities to clean up this incident, and to prevent intrusions like this in the future.

- Take the infected machine off the network so it can no longer be exploited via the reverse shell.
- Remove the malicious files off the infected client.
- Implement anti-virus on all your clients so that in the event malware is installed, it can be blocked before damage can be done.
- Implement an IDS such as Suricata so in the future similar attacks can be detected faster.
- Due to the likelihood of phishing being the original cause, implementing training for employees about safe cybersecurity practices.

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

## 4 Contributing Analysts

Lead Analyst: Griffin Refol