2021-09-10 Analysis

LAN Segment Data:

- LAN Segment range: 10.9.10.0/24 (10.9.10.0 through 10.9.10.255)
- Domain: angrypoutine.com
- Domain controller: 10.9.10.9 – ANGRYPOUTINE-DC
- LAN Segment gateway: 10.9.10.1
- LAN segment broadcast address: 10.9.10.255

Executive Summary:

On 2021-09-10 at 23:17 UTC a windows host with user hobart.gunnarsson has infected with BazarLoader malware.

Details:

IP Address: 10.9.10.102

Hostname: DESKTOP – KKITB6Q

Windows User account name: hobart.gunnarsson

MAC Address: 00:4f:49:b1:e8:c3

Indicators of Compromise(IOCs):

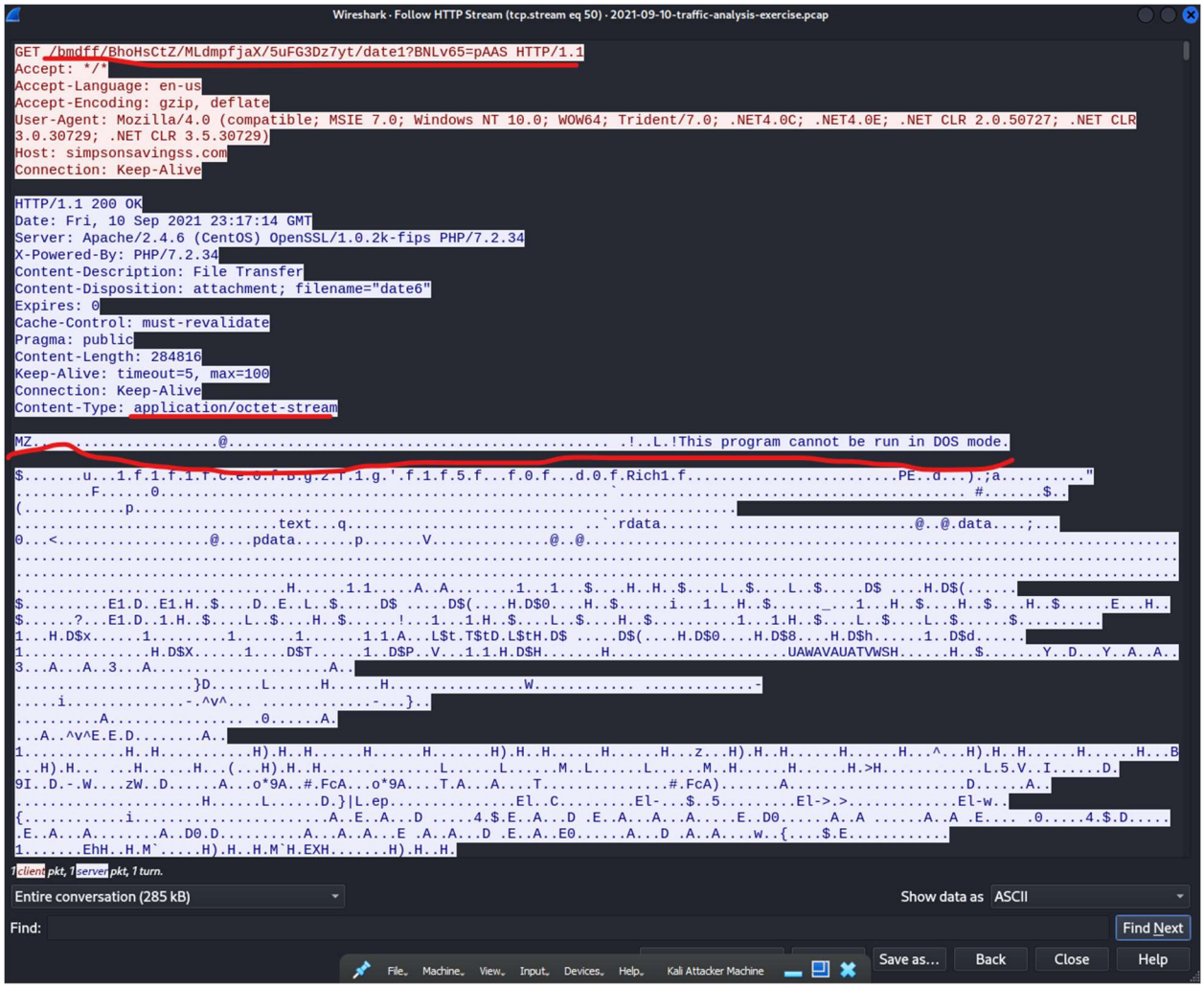
Traffic to retrieve BazarLoader malware is:

URL: http://simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjax/5uFG3Dz7yt/date1?BNLv65=pAAS

IP: 194.62.42.206 [found on Pastebin]

SHA256 hash of file: eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8

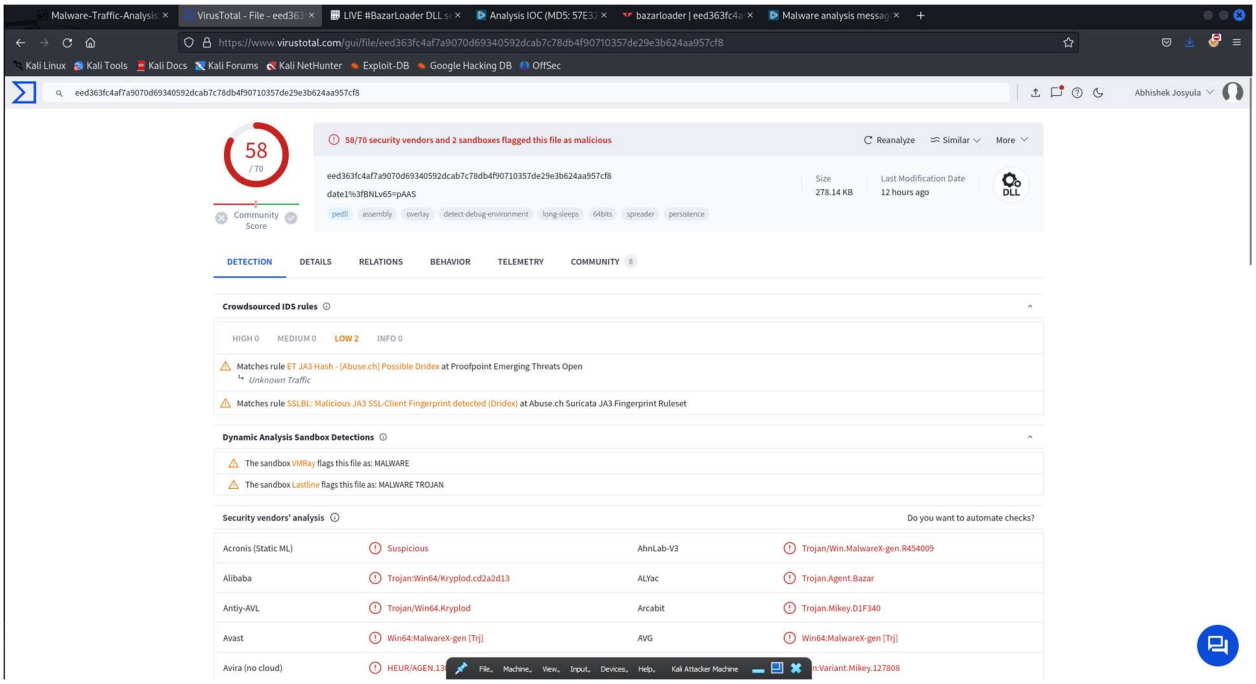
File size: 284,816 bytes.




```
┌──(aj㉿kali)-[~/Desktop/Cybersecurity-learnings/2021-09-10]
└─$ file IOC
IOC: PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 4 sections

┌──(aj㉿kali)-[~/Desktop/Cybersecurity-learnings/2021-09-10]
└─$ sha256sum IOC
eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8  IOC

┌──(aj㉿kali)-[~/Desktop/Cybersecurity-learnings/2021-09-10]
└─$
```


Malware-Traffic-Analysis
VirusTotal - File - eed363
LIVE #BazarLoader DLL
Analysis IOC (MD5: 57E3
bazarloader | eed363fc4a
Malware analysis messag
https://www.virustotal.com/gui/file/eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8
Abhishek Josyula
58
/ 70
Community Score
58/70 security vendors and 2 sandboxes flagged this file as malicious
Reanalyze
Similar
More
eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8
date1%3fBNLv65=pAAS
pedll
assembly
overlay
detect-debug-environment
long-sleeps
64bits
spreader
persistence
Size
278.14 KB
Last Modification Date
12 hours ago
DLL
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY 8
Crowdsourced IDS rules
HIGH 0
MEDIUM 0
LOW 2
INFO 0
Matches rule ET JA3 Hash - [Abuse.ch] Possible Dridex at Proofpoint Emerging Threats Open
Unknown Traffic
Matches rule SSLBL: Malicious JA3 SSL-Client Fingerprint detected (Dridex) at Abuse.ch Suricata JA3 Fingerprint Ruleset
Dynamic Analysis Sandbox Detections
The sandbox VMRay flags this file as: MALWARE
The sandbox Lastline flags this file as: MALWARE TROJAN
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Suspicious
AhnLab-V3
Trojan/Win.MalwareX-gen.R454009
Alibaba
Trojan:Win64/Kryplod.cd2a2d13
ALYac
Trojan.Agent.Bazar
Antiy-AVL
Trojan/Win64.Kryplod
Arcabit
Trojan.Mikey.D1F340
Avast
Win64:MalwareX-gen [Trj]
AVG
Win64:MalwareX-gen [Trj]
Avira (no cloud)
HEUR/AGEN.12
n:Variant.Mikey.127808
File
Machine
View
Input
Devices
Help
Kali Attacker Machine