SIGS: W32/Badspace.Backdoor - Rule Signatures - Emerging Threats

Published: 2024-05-13 · Archived: 2026-04-05 14:59:42 UTC

post by kevross33 on May 13, 2024

Hi,

Here is a backdoor I have given a temporary name based on the error in the user agent of extra space as all AV names are generic. You can get the PCAP from 6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f | Triage. The POST body is obsucated/encrypted as is the results of the base64 cookie value but the user agent is a good but very specific match given the error they have made (Mozilla / 4.0).

alert tcp $HOME_NET any → $EXTERNAL_NET $HTTP_PORTS (msg:“ET TROJAN W32/Badspace.Backdoor POST Request”; flow:established,to_server; content:“POST”; http_method; urilen:1; content:“/” http_uri; content:“Cookie|3A| “; http_header; content:“User-Agent|3A| Mozilla / 4.0 (compatible|3B| MSIE 6.0|3B| Windows NT 5.1|3B| SV1|3B|.NET CLR 1.0.3705)”; http_header; fast_pattern:12,20; content:“Host|3A|” http_header; content:“.”; http_header; within:4; content:“.”; http_header; within:4; content:“.”; http_header; within:4; content:!“Referer|3A|”; http_header; pcre:“/Host\x3A\x20\d{1,3}\x2E\d{1,3}\x2E\d{1,3}\x2E\d{1,3}/H”; classtype:trojan-activity; reference:md5,c16bdc61bbc82e9668f8cee9cc5c94c5; sid:172111; rev:1;)

alert tcp $HOME_NET any → $EXTERNAL_NET $HTTP_PORTS (msg:“ET TROJAN W32/Badspace.Backdoor GET Request”; flow:established,to_server; content:“GET”; http_method; urilen:1; content:“/” http_uri; content:“Cookie|3A| “; http_header; content:“User-Agent|3A| Mozilla / 4.0 (compatible|3B| MSIE 6.0|3B| Windows NT 5.1|3B| SV1|3B|.NET CLR 1.0.3705)”; http_header; fast_pattern:12,20; content:“Host|3A|” http_header; content:“.”; http_header; within:4; content:“.”; http_header; within:4; content:“.”; http_header; within:4; pcre:“/Host\x3A\x20\d{1,3}\x2E\d{1,3}\x2E\d{1,3}\x2E\d{1,3}/H”; classtype:trojan-activity; reference:md5,c16bdc61bbc82e9668f8cee9cc5c94c5; sid:172112; rev:1;)

post by ishaughnessy on May 13, 2024

Hey @kevross33 -

Thanks for the awesome tip! We got these signatures in today’s release!!

```
 2052557 - ET MALWARE W32/Badspace.Backdoor CnC Activity (GET)
2052558 - ET MALWARE W32/Badspace.Backdoor CnC Activity (POST)
```

Thanks,
Isaac

post by rgonzalez on May 14, 2024