FIN8: BADHATCH Threat Indicator Enrichment

team-cymru.com/blog/2021/03/15/fin8-badhatch-threat-indicator-enrichment/

S2 Research Team View all posts by S2 Research Team March 15, 2021

INTRODUCTION

Last week (10 March 2021), Bitdefender released a whitepaper on the recent activities of the FIN8 threat actor group, focusing particularly on their BADHATCH toolkit[1]. The research found that FIN8, a financially motivated group, had used this toolkit to target victims in the chemicals, insurance, retail and technology sectors. We've expanded on Bitdefender's findings by using Pure Signal™ Recon to identify infrastructure currently in use by the group.

METHODOLOGY

Two IP addresses were provided in the Bitdefender paper, described as BADHATCH command and control IOCs, and were used as seeds for this investigation:

- 104.168.145[.]204 (HOSTWINDS, US)
- 192.52.167[.]199 (QUADRANET, US)

Banner information was obtained for both IP addresses during December 2020, showing identical strings on ports TCP/22 and TCP/80.

TCP/22: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2

TCP/80: HTTP/1.1 404 Server: nginx/1.14.1 Content-Type: text/plain; charset=utf-8 Content-Length: 14 Connection: Close

Pivoting on the string observed on TCP/80 'HTTP/1.1 404 Server: nginx/1.14.1 Content-Type: text/plain; charset=utf-8 Content-Length: 14 Connection: Close', two further IP addresses were identified hosting the same banner information:

- 89.45.4[.]192 (M247, US)
- 108.62.118[.]100 (LEASEWEB, US)

A further set of queries for the two 'new' IP addresses identified the same banner information being hosted on TCP/22 'SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2', as observed with the original seeds.

Given the low volume of IP addresses [2] hosting the same banner information as observed on the seed IP addresses, the two strings (when viewed in combination) were considered a viable fingerprint for connected FIN8 activity.

Network traffic data was obtained for both 89.45.4[.]192 and 108.62.118[.]100 in order to help confirm this assertion. These findings are summarised as follows:

Repeated established inbound connections, during the period 24 January – 13 March 2021 (i.e., present day), to TCP/443 on both 89.45.4[.]192 and 108.62.118[.]100 sourced from numerous potential victims:

- A Germany-based logistics company
- A Sweden-based engineering company
- An US-based bank
- An US-based credit union
- An US-based engineering company

Some evidence to suggest 89.45.4[.]192 taking over as the primary C2 on or around 20 February 2021.

Note that the potential victims described above were notified of this activity prior to the release of this blog.

CONCLUSION

This investigation has highlighted two FIN8 command and control IP addresses, believed to be in active use by the threat actors in targeting potential victims in Germany, Sweden and the United States.

TECHNICAL APPENDIX

FIN8 C2s:

89.45.4[.]192

108.62.118[.]100

[1] https://labs.bitdefender.com/2021/03/fin8-group-is-back-in-business-with-improved-badhatch-kit/