Executive Summary:
On 2021-01-20 23:40 UTC, a Windows device used by Orlando McCoy was infected with Gozi malware.

Victim Details:
IP: 10.1.21.101
Hostname: DESKTOP-NB72TZA
Mac Address: 00:60:67:d3:47:8b - Acer workstation
User Account: Orlando.mccoy

IoC's:
209.141.51.196 port 80
- Zeus/perkesh Malware
- GET /files/1.bin
- GET /Lk9tdZ

185.186.244.130 port 80 - greatewallfirewall.xyz
- GET postfix string

72.21.81.200 port 80 - cs9.wpc.v0cdn.net
- JA3 Hash - Gozi

208.67.222.222 port 53 - resolver1.opendns.com
- External IP lookup

162.0.224.165 port 443 - agreement-put.quarantine-pnap-vlan51.web-hosting.com
- GET /grab32.rar

193.239.84.250 port 443 - booloolo3.com

84.252.95.102 port 443 - booloolo4.com

SHA256 hash:
236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b001d95c8 c90845cb

Suspicious urls/Malicious urls:

greatewallfirewall.xyz
/files/1.bin (malware was downloaded)
/Lk9tdZ
/grab32.rar