# Threat Report

Report Date: July 30, 2018 16:43
Data Range: 2018-07-23 00:00 2018-07-29 23:59 CST (FAZ local)

# Table of Contents

# Malware

## Malware Detected

| # | Malware Name | Malware Type | Counts |
|---|---|---|---|
| 1 | Malicious_Behavior.SB | Virus | 22 |
| 2 | VBA/TrojanDownloader.JMR!tr | Virus | 6 |
| 3 | W32/GenKryptik.CGHM!tr | Virus | 1 |
| 4 | Malware_Generic.P0 | Virus | 1 |
| 5 | W32/FareitVB.CGGL!tr | Virus | 1 |
| 6 | W32/VBKryptik.DZLN!tr | Virus | 1 |

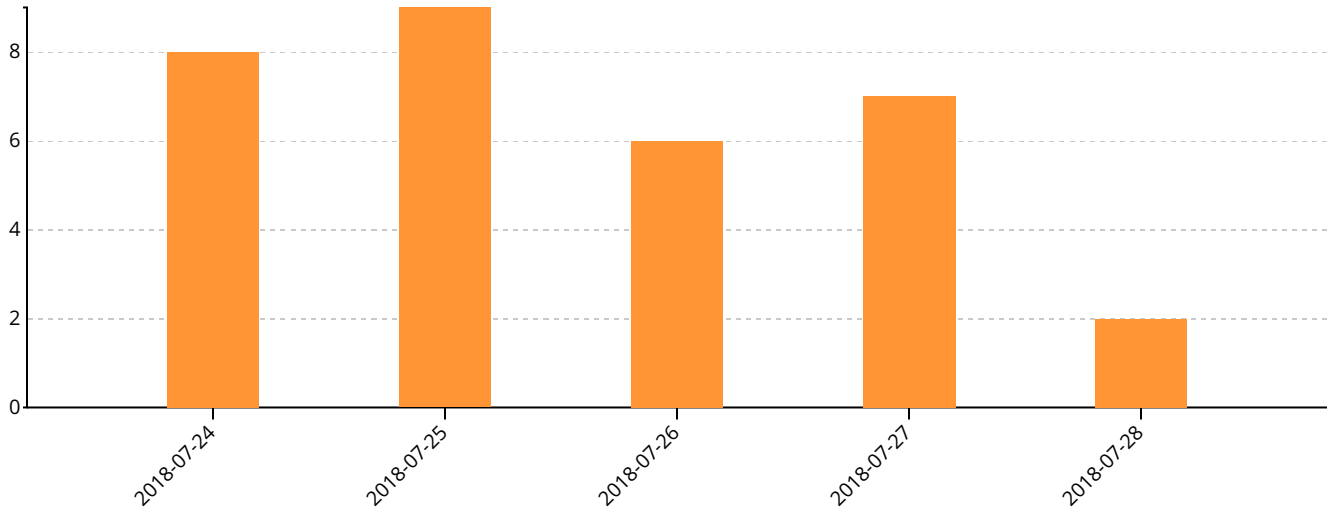
## Malware Victims

| # | Victim Name (or IP) | Counts |
|---|---|---|
| 1 | 80.211.46.224 | 21 |
| 2 | 95.211.151.57 | 3 |
| 3 | 192.190.42.62 | 2 |
| 4 | 219.83.54.102 | 1 |
| 5 | 196.46.182.42 | 1 |
| 6 | 103.250.184.30 | 1 |
| 7 | 191.101.26.140 | 1 |
| 8 | 50.76.89.49 | 1 |
| 9 | 185.82.203.158 | 1 |

## Malware Source

| # | Malware Source | Hostname (or IP) | Counts |
|---|---|---|---|
| 1 | 80.211.46.224 | 192.168.0.12 | 21 |
| 2 | 95.211.151.57 | 192.168.0.12 | 3 |
| 3 | 192.190.42.62 | 192.168.0.12 | 2 |
| 4 | 191.101.26.140 | 192.168.0.12 | 1 |
| 5 | 103.250.184.30 | 192.168.0.12 | 1 |
| 6 | 50.76.89.49 | 192.168.0.12 | 1 |
| 7 | 219.83.54.102 | 192.168.0.12 | 1 |
| 8 | 196.46.182.42 | 192.168.0.12 | 1 |
| 9 | 185.82.203.158 | 192.168.0.12 | 1 |

## Malware Timeline



# Botnets

## Botnet Detected

No matching log data for this report

## Botnet Victims

No matching log data for this report

## Botnet C&C

No matching log data for this report

## Botnet C&C Detected by DNS Filtering

No matching log data for this report

## Botnet Timeline

No matching log data for this report

# Intrusions

## Intrusions Detected

| # | Attack Name | Severity | CVE-ID | Counts |
|---|---|---|---|---|
| 1 | D-Link.DSL-2750B.CLI.OS.Command.Injection | Critical | | 32 |
| 2 | MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow | Critical | CVE-2017-7269 | 17 |
| 3 | Dasan.GPON.Remote.Code.Execution | Critical | CVE-2018-10561,CVE-2018-10562 | 13 |
| 4 | Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection | Critical | CVE-2017-3506,CVE-2017-10271 | 2 |
| 5 | JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution | high | | 38 |
| 6 | PHP.CGI.Argument.Injection | high | CVE-2012-1823,CVE-2012-2311 | 2 |
| 7 | ZmEu.Vulnerability.Scanner | low | | 6 |
| 8 | Masscan.Scanner | low | | 2 |

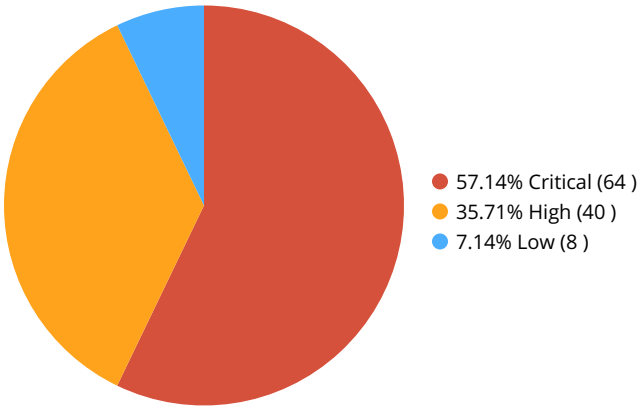
## Intrusion Victims

| # | Attack Victim | Counts |
|---|---|---|
| 1 | 192.168.0.11 | 62 |
| 2 | 192.168.0.12 | 50 |

## Intrusion Sources

| # | Attack Source | Counts |
|---|---|---|
| 1 | 89.248.172.196 | 6 |
| 2 | 47.97.186.104 | 2 |
| 3 | 124.246.230.97 | 2 |
| 4 | 59.57.118.90 | 2 |
| 5 | 122.14.217.104 | 2 |
| 6 | 158.181.147.43 | 2 |
| 7 | 114.180.42.251 | 2 |
| 8 | 156.196.115.148 | 2 |
| 9 | 80.82.70.118 | 2 |
| 10 | 115.159.186.223 | 2 |

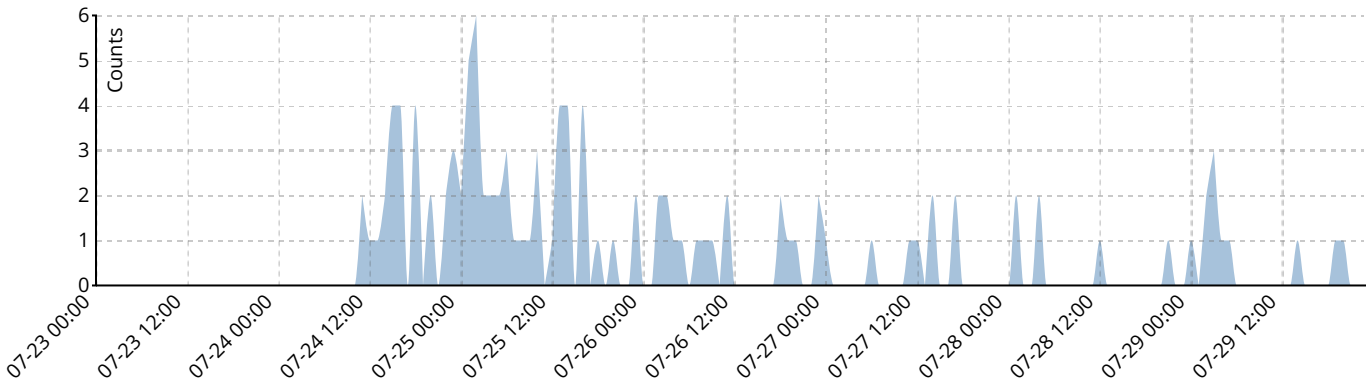
## Intrusions By Severity




## Intrusions Blocked

| # | Attack Name | Counts |
|---|---|---|
| 1 | JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution | 38 |
| 2 | D-Link.DSL-2750B.CLI.OS.Command.Injection | 32 |
| 3 | MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow | 17 |
| 4 | Dasan.GPON.Remote.Code.Execution | 13 |
| 5 | ZmEu.Vulnerability.Scanner | 6 |
| 6 | Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection | 2 |
| 7 | Masscan.Scanner | 2 |
| 8 | PHP.CGI.Argument.Injection | 2 |

## Intrusion Timeline



# Appendix A

## Devices

Teco