Template - Potential phishing web site

Link to alert

**Description**

A machine made a network connection to a web domain suspected of hosting a phishing web site. Phishing pages are used/designed by malicious actors to look like legitimate web portals and harvests user credentials.

**Classification**: Incident

**Alert detail**

User:

Device:

IP:

Time Generated:

Alert Severity:

**Remediation**

Make sure the machine is completely updated and all your software has the latest patch.

Install and run Microsoft’s Malicious Software Removal Tool (see https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx).

Run Microsoft’s Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx).

Run Process Explorer and try to identify unknown running processes (see https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx)."

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***