WSH RAT (A variant of H-Worm/Houdini)

github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/wsh_rat.md

jeFF0Falltrades

jeFF0Falltrades/
IoCs

A collection of Indicators of Compromise (IoCs), most aligning with samples derived from the signatures in the YARA-Signatures repo

1 Contributor

0 Issues

27 Stars

2 Forks

Reporting

https://cofense.com/houdini-worm-transformed-new-phishing-attack

YARA

```
rule wsh_rat_vbs_decoded
{
        meta:
                author = "jeFF0Falltrades"
                ref = "https://cofense.com/houdini-worm-transformed-new-
phishing-attack"
                description = "Alerts on the decoded WSH RAT VBScript"

        strings:
                $str_0 = "wshsdk" wide ascii nocase
                $str_1 = "wshlogs" wide ascii nocase
                $str_2 = "WSHRAT" wide ascii nocase
                $str_3 = "WSH Sdk for password recovery" wide ascii
nocase
                $str_4 = "wshlogs\\recovered_password_email.log" wide
ascii nocase
                $str_5 = "post (\"is-ready\",\"\")" wide ascii nocase
                $str_6 = "split (response,spliter)" wide ascii nocase
                $str_7 = "updatestatus(\"SDK+Already+Installed\")" wide
ascii nocase
                $str_8 = "case \"get-pass-offline\"" wide ascii nocase
                $str_9 = "case \"up-n-exec\"" wide ascii nocase
                $str_10 = "Unable to automatically recover password" wide
ascii nocase
                $str_11 = "reverseproxy" wide ascii nocase
                $str_12 = "keyloggerstarter" wide ascii nocase

        condition:
                3 of ($str*)
}

rule wsh_rat_keylogger
{
        meta:
                author = "jeFF0Falltrades"
                ref = "https://cofense.com/houdini-worm-transformed-new-
phishing-attack"
                description = "Alerts on the WSH RAT .NET keylogger
module"


        strings:
                $str_0 = "Keylogger" wide ascii nocase
                $str_1 = "RunKeyloggerOffline" wide ascii nocase
                $str_2 = "saveKeyLog" wide ascii nocase
                $str_3 = "sendKeyLog" wide ascii nocase
                $str_4 = "/open-keylogger" wide ascii nocase
                $str_5 = "wshlogs" wide ascii nocase
                $str_6 = "WSHRat Plugin" wide ascii nocase
                $str_7 = "Debug\\Keylogger.pdb" wide ascii nocase

        condition:
                3 of them
}
```

```
rule wsh_rat_rdp
{
        meta:
                author = "jeFF0Falltrades"
                ref = "https://cofense.com/houdini-worm-transformed-new-phishing-attack"
                description = "Alerts on the WSH RAT .NET RDP module"

        strings:
                $str_0 = "GET /open-rdp|" wide ascii nocase
                $str_1 = "WSHRat Plugin" wide ascii nocase
                $str_2 = "Debug\\RDP.pdb" wide ascii nocase
                $str_3 = "TakeShoot" wide ascii nocase
                $str_4 = "CompressJPEG" wide ascii nocase

        condition:
                3 of them
}


rule wsh_rat_reverse_proxy
{
        meta:
                author = "jeFF0Falltrades"
                ref = "https://cofense.com/houdini-worm-transformed-new-phishing-attack"
                description = "Alerts on the WSH RAT .NET reverse proxy module"

        strings:
                $str_0 = "RProxy:" wide ascii nocase
                $str_1 = "WSH Inc" wide ascii nocase
                $str_2 = "WSH Reverse Proxy" wide ascii nocase
                $str_3 = "Debug\\ReverseProxy.pdb" wide ascii nocase
                $str_4 = "WshRP" wide ascii nocase
                $str_5 = "NotifyBringNewSocket" wide ascii nocase

        condition:
                3 of them
}
```

Sample Hashes

Decoded VBS Script

```
956fb59036b01ebf0fb3a6345eafa2c4aed8dcbad8db63d5c9f3188ceb32bd17
023938e5f920989b356a897349137a70bf519c72f36219cb147525a650ef7ae4
```

Keylogger Module

```
272e64291748fa8be01109faa46c0ea919bf4baf4924177ea6ac2ee0574f1c1a
```

RDP Module

```
d65a3033e440575a7d32f4399176e0cdb1b7e4efa108452fcdde658e90722653
```