AIPC CYBER SECURITY INTELLIGENCE REPORT

December 2022

All intelligence is gathered across AIPC centres through ‘cyber@aipc.org’ and Open-Source Intelligence. All information is submitted by AIPC members across roles where suspicious digital feeds are seen.

EXCELLENCE IN
CONVENTION CENTRE
MANAGEMENT

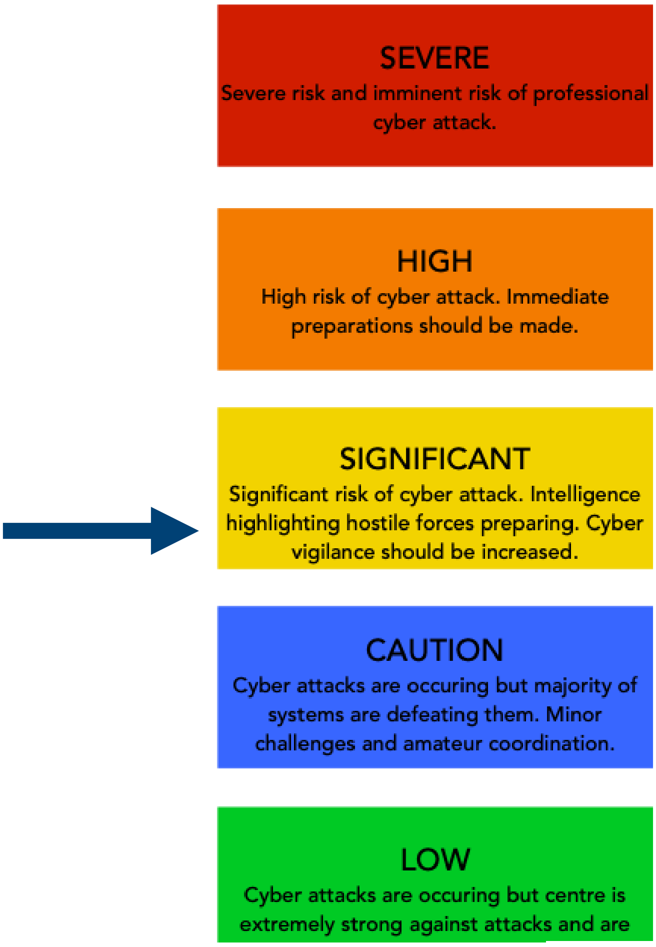
Submitting any threats seen across devices to cyber@aipc.org continues to keep our association and our members collectively safe together, and is designed to make the AIPC community stronger against cyber and digital threats, by creating understanding to common threats and attacks, so that we continuously stay ahead of cyber threats.

Update – AIPC IP Address Threat Community

During November, we saw several centres having a substantial increase in IP based request/ attack attempts. To assist in the intelligence gathering across our community, we have started an AIPC IP Address Threat Community, dedicated for convention centres. The aim of this alongside our other protections are:

1) All centres can report malicious, spam and other categories of unwanted IPs to enhance the protection of our community.
2) Reduce the ability for attackers to join and repeat attack methods across centres.
3) Have a designated list of dangerous IP addresses to input into your blacklisting abilities.
4) IP Exchange will assist more technical understanding of AIPC community threats.

AIPC Cyber Risk Threat



SEVERE
Severe risk and imminent risk of professional cyber attack.

HIGH
High risk of cyber attack. Immediate preparations should be made.

SIGNIFICANT
Significant risk of cyber attack. Intelligence highlighting hostile forces preparing. Cyber vigilance should be increased.

CAUTION
Cyber attacks are occuring but majority of systems are defeating them. Minor challenges and amateur coordination.

LOW
Cyber attacks are occuring but centre is extremely strong against attacks and are

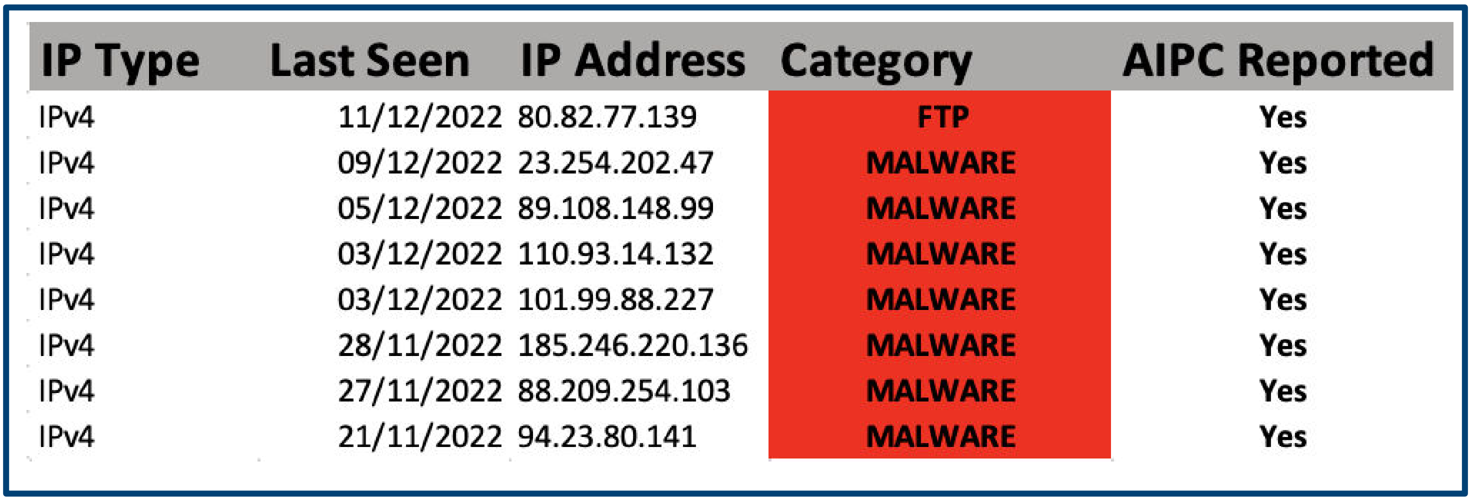
Important Numbers and Figures

- **AIPC CYBER RISK THREAT HAS STABILISED**
- **AVERAGE OF 1.5 ATTACK PER CENTRE PER WEEK HAS REMAINED STEADY.**
- **CHRISTMAS PERIOD HOWEVER IS EXPECTED AND HISTORICALLY A HIGH ATTACK MONTH.**
  - **EUROPE AND NORTH AMERICA HEAVIEST HIT**
  - **PREVIOUS (2021) WAS HIGH IN SPEAR PHISHING RELATING TO DRINKS, PARTIES AND PHOTOS (SIMILAR KEYWORDS).**
  - **EXTRA VIGILANCE IS HIGHLY SUGGESTED.**

Monthly Threats & Attack Example

Each month we make examples which are illustrations from submitted attempted attacks and threats. They have been changed and altered to keep the context and protection of each centre who submitted it.

This month a new 'IP Address Threat Community' was established for the AIPC, where we encourage simple emails with IP addresses to benefit the entire association.



IP Type	Last Seen	IP Address	Category	AIPC Reported
IPv4	11/12/2022	80.82.77.139	FTP	Yes
IPv4	09/12/2022	23.254.202.47	MALWARE	Yes
IPv4	05/12/2022	89.108.148.99	MALWARE	Yes
IPv4	03/12/2022	110.93.14.132	MALWARE	Yes
IPv4	03/12/2022	101.99.88.227	MALWARE	Yes
IPv4	28/11/2022	185.246.220.136	MALWARE	Yes
IPv4	27/11/2022	88.209.254.103	MALWARE	Yes
IPv4	21/11/2022	94.23.80.141	MALWARE	Yes

Concerns and Tips

The importance of IP address has several uses especially around identification. Attackers will often create and shield their true location through software (i.e VPNs or jacking vulnerable machines) but the IP addresses they use to create attacks tend to not change as often, as they wish to get the most value out of them before they change them.

By seeing the address, reporting them and blocking them it will assist your various interfaces with load capacity (including against simple spam) as well as create a 'prevention first' approach that is beneficial for all members of the AIPC.

A recent IP address (23.254.202.47) attempted to load malware through an open email at a convention centre. If it had been successful, it would have caused a created a significant attack.

The likelihood that it has been used across the AIPC centres especially in North America and South America is high.

TIP: IF CENTRE MEMBERS THROUGH THEIR IT AND RESPONSIBLE TEAMS CAN SUBMIT THE IP ADDRESSES, WE WILL SHARE THESE REGULARLY FOR CONSTANT UPDATES TO YOUR BLACKIST CAPABILITIES, GIVING FURTHER STRENGTH TO ALL OF OUR SYSTEMS.